Hallituksen esitys eduskunnalle kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi.

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan säädettäväksi laki kyberturvallisuuden riskienhallinnasta. Lisäksi esityksessä ehdotetaan muutettavaksi julkisen hallinnon tiedonhallinnasta annettua lakia, sähköisen viestinnän palveluista annettua lakia, ilmailulakia, raideliikennelakia, liikenteen palveluista annettua lakia, alusliikennepalvelulakia, eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annettua lakia, sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annettua lakia, sähkömarkkinalakia, maakaasumarkkinalakia, energiavirastosta annettua lakia, sähkö- ja maakaasumarkkinalakia ja vesihuoltolakia.

Esityksellä pantaisiin täytäntöön Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (jäljempänä *NIS2-direktiivi*). NIS2-direktiivin tavoitteena on vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa yhteiskunnan toiminnan kannalta kriittisiksi katsottujen sektoreiden ja toimijoiden osalta velvoittamalla jäsenvaltiot asettamaan direktiivin soveltamisalaan kuuluville toimijoille velvoittavia riskienhallintatoimia kyberturvallisuushäiriöiden varalta.

NIS2-direktiivi ehdotetaan pantavaksi täytäntöön säätämällä sen edellyttämistä velvoitteista keskitetysti uudessa kyberturvallisuuden riskienhallinnasta annettavassa laissa. Julkisen sektorin osalta velvoitteista säädettäisiin myös julkisen hallinnon tiedonhallinnasta annetussa laissa. Samalla kumottaisiin edeltävän ja kumoutuvan verkko- ja tietoturvallisuusdirektiivin täytäntöönpanosäännökset useista sektorikohtaisista laeista. Valvonnan järjestämisessä jatkettaisiin sektorikohtaisesti hajautettua mallia. Esityksellä säädettäisiin NIS2-direktiivin täytäntöönpanemiseksi myös tietoturvaloukkauksia tutkivasta ja niihin reagoivasta yksiköstä, joka sijaitsisi Liikenne- ja viestintävirastossa, sekä kansallisesta kyberturvallisuusstrategiasta ja kyberkriisinhallintakehyksestä. NIS2-direktiivin täytäntöönpano ehdotetaan tehtäväksi sen vähimmäistason mukaisesti ja kansallinen liikkumavara täysimääräisesti hyödyntäen.

Petteri Orpon hallitusohjelman mukaan kyberturvallisuutta koskevaa yhteistyötä viranomaisten ja elinkeinoelämän välillä vahvistetaan. Hallitus parantaa tietoturvaa kriittisillä toimialoilla sekä toteuttaa kyberturvallisuuden kehittämisohjelman (6.4). Hallitus uudistaa kansallisen kyberturvallisuusstrategian vastaamaan muuttunutta toimintaympäristöä (8.5). Lisäksi kyberturvallisuutta vahvistetaan tiiviissä yhteistyössä yritysten, elinkeinoelämän ja kolmannen sektorin kanssa huomioiden, että iso osa kriittisestä infrastruktuurista on yksityisessä omistuksessa (8.5). EU-lainsäädännön toimeenpanon yhteydessä vältetään kansallista lisäsääntelyä (6.1).

Lait on tarkoitettu tulemaan voimaan pääosin 18.10.2024.

_____

SISÄLLYS

PERUSTELUT

1 Asian tausta ja valmistelu

1.1 Tausta

Esityksen valmisteluun on johtanut Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (jäljempänä *NIS2-direktiivi*). Tähän esitykseen sisältyvät NIS2-direktiivin kansallisen toimeenpanon edellyttämät lainsäädäntömuutokset on valmisteltu liikenne- ja viestintäministeriön asettamassa poikkihallinnollisessa valmisteluhankkeessa.

NIS2-direktiivi korvaa aiemman EU:n verkko- ja tietoturvadirektiivin, eli Euroopan parlamentin neuvoston ja direktiivin (EU) 2016/1148 toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa (jäljempänä NIS1-direktiivi). NIS1-direktiivin uudelleentarkastelussa on tullut esiin jäljempänä kuvattuja seikkoja, joiden vuoksi direktiivi on päädytty korvaamaan uudella NIS2-direktiivillä. NIS1-direktiivi saatettiin pääosin voimaan kansallisesti 9. toukokuuta 2018 voimaan tulleilla lain muutoksilla (HE 192/2017 vp, LiVM 6/2018 vp ja EV 25/2018 vp). Lisäksi velvoitteiden soveltamisalaa on laajennettu kansallisesti 1.1.2019 voimaan tulleilla muutoksilla (HE 34/2018 vp, PeVL 16/2018 vp, LiVM 14/2018 vp ja EV 68/2018 vp).

NIS2-direktiivi on saatettava kansallisesti voimaan 17.10.2024 mennessä ja kansallisia säännöksiä on sovellettava 18.10.2024 alkaen.

1.2 Valmistelu

1.2.1 EU-säädöksen valmistelu

Euroopan komissio (jäljempänä *komissio*) uudelleenarvioi vuoden 2020 aikana NIS1-direktiiviä ja sen soveltamiskokemuksia jäsenvaltioissa. Komissio järjesti NIS1-direktiivistä myös julkisen kuulemisen vuoden 2020 aikana. Suomi vastasi osaltaan julkiseen kuulemiseen ennakkovaikuttamislinjausten pohjalta (E 107/2020 vp).

Komissio katsoi, että yhteiskuntien digitaalinen kehitys, jota COVID-19 –pandemia on vauhdittanut, on muuttanut oleellisesti nykyistä toimintaympäristöä ja tuonut mukanaan uusia haasteita, jotka edellyttävät innovatiivisia ratkaisuja. Kyberloukkausten määrä on kasvanut ja nämä ovat olleet entistä kehittyneempiä. Kyberturvallisuushäiriöt vaikeuttavat sisämarkkinoiden toimintaa, aiheuttavat taloudellisia menetyksiä ja heikentävät käyttäjien luottamusta unionin talous- ja yhteiskuntaelämään. Komission mukaan ehdotus uudeksi direktiiviksi uudistaisi olemassa olevaa lainsäädäntökehystä ottaen huomioon sisämarkkinoiden toimintaympäristön muutokset. Ehdotus on myös osa EU:n kyberturvallisuusstrategiaa (JOIN(2020) 18 final) ja sen tavoitteita.

Komissio antoi 16.12.2020 ehdotuksensa NIS2-direktiiviksi (COM(2020) 823 final). Samalla komissio julkaisi direktiiviehdotukseen liittyvän vaikutusarvioinnin (SWD(2020) 345 final, englanniksi). Direktiiviehdotusta käsiteltiin neuvoston horisontaalisessa kybertyöryhmässä ja parlamentin teollisuus-, tutkimus- ja energiavaliokunnassa.

Direktiiviehdotuksesta annettiin eduskunnalle valtioneuvoston U-kirjelmä (U 9/2021 vp) 11.2.2021. Suomi katsoi, että direktiiviehdotus vastasi pääosin kansallista ennakkovaikuttamista ja kannatti ehdotuksen tavoitetta vastata paremmin muuttuneeseen kybertoimintaympäristöön ja kehittää entisestään EU:n yhteistä kyberturvallisuuden tasoa. Suomi piti tärkeänä uusien velvoitteiden ja vaatimusten oikeasuhtaisuutta ja riskiperusteisuutta sekä sektorikohtaisten erityispiirteiden huomioimista. Lisäksi Suomi piti tärkeänä, että ehdotus säilyttää jäsenvaltioille riittävästi kansallista liikkumavaraa, jotta nämä voivat lisäksi ottaa käyttöön sellaisia kansallisia toimenpiteitä, joilla varmistetaan kyberturvallisuuden korkea taso. Eduskunta yhtyi valtioneuvoston kantaan painottaen lisäksi sääntelyn täsmällisyyttä ja yhteensovittamista muun EU-sääntelyn kanssa (LiVL 8/2021 vp, SuVEK 15/2021 vp).

Direktiiviehdotuksesta annettiin eduskunnalle U-jatkokirjelmä (UJ 23/2021 vp) komission ehdotuksen etenemisestä ja jatkokäsittelystä 20. joulukuuta 2021. U-jatkokirjelmässä katsottiin, että ehdotus oli edennyt kokonaisuudessaan pitkälti Suomen kannan mukaiseen suuntaan. Eduskunnalla ei ollut huomauttamista valtioneuvoston toimintalinjaan.

1.2.2 Hallituksen esityksen valmistelu

Liikenne- ja viestintäministeriö asetti työryhmän NIS2-direktiivin kansallisen toimeenpanon tueksi tammikuussa 2023 (jäljempänä *päätyöryhmä*). Päätyöryhmän tehtävänä oli arvioida tarpeelliset lainsäädäntömuutokset direktiivin toimeenpanemiseksi ja laatia yhteisesti hallituksen esitys tarvittaviksi lainsäädäntömuutoksiksi. Päätyöryhmän puheenjohtajisto oli liikenne- ja viestintäministeriöstä ja jäsenet oikeusministeriöstä, valtiovarainministeriöstä, ympäristöministeriöstä, maa- ja metsätalousministeriöstä, työ- ja elinkeinoministeriöstä, sosiaali- ja terveysministeriöstä, sisäministeriöstä, puolustusministeriöstä sekä ulkoministeriöstä. Opetus- ja kulttuuriministeriö ja valtioneuvoston kanslia eivät nimenneet jäsentä päätyöryhmään. Päätyöryhmän sihteeristö koostui liikenne- ja viestintäministeriön sekä Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen edustajista. Päätyöryhmä kokoontui x kertaa.

Liikenne- ja viestintäministeriö asetti päätyöryhmän osana myös julkishallinnon sektoriin keskittyvän alatyöryhmän (jäljempänä *alatyöryhmä*). Alatyöryhmän tehtävänä oli arvioida ja valmistella NIS2-direktiivin velvoitteiden toimeenpano soveltamisalaan kuuluvan julkishallinnon sektorin (NIS2-direktiivin liite I kohta 10) osalta. Alatyöryhmän puheenjohtajisto ja sihteeristö olivat valtiovarainministeriöstä ja jäsenet liikenne- ja viestintäministeriöstä, oikeusministeriöstä, Verohallinnosta, työ- ja elinkeinoministeriöstä, ympäristöministeriöstä, maa- ja metsätalousministeriöstä, sosiaali- ja terveysministeriöstä, sisäministeriöstä, puolustusministeriöstä, ulkoministeriöstä, valtioneuvoston kansliasta, opetus- ja kulttuuriministeriöstä ja Kuntaliitosta. Alatyöryhmä kokoontui x kertaa.

Päätyöryhmä kutsui alkuvuonna 2023 työryhmän kokouksiin kuultavaksi myös eräitä etujärjestöjä. Päätyöryhmän kokouksissa kävivät kuultavina Finanssiala ry, Elinkeinoelämän keskusliitto ry, FiCom ry, Kyberala ry, Elintarviketeollisuus ry, Energiateollisuus ry, Päivittäistavarakauppa ry ja Kemianteollisuus ry. Liikenne- ja viestintäministeriö järjesti yhdessä Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen kanssa myös kaikille avoimen sidosryhmätilaisuuden NIS2-direktiivin kansallisesta täytäntöönpanosta 30.3.2023. Lisäksi valtiovarainministeriö järjesti 4.5.2023 erityisesti julkishallinnon toimijoille suunnatun webinaarin, jossa kerrottiin NIS2-direktiivin sääntelystä ja kansallisesta toimeenpanosta julkishallinnon sektorilla. Molempien tilaisuuksien materiaalit löytyvät kansallisen toimeenpanohankkeen Hankeikkunasta (https://valtioneuvosto.fi/hanke?tunnus=LVM044:00/2022).

Työryhmätyöskentelyn lisäksi valmistelun aikana on järjestetty kahdenvälisiä keskusteluja muun muassa NIS2-direktiivin kansalliseen toimeenpanoon liittyvien muiden kansallisten

hankkeiden valmistelijoiden kanssa hankkeiden yhteensovittamiseksi. Pää- ja alatyöryhmien sihteeristöt ovat keskustelleet myös komission kanssa eräistä kansalliseen toimeenpanoon liittyvistä yksityiskohdista. Liikenne- ja viestintäministeriö on lisäksi ollut yhteydessä muihin EU-jäsenvaltioihin kansainvälisen vertailun tekemiseksi.

Hallituksen esityksen valmistelun aikana liikenne- ja viestintäministeriö teetti selvityksen[1] NIS2-direktiivin riskienhallintavelvoitteiden taloudellisista vaikutuksista erityisesti elintarvike- ja valmistussektoreille. Selvitys toteutettiin haastattelujen sekä sähköisen kyselylomakkeen avulla saatujen vastausten perusteella. Selvitykseen osallistui yhteensä 20 yritystä, joista 10 oli elintarvikesektorilta ja 10 valmistussektorilta. Selvitystä ja sen tuloksia on hyödynnetty esityksen vaikutusten arvioinnissa. Lisäksi NIS2-direktiivin kansallisen toimeenpanon valmisteluun liittyen valtiovarainministeriö selvitti helmi- ja maaliskuussa 2023 haastattelujen avulla julkishallinnon sektorin näkemyksiä muun muassa direktiivin soveltamisalaan ja toimivaltaiseen viranomaiseen julkishallinnon toimialalla.

2 EU-säädöksen tavoitteet ja pääasiallinen sisältö

2.1 Tavoitteet

NIS2-direktiivin tavoitteena on vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa kriittisiksi katsottujen sektoreiden ja toimijoiden osalta velvoittamalla jäsenvaltiot asettamaan direktiivin soveltamisalaan kuuluville toimijoille velvoittavia riskienhallintatoimia kyberturvallisuushäiriöiden varalta.

NIS2-direktiivillä pyritään poistamaan jäsenvaltioiden välillä havaittuja eroja NIS1-direktiivin velvoitteiden täytäntöönpanossa erityisesti vahvistamalla vähimmäissäännöt koordinoidun sääntelykehyksen toiminnalle, vahvistamalla järjestelyt kunkin jäsenvaltion vastuuviranomaisten toimivaa yhteistyötä varten, ajantasaistamalla luettelo aloista ja toiminnoista, joihin sovelletaan kyberturvallisuusvelvoitteita, ja säätämällä tehokkaista oikeussuojakeinoista ja täytäntöönpanotoimenpiteistä, jotka ovat olennaisen tärkeitä direktiivin velvoitteiden tehokkaan täytäntöönpanon kannalta.

NIS2-direktiivissä säädetään toimenpiteistä, joilla pyritään saavuttamaan kyberturvallisuuden yhteinen korkea taso Euroopan unionin jäsenvaltioissa. Direktiivissä säädetään jäsenvaltion velvollisuudesta hyväksyä kansallinen kyberturvallisuusstrategia, asettaa toimivaltaiset viranomaiset, kyberkriisinhallintaviranomaiset, kyberturvallisuusalan keskitetyt yhteyspisteet ja tietoturvaloukkauksiin reagoivat ja niitä tutkivat tahot (Computer security incident response teams, jäljempänä *CSIRT-yksikkö*). Lisäksi direktiivissä säädetään kyberturvallisuustietojen jakamista koskevista säännöistä ja velvoitteista.

2.2 Soveltamisala

NIS2-direktiivin yleinen soveltamisala määritellään sen 2 artiklassa. NIS2-direktiivin raportointi- ja riskienhallintavelvoitteet kohdistuvat sen 3 artiklassa määriteltäviin keskeisiin ja tärkeisiin toimijoihin.

NIS2-direktiivin 2 artiklan nojalla direktiiviä sovelletaan sen liitteissä I ja II tarkoitettua toimijatyyppiä oleviin julkisiin ja yksityisiin toimijoihin, jotka tarjoavat palvelujaan tai harjoittavat

[1] Selvitys kyberturvallisuusdirektiivin (NIS2-direktiivi) riskienhallintavelvoitteiden taloudellisista vaikutuksista elintarvike- ja valmistussektoreille, Insta Advance Oy (2023).

toimintaansa Euroopan unionissa. Lisäksi edellytyksenä on, että toimija täyttää komission suosituksessa 2003/361/EY olevat keskisuuria yrityksiä koskevat edellytykset tai ylittää keskisuurten yritysten määrittelyssä käytettävät kynnysarvot. Liitteissä I on listattu tarkemmin direktiivin soveltamisalaan kuuluvat toimijatyypit, jotka harjoittavat toimintaa seuraavilla toimialoilla: energia, liikenne, pankkitoiminta, finanssimarkkinoiden infrastruktuurit, terveys, juomavesi, jätevesi, digitaalinen infrastruktuuri, TVT-palvelujen hallinta, julkishallinto ja avaruus. Liitteessä II on listattu tarkemmin direktiivin soveltamisalaan kuuluvat toimijatyypit, jotka harjoittavat toimintaa seuraavilla toimialoilla: posti- ja kuriiripalvelut, jätehuolto, kemikaalien valmistus, tuotanto ja jakelu, elintarvikkeiden tuotanto, jalostus ja jakelu, valmistus, digitaalisen palvelun tarjoajat sekä tutkimustoiminta.

Komission suosituksen 2003/361/EY liitteen 2 artiklan nojalla keskisuuria yrityksiä, eli muita kuin mikro- ja pienyrityksiä, ovat yritykset, joiden palveluksessa on vähintään 50 työntekijää tai jonka vuosiliikevaihto ja taseen loppusumma ylittää 10 miljoonaa euroa. Keskisuuren yrityksen määrittelyssä käytettävät kynnysarvot ylittävä yritys on yritys, jonka palveluksessa on vähintään 250 työntekijää tai joiden vuosiliikevaihto ylittää 50 miljoonaa euroa ja taseen loppusumma ylittää 43 miljoonaa euroa. Komission suosituksen liitteen 3 artiklan 4 kohtaa julkisyhteisön hallinnasta toimijan pääomaan tai äänimäärään ei sovellettaisi arvioitaessa toimijan kuulumista NIS2-direktiivin soveltamisalaan.

Pien- ja mikroyritykset jäävät lähtökohtaisesti direktiivin soveltamisalan ulkopuolelle, ellei niitä koske poikkeus NIS2-direktiivin soveltamisalaan kuulumisesta koosta riippumatta. Koosta riippumatta NIS2-direktiivin soveltamisalaan kuuluvat direktiivin liitteissä I ja II tarkoitettua toimijatyyppiä olevat toimijat, kun palvelujen tarjoajat ovat:

a) yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajia;
b) luottamuspalvelun tarjoajia; tai
c) aluetunnusrekisterejä ja DNS-palveluntarjoajia.

Lisäksi koosta riippumatta NIS2-direktiivin soveltamisalaan kuuluvat Kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2022/2557 (jäljempänä *CER-direktiivi*) nojalla kriittisiksi toimijoiksi määritellyt toimijat sekä verkkotunnusten rekisteröintipalveluja tarjoavat toimijat.

Koosta riippumatta NIS2-direktiivin soveltamisalaan kuuluvat lisäksi liitteissä I ja II tarkoitettuja toimijatyyppiä olevat toimijat, kun:
a) toimija tarjoaa ainoana jäsenvaltiossa palvelua, joka on yhteiskunnan tai talouden kriittisten toimintojen ylläpitämisen kannalta keskeinen;
b) häiriö toimijan tarjoamassa palvelussa voisi vaikuttaa merkittävästi yleiseen järjestykseen, yleiseen turvallisuuteen tai kansanterveyteen;
c) häiriö toimijan tarjoamassa palvelussa voisi aiheuttaa merkittävän systeemisen riskin erityisesti aloilla, joilla tällaisella häiriöllä voisi olla rajatylittäviä vaikutuksia;
d) toimija on kriittinen, koska sillä on erityisen suuri merkitys kansallisella tai alueellisella tasolla kyseisen toimialan tai palvelutyypin tai jäsenvaltion muiden keskinäisriippuvaisten toimialojen kannalta.

NIS2-direktiivi velvoittaa julkishallinnon toimialalla lähtökohtaisesti keskus- ja aluehallinnon julkishallinnon toimijoita koosta riippumatta. Aluetason julkishallinnon toimijan osalta lisäedellytyksenä kuulumiselle NIS2-direktiivin vähimmäissoveltamisalan piiriin on, että toimija riskiperusteisen arvioinnin perusteella tarjoaa palveluja, joiden häiriintymisellä voisi olla merkittävä vaikutus yhteiskunnan tai talouden kriittisiin toimintoihin. Direktiivi ei kuitenkaan

koske julkishallinnon toimijoita, jotka harjoittavat toimintaa kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla, mukaan lukien rikosten ennalta estäminen, tutkiminen, paljastaminen ja rikoksiin liittyvät syytetoimet. Direktiivi ei myöskään koske oikeuslaitosta, parlamentteja eikä keskuspankkeja. Paikallistason julkishallinnon toimijoiden sekä opetus- ja koulutusalan laitoksien saattaminen direktiivin edellyttämän sääntelyn soveltamisalaan on kansallisen liikkumavaran alassa.

Lisäksi jäsenvaltioilla on kansallista liikkumavaraa vapauttaa riskienhallinta- ja raportointivelvoitteista toimijat, jotka harjoittavat toimintaa kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla, mukaan lukien rikosten ennalta estäminen, tutkiminen, paljastaminen ja rikoksiin liittyvät syytetoimet, tai jotka tarjoavat palveluja yksinomaan julkishallinnon toimijoille, jotka harjoittavat toimintaa kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla, mukaan lukien rikosten ennalta estäminen, tutkiminen, paljastaminen ja rikoksiin liittyvät syytetoimet. Vapautus koskisi mainittuja toimintoja tai palveluita. Jos erityisen toimijan harjoittama toiminta tai tarjoamat palvelut ovat yksinomaan edellä mainittuja, kansallinen liikkumavara kattaisi vapauttamisen myös jaksossa 2.4 tarkoitetuista rekisteröitymisvelvoitteista. Poikkeuksena tähän, sekä erityiseen toimijaan että julkishallinnon toimijaan on sovellettava direktiivin sääntelyä, jos toimija toimii luottamuspalvelun tarjoajana.

NIS2-direktiiviä ei sovellettaisi toimijoihin, jotka jäsenvaltiot ovat jättäneet asetuksen (EU) 2022/2554 (Euroopan parlamentin ja neuvoston asetus finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU) N:o 600/2014, (EU) N:o 909/2014 ja (EU) 2016/1011 muuttamisesta) soveltamisalan ulkopuolelle mainitun asetuksen 2 artiklan 4 kohdan mukaisesti.

2.3 Keskeiset ja tärkeät toimijat

NIS2-direktiivi asettaa velvoitteita keskeisille ja tärkeille toimijoille, jotka määritellään 3 artiklassa. Keskeisten ja tärkeiden toimijoiden erottelun osalta merkityksellistä on direktiivin niihin kohdistamat valvontatoimivaltuudet. Keskeisten toimijoiden osalta valvonnan tulee kattaa etukäteis- ja jälkikäteisvalvonta, mutta tärkeiden toimijoiden osalta pelkkä jälkikäteisvalvonta on direktiivin nojalla riittävä.

Keskeisiä toimijoita ovat direktiivin liitteessä I tarkoitetut toimijat jotka ylittävät keskisuuren yrityksen (suositus 2003/361/EY liitteessä olevan 2 artiklan 1 kohta) määrittelyssä käytetyt kynnysarvot. Muut keskeisen toimijan määritelmän täyttävät toimijat on listattu direktiivin 3 artiklan 1 kohdan b-g alakohdissa. Esimerkiksi CER-direktiivin nojalla kriittiseksi toimijaksi määriteltyjä toimijoita olisi siten pidettävä keskeisenä toimijana. Julkishallinnon toimialan osalta keskeisinä toimijoina on pidettävä keskustason julkishallinnon toimijoita. Keskeiset toimijat ovat pääosin niitä toimijoita, jotka ovat kuuluneet NIS1-direktiivin mukaiseen soveltamisalaan.

Tärkeinä toimijoina pidetään niitä toimijoita, jotka eivät täytä keskeisen toimijan määritelmää, mutta kuuluvat direktiivin liitteiden I tai II toimijatyyppeihin.

2.4 Toimijoiden rekisteri

NIS2-direktiivin 3 artikla velvoittaa jäsenvaltiot laatimaan luettelon keskeisistä ja tärkeistä sekä verkkotunnusten rekisteröintipalveluja tarjoavista toimijoista. Luettelon laatimiseksi keskeisten ja tärkeiden toimijoiden on toimitettava toimivaltaisille viranomaisille eräitä vähimmäistietoja.

Luetteloa on tarkasteltava ja päivitettävä säännöllisesti ja vähintään kahden vuoden välein. Luettelon nojalla komissiolle ja NIS yhteistyöryhmälle on ilmoitettava 3 artiklan 5 kohdan edellyttämät tiedot.

Lisäksi Euroopan unionin kyberturvallisuusvirasto ENISA perustaa 27 artiklan nojalla DNS-palveluntarjoajien, aluetunnusrekisterien, verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden, pilvipalvelujen tarjoajien, datakeskuspalvelujen tarjoajien, sisällönjakeluverkkojen tarjoajien, hallintapalvelun tarjoajien, tietoturvapalveluntarjoajien sekä verkossa toimivien markkinapaikkojen tarjoajien, verkossa toimivien hakukoneiden tarjoajien ja verkkoyhteisöalustojen tarjoajien rekisterin. Kansallisen keskitetyn yhteyspisteen tulee toimittaa ENISA:lle rekisterin perustamiseksi ja ylläpitämiseksi tarvittavat tiedot.

2.5 Riskienhallintavelvoitteet

NIS2-direktiivin riskienhallintavelvoitteet ovat vähimmäistason velvoitteita ja ne on pyritty muotoilemaan mahdollisimman teknologianeutraalisti, jotta ne kestäisivät aikaa ja soveltuisivat laajalle joukolle erilaisia toimijoita. Toimijat voisivat halutessaan ottaa käyttöön pidemmälle meneviä riskienhallintatoimia ja kansallisesti olisi jatkossankin mahdollista säätää tiukemmista riskienhallintavelvoitteista. Riskienhallintavelvoitteista on säädetty direktiivin 20 ja 21 artikloissa.

Artikla 20 edellyttää, että keskeisten ja tärkeiden toimijoiden hallintoelimet hyväksyvät näiden toimijoiden 21 artiklan noudattamiseksi toteuttamat kyberturvallisuusriskien hallintatoimenpiteet ja valvovat näiden täytäntöönpanoa. Hallintoelimet tulee voida saattaa vastuuseen, mikäli toimijat rikkovat 21 artiklaa. Hallintoelinten jäsenillä on velvollisuus osallistua koulutukseen ja jäsenmaiden tulisi kannustaa heitä tarjoamaan koulutusta myös työntekijöilleen.

Direktiivin 21 artiklassa on listattu ne osa-alueet, joita riskienhallinnassa ja riskienhallintatoimenpiteissä toimija on velvoitettu huomioimaan. Näitä osa-alueita ovat:

a) riskianalyysejä ja tietojärjestelmien turvallisuutta koskevat politiikat;

b) poikkeamien käsittely;

c) toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisinhallinta;

d) toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat;

e) verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen;

f) toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta;

g) perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus;

h) toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä;

i) henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta;

j) tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa.

Direktiivin mukaan toimijan tulee toteuttaa riskienhallintatoimenpiteet siten, että turvallisuuden taso on oikeassa suhteessa riskeihin. Arvioinnissa on huomioitava toimijan altistuminen riskeille, toimijan koko, poikkeamien esiintymisen todennäköisyys ja vakavuus, mukaan lukien niiden yhteiskunnalliset ja taloudelliset vaikutukset. Jäsenvaltioiden on varmistettava, että toteuttaessaan riskienhallintatoimenpiteensä, toimijat huomioivat ne haavoittuvuudet, jotka ovat ominaisia toimijan harjoittamalle toiminnalle.

2.6 Raportointivelvoitteet

Raportointivelvoitteesta säädetään NIS2-direktiivin 23 artiklassa. Keskeisten ja tärkeiden toimijoiden tulee raportoida merkittävästä poikkeamasta CSIRT-yksikölle tai toimivaltaiselle valvovalle viranomaiselle. Poikkeama katsotaan merkittäväksi, jos se on aiheuttanut tai voi aiheuttaa palvelujen vakavan toimintahäiriön tai asianomaiselle toimijalle taloudellisia tappioita tai jos poikkeama on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa. Raportointivelvoite sisältää kolme vaihetta.

Ennakkovaroitus tulee toimittaa ilman aiheetonta viivytystä ja joka tapauksessa 24 tunnin kuluessa merkittävän poikkeaman havaitsemisesta. Ilmoitukseen tulee tapauksen mukaan sisällyttää tieto siitä, epäilläänkö poikkeaman johtuvan lainavastaisista tai vihamielisistä teoista tai voiko sillä olla rajat ylittäviä vaikutuksia. Kun poikkeamalla on rajat ylittäviä vaikutuksia, siitä on tiedotettava niille muille jäsenvaltioille, joihin poikkeama vaikuttaa sekä ENISA:lle.

Poikkeamailmoitus tulee toimittaa ilman aiheetonta viivytystä ja joka tapauksessa 72 tunnin kuluessa merkittävän poikkeaman havaitsemisesta. Ilmoitukseen tulee tapauksen mukaan päivittää ennakkovaroituksen tiedot ja esittää ensimmäinen arvio merkittävästä poikkeamasta, sen vakavuudesta ja vaikutuksista sekä vaarantumisindikaattorit, jos sellaisia on saatavilla.

Loppuraportti laaditaan viimeistään kuukauden kuluttua poikkeamailmoituksen toimittamisesta ja sen tulee sisältää yksityiskohtainen kuvaus poikkeamasta, sen vakavuuksista ja vaikutuksista sekä tiedot poikkeaman todennäköisesti aiheuttaneen uhan tai juurisyyn tyypistä, toimenpiteistä, jotka on tehty tai joita suunnitellaan vaikutusten lieventämiseksi sekä tapauksen mukaan poikkeaman rajat ylittävistä vaikutuksista. Jos poikkeama on käynnissä edelleen loppuraportin määräajan umpeutuessa, toimijan tulee toimittaa edistymisraportti. Lopullinen raportti on toimitettava kuukauden kuluttua poikkeaman käsittelyn päättymisestä.

Väliraportti on toimitettava CSIRT-yksikön tai toimivaltaisen viranomaisen pyynnöstä. CSIRT-yksikön tai toimivaltaisen viranomaisen on ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 24 tunnin kuluessa ennakkovaroituksen vastaanottamisesta annettava vastaus ilmoituksen tehneelle toimijalle. Vastaukseen sisältyy alustava palaute merkittävästä poikkeamasta ja siihen voidaan toimijan pyynnöstä sisällyttää ohjeita ja neuvoja poikkeaman vaikutusten hallintaan liittyen.

Direktiivin 30 artiklassa säädetään vapaaehtoisesta ilmoittamisesta CSIRT-yksikölle tai valvovalle viranomaiselle. Vapaaehtoinen ilmoittaminen tarkoittaa muita ilmoituksia kuin niitä ilmoituksia merkittävistä poikkeamista, joiden tekemiseen soveltamisalaan kuuluvalla toimijalla on velvoite. Valvovan viranomaisen on 30 artiklan nojalla otettava toimialallaan vastaan ilmoituksia poikkeamista, kyberuhkista ja läheltä piti –tilanteista sekä NIS2-direktiivin soveltamisalaan kuuluvilta toimijoilta, että muiltakin toimijoilta. Vapaaehtoiset poikkeamailmoitukset on käsiteltävä samalla tavalla kuin velvoitteeseen perustuvat ilmoitukset, ja valvovalla viranomai-

sella on oikeus priorisoida velvoittavien ilmoitusten käsittelyä tarvittaessa. Suomessa NIS1-direktiivin valvoviksi viranomaisiksi määrätyt viranomaiset sekä Liikenne- ja viestintäviraston Kyberturvallisuuskeskus ovat ottaneet vastaan myös muita kuin NIS1-direktiivin mukaiseen velvoitteeseen perustuvia ilmoituksia, vaikka vapaaehtoisesta ilmoittamisesta ei ole erikseen säädetty. Viranomaiselle tehtävän raportoinnin lisäksi toimijan on ilman aiheetonta viivytystä tiedotettava palvelujensa vastaanottajille, joihin kyberuhka saattaa vaikuttaa, sellaisista toimenpiteistä ja korjaavista toimista, joita vastaanottajilla on mahdollista toteuttaa. Tarvittaessa palvelujen vastaanottajille tulee tiedottaa myös itse kyberuhasta. Jos yleinen tietoisuus merkittävästä poikkeamasta on tarpeen, CSIRT-yksikkö tai toimivaltainen viranomainen voivat tiedottaa merkittävästä poikkeamasta yleisölle tai vaatia toimijaa tekemän niin.

2.7 Valvonta ja hallinnolliset sanktiot

NIS2-direktiivissä säädetään vähimmäisvaatimukset valvontatoimenpiteille ja –keinoille, joita valvovien viranomaisten on voitava kohdistaa keskeisiin ja tärkeisiin toimijoihin. Valvontaa ja täytäntöönpanoa koskevista yleisistä näkökohdista säädetään NIS2-direktiivin 31 artiklassa, vähimmäistoimet keskeisten toimijoiden osalta säädetään 32 artiklassa ja tärkeiden toimijoiden osalta 33 artiklassa. Direktiivin 31 artiklassa annetaan jäsenvaltioille mahdollisuus sallia valvontatoimenpiteiden priorisointi riskiperusteista lähestymistapaa noudattaen. Lisäksi artiklassa edellytetään, että jäsenvaltiot varmistavat toimivaltaisten viranomaisten toiminnallisen riippumattomuuden valvomistaan julkishallinnon toimijoista.

NIS2-direktiivin tarkoituksena on sen johdanto-osan kappaleen122 mukaisesti säätää eri valvontajärjestelmästä keskeisille ja tärkeille toimijoille, jotta voidaan varmistaa kyseisten toimijoiden ja toimivaltaisten viranomaisten velvoitteiden oikeudenmukainen tasapaino. Keskeisiin toimijoihin olisikin sovellettava kattavaa valvontajärjestelmää, johon kuuluu etukäteis- ja jälkikäteisvalvonta, ja tärkeisiin toimijoihin olisi sovellettava kevyttä valvontajärjestelmää, johon kuuluu vain jälkikäteisvalvonta. Tärkeitä toimijoita ei tulisi siten NIS2-direktiivin nojalla vaatia raportoimaan valvovalle viranomaiselle järjestelmällisesti kyberturvallisuusriskien hallintatoimenpiteiden noudattamista, vaan valvovan viranomaisen olisi tärkeiden toimijoiden osalta harjoitettava yleisen valvonnan sijasta jälkikäteisvalvontaa.

Keskeisten toimijoiden osalta jäsenvaltioiden on varmistettava, että viranomaisilla on valtuudet suorittaa 32 artiklan 2 kohdan a-g alakohdissa listatut toimenpiteet. Näihin toimenpiteisiin sisältyy muun muassa erilaisten tarkastusten ja auditointien suorittaminen sekä pyynnöt saada pääsy dataan, asiakirjoihin tai tietoihin joita viranomaiset tarvitsevat valvontatehtäviensä suorittamiseksi. Lisäksi direktiivin 32 artiklan 4 kohdassa jäsenvaltiot velvoitetaan varmistamaan, että valvovalla viranomaisella on alakohdissa a-i määritellyt toimivaltuudet, kuten valtuus antaa toimijoille varoituksia, sitovia ohjeita tai määrätä toimija lopettamaan direktiivin vastainen toiminta. Lisäksi valvovalla viranomaisella tulee olla mahdollisuus määrätä tai pyytää asiaankuuluvia elimiä tai tuomioistuimia määräämään hallinnollisia sakkoja. Direktiivin 34 artiklassa on säädetty vähimmäisvaatimuksista hallinnollisten sakkojen enimmäismäärille. Keskeisille toimijoille määrättävän hallinnollisen sakon enimmäismäärän tulisi olla vähintään 10 000 000 euroa tai 2 prosenttia sen yrityksen, johon keskeinen toimija kuuluu, edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi. Tärkeille toimijoille määrättävän hallinnollisen sakon enimmäismäärän tulisi olla vähintään 7 000 000 euroa tai 1,4 prosenttia sen yrityksen, johon tärkeä toimija kuuluu, edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi. Direktiivin 34 artiklan 7 kohdan mukaan kukin jäsenvaltio voi vahvistaa säännöt siitä, voidaanko julkishallinnon toimijoille määrätä hallinnollisia sakkoja ja missä määrin.

Lisäksi valvovilla viranomaisilla tulisi olla NIS2-direktiivin 32 artiklan 5 kohdan a-b alakohdissa tarkoitetut toimivaltuudet, mikäli muut täytäntöönpanotoimenpiteet eivät tuota tulosta. Jäsenvaltioiden on varmistettava, että mikäli toimija ei kehotuksesta huolimatta korjaa toiminnassa havaittuja puutteita sille asetetussa määräajassa, toimivaltainen viranomainen voi muun muassa keskeyttää väliaikaisesti keskeisen toimijan tarjoamia palveluja tai toimintoja koskevan sertifioinnin tai luvan sekä pyytää asiaankuuluvia elimiä tai tuomioistuimia kieltämään väliaikaisesti luonnollista henkilöä toimimasta keskeisen toimijan johtotehtävissä. Direktiivin 32 artiklan 5 kohdan 3 alakohdan mukaan 5 kohdassa säädettyjä seuraamuksia ei sovelleta direktiivin soveltamisalaan kuuluviin julkishallinnon toimijoihin.

NIS2-direktiivin 33 artikla velvoittaa jäsenvaltiot säätämään valvoville viranomaisille lähes vastaavat toimivaltuudet kohdistaa erilaisia valvontatoimenpiteitä tärkeisiin toimijoihin. Tärkeisiin toimijoihin voisi kuitenkin kohdistaa valvontatoimenpiteitä vain, jos jäsenvaltiot saavat näyttöä, viitteitä tai tietoja, joiden mukaan tärkeä toimija ei väitetysti noudata direktiiviä ja erityisesti sen 21 ja 23 artiklaa.

2.8 Viranomaisyhteistyö

2.8.1 CSIRT-yksiköt

NIS2-direktiivin 10 artikla velvoittaa jokaisen jäsenvaltion nimeämään yhden tai useamman CSIRT-yksikön, jonka tehtävänä on reagoida tietoturvaloukkauksiin ja tutkia niitä. CSIRT-yksikön tehtäviä on täsmennetty 11 artiklassa, jonka mukaan CSIRT-yksikön tulee muun muassa seurata ja analysoida kyberuhkia, haavoittuvuuksia ja poikkeamia, antaa näitä koskevia ennakkovaroituksia, hälytyksiä, ilmoituksia ja tietoja, avustaa direktiivin soveltamisalaan kuuluvia toimijoita, reagoida poikkeamatilanteisiin, kerätä ja analysoida poikkeamatietoja, ylläpitää kyberturvallisuuden tilannekuvaa ja osallistua CSIRT-verkoston toimintaan. Tarkempi luettelo CSIRT-yksiköiden tehtävistä löytyy direktiivin 11 artiklan 3 kohdasta. CSIRT-yksiköille kohdistetut vaatimukset on sijoitettu direktiivin 11 artiklan 1 kohtaan. Lisäksi CSIRT-yksiköillä tulee olla tekniset valmiudet suorittaa niille annetut tehtävät.

2.8.2 Koordinoitu haavoittuvuuden julkistaminen ja haavoittuvuustietokanta

NIS2-direktiivin 12 artiklan mukaan jokaisen jäsenvaltion on nimettävä yksi CSIRT-yksiköistään koordinaattoriksi koordinoitua haavoittuvuuden julkistamista varten. Koordinaattorin tehtävänä on ottaa yhteyttä asianmukaisiin toimijoihin, avustaa haavoittuvuudesta ilmoittaneita ja neuvotella haavoittuvuuden julkistamisen aikataulusta. Lisäksi koordinaattorin tulee pyrkiä hallitsemaan sellaisia haavoittuvuuksia, joiden vaikutus ulottuu useisiin toimijoihin. Haavoittuvuudesta tulee direktiivin mukaan voida ilmoittaa nimettömästi.

ENISA:n tehtävänä on perustaa ja ylläpitää haavoittuvuustietokantaa, jonka tulee sisältää kuvaus haavoittuvuudesta, lista niistä TVT-tuotteista tai –palveluista, joihin haavoittuvuus vaikuttaa sekä ohjelmistokorjausten saatavuus tai muu ohjeistus siitä, miten haavoittuvuuden riskejä on mahdollista lieventää.

2.8.3 CSIRT-verkosto, NIS yhteistyöryhmä ja EU-CyCLONe

NIS2-direktiivi luo jäsenmaiden välille useita erilaisia verkostoja, joiden tarkoituksena on mahdollistaa kyberturvallisuusyhteistyö EU:n sisällä. Jo NIS1-direktiivin aikana perustettuja EU-verkostoja ovat NIS yhteistyöryhmä (14 artikla) ja CSIRT-verkosto (15 artikla). NIS yhteistyöryhmän tavoitteena on tukea ja helpottaa jäsenvaltioiden välistä strategista yhteistyötä ja tietojenvaihtoa sekä lujittaa maiden välistä luottamusta ja se koostuu jäsenvaltioiden, ENISA:n sekä

komission edustajista. CSIRT-verkosto koostuu CSIRT-yksiköiden edustajista sekä unionin toimielinten, elinten ja virastojen tietotekniikan kriisiryhmän (CERT-EU) edustajista. Verkosto pyrkii edistämään luottamusta sekä ripeää ja tuloksellista operatiivista yhteistyötä jäsenvaltioiden välillä.

Näiden verkostojen lisäksi NIS2-direktiivissä luodaan uusi Euroopan kyberkriisien yhteysorganisaatioiden verkosto (jäljempänä *EU-CyCLONe*). EU-CyCLONe:n tehtävänä on tukea laajamittaisten kyberturvallisuuspoikkeamien ja kriisien koordinoitua hallintaa operatiivisella tasolla sekä varmistaa säännöllinen asiaankuuluvien tietojen vaihto jäsenvaltioiden ja unionin toimielinten, elinten, laitosten ja virastojen välillä. EU-CyCLONe koostuu jäsenvaltioiden kyberkriisinhallintaviranomaisten edustajista sekä komission edustajista, kun mahdollisella tai meneillään olevalla laajamittaisella kyberturvallisuuspoikkeamalla on tai todennäköisesti on merkittävä vaikutus direktiivin soveltamisalaan kuuluviin palveluihin ja toimintoihin. Muulloin komissio osallistuu tarkkailijana verkoston toimintaan.

2.9 Kyberturvallisuusstrategia ja kansalliset kyberkriisinhallintakehykset

NIS2-direktiivin artikla 7 velvoittaa jäsenvaltiot hyväksymään kansallisen kyberturvallisuusstrategian kyberturvallisuuden korkean tason saavuttamiseksi ja ylläpitämiseksi. Artiklassa säädetään myös kansallisten kyberturvallisuusstrategioiden vähimmäissisällöstä. Kansallinen kyberturvallisuusstrategia on annettava komissiolle tiedoksi kolmen kuukauden kuluessa sen hyväksymisestä. Kyberturvallisuusstrategiaa on arvioitava jäsenvaltioissa säännöllisesti ja vähintään viiden vuoden välein.

NIS2-direktiivin mukainen kansallinen kyberkriisinhallintakehys muodostuu kyberkriisinhallintaviranomaisesta ja kyberkriisien hallintasuunnitelmasta, joista on säädetty 9 artiklassa. Jäsenvaltion on nimettävä tai perustettava yksi tai useampi kyberkriisinhallintaviranomainen, jonka tehtävänä on vastata laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallinnasta. Laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallintasuunnitelmassa tulee vahvistaa laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallinnan tavoitteet ja järjestelyt. Kyberkriisinhallintaviranomaisesta ja kriisien hallintasuunnitelmasta on ilmoitettava eräitä tietoja myös komissiolle.

2.10 Kansallinen liikkumavara

NIS2-direktiivi on luonteeltaan vähimmäisharmonisoiva. NIS2-direktiivin vähimmäistason sisältöön tai sen edellyttämiin toimenpiteisiin ei lähtökohtaisesti liity kansallista liikkumavaraa. Keskeinen kansallinen liikkumavara liittyy kuitenkin siihen, että NIS2-direktiivillä ei estetä jäsenvaltioita antamasta tai pitämästä voimassa säännöksiä, joilla varmistetaan kyberturvallisuuden korkeampi taso edellyttäen, että tällaiset säännökset ovat unionin oikeudessa säädettyjen jäsenvaltioiden velvoitteiden mukaisia (5 artikla).

Direktiivin vähimmäissoveltamisalaan sisältyvä liikkumavara on kuvattu jaksossa 2.2. Lisäksi kansallisesti voidaan säätää NIS2-direktiivin velvoitteiden kohdistamisesta myös sellaisiin toimijoihin, joita NIS2-direktiivi ei muuten koske edellyttäen, että tällaiset säännökset ovat unionin oikeudessa säädettyjen jäsenvaltioiden velvoitteiden mukaisia.

Keskeisen toimijan määritelmään sisältyy kansallista liikkumavaraa siten, että jäsenvaltio voi lisätä NIS2-direktiivissä tarkoitetun keskeisen toimijan määritelmän alle myös sellaiset toimijat, jotka ovat 16.1.2023 mennessä NIS1-direktiivin nojalla tai kansallisesti muutoin määritetty keskeisten palvelujen tarjoajiksi (3 artiklan 1 kohdan g –alakohta).

Kansallisia kyberkriisinhallintakehyksiä koskevan 9 artiklan osalta direktiivi jättää kansallista liikkumavaraa siten, että laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallinnasta vastaavaksi toimivaltaiseksi viranomaiseksi eli ns. kyberkriisinhallintaviranomaiseksi voidaan nimetä tai perustaa yksi tai useampi toimivaltainen viranomainen. Mikäli viranomaisia nimetään tai perustetaan useampi kuin yksi, jäsenvaltion on nimettävä näiden viranomaisten keskuudesta koordinaattori laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallintaan.

NIS2-direktiivi ei edellytä sen soveltamisalaan kuuluvia toimijoita käyttämään sertifioituja TVT-tuotteita, -palveluja tai –prosesseja, mutta jäsenvaltiot voivat 24 artiklan 1 kohdan mukaan vaatia keskeisiä ja tärkeitä toimijoita käyttämään Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 (jäljempänä *kyberturvallisuusasetus*) 49 artiklan nojalla hyväksyttyjen eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukaisesti sertifioituja TVT-tuotteita, -palveluja ja -prosesseja. Direktiivin 24 artiklan 2 kohdan nojalla komissiolla on toimivalta antaa delegoituja säädöksiä, joilla täsmennetään, mitä keskeisten ja tärkeiden toimijoiden luokkia on vaadittava käyttämään tiettyjä sertifioituja TVT-tuotteita, TVT-palveluja ja TVT-prosesseja tai hankkimaan sertifiointi kyberturvallisuusasetuksen 49 artiklan nojalla hyväksytyn eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti.

Valvonnan osalta NIS2-direktiivissä on säädetty toimivaltaisten viranomaisten valvonta- ja täytäntöönpanotoimenpiteiden vähimmäistasosta, joka ei sisällä kansallista liikkumavaraa. NIS2-direktiivi jättää jäsenvaltioille kuitenkin mahdollisuuden sallia se, että niiden toimivaltaiset viranomaiset asettavat valvontatoimenpiteitä etusijalle (31 artiklan 2 kohta). Etusijalle asettamisessa on sovellettava riskiperusteista lähestymistapaa.

NIS2-direktiivi edellyttää, että keskeisille ja tärkeille toimijoille voidaan määrätä hallinnollisia seuraamusmaksuja. Kansallista liikkumavaraa on kuitenkin jätetty sen osalta, voiko hallinnollisia seuraamusmaksuja määrätä myös julkishallinnon toimijoille ja voidaanko keskeisille tai tärkeille toimijoille määrätä uhkasakkoja (34 artiklan 6 ja 7 kohdat).

3 Nykytila ja sen arviointi

3.1 NIS1-direktiivin täytäntöönpano

NIS1-direktiivi saatettiin pääosin voimaan kansallisesti 9. toukokuuta 2018 voimaan tulleilla lain muutoksilla (HE 192/2017 vp). NIS1-direktiivin tavoitteena oli parantaa kyberturvallisuusvalmiutta unionin alueella ja kohdistaa raportointivelvoitteita keskeisiin toimijoihin tietoturvapoikkeamien osalta. Tieto- ja verkkoturvallisuudesta ei ole laadittu kansallista, horisontaalista yleislakia, vaan NIS1-direktiivin velvoitteet on toimeenpantu sisällyttämällä ne toimialakohtaiseen erityislainsäädäntöön. Tietoturvavelvoitteiden noudattamisen valvonta on hajautettu usealle sektorikohtaiselle viranomaiselle.

NIS1-direktiivin täytäntöönpanosäännöksiä sisältyy sähköisen viestinnän palveluista annettuun lakiin (917/2014), ilmailulakiin (864/2014), raideliikennelakiin (1302/2018), alusliikennepalvelulakiin (623/2005), eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annettuun lakiin (485/2004, jäljempänä *turvatoimilaki*), liikenteen palveluista annettuun lakiin (320/2017), sähkömarkkinalakiin (588/2013), maakaasumarkkinalakiin (587/2017) sekä vesihuoltolakiin (119/2001). Toimialakohtaisessa lainsäädännössä on säädetty keskeisten palveluntarjoajien velvollisuudesta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja ilmoittaa tietoturvapoikkeamasta valvovalle viranomaiselle sekä yleisölle.

NIS1-direktiivin mukainen valvonta on järjestetty sektorikohtaisesti eli sektorikohtaiset valvovat viranomaiset valvovat oman sektorinsa toimijoita. Valvovina viranomaisina ovat toimineet Energiavirasto, Liikenne- ja viestintävirasto, Finanssivalvonta, Valvira sekä Etelä-Savon elinkeino-, liikenne- ja ympäristökeskus.

Koska NIS2-direktiivillä kumotaan NIS1-direktiivi velvoitteineen ja säädetään vastaavan tavoitteen saavuttamiseksi uusista velvoitteista myös NIS1-direktiivin soveltamisalaan kuuluneille toimijoille, on kansallisia säädöksiä tarkasteltava NIS2-direktiivin täytäntöönpanon yhteydessä.

3.2 Energia

Energiasektorin osalta NIS2-direktiivin soveltamisalaan kuuluvia toimialoja ovat sähkö, öljy, kaasu, kaukolämmitys ja -jäähdytys sekä vety. Näistä toimialoista sähkö, öljy ja kaasu ovat kuuluneet jo aiemmin NIS1-direktiivin piiriin, jolloin kansallisen arvioinnin mukaan keskeisten palvelujen tarjoajiksi katsottiin kuuluvan sähköverkonhaltijat sekä maakaasun siirtoverkonhaltija. NIS2-direktiivin soveltamisala on merkittävästi laajempi kuin NIS1-direktiivin soveltamisala. Valvovana viranomaisena energiasektorilla on tähän saakka toiminut Energiavirasto.

3.2.1 Sähkö

Sähkömarkkinoiden turvallisuudesta on säädetty sähkömarkkinalaissa. NIS1-direktiivin kansallisen toimeenpanon yhteydessä sähkömarkkinalakiin lisättiin verkonhaltijan velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen (29 a §). Sähkömarkkinalain 29 a § olisi tarpeen kumota NIS2 -direktiivin toimeenpanon johdosta päällekkäisen sääntelyn välttämiseksi. Sähkömarkkinalaissa on myös muuta sähkömarkkinoiden turvallisuutta koskevaa sääntelyä, kuten verkon kehittämisvelvollisuus (19 §), vastuu varman, luotettavan ja tehokkaan sähköverkon käytöstä (21 c §), verkonhaltijan varautumissuunnittelu (28 §), verkonhaltijan yhteistoimintavelvollisuus häiriötilanteissa (29 §), kantaverkon toiminnan laatuvaatimukset (40 §), suurjännitteisen jakeluverkon toiminnan laatuvaatimukset (50 §), jakeluverkon toiminnan laatuvaatimukset (51 §) sekä jakeluverkonhaltijan velvoite tiedottaa verkon käyttäjille häiriötilanteissa (59 §). Lisäksi Säteilyturvakeskus on antanut Ydinturvallisuusohjeen (YVL-ohjeen) ydinlaitoksen tietoturvallisuuden toteuttamista koskien ydinenergialain (990/1987) 7 r §:n nojalla. EU-tasolla sähkökriisien ehkäisemisestä ja niihin varautumisesta säädetään riskeihin varautumisesta sähköalalla ja direktiivin 2005/89/EY kumoamisesta annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) 2019/941. Asetuksen johdanto-osan kappaleessa 7 on kuvattu sen suhdetta NIS-sääntelyyn: ”Tällä asetuksella täydennetään direktiiviä (EU) 2016/1148 varmistamalla, että kyberpoikkeamat tunnistetaan asianmukaisesti riskiksi ja että niiden käsittelemiseksi toteutettavat toimenpiteet otetaan asianmukaisesti huomioon riskeihinvarautumissuunnitelmissa.” Kyberturvallisuutta koskevia erityisiä sääntöjä sähkötoimialalla voidaan antaa sähkön sisämarkkinoista annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) 2019/943 vahvistetussa verkkosäännössä.

3.2.2 Öljy

Vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annetussa laissa (390/2005, jäljempänä *kemikaaliturvallisuuslaki*) ja sen nojalla annetuissa säädöksissä, säädetään eräistä turvallisuusvelvoitteista öljyä käsitteleville, varastoiville, siirtäville tai säilyttäville toimijoille. Sääntely kohdistuu ensisijaisesti öljyn käsittelystä syntyvien fyysisten uhkien torjumiseen, eikä tieto- tai kyberturvallisuutta ole huomioitu sääntelyssä. Kemikaaliturvallisuuslaissa, painelaite-

laissa (1144/2016) ja rakennustuotteiden kaupan pitämistä koskevien ehtojen yhdenmukaistamisesta ja neuvoston direktiivin 89/106/ETY kumoamisesta annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) N:o 305/2011 on säännöksiä, joissa säädetään öljyn varastoinnissa käytettävien säiliöiden ja putkistojen turvallisuusvaatimuksista. Kemikaaliturvallisuus- ja painelaitesääntelyä on kuvattu tarkemmin jaksossa 3.12 Kemikaalien valmistus, tuotanto ja jakelu. NIS1-direktiivin täytäntöönpanon yhteydessä ei tehty öljysektorin osalta muutoksia kansalliseen lainsäädäntöön, sillä kyseisellä sektorilla ei tunnistettu kansallisesti yhtään sellaista keskeistä toimijaa tai palvelua, joka olisi täyttänyt direktiivin asettamat kriteerit.

3.2.3 Maakaasu

Kemikaaliturvallisuuslaki on turvallisuutta koskeva yleislaki myös maakaasun osalta. Kemikaaliturvallisuuslaki asettaa sektorin toimijoille eräitä riskienhallinta- ja ilmoitusvelvoitteita. Nämä velvoitteet kohdistuvat kuitenkin ensisijaisesti aineellisten uhkien torjumiseen, eikä tieto- tai kyberturvallisuutta ole huomioitu kyseisessä sääntelyssä. Kemikaaliturvallisuuslain nojalla annetuissa valtioneuvoston asetuksissa säädetään myös maakaasun käsittelyn turvallisuudesta. Maakaasuverkkojen turvallisuudesta on säädetty maakaasumarkkinalaissa. NIS1-direktiivin kansallisen toimeenpanon yhteydessä maakaasumarkkinalakiin lisättiin 34 a § siirtoverkonhaltijan velvollisuudesta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja ilmoittaa tietoturvallisuuteen liittyvästä häiriöstä. Maakaasumarkkinalain 34 a §:ta olisi tarpeen muuttaa NIS2-direktiivin toimeenpanon johdosta. Lisäksi maakaasuverkkojen turvallisuuteen liittyvää sääntelyä on verkon kehittämisvelvollisuutta (14 §), verkonhaltijan varautumissuunnittelua (27 §) sekä verkonhaltijan yhteistoimintavelvollisuutta häiriötilanteissa (28 §) koskevissa säännöksissä. Maakaasunsiirtoverkkoihin pääsyä koskevista edellytyksistä ja asetuksen (EY) N:o 1775/2005 kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 715/2009 8 artiklan 6 alakohdan mukaan verkkosäännöillä voidaan vahvistaa muun muassa verkon varmuutta ja luotettavuutta koskevat säännöt sekä toimintatavat hätätilanteissa. Maakaasua varastoidaan ja käsitellään myös muualla kuin maakaasuverkossa (mm. LNG-terminaalit). Maakaasua varastoidaan, käsitellään ja siirretään paineistettuna. Painelaitteita koskevaa sääntelyä on kuvattu tarkemmin jaksossa 3.12 Kemikaalien valmistus, tuotanto ja jakelu.

3.2.4 Kaukolämmitys ja –jäähdytys

Kaukolämmityksen ja –jäähdytyksen haltijat tulevat uutena NIS2-direktiivin kyberturvallisuusvelvoitteiden soveltamisalaan. Kaukolämmityksen tai –jäähdytyksen haltijoita koskevaa tieto- tai kyberturvallisuussääntelyä ei ole tunnistettu. Kaukolämpöä tuotetaan pääasiassa kattilalaitoksissa, joiden turvallisuudesta säädetään painelaitelaissa (1144/2016). Myös muut paineistetut putkistot kuuluvat painelaitelain alle. Painelaitesääntelyä on kuvattu tarkemmin jaksossa 3.12 Kemikaalien valmistus, tuotanto ja jakelu.

3.2.5 Vety

Vedyn tuotantoa, varastointia tai siirtoa harjoittavat toimijat eivät ole kuuluneet NIS1-direktiivin soveltamisalaan. Vastaavasti kuin maakaasu, vety varastoidaan ja käsitellään paineistettuna ja painelaitelaki soveltuu myös vedyn käsittelyyn. Kemikaaliturvallisuuslaki on turvallisuutta koskeva yleislaki myös vedyn osalta. Kemikaaliturvallisuuslaki asettaa sektorin toimijoille eräitä riskienhallinta- ja ilmoitusvelvoitteita. Nämä velvoitteet kohdistuvat kuitenkin ensisijaisesti aineellisten uhkien torjumiseen, eikä tieto- tai kyberturvallisuutta ole huomioitu kyseisessä sääntelyssä. Vetymarkkinoita koskevaa yleissääntelyä ei Suomessa tällä hetkellä ole.

3.3 Liikenne

NIS2-direktiivin soveltamisalaan kuuluvat eräät ilmaliikenteen, rautatieliikenteen, tieliikenteen ja vesiliikenteen alan toimijat. NIS1-direktiivin kansallisen täytäntöönpanon yhteydessä verkko- ja tietoturvallisuusvelvoitteita asetettiin liikenteenohjauspalvelun tarjoajille, lennonvarmistuspalvelun tarjoajille, alusliikennepalvelun tarjoajille, älykkään liikennejärjestelmän ylläpitäjille, valtion rataverkon haltijalle sekä yhteiskunnan toiminnan kannalta merkittävän lentoaseman tai sataman pitäjälle. NIS1-direktiivin kansallisen täytäntöönpanon lisäksi muu kansallinen tieto- tai kyberturvallisuussääntely on liikennesektorilla pääosin erittäin vähäistä. Valvovana viranomaisena on liikennesektorin osalta toiminut sen kaikilla alasektoreilla Liikenne- ja viestintävirasto. Raideliikennelakiin ei ole raideliikennesektorin osalta sisällytetty erillistä säännöstä valvontavastuusta

3.3.1 Ilmaliikenne

Ilmailu on kansainvälistä toimintaa, ja siviili-ilmailun sääntely perustuu pääosin kansainvälisiin sopimuksiin ja EU-lainsäädäntöön. EU on hiljattain hyväksynyt useita ilmailun kyberturvallisuutta koskevia säädöksiä. Ilmailun turvatoimiin liittyvät kyberturvallisuussäädökset ovat jo voimassa, mutta muilta osin kyberturvallisuutta koskevat säädökset tulevat sovellettaviksi vasta lokakuussa 2025 tai helmikuussa 2026 eli vähintäänkin vuotta myöhemmin kuin NIS2-sääntely. Ilmailua koskevaa tietoturvasääntelyä sisältyy seuraaviin suoraan sovellettaviin EU-säädöksiin:

Komission täytäntöönpanoasetus (EU) 2015/1998 yksityiskohtaisista toimenpiteistä ilmailun turvaamista koskevien yhteisten perusvaatimusten täytäntöönpanemiseksi.	Sovelletaan lentoaseman pitäjiin, lentoliikenteen harjoittajiin ja kansallisessa siviili-ilmailun turvaohjelmassa määriteltyihin yksiköihin.
Komission täytäntöönpanoasetus (EU) 2023/203 Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1139 soveltamissäännöistä komission asetusten (EU) N:o 1321/2014, (EU) N:o 965/2012, (EU) N:o 1178/2011 ja (EU) 2015/340 ja komission täytäntöönpanoasetusten (EU) 2017/373 ja (EU) 2021/664 soveltamisalaan kuuluvia organisaatioita sekä komission asetusten (EU) N:o 748/2012, (EU) N:o 1321/2014, (EU) N:o 965/2012, (EU) N:o 1178/2011, (EU) 2015/340 ja (EU) N:o 139/2014 ja komission täytäntöönpanoasetusten (EU) 2017/373 ja (EU) 2021/664 soveltamisalaan kuuluvia toimivaltaisia viranomaisia varten ilmailun turvallisuuteen mahdollisesti vaikuttavien tietoturvariskien hallintaa koskevien vaatimusten osalta sekä komission asetusten (EU) N:o 1178/2011, (EU) N:o 748/2012, (EU) N:o 965/2012, (EU) N:o 139/2014, (EU) N:o 1321/2014 ja (EU) 2015/340 ja komission täytäntöönpanoasetusten (EU) 2017/373 ja (EU) 2021/664 muuttamisesta.	Sovelletaan 22.2.2026 alkaen eräisiin huolto-organisaatioihin, lentokelpoisuuden hallintaorganisaatioihin, lentotoiminnan harjoittajiin, koulutusorganisaatioihin, ilmailulääketieteen keskuksiin, lennonvarmistus- tai lennonjohtopalvelun tarjoajiin, lentoa simuloivien koulutuslaitteiden (FSTD) käyttäjiin, U-space palveluntarjoajiin, U-space ilmatilan yhteisen tietopalvelujen tarjoajiin ja viranomaisiin. Sovelletaan 1.1.2026 alkaen EGNOS-lennonvarmistuspalvelun tarjoajiin.
Komission delegoitu asetus (EU) 2022/1645 Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1139 soveltamista koskevista säännöistä siltä osin kuin on kyse ilmailun	Sovelletaan 16.10.2025 alkaen eräisiin tuotanto- ja suunnitteluorganisaatioihin,

turvallisuuteen mahdollisesti vaikuttavien tietoturvariskien hallintaa koskevista vaatimuksista komission asetusten (EU) N:o 748/2012 ja (EU) N:o 139/2014 soveltamisalaan kuuluville organisaatioille sekä komission asetusten (EU) N:o 748/2012 ja (EU) N:o 139/2014 muuttamisesta.	lentopaikkojen pitäjiin sekä asematasovalvontapalvelujen tarjoajiin.

Ilmailun tietoturvallisuutta koskeva EU-sääntely soveltuu laajempaan toimijajoukkoon kuin NIS2-direktiivi, ja toimijoille asetettavat velvoitteet vastaavat pitkälti NIS2-vaatimuksia. Tätä ilmailun erityislainsäädäntöä voidaan pitää NIS2-direktiivin 4 artiklassa tarkoitettuina alakohtaisena unionin lainsäädäntönä.

NIS1-direktiivi on ilmailun osalta pantu täytäntöön lisäämällä ilmailulakiin 128 a ja 128 b § viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä tietoturvapoikkeamista ilmoittamisesta. Ilmailulain 128 a §:n nojalla on annettu myös yhteiskunnan toiminnan kannalta merkittävistä lentoasemista ja satamista annettu valtioneuvoston asetus (361/2018), jossa määritellään yhteiskunnan toiminnan kannalta merkittävät lentoasemat ja satamat. Tällaisia lentoasemia ovat asetuksen mukaan Helsinki-Vantaan ja Turun lentoasemat.

Ilmailulain 128 a ja 128 b § olisi tarpeen kumota NIS2-direktiivin toimeenpanon johdosta päällekkäisen sääntelyn välttämiseksi. Samalla kumoutuu ilmailulain 128 a §:n ja turvatoimilain 7 e §:n nojalla annettu valtioneuvoston asetus yhteiskunnan toiminnan kannalta merkittävistä lentoasemista ja satamista. NIS2-direktiivin soveltamisala ei edellytä yhteiskunnan toiminnan kannalta merkittävien lentoasemien ja satamien määrittelemistä valtioneuvoston asetuksella.

3.3.2 Rautatieliikenne

Rautateiden turvallisuudesta on kansallisesti säädetty raideliikennelaissa, jonka 2 luku sisältää keskeiset rautatieturvallisuutta koskevat velvoitteet. Raideliikennelailla on pantu täytäntöön rautateiden turvallisuudesta annettu Euroopan parlamentin ja neuvoston direktiivi 2016/798/EU ja rautatiejärjestelmän yhteentoimivuudesta Euroopan unionissa annettu Euroopan parlamentin ja neuvoston direktiivi 2016/797/EU. Näiden direktiivien nojalla on annettu myös useita suoraan sovellettavia komission delegoituja säädöksiä ja täytäntöönpanoasetuksia. Raideliikennelaissa NIS1-direktiivi on suurelta osin täytäntöönpantu 169 §:ssä, joka velvoittaa valtion rataverkon haltijan sekä liikenteenohjauspalvelun tarjoajan huolehtimaan viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä ilmoittamaan tietoturvallisuuteen liittyvästä häiriöstä. Lisäksi 169 § antaa Liikenne- ja viestintävirastolle toimivallan tiedottaa häiriöistä, ilmoittaa häiriöstä muille ETA-jäsenvaltioille sekä antaa tarkempia määräyksiä, milloin häiriö on merkittävä ja määräyksiä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

Raideliikennelain 169 § olisi tarpeen kumota NIS2-direktiivin toimeenpanon johdosta päällekkäisen sääntelyn välttämiseksi. Rautatieyritysten tai palvelupaikan ylläpitäjien osalta ei ole voimassa olevaa tieto- tai kyberturvallisuussääntelyä.

NIS1-direktiiviin pohjautuva kansallinen sääntely ei koske yksityisraiteiden haltijoita. Yhteiskunnan kannalta merkittävien satamanpitäjien satama-alueilla on myös yksityisraiteita, mutta turvatoimilaissa satamanpitäjien viestintäverkkojen ja tietojärjestelmien riskienhallintavelvollisuuden ei ole tulkittu koskevan näiden merisatamien yksityisraiteita.

Raideliikennelain 171 §:ssä on säädetty rataverkon haltijan, rautateiden liikenteenohjauspalvelun tarjoajan sekä metro- ja raitioverkon liikenteenohjauspalvelun tarjoajan varautumisvelvoitteista poikkeusoloissa ja normaaliolojen häiriötilanteissa. Lisäksi liikenteen palveluista anne-

tussa laissa on säädetty rautatieliikenteen harjoittajan (58 §) ja kaupunkiraideliikenteen harjoittajan (66 §) velvollisuudesta varautua normaaliolojen häiriötilanteisiin sekä poikkeusoloihin. Liikenne- ja viestintävirasto on antanut määräyksen valmiussuunnittelun järjestämisestä liikennejärjestelmässä, joka sisältää vähäisiä kyberturvallisuuteen liittyviä vaatimuksia rataverkon haltijoille, liikenteenohjauspalvelun tarjoajille soveltuvin osin kaupunkiraideliikenteelle. Kaupunkiraideliikenteen toimijat eivät kuulu NIS2-direktiivin soveltamisalaan. Viraston antama määräys koskee myös eräitä ilmailun ja tieliikenteen toimijoita, mutta niiden osalta määräys ei sisällä kyberturvallisuuteen liittyviä vaatimuksia.

3.3.3 Tieliikenne

Tieliikenteen hallinta- ja ohjauspalveluja tarjoavien toimijoiden NIS1-direktiivin mukaisista riskienhallinta- ja raportointivelvoitteista on säädetty liikenteen palveluista annetussa laissa. Kansallisesti NIS1-velvoitteet pantiin täytäntöön lisäämällä lakiin 140 § koskien tietoturvaa tieliikenteen ohjaus- ja hallintapalvelussa sekä 141 § tieliikenteen ohjaus- ja hallintapalveluiden poikkeamailmoitusten laatimisvelvoitetta koskien. Liikenteen palveluista annetun lain 140 § olisi tarpeen muuttaa NIS2-direktiivin kansallisen toimeenpanon johdosta.

Älykkäiden tieliikennejärjestelmien käyttöönotosta säädetään tieliikenteen älykkäiden liikennejärjestelmien käyttöönotosta sekä tieliikenteen ja muiden liikennemuotojen rajapintojen puitteista annetussa Euroopan parlamentin ja neuvoston direktiivissä 2010/40/EU (jäljempänä ITS-direktiivi). ITS-direktiivi on kansallisesti toimeenpantu liikenteen palveluista annetulla lailla. NIS1-direktiivin täytäntöönpanon yhteydessä liikenteen palveluista annettuun lakiin lisättiin 161 §, joka koskee älykkään liikennejärjestelmän ylläpitäjän velvollisuutta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja ilmoittaa tietoturvallisuuteen liittyvästä häiriöstä. Liikenteen palveluista annetun lain 161 § olisi tarpeen kumota NIS2-direktiivin toimeenpanon johdosta päällekkäisen sääntelyn välttämiseksi.

3.3.4 Vesiliikenne

NIS2-direktiivin soveltamisalaan kuuluvista alusliikennepalvelujen tarjoajista säädetään alusliikennepalvelulaissa. Alusliikennepalvelulain 16 §:n 5 momentin mukaan alusliikennepalvelun eli VTS-palvelun tarjoajan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. Alusliikennepalvelulla tarkoitetaan lain 2 §:n 1 momentin määritelmän mukaan alusliikenteen valvontaa ja ohjausta, jolla on valmiudet toimia vuorovaikutuksessa liikenteen kanssa ja reagoida muuttuviin liikennetilanteisiin. Lisäksi alusliikennepalvelulain 18 a §:ssä säädetään tietoturvaan liittyvistä häiriöistä ilmoittamisesta ja 28 §:n 4 momentissa tietoturvavelvoitteiden valvomisesta. Alusliikennepalvelulain 18 a § olisi tarpeen kumota NIS2-direktiivin toimeenpanon johdosta päällekkäisen sääntelyn välttämiseksi.

NIS2-direktiivin soveltamisalaan kuuluvat myös satamien hallinnointielimet sekä toimijat, jotka huolehtivat rakenteista ja varusteista sataman alueella. Sataman ja satamarakenteen turvatoimet perustuvat kansainvälisen SOLAS-yleissopimuksen säännöksiin ja niihin liittyvään ISPS-säännöstöön. Säännöstö on toimeenpantu alusten ja satamarakenteiden turvatoimien parantamisesta annetulla Euroopan parlamentin ja neuvoston asetuksella (EY) N:o 725/2004 (jäljempänä *EU:n turvatoimiasetus*).

EU:n turvatoimiasetusta täydentävät kansalliset säännökset on lisätty turvatoimilakiin, jolla on täytäntöönpantu myös satamien turvallisuuden parantamisesta annettu Euroopan parlamentin ja neuvoston direktiivi 2005/65/EY. NIS1-direktiivin toimeenpanon yhteydessä turvatoimilakiin lisättiin 7 e ja 7 f §, jotka velvoittavat yhteiskunnan toiminnan kannalta merkittävän satamanpitäjän huolehtimaan viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta

sekä ilmoittamaan tietoturvallisuuteen liittyvistä häiriöistä. Lisäksi turvatoimilain 7 e §:n nojalla on annettu myös yhteiskunnan toiminnan kannalta merkittävistä lentoasemista ja satamista annettu valtioneuvoston asetus (361/2018), jossa määritellään yhteiskunnan toiminnan kannalta merkittävät lentoasemat ja satamat. Näitä satamia ovat Haminan, Kotkan, Helsingin, Turun ja Naantalin satamat. Kansallinen satamanpitäjän määritelmä suhteessa NIS2-direktiivin liitteessä määriteltyyn toimijatyyppiin voi edellyttää täsmentämistä.

Turvatoimilain 7 e ja 7 f § olisi tarpeen kumota NIS2-toimeenpanon johdosta päällekkäisen sääntelyn välttämiseksi. Samalla kumoutuu turvatoimilain 7 e §:n ja ilmailulain 128 a §:n nojalla annettu valtioneuvoston asetus yhteiskunnan toiminnan kannalta merkittävistä lentoasemista ja satamista. NIS2-direktiivin soveltamisala ei edellytä yhteiskunnan toiminnan kannalta merkittävien lentoasemien ja satamien määrittelemistä valtioneuvoston asetuksella.

NIS2-direktiivin soveltamisalaan vesiliikenteen osalta kuuluvat lisäksi matkustaja- ja rahtiliikennettä hoitavat yhtiöt, lukuun ottamatta näiden yhtiöiden liikennöimiä aluksia sekä toimijat, jotka huolehtivat tuotantolaitoksista ja laitteista satamien alueella. Nämä toimijat ovat kuuluneet myös NIS1-direktiivin sektoreihin. NIS1-direktiivin kansallisen täytäntöönpanon yhteydessä ei ole tehty muutoksia näitä toimijoita koskevaan kansalliseen lainsäädäntöön, sillä kyseisillä sektoreilla ei tunnistettu kansallisesti yhtään sellaista keskeistä toimijaa tai palvelua, joka olisi täyttänyt direktiivin asettamat kriteerit.

3.4 Pankkitoiminta ja finanssimarkkinoiden infrastruktuuri

3.4.1 Kansallinen sääntely

NIS2-direktiivin soveltamisalaan kuuluvat finanssialan toimijatyypeistä luottolaitokset, kauppapaikkojen ylläpitäjät sekä keskusvastapuolet. Samat toimijat ovat kuuluneet myös NIS1-direktiivin soveltamisalaan. NIS1-direktiivin täytäntöönpanon yhteydessä sääntelyn piiriin arvioitiin kuuluvan luottolaitostoiminnasta annetussa laissa (610/2014, jäljempänä luottolaitoslaki) tarkoitettu luottolaitostoiminta sekä kaupankäynnistä rahoitusvälineillä annetussa laissa (1070/2017) tarkoitetun pörssitoiminnan harjoittaminen.

Yleiset vaatimukset luottolaitoksen riskienhallintajärjestelmälle on säädetty luottolaitoslain 9 luvun 2 §:ssä. Luottolaitoslain 9 luvun 16 §:n 2 momentti velvoittaa luottolaitoksen ylläpitämään riittäviä, turvallisia ja toimintavarmoja tietojärjestelmiä ja 16 §:n 3 momentti edellyttää luottolaitoksia laatimaan varautumissuunnitelmat ja jatkuvuussuunnitelmat, joiden kautta häiriöihin on mahdollista varautua, toiminnan jatkuvuus voidaan turvata ja häiriötilanteista aiheutuvia vahinkoja voidaan rajoittaa. Lain 5 luvun 10 ja 11 § sisältävät säännökset ulkoistamisesta ja sen edellytyksistä sekä luvun 16 § varautumisvelvollisuudesta häiriöiden varalle. Luottolaitosten osalta Finanssivalvonta on toiminut näiden velvoitteiden noudattamista valvovana viranomaisena.

Laki kaupankäynnistä rahoitusvälineillä sisältää pörssitoiminnan harjoittamisen osalta toimijoihin kohdistettuja riskienhallinta- ja ilmoitusvelvoitteita. Lain 3 luvun 1 § säännellyn markkinan toiminnan järjestämistä koskevista vaatimuksista asettaa toimijoille velvoitteet varmistaa järjestelmien häiriönsietokyky ja toimintaansa liittyvien riskien hallinta. Lisäksi lain 3 luvun 2 §:n 2 momentti asettaa pörssille velvollisuuden ilmoittaa tietyistä häiriöistä Finanssivalvonnalle, joka toimii pörssitoiminnan valvovana viranomaisena.

Finanssivalvonnan antamat määräykset operatiivisen riskin hallinnasta rahoitussektorin valvottavissa (8/2014, muutettu 16.2.2022) täsmentävät luottolaitosten ja pörssitoiminnan operatiivi-

sia riskienhallintavelvoitteita. Määräyksen 6 luku sisältää velvoitteet tietojärjestelmiä sekä tietoturvallisuutta koskien ja 9 luku käsittelee raportointia Finanssivalvonnalle. Määräyksen 9.1 (2) kohdan mukaan ensi-ilmoitus Finanssivalvonnalle on tehtävä asiakkaille tarjotuissa palveluissa sekä maksu- ja tietojärjestelmissä esiintyneistä merkittävistä häiriöistä ja virheistä viipymättä niiden ilmaannuttua. 9.1 (4) kohdan mukaan valvottavan tulee tehdä täydentävä ilmoitus Finanssivalvonnalle häiriön tarkemmista yksityiskohdista mahdollisimman pian ensimmäisen ilmoituksen tekemisen jälkeen ja loppuraportti, kun häiriön varsinainen syy on selvitetty. Finanssivalvonta on myös antanut määräyksen ulkoistamisesta (Määräykset ja ohjeet 1/2012, muutettu 23.1.2018)

Näiden kansallisten velvoitteiden on katsottu täyttävän ne riskienhallinta- ja raportointivaatimukset, jotka NIS1-direktiivi on edellyttänyt sen soveltamisalaan kuuluvilta keskeisten palvelujen tarjoajilta. Tämän vuoksi NIS1-direktiivin täytäntöönpano ei edellyttänyt muutoksia kansalliseen lainsäädäntöön pankki- tai finanssisektorilla.

NIS2-direktiivissä samat toimijatyypit kattavat pankkitoiminta ja finanssimarkkinoiden infrastruktuurit on liitteessä I määritelty erittäin kriittisiksi toimialoiksi ja niitä pidetään siten kynnysarvojen ylittyessä direktiiviä sovellettaessa keskeisinä toimijoina. NIS2-direktiivissä asetetaan toimijoille yksityiskohtaisempia ja kattavampia riskienhallinta- ja raportointivelvoitteita kuin NIS1-direktiivissä. Tässä yhteydessä on kuitenkin syytä huomioida finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU) N:o 600/2014, (EU) N:o 909/2014 ja (EU) 2016/1011 muuttamisesta annettu Euroopan parlamentin ja neuvoston asetus (EU) 2022/2554 (jäljempänä *DORA-asetus*).

3.4.2 DORA-asetus

DORA-asetus julkaistiin samanaikaisesti NIS2-direktiivin kanssa ja sitä sovelletaan 24 kuukauden kuluttua sen voimaantulosta. DORA-asetuksen tavoitteena on vahvistaa rahoitusmarkkinoiden liiketoimintaprosessien verkko- ja tietojärjestelmien turvallisuutta. Säännökset koskevat TVT-riskienhallintaa, laajamittaisten TVT-liitännäisten poikkeamien raportointia ja vapaaehtoisista merkittävistä kyberuhkista ilmoittamista toimivaltaisille viranomaisille, tiettyjen finanssiyhteisöjen raportointia maksuihin liittyvistä laajavaikutteisista poikkeamista, digitaalisen häiriönsietokyvyn testausta, kyberuhka- ja haavoittuvuustietojen ja tiedustelutietojen jakamista, sekä toimenpiteitä kolmansiin osapuoliin liittyvän TVT-riskin hallinnoimiseksi. Lisäksi asetuksessa säädetään TVT-palveluntarjoajana olevien kolmansien osapuolten ja finanssiyhteisöjen välillä tehtävien sopimusjärjestelyiden vaatimuksista sekä valvontakehyksestä, jota sovelletaan finanssiyhteisöille palveluja tarjoaviin kriittisiin TVT-palveluntarjoajana oleviin kolmansiin osapuoliin.

DORA-asetuksen johdanto-osan kappale 16 ja NIS2-direktiivin johdanto-osan kappale 28 esittää asetuksen olevan erityissäädös (lex specialis) suhteessa NIS2-direktiiviin. DORA-asetuksessa asetetaan finanssialan toimijalle NIS2-direktiivin velvoitteita pidemmälle menevä velvoite kyberuhkiin varautumiseen. Johdanto-osien mukaan finanssialan toimijoihin ei sovellettaisi NIS2-direktiivin kyberturvallisuusriskien hallintaa, raportointivelvoitteita, valvontaa tai täytäntöönpanoa koskevia säännöksiä, vaan DORA-asetusta. Samalla on kuitenkin tunnistettu tarve säilyttää vahva yhteys finanssialan ja NIS2-direktiivissä tarkoitettujen viranomaistahojen välillä, sekä taata toimiva tietojenvaihto finanssialan kanssa. Lisäksi jäsenvaltioiden olisi edelleen sisällytettävä finanssiala kyberturvallisuusstrategioihinsa, ja CSIRT-yksiköt voisivat kattaa finanssialan toiminnassaan. DORA-asetuksen asettamien toimivaltaisten viranomaisten tulisi kuulla kansallisia CSIRT-yksiköitä ja tehdä niiden kanssa yhteistyötä. DORA-asetuksen soveltamisala on laaja ja kattaa lähes kaikki EU:n rahoitusmarkkinalainsäädännössä säännellyt toimijat. Soveltamisalasta säännellään tarkemmin asetuksen 2 artiklassa.

DORA-asetuksen ja NIS2-direktiivin välisessä suhteessa keskeistä on, että TVT-tapahtumiin liittyvien tietojen on kuljettava sekä viranomaisten että rahoitusmarkkinatoimijoiden välillä. DORA-asetukseen perustuvan toimivaltaisen viranomaisten tulee jakaa tietoja merkittävistä tapahtumista myös muille viranomaisille. NIS2-direktiivin mukaisten toimivaltaisten viranomaisten, keskitettyjen yhteyspisteiden ja CSIRT-yksiköiden tulee tehdä asianmukaista yhteistyötä jäsenvaltion lainvalvontaviranomaisten, tietosuojaviranomaisten ja DORA-asetuksen mukaisen toimivaltaisten viranomaisten kanssa.

DORA-asetus velvoittaa finanssiyhteisöt TVT:hen liittyvien poikkeamien hallintaprosessin toteuttamiseen (17 artikla) ja poikkeamien luokitteluun (18 artikla). Finanssiyhteisön on lisäksi 19 artiklan mukaan raportoitava laajavaikutteisista poikkeamista toimivaltaiselle viranomaiselle. Kyberuhista voidaan myös ilmoittaa vapaaehtoisesti, ellei havaittu poikkeama muodosta raportointivelvoitetta, mutta yhteisö pitää uhkaa merkittävänä. EU:ssa voimassa olevassa sektorikohtaisessa rahoitusmarkkinalainsäädännössä jo nimetyt toimivaltaiset viranomaiset olisivat lähtökohtaisesti myös DORA-asetuksessa tarkoitettuja toimivaltaisia viranomaisia, ja niillä olisi oltava säädösten edellyttämä toimivalta. Suomessa tämä viranomainen olisi Finanssivalvonta. Asetuksen 47 artiklan mukaan toimivaltaiset viranomaiset voivat tarvittaessa kuulla NIS2-direktiivin mukaisesti nimettyjä tai perustettuja keskitettyjä yhteyspisteitä ja CSIRT-yksiköitä sekä vaihtaa tietoja niiden kanssa, sekä tarvittaessa pyytää niiltä teknistä neuvontaa ja apua, sekä sopia yhteistyöjärjestelyistä, joiden perusteella voidaan ottaa käyttöön tehokkaita ja nopeaan reagointiin pystyviä koordinointimekanismeja.

3.5 Terveydenhuoltoala

NIS2-direktiivin soveltamisalaan kuuluvat terveydenhuollon tarjoajat, EU:n vertailulaboratoriot, lääkkeiden tutkimusta ja kehitystä harjoittavat toimijat, eräät lääkeaineiden ja lääkkeiden valmistusta harjoittavat toimijat sekä vakavan kansanterveysuhan aikana kriittisiksi katsottuja lääkinnällisiä laitteita valmistavat toimijat. Soveltamisala on huomattavasti laajempi kuin NIS1-direktiivissä, jonka soveltamisalaan kuuluivat terveydenhuoltosektorin osalta vain terveydenhuoltolaitokset. NIS1-direktiivin toimeenpanon yhteydessä voimassaolevan sääntelyn katsottiin täyttävän direktiivin vaatimukset, joten kansalliseen lainsäädäntöön ei tällöin tehty muutoksia.

3.5.1 Terveydenhuollon tarjoajat

NIS 2 –direktiivin soveltamisalaan kuuluvat Euroopan parlamentin ja neuvoston direktiivin 2011/24/EU (18) potilaiden oikeuksien soveltamisesta rajatylittävässä terveydenhuollossa 3 artiklan g alakohdassa määritellyt terveydenhuollon tarjoajat. Direktiivin 2011/24/EU (18) 3 artiklan g alakohdassa ’terveydenhuollon tarjoajalla’ tarkoitetaan luonnollista henkilöä tai oikeushenkilöä tai muuta kokonaisuutta, joka tarjoaa laillisesti terveydenhuoltoa jonkin jäsenvaltion alueella.

Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa (784/2021, jäljempänä *asiakastietolaki*) säädetään sosiaali- ja terveydenhuollon tietojärjestelmistä ja niiden turvallisuusvaatimuksista. Lain 7 § velvoittaa palvelunantajan liittymään valtakunnallisten tietojärjestelmäpalveluiden käyttäjäksi (Kanta-palvelut). Sääntely koskee julkisia terveydenhuollon tarjoajia sekä yksityisiä toimijoita, mikäli niillä on käytössään asiakas- ja potilastietojen käsittelyyn tarkoitettu tietojärjestelmä. Asiakastietolain 14 § edellyttää, että arkistointipalvelu tulee suojata valtion viranomaisten tietoturvallisuutta koskevien velvoitteiden mukaisesti. Näistä velvoitteista säädetään julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019), jonka 4 luku sisältää tietoturvaa koskevat säännökset, erityisesti 13 § tietoaineistojen ja tietojärjestelmien tietoturvallisuudesta ja 13 a § häiriötilanteista tiedottamisesta ja niihin varautumisesta.

Asiakastietolain 27 § velvoittaa palvelunantajan, välittäjän ja Kansaneläkelaitoksen laatimaan tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvän tietoturvasuunnitelman. Lain 39 §:n mukaan Terveyden- ja hyvinvoinnin laitos vastaa valtakunnallisten tietojärjestelmäpalvelujen suunnittelusta, ohjauksesta ja seurannasta. Terveyden- ja hyvinvoinnin laitokselle annetaan lisäksi valtuudet antaa tarkentavia turvallisuusmääräyksiä. Toimijan on lain mukaan ilmoitettava olennaisesta poikkeamasta tietojärjestelmässä Sosiaali- ja terveysalan lupa- ja valvontavirastolle Valviralle, mikäli poikkeama voi aiheuttaa merkittävän riskin asiakasturvallisuudelle tai tietoturvalle (41 §).

Asiakastietolakia on juuri päivitetty (HE 246/2022 vp, laki 703/2023), ja tässä yhteydessä lakiin lisättiin uusi 77 §, jossa säädetään palvelunantajalle, apteekille, välittäjälle ja Kansaneläkelaitokselle velvoite laatia tietoturvasuunnitelma, jossa käsitellään organisaation tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyviä keskeisiä asioita. Lisäksi lakiin lisättiin uusi 90 §, jossa säädetään toimijoiden velvoitteesta ilmoittaa tietojärjestelmän ja hyvinvointisovelluksen olennaisten vaatimusten poikkeamista sekä tietoverkkoihin kohdistuvasta tietoturvallisuuden häiriöstä. Muutokset tulevat voimaan 1.1.2024. Asiakastietolain 90 §:ää olisi tarpeen muuttaa NIS2-direktiivin toimeenpanon johdosta.

3.5.2 EU:n vertailulaboratoriot

EU:n vertailulaboratorioista säädetään Rajatylittävistä vakavista terveysuhkista ja päätöksen N:o 1082/2013/EU kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2371 15 artiklassa. Asetuksen 2022/2371 (19) 15 artiklan 1 kohdan mukaan kansanterveyden alalla tai tietyillä kansanterveyden aloilla, jotka ovat merkityksellisiä asetuksen tai kansallisten ehkäisy-, valmius- ja reagointisuunnitelmien täytäntöönpanon kannalta, komissio voi täytäntöönpanosäädöksillä nimetä EU:n vertailulaboratorioita, jotka tarjoavat tukea kansallisille vertailulaboratorioille hyvien käytäntöjen ja vapaaehtoiselta pohjalta tapahtuvan jäsenvaltioiden lähentymisen edistämiseksi diagnostiikan, testausmenetelmien sekä tiettyjen testien käytön osalta jäsenvaltioissa toteutettavaa tautien yhdenmukaista seurantaa, niistä ilmoittamista ja raportointia varten.

Asetuksen 2022/2371 (19) 15 artiklan 2 kohdan mukaan EU:n vertailulaboratoriot ovat vastuussa kansallisten vertailulaboratorioiden verkoston koordinoimisesta. 15 artiklan 3 kohdan mukaan EU:n vertailulaboratorioiden verkoston ylläpidosta ja koordinoinnista vastaa European Centre for Disease Prevention and Control (ECDC) yhteistyössä WHO:n vertailulaboratorioiden kanssa. Asetuksen 15 artiklan 5 kohdan mukaan EU:n vertailulaboratorioiden on oltava puolueettomia, niillä ei saa olla eturistiriitoja, eivätkä ne etenkään saa olla tilanteessa, joka suoraan tai epäsuorasti voisi vaikuttaa niiden ammattimaisen käytöksen puolueettomuuteen niiden EU:n vertailulaboratorion ominaisuudessa suorittamien tehtävien suhteen; niillä on oltava henkilöstöä, jolla on asianmukainen pätevyys ja riittävä koulutus omalla osaamisalueellaan, tai niiden on sopimusperusteisesti saatava käyttöönsä tällaista henkilöstöä; niillä on oltava käytössään tai saatava käyttöönsä infrastruktuuri, laitteet ja tuotteet, joita tarvitaan niille annettujen tehtävien suorittamiseksi; niiden on varmistettava, että niiden henkilöstöllä ja mahdollisella sopimussuhteisella henkilöstöllä on hyvä tietämys kansainvälisistä standardeista ja käytännöistä ja että niiden työssä otetaan huomioon kansallisella, unionin ja kansainvälisellä tasolla tehdyn tutkimuksen uusin kehitys; niillä on oltava käytössään tai mahdollisuus saada käyttöönsä laitteet, joiden avulla ne voivat suorittaa tehtävänsä hätätilanteissa, ja niillä on tarvittaessa oltava varusteet, joiden avulla ne voivat täyttää asiaankuuluvat bioturvallisuusvaatimukset.

EU:n vertailulaboratorioista ei ole annettu EU-sääntelyä täydentävää kansallista lainsäädäntöä. Kansallisen lainsäädännön tarvetta harkitaan, kun EU-tasolla on saatu valmiiksi asetusta täydentävä ohjeistus.

3.5.3 Lääkkeiden tutkimusta, kehitystä ja valmistusta harjoittavat toimijat

NIS 2 –direktiivin soveltamisalaan kuuluvat Euroopan parlamentin ja neuvoston direktiivin 2001/83/EY (202) 1 artiklan 2 alakohdassa määriteltyjen lääkkeiden tutkimusta ja kehitystä harjoittavat toimijat. Direktiivin 2001/83/EY (202) 1 artiklan 2 alakohdassa lääkkeellä tarkoitetaan aineita tai aineiden yhdistelmiä, jotka on tarkoitettu ihmisen sairauden hoitoon tai ehkäisyyn, tai aineita tai aineiden yhdistelmiä, joita voidaan käyttää ihmisiin tai antaa ihmisille joko elintoimintojen palauttamiseksi, korjaamiseksi tai muut-tamiseksi farmakologisen, immunologisen tai metabolisen vaikutuksen avulla taikka sairauden syyn selvittämiseksi Lisäksi NIS 2 –direktiivin soveltamisalaan kuuluvat NACE Rev. 2 –luokituksen C jakson kaksinumerotasossa 21 tarkoitetut lääkeaineiden ja lääkkeiden valmistusta harjoittavat toimijat.

Lääkelaki (395/1987) sääntelee lain 2 §:n mukaisesti lääkkeiden valmistusta, maahantuontia, jakelua, välittämistä ja myyntiä sekä muuta kulutukseen luovutusta, edellä mainittua toimintaa harjoittavia lääketehtaita, lääketukkukauppoja, lääkkeiden välittäjiä ja apteekkeja, lääkkeiden prekliinisiä turvallisuustutkimuksia tekeviä laboratorioita sekä lääkkeiden valmistusta ja jakelua sairaaloissa ja terveyskeskuksissa. Lääkealan sääntely perustuu pitkälti EU-tason sääntelyyn, pääasiassa ihmisille tarkoitettuja lääkkeitä koskevista yhteisön säännöistä annettuun Euroopan parlamentin ja neuvoston direktiiviin 2001/83/EY (jäljempänä *lääkedirektiivi*). Lääkelaissa tai lääkedirektiivissä ei ole kyberturvallisuutta koskevaa sääntelyä.

Lääkkeiden kliinisestä tutkimuksesta säädetään lääkkeiden kliinisestä tutkimuksesta annetussa laissa (983/2021, jäljempänä *lääketutkimuslaki*). Lääketutkimuslakia sovelletaan lain 1 §:n mukaan ihmisille tarkoitetun lääkkeen kliinisen lääketutkimuksen ennakkoarviointiin, suorittamiseen ja valvontaan siten kuin kliininen lääketutkimus on määritelty ihmisille tarkoitettujen lääkkeiden kliinisistä lääketutkimuksista ja direktiivin 2001/20/EY kumoamisesta annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) N:o 536/2014 (jäljempänä *lääketutkimusasetus*). Kansallisessa laissa annetaan lääketutkimusasetusta täydentävät säännökset. Lääketutkimusasetus tai kansallinen lääketutkimuslaki eivät sisällä kyberturvallisuutta koskevaa sääntelyä.

3.5.4 Vakavan kansanterveysuhan aikana kriittisiksi katsottuja lääkinnällisiä laitteita valmistavat toimijat

NIS 2 –direktiivin soveltamisalaan kuuluvat Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/123 22 artiklassa tarkoitetut vakavan kansanterveysuhan aikana kriittisiksi katsottujen lääkinnällisten laitteiden (kansanterveysuhan aikana kriittisten lääkinnällisten laitteiden luettelo) valmistavat toimijat. Asetuksen (EU) 2022/123 22 artiklan mukaan heti sen jälkeen, kun kansanterveysuhka on todettu, lääkinnällisten laitteiden pulaa käsittelevän ohjausryhmän on kuultava asetuksen 21 artiklan 5 kohdassa tarkoitettua työryhmää. Heti kyseisen kuulemisen jälkeen lääkinnällisten laitteiden pulaa käsittelevän ohjausryhmän on vahvistettava luettelo kriittisten lääkinnällisten laitteidenluokista, joiden se katsoo olevan kriittisiä kansanterveysuhan aikana, jäljempänä ’kansanterveysuhan aikana kriittisten lääkinnällisten laitteiden luettelo’. Asiaankuuluvat tiedot kriittisistä lääkinnällisistä laitteista ja niiden valmistajista on mahdollisuuksien mukaan kerättävä Eudamedista, sitten kun se on täysin toimintavalmis. Tiedot on tarvittaessa kerättävä myös maahantuojilta ja jakelijoilta. Siihen saakka, kun Eudamed on täysin toimintavalmis, saatavilla olevia tietoja voidaan kerätä myös kansallisista tietokannoista tai muista käytettävissä olevista lähteistä. Lääkinnällisten laitteiden pulaa käsittelevän ohjausryhmän on päivitettävä kansanterveysuhan aikana kriittisten lääkinnällisten laitteiden luetteloa aina tarpeen tullen, kunnes kansanterveysuhan on todettu päättyneen. Sovellettaessa 25 artiklan 2 kohtaa lääkinnällisten laitteiden pulaa käsittelevän ohjausryhmän on hyväksyttävä ja asetettava julkisesti saataville 25 artiklan 2 kohdan c ja d alakohdassa tarkoitettu tietopaketti, joka on tarpeen

kansanterveysuhan aikana kriittisten lääkinnällisten laitteiden luetteloon sisältyvien lääkinnällisten laitteiden tarjonnan ja kysynnän seuraamiseksi, ja annettava kyseinen tietopaketti tiedoksi 21 artiklan 5 kohdassa tarkoitetulle työryhmälle. Lääkeviraston on julkaistava www-portaalissaan olevalla tähän tarkoitukseen varatulla verkkosivustolla kansanterveysuhan aikana kriittisten lääkinnällisten laitteiden luettelo ja kyseisen luettelon päivitykset ja tiedot, jotka koskevat kansanterveysuhan aikana kriittisten lääkinnällisten laitteiden luetteloon sisältyvien kriittisten lääkinnällisten laitteiden todellista pulaa.

Vakavan kansanterveysuhan aikana kriittisiksi katsottavien lääkinnällisten laitteiden valmistavista toimijoista ei ole annettu EU-sääntelyä täydentävään kansallista lainsäädäntöä.

3.6 Juomavesi ja jätevesi

Sekä juomavesi että jätevesi ovat kuuluneet NIS1-direktiivin mukaiseen kansalliseen soveltamisalaan, jonka mukaiset vaatimukset toimeenpantiin Suomessa vesihuoltolain muutoksella. Vesihuoltolaki soveltuu sekä talousveden että jäteveden käsittelyyn. Vesihuollon toimialalla ei ole muuta sektorikohtaista kyberturvallisuussääntelyä, mutta talousvettä toimittavalta laitokselta edellytetään jo nykyisin veden laatuun liittyvää riskinarviointia ja riskienhallintaa toiminnan harjoittajan, viranomaisten ja muiden sidosryhmien yhteistyönä.

Vesihuoltolain 15 b §:ssä velvoitetaan sellainen vesihuoltolaitos, joka toimittaa vettä tai ottaa vastaan jätevettä vähintään 5 000 kuutiometriä vuorokaudessa, ilmoittamaan merkittävästä häiriötilanteesta elinkeino-, liikenne- ja ympäristökeskukselle. Lisäksi lain 35 §:n 2 momentissa säädetään oikeudesta luovuttaa tietoja tietoturvallisuuteen liittyen Liikenne- ja viestintävirastolle julkisuuslain salassapitovelvollisuuden estämättä. Vesihuoltolaissa säädetään myös vesihuoltolaitoksen velvollisuudesta turvata palvelujensa saatavuus häiriötilanteissa (15 a §) sekä ilmoittaa merkittävästä häiriötilanteesta viipymättä elinkeino- liikenne- ja ympäristökeskukselle (15 b §).

Terveydensuojelulain (763/1994) 5 luvussa säädetään talousvettä toimittavan laitoksen riskienhallintavelvoitteista. Lailla on toimeenpantu ihmisten käyttöön tarkoitetun veden laadusta annetun Euroopan parlamentin ja neuvoston direktiivin (EU 2020/2184) riskienhallintavelvoitteet. Lain mukaan laitoksen on harjoitettava omavalvontaan liittyvää riskinarviointia ja riskienhallintaa toiminnan harjoittajan, viranomaisten ja muiden sidosryhmien yhteistyönä. Lain 19 a §:n mukaan toimijan on laadittava riskienhallintasuunnitelma riskien hallitsemiseksi ja ehkäisemiseksi. Riskinarvioinnilla tarkoitetaan pääasiassa veden laatuun vaikuttavia riskejä. Valtioneuvoston asetuksessa talousveden tuotantoketjun riskien hallinnasta ja omavalvonnasta (7/2023) on täsmennetty näitä velvoitteita. Asetus on annettu terveydensuojelulain 19 a §:n 5 momentin ja vesihuoltolain 15 §:n 5 momentin nojalla.

Vesihuollon osalta NIS2-direktiivin soveltamisala edellyttää, että kansallisesta 5000 kuutometrin määritelmästä luovutaan. Soveltamisalan olisi määriydyttävä jatkossa toimijatyypin ja toimijan koon perusteella. Lisäksi NIS2-direktiiviä on sovellettava toimijan koosta riippumatta myös sellaisiin toimijoihin, joiden tarjoamassa palvelussa tapahtuva häiriö voisi vaikuttaa merkittävästi yleiseen järjestykseen, yleiseen turvallisuuteen tai kansanterveyteen, mikä saattaa laajentaa soveltamisalaa vesihuollon osalta. Vesihuoltolain 15 b §:ssä säädettyyn velvoitteeseen ilmoittaa häiriötilanteesta ei arvioida välttämättömäksi tehdä muutoksia NIS2-direktiivin toimeenpanon johdosta, koska säännös tulee sovellettavaksi myös muissa kuin viestintäverkkoihin ja tietojärjestelmiin kohdistuvissa häiriötilanteissa. Lain 15 b §:n osalta tarvittavat muutokset arvioidaan CER-direktiivin toimeenpanon yhteydessä. Lain 35 § 2 momentin 3 kohta ehdotetaan kumottavan NIS2-direktiivin toimeenpanon johdosta päällekkäisen sääntelyn välttämiseksi.

3.7 Digitaalinen infrastruktuuri ja digitaalisen palvelun tarjoajat

Digitaalisen palvelun tarjoajat ovat pääosin kuuluneet NIS1-direktiivin mukaiseen soveltamisalaan, mutta etenkin digitaalisen infrastruktuurin toimijoita on tulossa uusina toimijoina NIS2-direktiivin soveltamisalaan. NIS2-direktiivin soveltamisalaan tulisi uusina toimijoina viestintäverkkojen ja –palvelujen tarjoajat, sähköisten luottamuspalvelujen tarjoajat, sisällönjakeluverkkojen tarjoajat sekä datakeskuspalvelujen tarjoajat. Sektorin valvovana viranomaisena on NIS1-direktiivin aikana toiminut Liikenne- ja viestintäviraston Kyberturvallisuuskeskus. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus valvoo jo nykyään myös viestintäverkkojen ja –palvelujen sekä sähköisten luottamuspalvelujen tarjoamista. Voimassa olevassa lainsäädännössä ei ole nimenomaan sisällönjakeluverkkojen tarjoajia ja datakeskuspalvelun tarjoajia koskevaa sääntelyä, ellei toiminta tapauskohtaisen arvioinnin perusteella täytä viestinnän välittämisen määritelmää.

3.7.1 Digitaalisen palvelun tarjoajat

Sähköisen viestinnän palveluista annetussa laissa säädetään eräistä digitaalisten palvelujen tarjoajia eli verkossa toimivaa markkinapaikkaa, hakukonepalvelua ja pilvipalvelun tarjoajaa koskevista tietoturvavelvoitteista. Säännökset on lisätty sähköisen viestinnän palveluista annettuun lakiin NIS1-direktiivin täytäntöönpanon yhteydessä. Sähköisen viestinnän palveluista annetun lain 247 a §:ssä säädetään digitaalisten palvelujen tarjoajien velvollisuudesta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. Lisäksi lain 275 §:n 2 momentissa on säädetty häiriöilmoituksen tekemisestä Liikenne- ja viestintävirastolle. Lain 247 a § ja 275 §:n 2 momentti ehdotetaan kumottavan NIS2-direktiivin toimeenpanon johdosta päällekkäisen sääntelyn välttämiseksi.

3.7.2 Verkkotunnustoiminta

Sähköisen viestinnän palveluista annetun lain 21 luvussa säädetään fi-verkkotunnuksista sekä niihin liittyvästä verkkotunnustoiminnasta ja verkkotunnusten välittämisestä. Osa fi-verkkotunnusvälittäjistä toimii samanaikaisesti sekä verkkotunnusten rekisteröintipalveluntarjoajina, että DNS-palveluntarjoajina. Fi-verkkotunnustoimintoa ja fi-verkkotunnusvälittäjiä koskevat tietoturvavelvoitteet säädettiin lakiin jo vuonna 2015, verkkotunnustoimintoon sekä -välittäjiin säännöksiä on sovellettu syyskuusta 2016 lähtien. NIS1-direktiivin kansallisen toimeenpanon yhteydessä katsottiin jo olemassa olevien tietoturva- ja raportointivelvoitteiden riittävän eikä muutoksia lainsäädäntöön enää erikseen tehty.

Sähköisen viestinnän palveluista annetun lain 170 §:ssä ja 171 §:ssä säädetään verkkotunnusvälittäjän ja Liikenne- ja viestintäviraston velvollisuudesta huolehtia toimintansa tietoturvasta. Lain 170 §:ssä säädetään verkkotunnusvälittäjän velvollisuudesta tehdä häiriöilmoitus Liikenne- ja viestintävirastolle. Liikenne- ja viestintävirasto on lisäksi antanut verkkotunnusmääräyksen 68/2016 M, jossa määrätään tarkemmin verkkotunnusvälittäjien tietoturvallisuuden hallintavelvoitteista ja häiriöitä koskevasta ilmoitusvelvollisuudesta. Liikenne- ja viestintävirasto valvoo jo nykyään fi-verkkotunnusvälittäjiä lain 171 §:n mukaisesti. Lain 21 lukuun olisi tarpeen tehdä NIS2-direktiivin artiklojen 27 ja 28 edellyttämiä täydennyksiä.

3.7.3 Viestintäverkot ja -palvelut

Viestintäverkoista ja-palveluista säädetään sähköisen viestinnän palveluista annetussa laissa. Lain 247 §:ssä säädetään viestinnän välittäjän ja lisäarvopalvelun tarjoajan velvollisuudesta huolehtia palveluidensa tietoturvasta ja 243 sekä 244 a §:ssä säädetään yleisiä velvoitteita siitä, millä tavoin viestintäverkkojen ja –palvelujen tietoturvasta on huolehdittava. Lisäksi lain X

osassa säädetään viestinnän ja palvelujen jatkuvuuden turvaamisesta, mikä pitää sisällään muun muassa toimenpiteitä tietoturvan toteuttamiseksi, velvoitteen korjata viestintäverkon, viestintäpalvelun tai laitteen aiheuttama merkittävä haitta tai häiriö, velvoitteen ilmoittaa häiriöistä Liikenne- ja viestintävirastolle sekä palvelun tilaajalle ja käyttäjälle. Teleyrityksiä koskeva häiriöilmoitusvelvollisuus kattaa palvelun toimivuuteen kohdistuvien häiriöiden lisäksi tietoturvaa koskevat häiriöt sekä sähköisen viestinnän tietosuojadirektiivin mukaisen velvoitteen ilmoittaa henkilötietoja koskevista tietoturvaloukkauksista. Lisäksi lain X osassa säädetään teleyrityksen varautumissuunnittelusta sekä velvollisuudesta varautua normaaliolojen häiriötilanteisiin ja poikkeusoloihin. Liikenne- ja viestintävirasto on lisäksi antanut määräyksiä koskien teletoiminnan tietoturvaa, teletoiminnan häiriötilanteita, viestintäverkon kriittisisiä osia, viestintäverkkojen ja -palvelujen varmistamista ja viestintäverkkojen synkronointia sekä verkkotunnuksia.

3.7.4 Sähköiset luottamuspalvelut

Sähköisiä luottamuspalveluja säännellään sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) N:o 910/2014 (jäljempänä *eIDAS-asetus*) sekä sitä täydentävässä vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (617/2009, jäljempänä *tunnistus- ja luottamuspalvelulaki*). Sähköisten luottamuspalvelujen tarjoajiin sovellettavista tietoturvavaatimuksista säädetään eIDAS-asetuksen 19 artiklassa, joka NIS2-direktiivin 42 artiklan mukaisesti kumotaan 18. lokakuuta 2024. Sähköiset luottamuspalvelut voivat olla joko hyväksyttyjä tai ei-hyväksyttyjä. Hyväksytyn luottamuspalvelun tarjoaminen edellyttää akkreditoidun vaatimustenmukaisuuden arviointilaitoksen tekemää vaatimustenmukaisuuden arviointia, sekä Liikenne- ja viestintäviraston hyväksyntää. Tunnistus- ja luottamuspalvelulain 32 §:ssä säädetään tarkemmin hyväksytyn luottamuspalvelun vaatimustenmukaisuuden vahvistamisesta. Lisäksi Liikenne- ja viestintäviraston määräyksessä M72 on annettu tarkempia määräyksiä hyväksyttyjen sähköisten luottamuspalveluiden vaatimustenmukaisuuden arviointiperusteista ja niiden vaatimuksenmukaisuuden arvioinnin pätevyyskriteereistä. Tunnistus- ja luottamuspalvelulakiin ei ole tunnistettu tarpeelliseksi tehdä muutoksia NIS2-täytäntöönpanon johdosta.

3.8 Tieto- ja viestintätekniikan palvelujen (TVT-palvelut) hallinta

Tieto- ja viestintätekniikan palvelujen tarjoajat eli TVT-palvelutarjoajat eivät ole kuuluneet NIS1-direktiivin soveltamisalaan, vaan tulevat uutena sektorina NIS2-direktiivin soveltamisalan piiriin. NIS2-direktiivin alaan kuuluvia TVT-palvelutarjoajia ovat yritysten väliset hallinta- ja tietoturvapalveluntarjoajat, jotka ovat keskisuuria tai suuria yrityksiä. NIS2-direktiivissä hallintapalvelun tarjoajalla tarkoitetaan toimijaa, joka tarjoaa TVT-tuotteiden, verkkojen, infrastruktuurin, sovellusten tai muiden verkko- ja tietojärjestelmien asentamiseen, hallintaan, käyttöön tai ylläpitoon liittyviä palveluja joko asiakkaan tiloissa tai etäyhteyden välityksellä toteutettavan tuen tai aktiivisen ylläpidon muodossa. Tietoturvapalveluntarjoajalla tarkoitetaan sellaista hallintapalvelun tarjoajaa, joka toteuttaa kyberturvallisuusriskien hallintatoimia tai antaa tukea niitä varten. TVT-palvelulla tarkoitetaan kyberturvallisuusasetuksen 2 artiklan 13 alakohdan mukaan mitä tahansa palvelua, jonka sisältönä on kokonaan tai pääasiassa tiedon välittäminen, tallentaminen, hakeminen tai käsittely verkko- ja tietojärjestelmien avulla.

TVT-palvelujen tarjoamista ei tällä hetkellä säännellä kattavasti lainsäädännössä. Sähköisen viestinnän palveluista annetun lain näkökulmasta kyseessä saattaa olla viestinnän välittäjän alihankkijana toimiva taho, jolle ei laissa kuitenkaan aseteta suoraan omia velvoitteita. Joissakin tapauksissa tietoturvapalvelun tarjoaja saattaa olla em. laissa tarkoitettu lisäarvopalvelun tarjoaja, jolloin sitä koskisi lain 247 §:n 2 momentin mukainen velvollisuus huolehtia palvelujensa tietoturvasta.

3.9 Avaruus

Avaruussektori ei ole kuulunut NIS1-direktiivin soveltamisalaan, vaan se lisätään uutena NIS2-direktiivin soveltamisalan piiriin. Suomessa avaruustoimintaa on kansallisesti säännelty maa-asemista ja eräistä tutkista annetussa laissa (96/2023, jäljempänä *maa-asemalaki*) sekä avaruustoiminnasta annetussa laissa (63/2018). NIS2-direktiivin soveltamisalaan kuuluvat avaruuspohjaisten palvelujen tarjoamista tukevan, maassa sijaitsevan infrastruktuurin ylläpitäjät.

Maa-asemalaissa säädetään maa-aseman ja tutkan perustamisen sekä maa-asema- ja tutkatoiminnan luvanvaraisuudesta ja valvonnasta. Maa-aseman ja tutkan perustaminen on luvanvaraista toimintaa lukuun ottamatta tavanomaista satelliittipalveluiden käyttöä. Lupa- ja valvontaviranomaisena lain velvoitteiden noudattamisessa toimii Liikenne- ja viestintävirasto.

Lain 2 §:n 5 kohdan mukaan maa-asema- ja tutkatoiminnan harjoittajalla tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, joka harjoittaa tai jonka on tarkoitus harjoittaa maa-asema- tai tutkatoimintaa tai joka tosiasiallisesti vastaa tällaisesta toiminnasta. Edellä mainitut avaruuspohjaisten palvelujen tarjoamista tukevien, maassa sijaitsevan infrastruktuurien ylläpitäjät ovat maa-asemalain tarkoittamia toiminnanharjoittajia. Kaikki nykyiset toiminnanharjoittajat eivät kuitenkaan kuulu NIS2-soveltamisalaan.

Toiminnan ja toiminnanharjoittajien on täytettävä tietyt vaatimukset riskien hallitsemiseksi, mukaan lukien toiminnan suojaaminen ulkoisilta häiriöiltä ja tietoturvauhilta, tietoturvallisuuden ja fyysisen turvallisuuden varmistaminen, kyky havaita tietoturvaloukkauksia ja -uhkia, jatkuvuuden ja kriisitilanteiden hallinta, toimitusketjujen turvallisuus sekä riskienhallintamenettelyiden ja tietojärjestelmäturvallisuutta koskevien käytäntöjen dokumentoiminen (6 §). Liikenne- ja viestintävirastolla on tiedonsaantioikeus tietoturvaloukkausten selvittämistä koskien (14 §) ja oikeus suorittaa toimintaan kohdistuvia tarkastuksia (13 §). Toiminnanharjoittaja on velvollinen ilmoittamaan tietoturvahäiriöstä Liikenne- ja viestintävirastolle (11 §).

Maa-asemalain valmistelussa (HE 113/2022 vp) pyrittiin huomioimaan osa silloisten valmisteluvaiheessa olleiden NIS2- ja CER-direktiiviehdotuksien vaatimuksista. Maa-asemalain valmistelun yhteydessä ei ollut tiedossa, miten NIS2-direktiivi tultaisiin kansallisesti toimeenpanemaan. Lain valmistelussa tavoiteltiin, ettei esitys olisi ristiriidassa silloisen NIS2-direktiiviehdotuksen kanssa ja siinä pyrittiin huomioimaan erityisesti velvoitteet tietoturvariskien hallinnan ja häiriötilanteista ilmoittamisen osalta myöhempien säädösmuutostarpeiden minimoimiseksi. Kyseiset riskienhallinta-, tietoturva- ja häiriöilmoitusvelvoitteet koskevat kaikkia maa-asema- ja tutkatoiminnan harjoittajia koosta riippumatta ja viranomaisia koskevia tiettyjä poikkeuksia lukuun ottamatta. Edellä mainittujen velvoitteiden täyttyminen on osa luvan myöntämisen ja toiminnan harjoittamisen edellytyksiä.

3.10 Posti- ja kuriiripalvelut

NIS2-direktiiviin soveltamisalaan on uutena sektorina lisätty posti- ja kuriiripalvelut. Kansallisesti postipalveluista säädetään postilaissa (415/2011). Kansallinen sääntely postipalvelujen osalta on kuitenkin perinteisesti keskittynyt postimarkkinoiden avaamiseen ja datan avoimuuteen eikä turvallisuusnäkökohtiin. Tämän lisäksi postipalveluista säädetään yhteisön postipalvelujen sisämarkkinoiden kehittämistä ja palvelun laadun parantamista koskevista yhteisistä säännöistä annetussa Euroopan parlamentin ja neuvoston direktiivissä 97/67/EY (jäljempänä *postidirektiivi*) sekä rajatylittävistä pakettipalveluista annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) 2018/644. Postidirektiivin sääntely on vanhentunutta, ja jäsenvaltiot ovat toivoneet sen pikaista päivittämistä. Nykyisellään kyberturvallisuutta koskeva sääntely on

postipalvelujen osalta vähäistä. Postilain 64 – 66 §:ssä säädetään postiyrityksen velvollisuudesta varautua poikkeustilanteisiin. Kuriiripalvelujen tarjoamiselle ei ole Suomessa erityissääntelyä, ja toiminta on siviilioikeudellisten yleissäännösten varassa.

Postilakiin tai muuhun posti- ja kuriiripalveluiden toimialaa koskevaan erityissääntelyyn ei ole tunnistettu tarpeelliseksi tehdä muutoksia NIS2-direktiivin toimeenpanon johdosta.

3.11 Jätehuolto

Jätehuolto ei ole kuulunut NIS1-direktiivin soveltamisalaan, vaan se on lisätty uudeksi toimialaksi vasta NIS2-direktiivin myötä. Jätehuollon sektori on laaja-alainen ja sisältää lukuisan määrän erilaisia ja erikokoisia toimijoita, mutta käytännössä vain muutama kymmenen toimijaa kuuluu henkilöstömäärältään tai liikevaihdoltaan NIS2-direktiivin soveltamisalaan. Kansallisesti jätehuoltoa ja siihen liittyvää varautumissääntelyä sääntelee jätelaki (646/2011), valtioneuvoston asetus jätteistä (978/2021, jäljempänä *jäteasetus*), ympäristönsuojelulaki (527/2014) ja valtioneuvoston asetus ympäristönsuojelusta (713/2014).

Jätelain 6 §:n 16 kohdassa jätehuollon on määritelty tarkoittavan jätteen keräystä, kuljetusta, hyödyntämistä ja loppukäsittelyä, mukaan lukien tällaisen toiminnan tarkkailu ja seuranta sekä loppukäsittelypaikkojen jälkihoito ja toiminta välittäjänä. Lain 120 § asettaa toiminnanharjoittajalle velvoitteen tarkkailla ja seurata jätehuoltoa varmistaakseen, että toiminta täyttää lakien ja asetusten nojalla sille annetut velvoitteet. Lain 120 §:n 2 momentin mukaan ympäristöluvanvaraisen jätteen käsittelytoiminnan harjoittajan on laadittava seuranta- ja tarkkailusuunnitelma, joka tulee esittää lupaviranomaiselle. Jäteasetuksen 41 §:ssä on tarkennettu niitä tietoja, joita suunnitelmaan tulee sisällyttää.

Ympäristönsuojelulain 15 § velvoittaa ilmoituksen- tai luvanvaraisen toiminnan harjoittajan varautumaan ennalta toimiin onnettomuuksien tai muiden poikkeuksellisten tilanteiden estämiseksi ja haitallisten seurausten rajoittamiseksi. Lisäksi lain 6 luvussa lupaharkintaa ja lupamääräyksiä koskien määritellään esimerkiksi luvan myöntämisen edellytykset (49 §), lupamääräykset pilaantumisen ehkäisemiseksi (52 §) ja seuranta- sekä tarkkailumääräykset (62 §). Ympäristönsuojeluasetuksen 3 §, 6 § ja 16 § täsmentävät lupahakemusten ja ilmoitusten sisältöä.

Kansallinen sääntely ei kuitenkaan jätehuoltovelvoitteiden osalta erityisesti kohdistu tieto- tai kyberturvallisuuskysymyksiin, eikä NIS2-direktiivin vaatimusten mukaista sääntelyä ole kansallisesti tunnistettu.

3.12 Kemikaalien valmistus, tuotanto ja jakelu

Kemikaalien valmistus, tuotanto ja jakelu ei kuulunut NIS1-direktiivin soveltamisalaan. Kansallisesti kemikaalien turvallisuutta koskeva keskeinen sääntely sisältyy kemikaaliturvallisuuslakiin ja sen nojalla annettuihin asetuksiin. Kemikaalisektoria säännellään lisäksi kansallisesti kemikaalilaissa, jonka tarkoituksena on ihmisten ja ympäristön suojelu kemikaalien aiheuttamilta vaaroilta ja haitoilta. EU-sääntelyä kemikaalien turvallisuutta koskien sisältyy kemikaalien rekisteröinnistä, arvioinnista, lupamenettelyistä ja rajoituksista (REACH), Euroopan kemikaaliviraston perustamisesta, direktiivin 1999/45/EY muuttamisesta sekä neuvoston asetuksen (ETY) N:o 793/93, komission asetuksen (EY) N:o 1488/94, neuvoston direktiivin 76/769/ETY ja komission direktiivien 91/155/ETY, 93/67/ETY, 93/105/EY ja 2000/21/EY kumoamisesta annettuun Euroopan parlamentin ja neuvoston asetukseen (EY) N:o 1907/2006 (jäljempänä *REACH-asetus*) sekä aineiden ja seosten luokituksesta, merkinnöistä ja pakkaamisesta sekä direktiivien 67/548/ETY ja 1999/45/EY muuttamisesta ja kumoamisesta ja asetuksen (EY) N:o

1907/2006 muuttamisesta annettuun Euroopan parlamentin ja neuvoston asetukseen (EY) N:o 1272/2008 (jäljempänä *CLP-asetus*). REACH-asetuksen tehtävänä on varmistaa korkeatasoinen ihmisten terveyden ja ympäristön suojelu, mukaan lukien vaihtoehtoisten keinojen edistäminen aineiden vaarojen arvioimiseksi, sekä aineiden vapaa liikkuvuus sisämarkkinoilla samalla kilpailukykyä ja innovointia edistäen ja CLP-asetuksen tavoitteena on yhdenmukaistaa käytäntöjä aineiden ja seosten luokituksesta, merkinnöistä ja pakkaamisesta.

3.12.1 Kemikaalit ja räjähteet

Kemikaaliturvallisuuslain tarkoituksena on ehkäistä ja torjua kemikaalien käsittelystä aiheutuvia vahinkoja ja edistää yleistä turvallisuutta (1 §). Kemikaaliturvallisuuslain soveltamisala on laaja, ja koskee niin yksityisiä henkilöitä, kuin suuria toiminnanharjoittajiakin. Soveltamisala ei myöskään perustu NIS2-direktiivin mukaiseen toimialajaotteluun. Lain 4 § säätää soveltamisalan rajauksista.

Lain nojalla annetuissa valtioneuvoston asetuksissa on täsmennetty kemikaaliturvallisuuslain turvallisuusvaatimuksia. Vaarallisten kemikaalien osalta keskeisiä asetuksia ovat valtioneuvoston asetus vaarallisten kemikaalien käsittelyn ja varastoinnin valvonnasta (685/2015), valtioneuvoston asetus vaarallisten kemikaalien teollisen käsittelyn ja varastoinnin turvallisuusvaatimuksista (856/2012), valtioneuvoston asetus nestekaasulaitosten turvallisuusvaatimuksista (858/2012) ja valtioneuvoston asetus maakaasun käsittelyn turvallisuudesta (551/2009). Räjähteiden valmistuksen ja varastoinnin osalta keskeisiä asetuksia ovat valtioneuvoston asetus räjähteiden valmistuksen ja varastoinnin valvonnasta (819/2015) sekä valtioneuvoston asetus räjähteiden valmistuksen, käsittelyn ja varastoinnin turvallisuusvaatimuksista (1101/2015).

Kemikaaliturvallisuuslailla ja sen nojalla annetuilla asetuksilla on kansallisesti toimeenpantu EU-velvoitteita kuten vaarallisista aineista aiheutuvien suuronnettomuusvaarojen torjunnasta sekä neuvoston direktiivin 96/82/EY muuttamisesta ja myöhemmästä kumoamisesta annettu Euroopan parlamentin ja neuvoston direktiivi 2012/18/EU (jäljempänä *Seveso III –direktiivi*). Kemikaaliturvallisuuslain osalta suuronnettomuusvaarallisten tuotantolaitosten valvonnasta vastaa Turvallisuus- ja kemikaalivirasto (Tukes).

Kemikaaliturvallisuuslain 3 luku sisältää säännökset vaarallisista kemikaaleista aiheutuvien suuronnettomuuksien ehkäisemiseksi (erityisesti 30 §) ja perustuu Seveso III-direktiivin velvoitteisiin. Lain 30 §:ssä säädetään toiminnanharjoittajan velvollisuudesta laatia turvallisuusselvitys tai muu asiakirja, jossa selostetaan onnettomuuden ehkäisy- ja rajoitustoimet. Laissa säädetään lisäksi tuvallisuusselvityksen esillä pitämisestä (32 §) ja toiminnanharjoittajan tiedottamisvelvollisuudesta (31 §). Laki määrää Tukesin laatimaan tarkastussuunnitelman ja –ohjelman (27 §) sekä muuten valvomaan toiminnanharjoittajia (26 a §). Vaarallisen kemikaalin laajamittaista teollista käsittelyä ja varastointia varten tarvitaan kemikaaliturvallisuuslain 23 §:n mukainen lupa sekä räjähteiden valmistusta ja varastointia varten tarvitaan kemikaaliturvallisuuslain 58 §:n mukainen lupa.

Kemikaaliturvallisuuslain osalta on tunnistettu tarve lain kokonaisuudistukselle, erityisesti muutospaineita aiheuttavat sääntely-ympäristön muuttuminen ja perustuslailliset syyt. Turvauhkiin varautuminen on kuitenkin arvioitu perustelluksi toteuttaa erillisenä kokonaisuutena. Työ- ja elinkeinoministeriössä valmistellaan hallituksen esitystä eduskunnalle laeiksi vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annetun lain ja turvallisuusselvityslain (726/2014) 21 §:n muuttamisesta turvauhkiin varautumiseksi (Hankeikkuna: TEM063:00/2018). Esityksessä ehdotetaan lain soveltamisalan laajentamista kattamaan toimintojen suojaaminen turvauhilta. Esityksen tarkoitus olisi säätää turvauhkiin varautumisesta ja turvallisuusjärjestelyjen yleisistä perusteista kaikkia toiminnanharjoittajia velvoittavasti.

Kemikaaliturvallisuuslakiin lisättäisiin edellä mainitun hankkeen yheydessä uusi 12 a §, jonka tarkoituksena olisi velvoittaa toiminnanharjoittajat suunnittelemaan, rakentamaan ja ylläpitämään tietojärjestelmiä siten, että prosessien ohjaus, valvonta ja turvallisuuskriittiset laitteet eivät menettäisi hallittavuuttaan ja aiheuttaisi vaaraa turvallisuudelle. 12 a §:n 2 momentin mukaan toiminnanharjoittajan tulisi lisäksi kyetä havaitsemaan tietoturvauhat ja –loukkaukset sekä rajoittamaan näiden vaikutuksia. Turvauhkiin varautumisen lupa- ja valvontaviranomaistehtävät ehdotetaan säädettäväksi nykyisille lain lupa- ja valvontaviranomaisille, joita ovat Turvallisuus- ja kemikaalivirasto sekä pelastusviranomainen. Luonnoksen mukaiset toimenpidevelvoitteet vastaavat monilta osilta NIS2-direktiivin velvoitteita.

Kemikaaliturvallisuuslain 3 §:n 1 momentin mukaan lakia sovelletaan puolustusvoimien toimintaan, ellei kemikaaliturvallisuuslaissa muuta säädetä. Puolustusministeriö on antanut asetuksia koskien kemikaalien teollisen käsittelyn ja varastoinnin turvallisuusvaatimuksia (712/2017) ja valvontaa (713/2017) puolustushallinnossa. Lisäksi sotilasräjähteistä säädetään puolustusministeriön asetuksella (772/2009). Sotilasräjähteitä koskeva sääntely on tarkoitus uudistaa (Hankeikkuna: PLM010:00/2020). Tämä turvallisuussääntely keskittyy ensisijaisesti fyysisen turvallisuuden takaamiseen, eikä kyberturvallisuutta ole sääntelyssä erityisesti huomioitu.

Voimassaolevan sääntelyn lisäksi Turvallisuus- ja kemikaaliviraston opas turvauhkiin varautumisesta vaarallisten kemikaalien käsittelyssä ja varastoinnissa sisältää ohjeita tietoturva- ja kyberhyökkäyksiin varautumisesta ja kyberuhkien arvioinnista sekä tarkistuslistan kyberuhkiin varautumisesta. Kemianteollisuuden eurooppalainen kattojärjestö Cefic ylläpitää Responsible Care –ohjelmaa, joka kattaa myös kyberuhkiin varautumisen. Suomessa Ceficin ohjelmaan on sitoutunut noin sata yritystä, jotka edustavat noin 80%:a kemianteollisuuden tuotannosta.

3.12.2 Painelaitesääntely

Kemikaalien valmistukseen, tuotantoon ja jakeluun osallistuviin toimijoihin saattaa soveltua myös painelaitteita koskeva sääntely. Painelaitelailla (1144/2016) on pantu täytäntöön painelaitteiden asettamista saataville markkinoilla koskevan jäsenvaltioiden lainsäädännön yhdenmukaistamisesta annettu Euroopan parlamentin ja neuvoston direktiivi 2014/68/EU (uudelleenlaadittu) sekä yksinkertaisten painesäiliöiden asettamista saataville markkinoilla koskevan jäsenvaltioiden lainsäädännön yhdenmukaistamisesta annettu Euroopan parlamentin ja neuvoston direktiivi 2014/29/EU. Laissa on lisäksi kansallista sääntelyä käytön aikaista turvallisuutta koskien. Siinä säädetään esimerkiksi painelaitteiden turvallisuusvaatimuksista, onnettomuuksien ehkäisemisestä sekä onnettomuuksien ja vaaratilanteiden ilmoittamisesta viranomaiselle. Lain velvoitteiden noudattamista valvova viranomainen on Turvallisuus- ja kemikaalivirasto Tukes. Painelaitelain soveltamisala ei ole yhdenmukainen NIS2-direktiivin toimialajaottelun kanssa, vaan soveltamisalaan kuuluu toimijoita eri toimialoilta. Painelaitesääntelyn soveltamisalaan kuuluvat myös painelaitteiden ohjaus- ja varolaitteet, joita voidaan painelaitelaissa ja sen nojalla annetussa valtioneuvoston asetuksessa painelaitteista (1548/2016) mainituin edellytyksin käyttää myös painelaitteiden etäohjauksessa varmennetun yhteyden kautta. Painelaitesääntelyn turvallisuussääntely perustuu onnettomuuksien ennaltaehkäisemiseen, eikä siinä ole säännöksiä kyberhyökkäyksiin liittyen. Kemikaaliturvallisuuslain turvauhkia koskevan muutoshankkeen yhteydessä ei ole tarkoitus muuttaa painelaitesääntelyä.

Sekä kemikaaliturvallisuuslain että painelaitelain lähtökohtana on onnettomuuksiin varautuminen. Kemikaaliturvallisuuslakiin ehdotettavat turvauhkiin varautumista koskevat säännökset soveltuvat myös painelaitteisiin, mikäli nämä sijaitsevat kemikaaliturvallisuuslain soveltamisalan mukaisessa kohteessa. Toimintaympäristömuutosten vuoksi myös painelaitesääntelyn turvauhkasääntelyn tarvetta tulee lähiaikoina arvioida uudelleen.

3.13 Elintarvikkeiden tuotanto, jalostus ja jakelu

Elintarvikkeiden tuotanto, jalostus ja jakelu eivät ole kuuluneet NIS1-direktiivin soveltamisalaan. Kansallisesti elintarvikesektoria on säännelty elintarvikelailla (297/2021), jolla on pantu täytäntöön elintarvikelainsäädäntöä koskevista yleisistä periaatteista ja vaatimuksista, Euroopan elintarviketurvallisuusviranomaisen perustamisesta sekä elintarvikkeiden turvallisuuteen liittyvistä menettelyistä annettu Euroopan parlamentin ja neuvoston asetus (EY) N:o 178/2002 (jäljempänä *yleinen elintarvikeasetus*). Kansallista sektorikohtaista sääntelyä sisältyy lisäksi rehulakiin (1263/2020), eläintautilakiin (76/2021), valmiuslakiin (1522/2011) ja kasvinterveyslakiin (1110/2019)

Elintarvikelainsäädäntö kattaa elintarvikkeiden lisäksi myös elintarvikkeiden kanssa kosketuksiin joutuvat materiaalit. Näitä materiaaleja koskevista vaatimuksista ja velvoitteista säädetään kansallisesti elintarvikelaissa. Rehulaissa säädetään lisäksi rehujen turvallisuuteen liittyvistä yleisistä periaatteista sekä rehualan toimijoiden ja valvontaviranomaisten velvollisuuksista. Ensisijainen vastuu elintarvikkeiden ja rehujen turvallisuudesta on yleisen elintarvikeasetuksen mukaan elintarvike- ja rehualan toimijalla. Viranomaisten velvollisuus on omilla toimillaan varmistaa, että elintarvike- ja rehualan toimijat täyttävät heitä koskevat velvoitteet. Elintarvikelainsäädännössä ei kuitenkaan ole toimijoiden tieto- tai kyberturvallisuuteen liittyvää sääntelyä, vaan riskienhallintaa ja varautumista koskevat velvoitteet kohdistuvat muihin riskeihin, kuten ruokamyrkytysten, zoonoosien ja eläintautien ehkäisemiseen.

Elintarvikelain tarkoituksena on suojella kuluttajan terveyttä ja taloudellisia etuja varmistamalla elintarvikkeiden ja elintarvikekontaktimateriaalien turvallisuus, elintarvikkeiden hyvä terveydellinen ja muu elintarvikesäännösten mukainen laatu ja elintarvikkeista ja elintarvikekontaktimateriaaleista annettavien tietojen riittävyys ja oikeellisuus. Lain soveltamisala kattaa elintarvikkeet, elintarviketuotantoon käytettävät eläimet, elintarvikekontaktimateriaalit, elintarvike- ja kontaktimateriaalitoiminnan, elintarvikealan ja kontaktimateriaalialan toimijat sekä elintarvikevalvonnan kaikissa elintarvikkeiden ja elintarvikekontaktimateriaalien tuotanto-, jalostus- ja jakeluvaiheissa (2 §).

Elintarvikelain 14 §:n mukaan toimijan on ilmoitettava vastaanottajalle elintarvikkeista, elintarviketuotantoon käytettävistä eläimistä ja elintarvikekontaktimateriaaleista edellytetyt jäljitettävyystiedot. Elintarviketuotantoon käytetyt eläimet ja muut mahdolliset aineet, jotka on tarkoitettu tai joiden voidaan olettaa tulevan lisätyiksi elintarvikkeeseen, tulee voida jäljittää. Tätä varten toimijalla on oltava järjestelmä, josta toimivaltaiset valvontaviranomaiset saavat tiedot käyttöönsä. Lain 15 § omavalvontaa koskien velvoittaa toimijan ylläpitämään järjestelmää, jonka avulla toimija tunnistaa ja hallitsee toimintaansa liittyvät vaarat ja varmistaa, että toiminta täyttää elintarvikesäännöksissä asetetut vaatimukset. 15 §:n 2 momentissa säädetään lisäksi toimijan velvoitteesta laatia näytteenotto- ja tutkimussuunnitelma salmonellan varalta, mikäli salmonellaa koskevien erityistakuiden piiriin kuuluvia elintarvikkeita tuodaan jäsenmaasta toiseen. Omavalvonnan tulokset tulee kirjata riittävällä tarkkuudella ja toimijan on osoitettava noudattavansa vaatimuksia viranomaisen edellyttämällä tavalla.

Elintarvikelain 17 §:n mukaan toimijan on välittömästi ilmoitettava toimivaltaiselle valvontaviranomaiselle omavalvonnassa tai muulla tavalla esille tulleista vakavista vaaroista ihmisen terveydelle sekä toimenpiteistä, joihin epäkohtien korjaamiseksi on ryhdytty. Lisäksi 17 §:n 2 momentissa on säädetty toimijalle velvollisuus ilmoittaa valvontaviranomaiselle elintarvikkeen aiheuttamasta ruokamyrkytyksestä tai sen vaarasta. Valvontaviranomainen voi määrätä tuotteen poistettavaksi markkinoilta, mikäli toimiin ei ryhdytä oma-aloitteisesti ja tuotteen tiedot ovat

olennaisesti säännösten vastaisia (57 §). Pykälään sisältyy myös valvontaviranomaisen yleinen oikeus tiedottaa asiasta.

Elintarvikesektorin viranomaisvelvollisuuksista säädetään muun muassa elintarvikelain 24 §:ssä, 47 §:ssä, 48 §:ssä ja 82 §:ssä. Ruokaviraston tehtäviä koskeva 24 § velvoittaa Ruokaviraston suunnittelemaan, ohjaamaan, kehittämään ja suorittamaan valtakunnallisesti elintarvikevalvontaa. Lisäksi Ruokavirasto toimii Euroopan unionin lainsäädännössä ja kansainvälisissä sopimuksissa edellytettynä kansallisena viranomaisena tai yhteyspisteenä elintarvikevalvonnan osalta (esimerkiksi yleisen elintarvikeasetuksen 50 artiklassa tarkoitettu nopean hälytysjärjestelmän (RASFF) kansallinen yhteyspiste, EFSA Focal Point –yhteyspiste sekä elintarvikepetoksiin liittyvän tiedonvälitysverkoston yhteyspiste). Ruokavirasto myös laatii elintarvikkeita koskevan valtakunnallisen valmiussuunnitelman, jossa yksilöidään toimenpiteet, jotka toteutetaan, jos elintarvikkeiden on todettu aiheuttavan vakavan riskin ihmisten terveydelle.

Elintarvikelain 48 § velvoittaa Ruokaviraston laatimaan zoonoosien seurantaan ja valvontaan tarvittavat näytteenottosuunnitelmat ja tekemään tarvittavat ilmoitukset zoonoositutkimusten tuloksista elintarvikealan toimijoille sekä viranomaisille. Myös kunnalle asetetaan velvollisuus ryhtyä toimenpiteisiin, mikäli zoonoosia esiintyy toistuvasti eläinten pitopaikassa tai pitopaikan epäillään olevan lähde ihmisessä todetulle zoonoosille. Kunnan velvollisuudesta laatia selvitys ruokamyrkytystä koskien säädetään 47 §:ssä. Lain 82 § säätää valvonnassa saatujen tietojen salassapitovelvollisuudesta.

Elintarviketurvallisuutta koskee myös eläintautilaki (76/2021), jonka tavoitteena on eläintautien vastustaminen. Eläintautilain 18 §:n mukaan elintarvikelaissa tarkoitetun teurastamon, eläinsuojelulaissa (247/1996) tarkoitetun eläintarhan sekä eläinterveyssäännöstön tai tämän lain mukaista hyväksymistä edellyttävän sukusolujen pitopaikan on laadittava valmiussuunnitelma aluokan tautien varalle, jos niissä käsitellään luetteloituihin lajeihin kuuluvia eläimiä. Maa- ja metsätalousministeriön asetuksella määritellään valmiussuunnitelman edellyttävät eläintaudit ja tarkennetaan valmiussuunnitelman sisältöä. Eläintautilaki velvoittaa toimijat (19 §) ja eläinlääkärit sekä laboratoriot (20 §) ilmoittamaan eläintaudeista kunnaneläinlääkärille tai aluehallintovirastolle. 22 §:n nojalla kunnanlääkärillä on velvollisuus ilmoittaa aluehallintovirastolle 19 ja 20 § mukaisesti hänelle ilmoitetusta eläintaudista.

Valmiussuunnittelua koskevaa sääntelyä sisältyy myös tarttuvista eläintaudeista sekä tiettyjen eläinterveyttä koskevien säädösten muuttamisesta ja kumoamisesta annettuun Euroopan parlamentin ja neuvoston asetukseen (EU) 2016/429 ja virallisesta valvonnasta ja muista virallisista toimista, jotka suoritetaan elintarvike- ja rehulainsäädännön ja eläinten terveyttä ja hyvinvointia, kasvien terveyttä ja kasvinsuojeluaineita koskevien sääntöjen soveltamisen varmistamiseksi, sekä Euroopan parlamentin ja neuvoston asetusten (EY) N:o 999/2001, (EY) N:o 396/2005, (EY) N:o 1069/2009, (EY) N:o 1107/2009, (EU) N:o 1151/2012, (EU) N:o 652/2014, (EU) 2016/429 ja (EU) 2016/2031, neuvoston asetusten (EY) N:o 1/2005 ja (EY) N:o 1099/2009 ja neuvoston direktiivien 98/58/EY, 1999/74/EY, 2007/43/EY, 2008/119/EY ja 2008/120/EY muuttamisesta ja Euroopan parlamentin ja neuvoston asetusten (EY) N:o 854/2004 ja (EY) N:o 882/2004, neuvoston direktiivien 89/608/ETY, 89/662/ETY, 90/425/ETY, 91/496/ETY, 96/23/EY, 96/93/EY ja 97/78/EY ja neuvoston päätöksen 92/438/ETY kumoamisesta annettuun Euroopan parlamentin ja neuvoston asetukseen (EU) 2017/625.

Elintarvikesektorin varautumis- ja riskinhallintavelvoitteista on säädetty lisäksi kasvinterveyslaissa ja osin tuotantopanoksia, kuten rehuja, lannoitteita ja kasvinsuojeluaineita koskevissa säädöksissä. Lisäksi CER-direktiivin kansallisen täytäntöönpanon arvioidaan edellyttävän muutoksia ja tarkennuksia elintarvikesektorin säädöksiin.

Elintarvikevalvontaan liittyviä ohjeistuksia ja suunnitelmia ovat esimerkiksi ohje elintarvikehuoneiston ja kontaktimateriaalitoiminnan riskiluokituksesta ja elintarvikelainsäädännön mukaisen valvontatarpeen määrittämisestä, Elintarvikeketjun monivuotinen kansallinen valvontasuunnitelma 2021-2024 sekä monivuotinen kansallinen valvontasuunnitelma (VASU).

Elintarvikelaissa taikka muissakaan elintarvikesektoria koskevissa laeissa ei ole tunnistettu päällekkäisyyksiä tai ristiriitaisuuksia NIS-sääntelyn kanssa, eikä sektorikohtaisen lainsäädännön muutostarpeita ole tunnistettu.

3.14 Valmistussektori

Valmistussektori ei ole kuulunut NIS1-direktiivin soveltamisalaan. Valmistussektorin keskeisiä turvallisuusvelvollisuuksia sisältyy vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annettuun lakiin (390/2005), sähköturvallisuuslakiin (1135/2016) ja lakiin lääkinnällisistä laitteista. Säteilyturvallisuudesta säädetään säteilylaissa (859/2018). Valmistussektori on NIS2-direktiivin II-liitteessä jaettu lääkinnällisten laitteiden, tietokoneiden sekä elektronisten ja optisten tuotteiden, sähkölaitteiden, muiden koneiden ja laitteiden, moottoriajoneuvojen, perävaunujen ja puoliperävaunujen sekä muiden kulkuneuvojen valmistuksen osa-alueisiin. Valmistustoimialaa koskeva normaaliolojen sääntely on turvallisuussääntelyä, joka kohdistuu joko tuotteiden laatuun ja turvallisuuteen tai valmistuksessa käytettävien koneiden, laitteistojen tai kemikaalien käsittelyyn.

3.14.1 Lääkinnällisten laitteiden valmistus

Lääkinnällisten laitteiden osa-alue kattaa lääkinnällisistä laitteista, direktiivin 2001/83/EY, asetuksen (EY) N:o 178/2002 ja asetuksen (EY) N:o 1223/2009 muuttamisesta sekä neuvoston direktiivien 90/385/ETY ja 93/42/ETY kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2017/745 (jäljempänä *MD-asetus*) 2 artiklan 1 alakohdassa määriteltyjä lääkinnällisiä laitteita valmistavat toimijat sekä in vitro -diagnostiikkaan tarkoitetuista lääkinnällisistä laitteista sekä direktiivin 98/79/EY ja komission päätöksen 2010/227/EU kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2017/746 (jäljempänä *IVD-asetus*) 2 artiklan 2 alakohdassa määriteltyjä in vitro -diagnostiikkaan tarkoitettuja lääkinnällisiä laitteita valmistavat toimijat.

MD- ja IVD-asetuksissa vahvistetaan olennaiset vaatimukset muiden muassa lääkinnällisille laitteille, jotka toimivat sähköisen järjestelmän kautta tai jotka ovat itsessään ohjelmistoja. Asetukset kattavat myös tietyt sulauttamattomat ohjelmistot ja niissä noudatetaan koko elinkaareen perustuvaa lähestymistapaa. Olennaisissa vaatimuksissa edellytetään, että valmistajat kehittävät ja toteuttavat tuotteensa soveltaen riskinhallintaperiaatteita ja täyttäen tietoturvatoimenpiteitä koskevat vaatimukset sekä käyden läpi vastaavat vaatimustenmukaisuuden arviointimenettelyt. Lääkinnällisten laitteiden koordinointiryhmä (Medical Devices Coordination Group, MDCG) antoi joulukuussa 2019 erillisen ohjeistuksen siitä, miten MD- ja IVD-asetusten liitteissä I vahvistetut kyberturvallisuutta koskevat olennaiset vaatimukset voidaan täyttää (Guidance on Cybersecurity for Medical Devices, MDCG 2019-16).

MD- ja IVD-asetuksia täydentävät laki lääkinnällisistä laitteista (719/2021) ja eräistä EU-direktiiveissä säädetyistä lääkinnällisistä laitteista annettu laki (629/2010). Laeissa tarkoitettuna valvovana viranomaisena toimii lääkealan turvallisuus- ja kehittämiskeskus Fimea. Näissä kansallisissa laeissa ei ole erikseen säädetty kyberturvallisuusvaatimuksista lääkinnällisissä laitteissa tai niiden valmistuksessa.

3.14.2 Tietokoneiden sekä elektronisten ja optisten tuotteiden valmistus

NIS2-direktiivissä tarkoitettu tietokoneiden sekä elektronisten ja optisten tuotteiden valmistuksen osa-alue kattaa NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 26 tarkoitettua taloudellista toimintaa harjoittavat yritykset. Tuotteiden valmistukseen liittyen ei ole tunnistettu sektorikohtaista sääntelyä.

NACE Rev. 2 C 26 luokka:

26			Tietokoneiden sekä elektronisten ja optisten tuotteiden valmistus
	26.1		Elektronisten komponenttien ja piirilevyjen valmistus
		26.11	Elektronisten komponenttien valmistus
		26.12	Kalustettujen piirilevyjen valmistus
	26.2		Tietokoneiden ja niiden oheislaitteiden valmistus
		26.20	Tietokoneiden ja niiden oheislaitteiden valmistus
	26.3		Viestintälaitteiden valmistus
		26.30	Viestintälaitteiden valmistus
	26.4		Viihde-elektroniikan valmistus
		26.40	Viihde-elektroniikan valmistus
	26.5		Mittaus-, testaus- ja navigointivälineiden ja -laitteiden valmistus; kellot
		26.51	Mittaus-, testaus- ja navigointivälineiden ja -laitteiden valmistus
		26.52	Kellojen valmistus
	26.6		Säteilylaitteiden sekä elektronisten lääkintä- ja terapialaitteiden valmistus
		26.60	Säteilylaitteiden sekä elektronisten lääkintä- ja terapialaitteiden valmistus
	26.7		Optisten instrumenttien ja valokuvausvälineiden valmistus
		26.70	Optisten instrumenttien ja valokuvausvälineiden valmistus
	26.8		Tallennevälineiden valmistus
		26.80	Tallennevälineiden valmistus

3.14.3 Sähkölaitteiden valmistus

Sähkölaitteiden valmistuksen osa-alue kattaa ne toimijat, jotka harjoittavat NACE Rev. 2 –luokituksen C jakson kaksinumerotasossa 27 tarkoitettua taloudellista toimintaa. Sähköturvalli-

suussääntelyssä ei ole toimijoiden tieto- tai kyberturvallisuuteen liittyviä säännöksiä, vaan keskeinen turvallisuussääntely perustuu onnettomuuksien ennaltaehkäisemiseen ja tuotteiden turvallisuuteen.

Sähköturvallisuuslaissa säädetään sähkölaitteiden ja –laitteistojen turvallisuudesta. Laki koostuu tiettyjen EU-tuotedirektiivien täytäntöönpanosta ja kansallisesta sääntelystä. Lakia sovelletaan sen 3 §:ssä mainituin rajoituksin sähkölaitteisiin ja -laitteistoihin, joita käytetään sähkön tuottamisessa, siirrossa, jakelussa tai käytössä ja joiden sähköisistä tai sähkömagneettisista ominaisuuksista voi aiheutua vahingon vaara tai häiriötä. Lakia sovelletaan myös radiolaitteisiin ja viestintäverkkoihin siltä osin kuin niistä voi aiheutua vaaraa hengelle, terveydelle tai omaisuudelle taikka haitallisia häiriöitä, joista ei säädetä sähköisen viestinnän palveluista annetussa laissa tai sen nojalla annetuissa säännöksissä. Tukes on lain keskeinen valvova viranomainen. Mikäli sähkölaite tai sähkölaitteisto aiheuttaa vahinkoa, viranomainen voi rajoittaa laitteen tai laitteiston käyttöä ja tarvittaessa poistaa laitteen tai laitteiston verkosta.

NACE Rev. 2 C 27 luokka:

27			Sähkölaitteiden valmistus
	27.1		Sähkömoottorien, generaattorien, muuntajien sekä sähkönjakelu- ja valvontalaitteiden valmistus
		27.11	Sähkömoottorien, generaattorien ja muuntajien valmistus
		27.12	Sähkönjakelu- ja valvontalaitteiden valmistus
	27.2		Paristojen ja akkujen valmistus
		27.20	Paristojen ja akkujen valmistus
	27.3		Sähköjohtojen ja kytkentälaitteiden valmistus
		27.31	Optisten kuitukaapelien valmistus
		27.32	Muiden elektronisten ja sähköjohtojen sekä -kaapelien valmistus
		27.33	Kytkentälaitteiden valmistus
	27.4		Sähkölamppujen ja valaisimien valmistus
		27.40	Sähkölamppujen ja valaisimien valmistus
	27.5		Kodinkoneiden valmistus
		27.51	Sähköisten kodinkoneiden valmistus
		27.52	Sähköistämättömien kodinkoneiden valmistus
	27.9		Muiden sähkölaitteiden valmistus
		27.90	Muiden sähkölaitteiden valmistus

3.14.4 Muiden koneiden ja laitteiden valmistus

NIS2-direktiivissä tarkoitettu muiden koneiden ja laitteiden valmistuksen osa-alue kattaa NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 28 tarkoitettua taloudellista toimintaa harjoittavat yritykset. Tuotteiden valmistukseen liittyen ei ole tunnistettu sektorikohtaistasäänтelyä.

NACE Rev. 2 C 28 luokka:

28			Muiden koneiden ja laitteiden valmistus
	28.1		Yleiskäyttöön tarkoitettujen voimakoneiden valmistus
		28.11	Moottorien ja turbiinien valmistus (pl. lentokoneiden ja ajoneuvojen moottorit)
		28.12	Hydraulisten voimalaitteiden valmistus
		28.13	Pumppujen ja kompressoreiden valmistus
		28.14	Muiden hanojen ja venttiilien valmistus
		28.15	Laakereiden, hammaspyörien, vaihteisto- ja ohjauselementtien valmistus
	28.2		Muiden yleiskäyttöön tarkoitettujen koneiden valmistus
		28.21	Teollisuusuunien, lämmitysjärjestelmien ja tulipesäpolttimien valmistus
		28.22	Nosto- ja siirtolaitteiden valmistus
		28.23	Konttorikoneiden ja -laitteiden valmistus (pl. tietokoneet ja niiden oheislaitteet)
		28.24	Voimakäyttöisten käsityökalujen valmistus
		28.25	Muuhun kuin kotitalouskäyttöön tarkoitettujen jäähdytys- ja tuuletuslaitteiden valmistus
		28.29	Muualla luokittelematon yleiskäyttöön tarkoitettujen koneiden valmistus
	28.3		Maa- ja metsätalouskoneiden valmistus
		28.30	Maa- ja metsätalouskoneiden valmistus
	28.4		Metallin työstökoneiden ja konetyökalujen valmistus
		28.41	Metallin työstökoneiden valmistus
		28.49	Muiden konetyökalujen valmistus
	28.9		Muiden erikoiskoneiden valmistus

		28.91	Metallinjalostuskoneiden valmistus
		28.92	Kaivos-, louhinta- ja rakennuskoneiden valmistus
		28.93	Elintarvike-, juoma- ja tupakkateollisuuden koneiden valmistus
		28.94	Tekstiili-, vaate- ja nahkateollisuuden koneiden valmistus
		28.95	Paperi-, kartonki- ja pahviteollisuuden koneiden valmistus
		28.96	Muovi- ja kumiteollisuuden koneiden valmistus
		28.99	Muualla luokittelematon erikoiskoneiden valmistus

3.14.5 Moottoriajoneuvojen ja perävaunujen valmistus

NIS2-direktiivissä tarkoitettu moottoriajoneuvojen ja perävaunujen valmistuksen osa-alue kattaa NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 29 tarkoitettua taloudellista toimintaa harjoittavat yritykset. Ajoneuvovalmistajille ja ajoneuvoille on asetettu yhdenmukaiset vaatimukset ajoneuvojen kyberturvallisuuden ja hallintajärjestelmän hyväksynnän osalta. Nämä vaatimukset perustuvat Euroopan parlamentin ja neuvoston moottoriajoneuvojen ja niiden perävaunujen sekä tällaisiin ajoneuvoihin tarkoitettujen järjestelmien, komponenttien ja erillisten teknisten yksiköiden hyväksynnästä ja markkinavalvonnasta, asetusten (EY) N:o 715/2007 ja (EY) N:o 595/2009 muuttamisesta sekä direktiivin 2007/46/EY kumoamisesta annettuun asetukseen (2018/858) sekä E-sääntöön nro 155.

NACE Rev. 2 C 29 luokka:

29			Moottoriajoneuvojen, perävaunujen ja puoliperävaunujen valmistus
	29.1		Moottoriajoneuvojen valmistus
		29.10	Moottoriajoneuvojen valmistus
	29.2		Moottoriajoneuvojen korien valmistus; perävaunujen ja puoliperävaunujen valmistus
		29.20	Moottoriajoneuvojen korien valmistus; perävaunujen ja puoliperävaunujen valmistus
	29.3		Osien ja tarvikkeiden valmistus moottoriajoneuvoihin
		29.31	Sähkö- ja elektroniikkalaitteiden valmistus moottoriajoneuvoihin
		29.32	Muiden osien ja tarvikkeiden valmistus moottoriajoneuvoihin

3.14.6 Muiden kulkuneuvojen valmistus

NIS2-direktiivissä tarkoitettu muiden kulkuneuvojen valmistuksen osa-alue kattaa NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 30 tarkoitettua taloudellista toimintaa harjoittavat yritykset. Luokkaan 30 kuuluvat laivojen ja veneiden, kelluvien rakenteiden, huvi- ja urheiluveneiden, raideliikenteen kulkuneuvojen, ilma- ja avaruusalusten ja niihin liittyvien koneiden, taisteluajoneuvojen, moottoripyörien, polkupyörien ja invalidiajoneuvojen sekä muiden luokittelemattomien kulkuneuvojen valmistus. Muiden kulkuneuvojen valmistuksen osa-alueesta ei ole tunnistettu sektorikohtaista kyberturvallisuuden riskienhallintaa koskevaa sääntelyä, lukuunottamatta jaksossa 3.3 kuvattua ilmailun kyberturvallisuussääntelyä.

NACE Rev. 2 C 30 luokka:

30			Muiden kulkuneuvojen valmistus
	30.1		Laivojen ja veneiden rakentaminen
		30.11	Laivojen ja kelluvien rakenteiden rakentaminen
		30.12	Huvi- ja urheiluveneiden rakentaminen
	30.2		Raideliikenteen kulkuneuvojen valmistus
		30.20	Raideliikenteen kulkuneuvojen valmistus
	30.3		Ilma- ja avaruusalusten ja niihin liittyvien koneiden valmistus
		30.30	Ilma- ja avaruusalusten ja niihin liittyvien koneiden valmistus
	30.4		Taisteluajoneuvojen valmistus
		30.40	Taisteluajoneuvojen valmistus
	30.9		Muualla luokittelematon kulkuneuvojen valmistus
		30.91	Moottoripyörien valmistus
		30.92	Polkupyörien ja invalidiajoneuvojen valmistus
		30.99	Muiden muualla luokittelemattomien kulkuneuvojen valmistus

3.15 Tutkimusorganisaatiot

Tutkimusorganisaatiot eivät kuuluneet NIS1-direktiivin soveltamisalaan NIS 2 -direktiivin 6 artiklan 41 kohdan mukaan tutkimusorganisaatiolla tarkoitetaan sellaista toimijaa, jonka ensisijaisena tavoitteena on harjoittaa soveltavaa tutkimusta tai kokeellista kehitystyötä kyseisen tutkimuksen tulosten hyödyntämiseksi kaupallisiin tarkoituksiin mutta joka ei ole opetus- ja koulutusalan laitos. Määritelmän mukaiseen soveltamisalaan on kansallisesti tunnistettu kuuluvan Teknologian Tutkimuskeskus VTT Oy (VTT).

Teknologian tutkimuskeskus VTT Oy:stä säädetään laissa Teknologian tutkimuskeskus Oy –nimisestä osakeyhtiöstä (761/2014, jäljempänä *VTT-laki*). Lain 2 §:n mukaan yhtiön tehtävänä on riippumattomana ja puolueettomana tutkimuslaitoksena edistää tutkimuksen ja teknologian laaja-alaista hyödyntämistä sekä kaupallistamista elinkeinoelämässä ja yhteiskunnassa. Lain 6 §:ssä säädetään varautumisvelvollisuudesta ja yhtiön velvollisuudesta varmistaa tehtäviensä mahdollisimman hyvä hoitaminen myös poikkeusoloissa valmiussuunnitelmien ja poikkeusoloissa tapahtuvan toiminnan etukäteisvalmistelujen sekä muiden toimenpiteiden avulla.

VTT-laissa ei säädetä yhtiöön kohdistuvista kyberturvallisuusvaatimuksista.

3.16 Julkishallinnon toimiala

Julkishallinnon toimiala ei ole kuulunut NIS1-direktiivin soveltamisalaan, vaan se on lisätty erittäin kriittiseksi toimialaksi vasta NIS2-direktiivissä. Julkishallinnon toimialalla verkko- ja tietoturvallisuuteen kohdistuva yleislain tasoinen sääntely sisältyy julkisen hallinnon tiedonhallinnasta annettuun lakiin (906/2019, *tiedonhallintalaki*). Julkisia toimijoita on kuulunut myös NIS1-direktiivin sääntelyn piiriin esimerkiksi terveydenhuollon sektorilla.

3.16.1 NIS2-direktiivin sääntelyn soveltaminen julkishallinnon toimialalla

Tiedonhallintalain 4 luvun tietoturvallisuussääntelyä sovelletaan laajasti julkishallinnossa. Sääntelyä sovelletaan julkisuuslain 4 §:n 1 momentissa tarkoitettuihin viranomaisiin ja myös yksityisiin henkilöihin tai yhteisöihin taikka muihin kuin viranomaisena toimiviin julkisoikeudellisiin yhteisöihin siltä osin kuin ne hoitavat julkista hallintotehtävää.

Kansallisesti ehdotetaan, että NIS2-direktiivistä johtuva yksinomaan direktiivin liitteen I kohdassa 10 tarkoitettua julkishallinnon toimialaa koskeva sääntely - eli julkishallinnon toimialan toimijaan kohdistuvat kyberturvallisuusvelvoitteet ja niiden noudattamisen valvonta - lisätään tiedonhallintalakiin. Tiedonhallintalaki olisi NIS2-direktiivin erityislaki suhteessa esitettyyn yleislakiin, eli lakiin kyberturvallisuuden riskienhallinnasta. NIS2-direktiivistä johtuvaa tiedonhallintalain sääntelyä esitetään sovellettavaksi rajatumpaan joukkoon kuin tiedonhallintalain 4 luvun tietoturvallisuussääntelyä sovelletaan. Lähtökohtana on direktiivin vähimmäistason täyttäminen. On huomioitavaa, että jos julkinen toimija toimii jollain direktiivin muista toimialoista, se voi kuulua NIS2-sääntelyn piiriin ehdotetun kyberturvallisuuden riskienhallinnasta annetun lain nojalla. Lailla kyberturvallisuuden riskienhallinnasta pantaisiin täytäntöön kaikkia muita direktiivin liitteissä kuvattuja toimialoja koskevat velvoitteet.

Direktiivissä edellytetään, että poikkeamailmoituksia tulee voida tehdä laajasti myös niiden tahojen, jotka eivät kuulu direktiivissä määriteltyihin toimijoihin. Näin ollen myös muut julkishallinnon toimijat kuin ne, joihin NIS2-sääntelyä ehdotetaan sovellettavaksi, voisivat tehdä poikkeamailmoituksia valvovalle viranomaiselle ja siten rikastaa kyberturvallisuuden tilannekuvaa. Nämä muut toimijat voisivat myös saada tukea valvovalta viranomaiselta ja CSIRT-yksiköltä poikkeaman käsittelyssä.

3.16.2 Käsitteet ja määritelmät

Tiedonhallinnalla tarkoitetaan tiedonhallintalain 2 §:n 9 kohdan mukaan viranomaisen tehtävien hoidossa tai sen muussa toiminnassa syntyviin tarpeisiin perustuvia toimia ja tietoturvallisuustoimenpiteitä viranomaisen tietoaineistojen, niiden käsittelyvaiheiden ja tietoaineistoihin sisältyvien tietojen hallinnoimiseksi riippumatta tietoaineistojen tallentamistavasta ja muista käsittelytavoista. Tietojärjestelmällä tarkoitetaan lain 2 §:n 3 kohdan mukaan tietojenkäsittelylait-

teista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä. Tietoturvallisuustoimenpiteillä puolestaan tarkoitetaan lain 2 §:n 8 kohdan mukaan tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä.

NIS2 –direktiivissä käytetään tietoturvallisuuden sijaan esimerkiksi seuraavia käsitteitä:

- ”kyberturvallisuus”, jolla tarkoitetaan toimia, joita tarvitaan verkko- ja tietojärjestelmien, tällaisten järjestelmien käyttäjien ja muiden asianosaisten henkilöiden suojaamiseksi kyberuhilta;
- ”kyberuhka”, jolla tarkoitetaan potentiaalista tilannetta, tapahtumaa tai toimintaa, joka voi vahingoittaa tai häiritä verkko- ja tietojärjestelmiä, tällaisten järjestelmien käyttäjiä ja muita henkilöitä tai muulla tavoin vaikuttaa näihin haitallisesti;
- ”verkko- ja tietojärjestelmä”, jolla tarkoitetaan
  a) direktiivin (EU) 2018/1972 2 artiklan 1 alakohdassa määriteltyä sähköistä viestintäverkkoa;
  b) laitetta taikka yhteen kytkettyjen tai toisiinsa yhteydessä olevien laitteiden ryhmää, joista yksi tai useampi suorittaa ohjelman avulla digitaalisten tietojen automaattista käsittelyä; tai
  c) digitaalisia tietoja, joita a ja b alakohdassa tarkoitetuissa järjestelmissä säilytetään, käsitellään, haetaan tai siirretään näiden järjestelmien toimintaa, käyttöä, suojausta tai ylläpitoa varten;

Tiedonhallintalaissa käytetyt käsitteet poikkeavat jonkin verran NIS2-direktiivissä käytetyistä, joten NIS2 –direktiivin voimaan saattamisen kannalta välttämättömät direktiivissä käytetyt käsitteet tulisi lisätä tiedonhallintalakiin.

3.16.3 Kyberturvallisuuden riskienhallintatoimenpiteet

Direktiivin 21 artiklan mukaan on säädettävä, että toimijat toteuttavat asianmukaiset ja oikeasuhteiset tekniset, operatiiviset ja organisatoriset toimenpiteet hallitakseen riskejä, joita niiden toiminnoissaan tai palveluntarjonnassaan käyttämien verkko- ja tietojärjestelmien turvallisuuteen kohdistuu, ja estääkseen tai minimoidakseen poikkeamien vaikutuksen palvelujensa vastaanottajiin ja muihin palveluihin. Lisäksi direktiivin 21 artiklan 2 kohtaan sisältyy yksityiskohtainen luettelo toimenpiteistä, joiden on ainakin sisällyttävä kyberturvallisuuden riskienhallintatoimenpiteisiin.

Tiedonhallintalain 13 §:ssä säädetään riskiarvioon perustuvasta tietoturvallisuustoimenpiteiden toteuttamisvelvollisuudesta (1 mom) sekä viranomaisen velvollisuudesta varmistua hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet (4 mom). Lain 13 a §:ssä säädetään tiedonhallinnan häiriötilanteista tiedottamisesta ja varautumisesta häiriötilanteisiin. Henkilöstöturvallisuuden osalta lain 12 §:ssä säädetään velvollisuudesta tunnistaa ne tehtävät, joiden suorittaminen edellyttää palveluksessa olevilta tai lukuun toimivilta henkilöiltä erityistä luotettavuutta. Lain 14 §:n 1 momentissa velvoitetaan toteuttamaan tietojensiirto yleisessä tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä, jos siirrettävät tiedot ovat salassa pidettäviä. Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja. Lain 16 § liittyy direktiivin 21 artiklassa edellytettyyn pääsynhallintaan. Säännöksen mukaan tietojärjestelmästä vastuussa olevan viranomaisen on määriteltävä tietojärjestelmän käyttöoikeudet käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan, ja pidettävä ne ajantasaisina.

Tiedonhallintalain edellä kuvatut säännökset kattavat osin direktiivin 21 artiklan velvoitteet, mutta direktiivin osin tarkemman sääntelyn sekä direktiivissä käytettyjen käsitteiden johdosta toimijoihin kohdistuvaa kyberturvallisuuden riskienhallintaa koskevaa sääntelyä on täydennettävä.

3.16.4 Johdon (hallintoelimen) vastuu

NIS2-direktiivin 20 artiklan 1 kohdan ensimmäisen alakohdan mukaan toimijan hallintoelimen on hyväksyttävä toimijan 21 artiklan noudattamiseksi toteuttamat kyberturvallisuusriskien hallintatoimenpiteet ja valvottava mainitun artiklan velvoitteiden täytäntöönpanoa. Lisäksi hallintoelin tulee voida saattaa vastuuseen, jos toimija rikkoo kyseistä artiklaa. Direktiivin 20 artiklan 1 kohdan toisen alakohdan mukaan ”*kohdan soveltaminen ei rajoita kansallisen lainsäädännön soveltamista, kun on kyse julkisiin laitoksiin sovellettavista vastuusäännöistä taikka virkamiesten tai vaalilla valittujen tai nimettyjen toimenhaltijoiden vastuusta”*. Direktiivin 20 artiklan 2 kohdan mukaan toimijoiden hallintoelinten jäsenillä tulee olla velvollisuus osallistua kyberturvallisuuden riskienhallintaa koskevaan koulutukseen. Lisäksi jäsenvaltioiden on kannustettava keskeisiä ja tärkeitä toimijoita tarjoamaan säännöllisesti vastaavaa koulutusta työntekijöilleen, jotta he voivat hankkia riittävät tiedot ja taidot kyetäkseen tunnistamaan riskejä ja arvioimaan kyberturvallisuuden riskienhallintakäytäntöjä ja niiden vaikutusta toimijan tarjoamiin palveluihin.

Tiedonhallintalain 4 §:n 2 momentissa on osin säädetty johdon vastuusta ja koulutuksen tarjoamisesta sekä valvonnan järjestämisestä. Säännöksen mukaan tiedonhallintayksikön johdon on huolehdittava muun muassa siitä, että tiedonhallintayksikössä on määritelty tiedonhallinnan toteuttamiseen liittyvien tehtävien vastuut; ajantasaiset ohjeet tietoturvallisuustoimenpiteistä; tarjolla koulutusta tiedonhallintaa koskevista säädöksistä määräyksistä ja tiedonhallintayksikön ohjeista; sekä järjestetty riittävä valvonta tiedonhallintaan liittyvien säädösten, määräysten ja ohjeiden noudattamisesta.

Kuten edellä on todettu, käytetyt käsitteet poikkeavat jonkin verran NIS2-direktiivissä käytetyistä, joten 4 §:n 2 momentin muotoilut eivät sellaisenaan täysin vastaa direktiivissä säädettyä. Tiedonhallintalaissa ei myöskään ole säädetty tiedonhallintayksikön tai viranomaisen johdon velvollisuudesta hyväksyä kyberturvallisuuden riskienhallintatoimenpiteitä eikä myöskään nimenomaisesta johdon velvollisuudesta valvoa kyberturvallisuuden riskienhallintatoimenpiteiden täytäntöönpanoa. Myöskään ei ole säädetty johdon velvollisuudesta osallistua koulutukseen. Koulutuksen tarjoamisesta henkilöstölle on säädetty (4 § 2 mom 3 k). Johdon vastuun osalta virkavastuuta voidaan pitää riittävänä, koska NIS2-drektiivi ja ehdotettu sääntely korostaa johdon tehtäviä ja vastuuta kyberturvallisuuden riskienhallinnassa.

3.16.5 Ilmoitusvelvollisuudet ja valvonta

NIS2-direktiivissä edellytetään, että soveltamisalaan kuuluville toimijoille säädetään velvollisuus ilmoittaa tietyt toimintaansa koskevat tiedot toimivaltaiselle viranomaiselle. Direktiivissä edellytetään myös säädettäväksi velvollisuudesta ilmoittaa toimivaltaiselle viranomaiselle tai CSIRT-yksikölle merkittävistä kyberturvallisuuspoikkeamista. Lisäksi direktiivissä edellytetään säädettäväksi toimijoiden valvonnasta.

Tiedonhallintalakiin ei sisälly ilmoitusvelvollisuutta toiminnasta, poikkeamien ilmoitusvelvollisuutta eikä varsinaista valvontaa koskevaa sääntelyä. Tiedonhallintalautakunnalle on lain 10 §:ssä säädetty arviointitehtävä, mutta se ei koske lain 4 luvun tietoturvallisuussääntelyn noudattamista. Lisäksi tiedonhallintalautakunnan tehtävänä on edistää tiedonhallintalaissa säädettyjen tiedonhallinnan ja tietoturvallisuuden menettelytapojen ja lain vaatimusten toteuttamista. Näin

ollen tiedonhallintalain sääntelyä on täydennettävä ilmoitusvelvollisuuksien ja valvonnan osalta.

3.16.6 Julkishallinnon toimialaa koskevan sääntelyn sijoittaminen tiedonhallintalakiin

Tiedonhallintalailla ohjataan myös manuaalista, paperilla tapahtuvaa tietojenkäsittelyä, joten tiedonhallintalain tietoturvallisuuteen liittyviä säännöksiä ei ole mahdollista korvata NIS2-direktiivin säännöksillä. Tiedonhallintalain sääntely ei myöskään kaikilta yksityiskohdiltaan eikä ilmoitusvelvollisuuksia ja valvontaa koskevilta osin täytä NIS2-direktiivissä edellytettyä.

Tästä syystä uudet nimenomaan kyberturvallisuuden riskienhallintaan ja muihin NIS2 –direktiivin velvoitteisiin sekä niiden noudattamisen valvontaan liittyvät säännökset ehdotetaan lisättäväksi omaan lukuunsa tiedonhallintalaissa. Tämä on perusteltua myös siksi, että NIS2-sääntelyä ehdotetaan sovellettavan rajatumpaan joukkoon kuin tiedonhallintalain tietoturvallisuussääntelyä. Myös NIS2 -direktiivissä edellytetty valvonta voidaan näin kohdentaa omassa luvussaan sijaitsevien NIS2 –direktiivissä säädettyjen velvoitteiden noudattamiseen.

3.16.7 Kansallisista syistä johtuvat tiedonhallintalain muutostarpeet

Asiakirjojen turvallisuusluokittelua koskeva velvollisuus tiedonhallintalain 18 §:ssä kohdistuu valtion virastoissa, laitoksissa ja valtion liikelaitoksissa toimiviin viranomaisiin, tuomioistuimiin ja valitusasioita käsittelemään perustettuihin lautakuntiin. Turvallisuusluokitteluvelvollisuuden laajentamiseen on tiedonhallintalain voimassaolon aikana ilmennyt tarvetta erityisesti julkisen hallinnon turvallisuusverkkotoiminnasta annetun lain (10/2015, jäljempänä *turvallisuusverkkolaki*) mukaisia tehtäviä hoitavan Suomen Erillisverkot Oy:n taholta. Turvallisuusluokitteluvelvollisuus ehdotetaan laajennettavaksi koskemaan myös Suomen Erillisverkot Oy:tä ja sen kokonaan omistamaa tytäryhtiötä niiden hoitaessa turvallisuusverkkolaissa tarkoitettuja tehtäviä.

3.17 Kyberturvallisuusstrategia

Voimassa oleva kansallinen kyberturvallisuusstrategia on hyväksytty valtioneuvoston periaatepäätöksenä 3.10.2019. Strategia perustuu Suomen 2013 kyberturvallisuusstrategiassa määriteltyihin yleisiin periaatteisiin. Kyberturvallisuusstrategian uudistus ja toimeenpano vuonna 2019 laadittiin hallitusohjelmakirjauksen pohjalta, ja oli myös osa EU:n kyberturvallisuusstrategian toimeenpanoa. Syinä vuoden 2019 uudistukseen ovat lisäksi olleet toimintaympäristössä tapahtuneet muutokset sekä kansallisesti havaitut kehittämiskohteet.

Kyberturvallisuusstrategia asettaa keskeiset kansalliset tavoitteet, joilla pyritään kehittämään kybertoimintaympäristöä ja turvaamaan yhteiskunnan kannalta tärkeät toiminnot. Sen kolme strategista linjausta ovat kansainvälisen yhteistyön kehittäminen, kyberturvallisuuden johtamisen, suunnittelun ja varautumisen parempi koordinaatio sekä kyberturvallisuuden osaamisen kehittäminen.

Kyberturvallisuusstrategian mukaisesti valtioneuvostoon on vuonna 2020 perustettu valtion kyberturvallisuusjohtajan tehtävä. Valtion kyberturvallisuusjohtajan johdolla on valmisteltu kyberturvallisuuden kehittämisohjelma. Valtioneuvoston periaatepäätös kyberturvallisuuden kehittämisohjelmasta on niin ikään laadittu vuoden 2019 kyberturvallisuusstrategian pohjalta valtion kyberturvallisuusjohtajan johdolla. Kehittämisohjelma on konkreettinen toimeenpanosuunnitelma, jonka tavoitteena on parantaa kyberturvallisuutta pitkäjänteisesti koko yhteiskunnassa. Suomen kyberturvallisuusstrategian täytäntöönpanoa seuraa Turvallisuuskomitea, joka toimii puolustusministeriön yhteydessä.

Kyberturvallisuusstrategiaa on tarpeen päivittää tulevan hallituskauden aikana muuttuneen ympäristön sekä uusien sääntelyvelvoitteiden vuoksi. Nykyinen kyberturvallisuusstrategia tai kyberturvallisuuden kehittämisohjelma eivät sisällöllisesti täytä niitä vaatimuksia, jotka NIS2-direktiivi kyberturvallisuusstrategialle asettaa.

Pääministeri Orpon hallitusohjelman mukaan kokonais- ja kyberturvallisuuden johtamisrakenne uudistetaan hallituskauden aikana pääministerin johdolla (luku 8) ja hallitus uudistaa kansallisen kyberturvallisuusstrategian vastaamaan muuttunutta toimintaympäristöä(luku 8.5).

4 Ehdotukset ja niiden vaikutukset

4.1 Keskeiset ehdotukset

Esityksessä ehdotetaan, että NIS2-direktiivin täytäntöönpanemiseksi säädettäisiin uusi laki kyberturvallisuuden riskienhallinnasta, joka sisältäisi NIS2-direktiivin edellyttämät vähimmäisvelvoitteet sen soveltamisalaan kuuluville toimijoille. Laissa noudatettaisiin NIS2-direktiivin edellyttämää vähimmäistasoa velvoitteiden soveltamisalan, laajuuden ja valvonnan suhteen. Lisäksi laissa säädettäisiin direktiivin edellyttämällä tavalla velvoitteiden noudattamisen valvonnasta sekä tietoturvaloukkauksiin reagoivasta ja niitä tutkivasta yksiköstä (CSIRT-yksikkö) ja sen tehtävistä. Direktiivin pääasiallinen täytäntöönpanomenetelmä olisi uudelleenkirjoittaminen. Direktiivin velvoitteet ja vaatimukset uudelleenkirjoitettaisiin kansalliseen lainsäädäntöön erityisesti siltä osin, kun ne kohdistuvat toimijoihin. Eräiden teknisluontoisten, yksityiskohtaisten ja viranomaiseen kohdistuvien säännösten osalta täytäntöönpanossa käytettäisiin myös viittausmenetelmää. Täytäntöönpano tehtäisiin direktiivin vähimmäisvaatimusten mukaisesti.

Yksinomaan julkishallinnon toimialaan kohdistuvista velvoitteista ja niiden noudattamisen valvonnasta säädettäisiin erikseen tiedonhallintalaissa. Tiedonhallintalaki olisi erityislaki suhteessa esitettyyn kyberturvallisuuden riskienhallinnasta annettuun lakiin. Kyberturvallisuuden riskienhallinnasta annetun lain CSIRT-yksikköä koskevaa sääntelyä, tietojen vaihtoa ja viranomaisyhteistyötä koskevaa sääntelyä sovellettaisiin myös julkishallinnon toimialalla siltä osin kuin niistä ei säädettäisi tiedonhallintalaissa. Jos julkinen toimija toimii jollain NIS2-direktiivin muista toimialoista, se voi kuulua NIS2-sääntelyn piiriin myös tai vain kyberturvallisuuden riskienhallinnasta annetun lain nojalla. Tämä koskee esimerkiksi hyvinvointialueita ja -yhtymiä, Helsingin kaupunkia sekä niitä kuntia, jotka harjoittavat toimintaa, joka on kuvattu muissa NIS2-direktiivin liitteiden I ja II kohdissa kuin liitteen I kohdassa 10. Vaikka tiedonhallintalakiin esitettyjä NIS2-direktiivistä johtuvia velvoitteita ei ehdoteta sovellettavaksi muiden kuntien kuin Helsingin kaupungin (siltä osin kuin se hoitaa laissa hyvinvointialueen järjestämisvastuulle säädettyjä tehtäviä) toimintaan, voisi muukin kunta kuulua NIS2-sääntelyn piiriin kyberturvallisuuden riskienhallinnasta annetun lain perusteella, mikäli sen palvelu kuuluu NIS2-direktiivin liitteissä määriteltyihin palveluihin ja kunta täyttää kyberturvallisuuden riskienhallinnasta annetun lain mukaisen toimijan määritelmän kokonsa puolesta.

Finanssialan toimijoita ei ehdoteta sisällytettävän kyberturvallisuuden riskienhallinnasta annetun lain soveltamisalaan, sillä kyseisiin toimijoihin sovellettaisiin DORA-asetusta ja sitä täytäntöönpanevaa sääntelyä. DORA-asetuksessa asetetaan finanssialan toimijoille NIS2-direktiivin velvoitteita pidemmälle meneviä velvoitteita kyberuhkiin varautumiseksi.

Sähköisen viestinnän palveluista annetussa laissa pantaisiin täytäntöön verkkotietojen rekisteröintitietojen tietokantaa koskevan NIS2-direktiivin 28 artiklan edellyttämät seikat aluetunnusrekisteriä ja verkkotunnusvälittäjiä koskien.

Kyberturvallisuuden riskienhallinta- ja raportointivelvoitteet kohdistuisivat yksityisiin tai julkisiin toimijoihin, jotka harjoittaisivat liitteessä I tai II tarkoitettua toimintaa, ja olisivat kooltaan komission pk-yrityksiä koskevan kokomääritelmän mukaisesti keskisuuria tai suurempia. Eräin poikkeuksin velvoitteet voisivat koskea myös tätä pienempiä yrityksiä. Lakiin sisältyisi myös säännös, jonka nojalla valtioneuvoston asetuksella voitaisiin tietyin edellytyksin säätää toimijan kuulumisesta lain soveltamisalaan sen koosta riippumatta. Laissa säädettäisiin myös näihin toimijoihin kohdistuvien riskienhallinta- ja raportointivelvoitteiden valvonnasta.

Valvovat viranomaiset nimettäisiin sektorikohtaisesti NIS1-direktiivin mukaista valvontamallia jatkaen. Valvova viranomainen määräytyisi sektorikohtaisen toimijan mukaan. Valvovia viranomaisia olisivat sektoreittain Liikenne- ja viestintävirasto, Energiavirasto, Turvallisuus- ja kemikaalivirasto, Sosiaali- ja terveydenalan lupa- ja valvontavirasto, Etelä-Savon ELY-keskus, Ruokavirasto, Lääkealan turvallisuus ja kehittämiskeskus sekä Finanssivalvonta. Valvontavastuu toimialoittain jakautuisi seuraavasti:

Valvova viranomainen	**NIS2-direktiivin liitteen I tai II mukainen toimiala**
Liikenne- ja viestintävirasto	Ilmaliikenne, raideliikenne, vesiliikenne, tieliikenne, avaruus, digitaalinen infrastruktuuri, TVT-palvelujen hallinta, kuriiri- ja postipalvelun tarjoajat, digitaalisen palvelun tarjoajat, valmistus (moottoriajoneuvojen, perävaunujen ja puoliperävaunujen valmistusta harjoittavat toimijat, muiden kulkuneuvojen valmistusta harjoittavat toimijat), tutkimusorganisaatiot, julkishallinto.
Energiavirasto	Sähkö, kaukolämmityksen tai kaukojäähdytyksen haltijat, kaasu (jakelu- ja siirtoverkonhaltijat)
Turvallisuus- ja kemikaalivirasto	Kaasu (maakaasun toimittajat, varastointilaitteiston haltijat, maakaasun käsittelylaitteiston haltijat, maakaasualan yritykset sekä maakaasun jalostus- ja käsittelylaitteistojen haltijat), öljy, vedyn tuotantoa, varastointia ja siirtoa harjoittavat toimijat, aineiden valmistusta ja aineiden tai seosten jakelua harjoittavat yritykset ja yritykset, jotka tuottavat esineitä aineista tai seoksista sekä valmistus (tietokoneiden sekä elektronisten ja optisten tuotteiden valmistusta harjoittavat toimijat, sähkölaitteiden valmistusta harjoittavat toimijat ja muiden koneiden ja laitteiden valmistusta harjoittavat toimijat).
Sosiaali- ja terveydenalan lupa- ja valvontavirasto	Terveys
Etelä-Savon ELY-keskus	Juomavesi, jätevesi ja jätehuolto
Ruokavirasto	Elintarvikeyritykset, jotka harjoittavat tukkukauppaa, teollista tuotantoa tai jalostusta
Lääkealan turvallisuus ja kehittämiskeskus	Lääkinnällisiä laitteita valmistavat toimijat ja In vitro –diagnostiikkaan tarkoitettuja lääkinnällisiä laitteita valmistavat toimijat

Finanssivalvonta	Pankkitoiminta ja finanssimarkkinoiden infrastruktuuri

Esityksessä ehdotetaan käytettäväksi kansallinen liikkumavara siitä, että valvova viranomainen saisi kohdentaa valvontaa riskiperusteisesti ja ensisijaisesti keskeisiin toimijoihin.

Tietoturvaloukkauksiin reagoivana ja niitä tutkivana CSIRT-yksikkönä sekä keskitettynä yhteyspisteenä toimisi jatkossakin Liikenne- ja viestintäviraston Kyberturvallisuuskeskus.

NIS2-direktiivin edellyttämien hallinnollisten sanktioiden enimmäismäärät olisivat tasolla, joka on direktiivin alin sallima enimmäismäärä. Hallinnolliset sanktiot määräisi seuraamusmaksulautakunta valvovan viranomaisen esityksestä. Seuraamusmaksulautakunta olisi uusi sivutoiminen elin, joka koostuisi valvovien viranomaisten nimeämistä jäsenistä. Kansallista liikkumavaran nojalla ehdotetaan säädettäväksi, ettei NIS2-direktiivin hallinnollisia seuraamusmaksuja voitaisi määrätä julkishallinnon toimijoille.

Esityksellä säädettäisiin valtioneuvostolle velvoite hyväksyä kyberturvallisuusstrategia, jossa on NIS2-direktiivin edellyttämä vähimmäissisältö. NIS2-direktiivin tarkoittamana kyberkriisinhallintaviranomaisena toimisi kukin viranomainen sille laissa säädettyjen tehtävien mukaisesti. Kyberkriisinhallintaviranomaisten välisenä koordinaattorina toimisi Liikenne- ja viestintäviraston Kyberturvallisuuskeskus, joka vastaisi myös kansallisen NIS2-direktiivin edellyttämän kyberkriisinhallintakehyksen laatimisesta laajamittaisten kyberturvallisuuspoikkeamien ja –kriisien hallitsemiseksi yhteistyössä muiden viranomaisten kanssa. Esityksellä ei ehdoteta muutettavaksi turvallisuusviranomaisten nykyisiä toimivaltuuksia tai tehtävänjakoa laajamittaisen kyberturvallisuuspoikkeaman ja –kriisin hallitsemisessa.

Esityksellä kumottaisiin sektorikohtaisesta sääntelystä NIS1-direktiivin täytäntöönpanemiseksi annettuja säännöksiä, koska säännökset olisivat jatkossa päällekkäisiä suhteessa uuteen NIS2-direktiivin täytäntöönpanemiseksi annettavaan lakiin ja NIS1-direktiivi on muutoinkin kumottu NIS2-direktiivillä. Kumottavaksi tai muutettavaksi ehdotetaan säännöksiä sähköisen viestinnän palveluista annetusta laista, ilmailulaista, raideliikennelaista, liikenteen palveluista annetusta laista, alusliikennepalvelulaista, eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetusta laista, sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetusta laista, sähkömarkkinalaista, maakaasumarkkinalaista ja sähkö- ja maakaasumarkkinoiden valvonnasta annetusta laista. Lisäksi NIS2-direktiivin täytäntöönpanoon liittyviä teknisiä muutoksia tehtäisiin Energiavirastosta annettuun lakiin.

Esityksessä ei käytettäisi NIS2-direktiivin kansallista liikkumavaraa keskeisen toimijan määritelmän laajentamisesta siten, että määritelmään sisällytettäisiin erikseen myös NIS1-direktiivin nojalla tunnistetut keskeisten palvelujen tarjoajat tilanteessa, jossa ne eivät muuten olisi NIS2-direktiivin nojalla keskeisiä toimijoita.

Esityksessä ei ehdoteta käytettäväksi kansallista liikkumavaraa NIS2-direktiivin soveltamisesta paikallistason julkishallinnon toimialan toimijoihin tai opetus- ja koulutusalan laitoksiin. Poikkeuksena velvoitteita sovellettaisiin Helsingin kaupunkiin siltä osin kuin se hoitaa tehtäviä, jotka on laissa säädetty hyvinvointialueen järjestämisvastuulle.

Esityksessä ehdotetaan säädettäväksi kansallisen liikkumavaran sallima poikkeus NIS2-direktiivistä aiheutuvien velvoitteiden soveltamiseen erityisiin toimijoihin, jotka tarjoavat palveluita sellaisille julkishallinnon toimijoille, jotka harjoittavat toimintaa kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla, mukaan lukien rikosten ennalta

estäminen, tutkiminen, paljastaminen ja rikoksiin liittyvät syytetoimet, tai harjoittavat sellaista toimintaa itse. Kansallista liikkumavaraa käytettäisiin täysimääräisesti NIS2-direktiivin sallimalla tavalla velvoitteiden kohdistumisesta näihin toimijoihin.

Esityksessä ei ehdoteta säädettäväksi kansallisia lisävaatimuksia eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien käytölle.

4.2 Pääasialliset vaikutukset

4.2.1 Ehdotuksen pääasialliset vaikutukset

Esityksellä on vaikutuksia sekä julkiselle sektorille että yksityisiin toimijoihin. Yleisellä tasolla esityksellä parannetaan yhteiskunnan toiminnan kannalta kriittisten toimijoiden ja keskeisten palveluiden kyberturvallisuutta sekä kyberhäiriöiden sietokykyä ja kykyä palautua kyberhyökkäyksistä tai muista tietojärjestelmiin ja viestintäverkkoihin haitallisesti vaikuttavista häiriöistä. Yhteiskunnan kriittiseen infrastruktuuriin kohdistuvilla kyberhyökkäyksillä tai muilla tietojärjestelmien ja viestintäverkkojen häiriötilanteilla voi olla merkittäviä ja laajamittaisia haitallisia vaikutuksia, joiden realisoitumista ehdotetuilla toimenpiteillä pyritään välttämään.

Esityksen mukaisten velvoitteiden täytäntöönpano tulee lisäämään sääntelyn kohteena olevien toimijoiden kustannuksia velvoitteiden noudattamiseksi. Kustannuksia velvoitteiden noudattamiseksi syntyy erityisesti toimialoilla, jotka eivät ole ennestään NIS1-direktiivin velvoitteiden piirissä. Julkiselle sektorille ja julkistaloudelle aiheutuu kustannuksia NIS2-direktiivin täytäntöönpanon edellyttämistä viranomaistehtävistä erityisesti velvoitteiden valvonnasta ja CSIRT-yksikön toiminnasta. Velvoitteiden valvonnasta ja CSIRT-yksikön toiminnasta aiheutuu lisäresurssitarpeita niille viranomaisille, joille näitä tehtäviä osoitetaan. Julkiselle sektorin toimijoille aiheutunee myös jonkin verran kustannuksia direktiivin kyberturvallisuuteen liittyvien vaatimusten noudattamisesta. Toisaalta velvoitteiden myötä paremmalla kyberhyökkäyksiin varautumisella, reagoinnilla ja tiedonvaihdolla saavutetaan toimijoiden toiminnassa parempi kyberturvallisuuden taso, minkä avulla pystytään ehkäisemään kyberhyökkäyksiä ja niiden haitallisia vaikutuksia, jotka muutoin voisivat aiheuttaa merkittäviä haitallisia vaikutuksia ja kustannuksia sekä toimijoille että laajemminkin yhteiskunnassa tahoille, jotka käyttävät toimijoiden tuotteita tai palveluita.

Esityksellä yhdenmukaistettaisiin tietoturvan riskienhallintaa koskevat horisontaaliset vähimmäisvaatimukset soveltamisalaan kuuluville toimijoille lain tasolla. Muutoksena aiempaan toimijoiden velvollisuutena olisi itse tunnistaa, kuuluvatko he sääntelyn soveltamisalaan, sekä ilmoittautua valvovalle viranomaiselle toimijaluetteloon, toteuttaa riskienhallintaa lain edellyttämällä tavalla ja raportoida merkittävistä poikkeamista valvovalle viranomaiselle ja CSIRT-yksikölle. Verrattuna NIS1-direktiivin aikaisiin riskienhallintavelvoitteisiin, laissa säädettäisiin yksityiskohtaisemmin osa-alueista, jotka riskienhallinnassa on huomioitava. Lisäksi riskienhallinta- ja raportointivelvoitteita sovellettaisiin NIS1-direktiiviä laajempaan joukkoon toimijoita. Soveltamisalaan kuuluisivat kaikki lain liitteessä tarkoitettua toimintaa harjoittavat tai toimijatyyppiä olevat toimijat, jotka olisivat kooltaan keskisuuria tai suurempia, eli täyttäisivät soveltamisalaa koskevan kokokriteerin. Soveltamisalaan kuuluisivat myös ne lain liitteessä tarkoitettua toimintaa harjoittavat tai toimijatyyppiä olevat toimijat, jotka eivät täyttäisi kokokriteeriä, mutta joita koskisi NIS2-direktiivin edellyttämä poikkeus soveltamisesta toimijan koosta riippumatta. Uusia soveltamisalaan kuuluvia sektoreita ovat jätevesi ja jätehuolto, kemikaalien valmistus, tuotanto ja jakelu, elintarvikkeiden tuotanto, jalostus ja jakelu, valmistussektori, johon kuuluu muun muassa lääkinnälliset laitteet, tietokoneet, sähkölaitteet ja moottoriajoneuvot sekä

avaruussektori, tele- ja luottamuspalvelut, CDN-palvelujen tarjoajat, verkkoyhteisöalustat ja julkinen sektori. Lisäksi kaikki CER-direktiivin nojalla kriittiseksi tunnistettavat toimijat kuuluisivat lain soveltamisalaan. Yhdessä jo aikaisemmin NIS-sääntelyn piiriin kuuluvien toimialojen kanssa soveltamisalaan kuuluva toimijoiden joukko on kooltaan huomattava. Vaikutusten voidaan arvioida vaihtelevan sektorikohtaisesti erityisesti toimijoiden kokoon liittyvän rajoituksen perusteella, sillä monien sektorien toiminta on muodostunut pienempien toimijoiden joukosta, jolloin velvoitteita ei lähtökohtaisesti sovellettaisi näihin toimijoihin.

Ehdotuksella olisi vaikutuksia julkisen sektorin toimijoihin sekä sääntelyn valvojana että kohteena. NIS2-direktiivin edellyttämät riskienhallintaa ja poikkeamaraportointia koskevat vaatimukset koskisivat myös julkisen sektorin toimijoita muulla kuin paikallishallinnon tasolla. NIS2-direktiivin edellyttämiä viranomaistehtäviä ovat valvovan viranomaisen tehtävä kullakin toimialalla, tietoturvaloukkauksiin reagoivan ja niitä tutkivan CSIRT-yksikön tehtävä sekä kansainvälinen yhteistyö muiden EU-jäsenvaltioiden, komission ja ENISA:n kanssa kyberhäiriöiden haitallisten vaikutusten torjumiseksi. NIS2-direktiivi asettaisi myös velvoitteen hyväksyä ja ylläpitää ajantasaisena kyberturvallisuusstrategia, josta vastaisi valtioneuvosto.

Kokonaisuutena NIS2-direktiivin täytäntöönpanon myötä viestintäverkkojen ja tietojärjestelmien turvallisuuden voidaan arvioida parantuvan niin julkisissa kuin yksityisissäkin toimijoissa. Kyberturvallisuuden korkean tason ylläpitämisellä on välillisesti merkitystä yhteiskunnassa laajemminkin. Yksityisellä sektorilla on merkittäviä kriittisen infrastruktuurin ylläpitämisen kannalta olennaisia palveluita tai toimintoja, joiden häiriönsietokyvyn parantuminen parantaa yhteiskunnan kriisinkestävyyttä. Poikkeamaraportoinnin ja riskienhallinnan valvonnan kautta on mahdollista saada nykyistä parempaa ja yksityiskohtaisempaa kyberturvallisuuden tilannekuvaa eri sektoreilla ja yleiselläkin tasolla yhteiskunnassa. Uusien vaatimuksien ja niiden valvonnan myötä kyberturvallisuuteen liittyvä tietoisuus ja osaamistaso kasvaa sekä yksityisellä että julkisella sektorilla.

Ehdotus yhdenmukaistaisi soveltamisalaan kuuluvien toimijoiden kriteerit EU:n laajuisesti ja vähentäisi tämän osalta jäsenvaltioiden hallinnollista taakkaa toimijoiden tunnistamisesta sekä yhdenmukaistaisi toimijoihin kohdistuvia vaatimuksia EU-jäsenvaltioissa. NIS2-direktiivin liitteissä tarkoitettua toimintaa harjoittavat keskisuuret tai suuremmat toimijat kuuluisivat lähtökohtaisesti soveltamisalaan toiminnan luonteen ja toimijan koon perusteella. Pienet- ja mikroyritykset jäävät lähtökohtaisesti soveltamisalan ulkopuolelle, ellei niitä koske poikkeus NIS2-direktiivin soveltamisalaan kuulumisesta koosta riippumatta. Jäsenvaltio voisi tietyin edellytyksin edelleen saattaa soveltamisalaan ja tunnistaa keskeisiksi myös pieniä ja mikrotoimijoita, mikäli näiden tuottamat palvelut voidaan katsoa yhteiskunnan toiminnan jatkuvuuden kannalta keskeisiksi. Ehdotus yhdenmukaistaisi kyberturvallisuus- ja raportointivelvoitteita ja laajentaa soveltamisalaa koskettamaan uusia sektoreita ja toimijoita. Valvoville viranomaisille tulee myös olemassa olevien tehtävien lisäksi uusia valvontatehtäviä, kuten soveltamisalaan lisättyjen toimijoiden valvonta.

Soveltamisalaan kuuluvan toimijan kokokriteeri vastaisi NIS2-direktiivin soveltamisalan kokokriteeriä. Komission suosituksen 2003/361/EY liitteen 2 artiklan nojalla keskisuuria yrityksiä, eli muita kuin mikro- ja pienyrityksiä, ovat yritykset, joiden palveluksessa on vähintään 50 työntekijää tai jonka vuosiliikevaihto ja taseen loppusumma ylittää 10 miljoonaa euroa. Keskisuuren yrityksen määrittelyssä käytettävät kynnysarvot ylittävänä yrityksenä ja siten laissa tarkoitettuna keskeisenä yrityksenä koon perusteella pidettäisiin yritystä, jonka palveluksessa olisi vähintään 250 työntekijää tai joiden vuosiliikevaihto ylittää 50 miljoonaa euroa ja taseen loppusumma ylittää 43 miljoonaa euroa. Komission suosituksen liitteen 3 artiklan 4 kohtaa julkisyhteisön hallinnasta toimijan pääomaan tai äänimäärään ei sovellettaisi arvioitaessa toimijan kuulumista soveltamisalaan.

Toimijoihin sovellettaisiin yhteisiä riskienhallinta- ja raportointivelvoitteita toimialasta ja –koosta riippumatta. Toimialan erityispiirteet olisi otettava huomioon toimintaan kohdistuvien riskien ja tarpeellisten riskienhallintatoimenpiteiden määrittelyssä. Merkittävän poikkeaman raportointivelvoite muuttuu kaksiportaiseksi. Ensi-ilmoitus tulisi toimittaa 24 tunnin kuluessa merkittävän poikkeaman havaitsemisesta. Ilmoitukseen tulee tapauksen mukaan sisällyttää tieto siitä, epäilläänkö poikkeaman johtuvan lainavastaisista tai vihamielisistä teoista tai voiko sillä olla rajat ylittäviä vaikutuksia. Kun poikkeamalla on rajat ylittäviä vaikutuksia, siitä on tiedotettava niille muille jäsenvaltioille, joihin poikkeama vaikuttaa sekä ENISA:lle.

Jatkoilmoitus tulisi toimittaa 72 tunnin kuluessa merkittävän poikkeaman havaitsemisesta. Ilmoitukseen tulee tapauksen mukaan päivittää ennakkovaroituksen tiedot ja esittää ensimmäinen arvio merkittävästä poikkeamasta, sen vakavuudesta ja vaikutuksista sekä vaarantumisindikaattorit, jos sellaisia on saatavilla. Ensi- ja jatkoilmoitus voitaisiin toimittaa myös yhdellä ilmoituksella, mikäli toimijalla olisi ensi-ilmoituksen määräajassa käytettävissään myös jatkoilmoituksen edellyttämät tiedot. Jatkoilmoituksella voitaisiin myös täydentää ensi-ilmoituksen mukaisia tietoja.

Lisäksi merkittävästä poikkeamasta olisi laadittava loppuraportti viimeistään kuukauden kuluttua poikkeamailmoituksen toimittamisesta ja sen tulisi sisältää yksityiskohtaisen kuvauksen poikkeamasta, sen vakavuuksista ja vaikutuksista, poikkeaman todennäköisesti aiheuttaneen uhan tai juurisyyn tyypin, toimenpiteet, jotka on tehty tai joita suunnitellaan vaikutusten lieventämiseksi sekä tapauksen mukaan poikkeaman rajat ylittävät vaikutukset. Väliraportti tai lisätietoja asian käsittelystä olisi toimitettava valvovan viranomaisen pyynnöstä, sekä pitkäkestoisen poikkeaman kohdalla kuukauden kuluttua jatkoilmoituksen toimittamisesta.

4.2.2 Riskienhallinta- ja raportointivelvoitteiden soveltamisalaan kuuluvat toimijat

Esitys muuttaisi kyberturvallisuuden riskienhallinta- ja raportointivelvoitteiden soveltamisalaa NIS1-direktiivin täytäntöönpanosta. Esityksen mukainen kyberturvallisuuden riskienhallinta- ja raportointivelvoitteiden soveltamisala kattaisi toimijat, jotka harjoittavat lain liitteessä tarkoitettua toimintaa tai ovat liitteessä tarkoitettua toimijatyyppiä ja täyttävät tai ylittävät soveltamisalan kokokriteerin tai niitä koskee poikkeus velvoitteiden soveltamisesta koosta riippumatta. Lisäksi velvoitteita sovellettaisiin CER-direktiivin nojalla kriittisiksi tunnistettuihin toimijoihin koosta riippumatta. Muutoksena NIS1-direktiiviin soveltamisalaan kuuluvia toimijoita ei määriteltäisi toimialoilla, vaan kaikki liitteessä tarkoitettua toimintaa harjoittavat tai toimijatyyppiä olevat, kokokriteerin täyttävät tai kokopoikkeuksen piiriin kuuluvat toimijat kuuluisivat soveltamisalaan suoraan. Lisäksi toimijoita koskevat NIS-velvoitteet kumottaisiin sektorikohtaisista laeista ja siirrettäisiin kyberturvallisuuden riskienhallinnasta annettavaan lakiin muiden kuin julkishallinnon toimijoiden osalta.

Velvoitteiden soveltamisalan kokokriteerinä olisi keskisuuren yrityksen määritelmä. Komission suosituksen 2003/361/EY liitteen 2 artiklan nojalla keskisuuria yrityksiä, eli muita kuin mikro- ja pienyrityksiä, ovat yritykset, joiden palveluksessa on vähintään 50 työntekijää tai jonka vuosiliikevaihto ja taseen loppusumma ylittää 10 miljoonaa euroa. Komission suosituksen liitteen 3 artiklan 4 kohtaa julkisyhteisön hallinnasta toimijan pääomaan tai äänimäärään ei sovellettaisi arvioitaessa toimijan kuulumista NIS2-direktiivin soveltamisalaan. Soveltamisalan yleinen kokokriteeri olisi siten se, että toimijan palveluksessa on vähintään 50 työntekijää tai sen vuosiliikevaihto ja taseen loppusumma ylittää 10 miljoonaa euroa, eli toimija täyttää komission suosituksessa tarkoitetun keskisuuren yrityksen määritelmän. Toimijat, jotka ylittäisivät keskisuuren toimijan määritelmän, olisivat ehdotuksessa tarkoitettuja keskeisiä toimijoita. Komission suosituksen mukaisesti keskisuuren yrityksen määrittelyssä käytettävät kynnysarvot ylittävä yritys

on yritys, jonka palveluksessa on vähintään 250 työntekijää tai joiden vuosiliikevaihto ylittää 50 miljoonaa euroa ja taseen loppusumma ylittää 43 miljoonaa euroa.

Lisäksi velvoitteiden soveltamisalaan kuuluisivat niiden koosta riippumatta julkishallinnon sektorin toimijat sekä toimijat silloin, jos toimijat ovat yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajia; luottamuspalvelun tarjoajia; aluetunnusrekisterejä; tai DNS-palveluntarjoajia.

Lisäksi velvoitteiden soveltamisalaan kuuluisivat CER-direktiivin nojalla kriittisiksi toimijoiksi määriteltävät toimijat niiden koosta riippumatta.

Lisäksi velvoitteiden soveltamisala voitaisiin ulottaa valtioneuvoston asetuksella liitteissä I ja II tarkoitettuja toimijatyyppiä oleviin toimijoihin silloin, kun: a) toimija tarjoaa ainoana jäsenvaltiossa palvelua, joka on yhteiskunnan tai talouden kriittisten toimintojen ylläpitämisen kannalta keskeinen; b) häiriö toimijan tarjoamassa palvelussa voisi vaikuttaa merkittävästi yleiseen järjestykseen, yleiseen turvallisuuteen tai kansanterveyteen; c) häiriö toimijan tarjoamassa palvelussa voisi aiheuttaa merkittävän systeemisen riskin erityisesti aloilla, joilla tällaisella häiriöllä voisi olla rajatylittäviä vaikutuksia; d) toimija on kriittinen, koska sillä on erityisen suuri merkitys kansallisella tai alueellisella tasolla kyseisen toimialan tai palvelutyypin tai jäsenvaltion muiden keskinäisriippuvaisten toimialojen kannalta.

Kyberturvallisuuden riskienhallinnasta annetun lain mukaisia velvoitteita sovellettaisiin liitteissä määriteltyihin toimijatyyppeihin seuraavilla toimialoilla.

Toimialat, jotka kuuluivat myös NIS1-direktiivin soveltamisalaan	**Toimialat, joilla toimijat tulevat uutena NIS-velvoitteiden soveltamisalaan**
Energia	Jätehuolto, jätevesi
Liikenne	Kemikaalien valmistus, tuotanto ja jakelu
Pankkitoiminta ja finanssimarkkinoiden infrastruktuuri	Elintarvikkeiden tuotanto, jalostus ja jakelu
Terveys	Valmistus: lääkinnällisten laitteiden valmistus, tietokoneiden sekä elektronisten ja optisten tuotteiden valmistus, sähkölaitteiden valmistus, muiden koneiden ja laitteiden valmistus, moottoriajoneuvojen, perävaunujen ja puoliperävaunujen valmistus sekä muiden kulkuneuvojen valmistus.
Juomavesi	Avaruus
Digitaalinen infrastruktuuri	TVT-palvelujen hallinta
Digitaalisen palvelun tarjoajat	Posti- ja kuriiripalvelut
	Tutkimustoiminta

	Julkishallinto

Toimialoista ja toimijatyypeistä osa on kuulunut riskienhallinta- ja raportointivelvoitteiden soveltamisalaan NIS1-direktiivin täytäntöönpanon myötä ja osa tulee soveltamisalaan uutena. Soveltamisalaan kuuluvien toimijatyyppien määritelmät laajenevat osin myös NIS1-direktiivin soveltamisalaan kuuluneilla toimialoilla. Seuraavassa käsitellään toimialoittain soveltamisalaan kuuluvia toimijatyyppejä sekä riskienhallinta- ja raportointivelvoitteiden alaan kuuluvien toimijoiden määrää. Julkishallinnon velvoitteista säädettäisiin julkisen hallinnon tiedonhallinnasta annetussa laissa. Toimialakohtaisesti soveltamisalaan kuuluvat toimijatyypit kuvataan tarkemmin taulukon alla.

Energiasektori

Energiasektori on ollut NIS1-direktiivin piirissä ja velvoitteet otettiin osaksi sektorikohtaista lainsäädäntöä. Keskeisten palveluiden tarjoajiksi Suomessa katsottiin energiasektorin osalta sähköverkonhaltijat sekä maakaasun siirtoverkonhaltijat. Velvoitteet sisältävät toimijan velvollisuuden huolehtia käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä ilmoittaa järjestelmiensä tietoturvallisuuteen liittyvästä merkittävästä häiriöstä Energiavirastolle (NIS-ilmoitus). NIS1-direktiivin mukaisia valvottavia toimijoita oli energiasektorilla vuoden 2023 alussa yhteensä 88 yritystä. Valvova viranomainen on ollut Energiavirasto.

NIS2-direktiivissä sääntelyn ulottuvuutta laajennetaan energiasektorin osalta. Direktiivin soveltamisalaan kuuluvat energiasektorin osalta seuraavat toimijatyypit:

Sähkö	Sähköntoimittajat ja -tuottajat, jakeluverkonhaltijat, kantaverkonhaltijat, sähkömarkkinaoperaattorit, eräät sähkömarkkinoiden osapuolet sekä latauspisteiden operaattorit
Kaukolämmitys ja –jäähdytys	Kaukolämmityksen tai –jäähdytyksen haltijat
Öljy	Öljynsiirtoputkistojen haltijat, öljyn tuotanto-, jalostus-, ja käsittelylaitteistojen haltijat sekä varastointia ja siirtoa hoitavat operaattorit sekä keskusvarastointiyksiköt
Kaasu	Jakeluverkonhaltijat, siirtoverkonhaltijat, maakaasun toimittajat, varastointilaitteiston haltijat, nesteytetyn maakaasun käsittelylaitteiston haltijat, maakaasun jalostus- ja käsittelylaitteistojen haltijat sekä eräät maakaasualan yritykset
Vety	Vedyn tuotantoa, varastointia ja siirtoa harjoittavat toimijat

NIS1-direktiivin alaan kuului energiasektorin toimijatyypeistä osittain sähkö, kaasu ja öljy. NIS2-direktiivissä esitettyjen muutosten myötä energiasektorilla soveltamisalaan kuuluvien toimijoiden määrä kasvaa merkittävästi siitä, mitä toimijoita Suomessa on NIS1-direktiivin nojalla tunnistettu keskeisiksi. Direktiivi koskettaisi laajasti energiasektorilla edellä kuvattua toimintaa

harjoittavia organisaatioita. Energiasektorilla valvovana viranomaisena toimisi jatkossakin Energiavirasto sekä osin Turvallisuus- ja kemikaalivirasto.

Liikennesektori

Liikennesektori on ollut NIS1-direktiivin piirissä ja velvoitteet keskeisten palveluntarjoajien velvollisuudesta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta otettiin osaksi sektorikohtaista lainsäädäntöä. Sääntelyn piirissä on ollut vajaa kymmenen ilma-, vesi-, raide- ja tieliikenteen toimijaa. NIS1-direktiivi implementoitiin koskemaan liikenteen ohjausta, lennonvarmistusta, rataverkon haltijaa sekä TEN-T -ydinverkon satamia ja -lentokenttiä, jotka kattavat osan NIS1-direktiivissä määritellyistä liikennesektorin toimijatyypeistä. NIS2-direktiivin myötä sääntely ulottuisi myös muihin toimijatyyppeihin, kuten kaupallisen lentoliikenteen harjoittajat, rautatieyritykset sekä eräät sisävesillä, merillä ja rannikoilla matkustaja- tai rahtiliikennettä hoitavat yritykset. Valvova viranomainen on ollut Liikenne- ja viestintävirasto.

NIS2-direktiivin myötä velvoitteiden soveltamisala laajenee myös liikennesektorilla. Uusina toimijatyyppeinä soveltamisalaan tulevat muun muassa lentoliikenteen harjoittajat, rautatieyritykset sekä eräät matkustaja- tai rahtiliikennettä hoitavat yritykset. Liikennesektorin osalta soveltamisalaan kuuluisivat seuraavat toimijatyypit:

Ilmailu	Kaupallisen lentoliikenteen harjoittajat, lentoaseman pitäjät ja lennonjohtopalvelun tarjoajat
Raideliikenne	Rataverkon haltijat ja liikenteenohjauspalvelua tarjoavat yhtiöt, rautatieyritykset ja palvelupaikan ylläpitäjät
Vesiliikenne	Eräät sisävesillä, merillä ja rannikoilla matkustaja- ja rahtiliikennettä hoitavat yhtiöt, satamanpitäjät ja toimijat jotka huolehtivat rakenteista ja varusteista satamien alueella, ja VTS-palveluntarjoajat
Tieliikenne	Liikenteenhallinta ja älykkäiden liikennejärjestelmien ylläpitäjät

Liikennesektorilla soveltamisalaan kuuluvien toimijoiden määrä kasvaa sekä uusilla toimijatyypeillä että NIS1-direktiivin mukaisilla sektoreilla. Liikennesektorilla soveltamisalaan kuuluisi arviolta noin 40-80 toimijaa painottuen määrällisesti ilmailun, raideliikenteen ja vesiliikenteen sektoreille. Valvovana viranomaisena toimisi jatkossakin Liikenne- ja viestintävirasto.

Uusien toimijatyyppien osalta olemassaolevaa velvoittavaa tieto- tai kyberturvallisuussääntelyä on vähän, lukuun ottamatta ilmailua, jossa liikennemuotokohtainen yhteiseurooppalainen sääntely on voimakkaasti lisääntymässä. Ilmailun tietoturvallisuutta koskevaa lainsäädäntöä on jo osittain voimassa ja vuodesta 2026 eteenpäin sitä on sovellettava kattavasti lähes koko ilmailusektorilla. Kyseinen EU-sääntely soveltuu laajempaan toimijajoukkoon kuin NIS2-direktiivi, ja toimijoille asetettavat velvoitteet vastaavat pitkälti NIS2-vaatimuksia.

Pankkitoiminta ja finanssimarkkinoiden infrastruktuuri

Pankkitoiminta ja finanssimarkkinoiden infrastruktuuri on NIS2-direktiivissä määriteltyjen toimijatyyppien osalta ollut NIS1-direktiivin piirissä. Soveltamisalaan ovat kuuluneet luottolaitokset, kauppapaikkojen ylläpitäjät sekä keskusvastapuolet. NIS2-direktiivin liitteessä I määritelty pankkitoiminta ja finanssimarkkinoiden infrastruktuurit kattavat samat toimijatyypit. Valvovana viranomaisena on toiminut ja toimisi jatkossa Finanssivalvonta.

NIS2-direktiivin velvoitteiden sijasta toimijoihin sovellettaisiin käytännössä kyberturvallisuuden riskienhallinnan kannalta olennaisten toimenpiteiden finanssialan sektorikohtaista erityissääntelyä ja erityisesti DORA-asetusta. DORA-asetuksessa asetetaan pankki- ja finanssialan toimijoille NIS2-direktiivin velvoitteita pidemmälle menevä velvoite kyberuhkiin varautumiseen, eikä kyseisiin toimijoihin sovellettaisi NIS2-direktiivin kyberturvallisuusriskien hallintaa, raportointivelvoitteita, valvontaa tai täytäntöönpanoa koskevia säännöksiä, vaan DORA-asetusta. NIS2-direktiivi ei aiheuttaisi pankki- tai finanssialalla merkittäviä sektorikohtaisia vaikutuksia.

Terveyssektori

Terveyssektorilla keskeinen soveltamisalaan kuuluva toimijatyyppi ovat terveydenhuollon tarjoajat. Sosiaali- ja terveydenhuollon palveluntarjoajat ovat olleet NIS1-direktiivin piirissä, eikä NIS2-direktiivi tuo merkittäviä muutoksia soveltamisalaan näiden toimijatyyppien osalta. Julkisia sosiaali- ja terveydenhuollon palveluntuottajia ovat vuoden 2023 alusta lähtien olleet hyvinvointialueet, joiden NIS2-direktiiviin perustuvista riskienhallinta- ja raportointivelvoitteista säädettäisiin tiedonhallintalaissa osana julkisen sektorin velvoitteita. Yksityiset sosiaali- ja terveydenhuollon toimijat kuuluisivat kyberturvallisuuden riskienhallinnasta annettavan lain soveltamisalaan. Valvovana viranomaisena on toiminut NIS1-velvoitteiden osalta Valvira.

Uusina toimijoina NIS2-direktiivin myötä soveltamisalaan tulevat EU:n vertailulaboratoriot, lääkkeiden tutkimus ja kehitystoiminta sekä lääkkeiden, lääkeaineiden tai lääkinnällisten laitteiden valmistus. Terveyssektorilla NIS2-direktiivin laajeneva soveltamisala toisi velvoitteiden alaan uusia toimijatyyppejä ja siten kasvattaisi valvottavien toimijoiden määrää. Valvovana viranomaisena toimisi jatkossakin Valvira.

Tällä hetkellä julkisen terveydenhuollon yksiköillä on velvollisuus liittyä Kanta-palveluihin. Tämä edellyttää käyttämään turvallisuusvaatimukset täyttäviä tietojärjestelmiä, jotka sertifioidaan ulkopuolisen tahon puolesta. Organisaatioiden on myös tehtävä turvallisuussuunnitelma. Asiakastietolaissa on säädetty Kanta-palveluihin liittymisestä, sertifioinnista sekä annettu Terveyden- ja hyvinvoinnin laitokselle valtuudet antaa määräyksiä vaadittavista turvallisuusominaisuuksista sekä turvallisuussuunnitelman sisällöstä. Lisäksi on säädetty velvollisuudesta ilmoittaa poikkeamista Valviralle. NIS2-direktiivi ei aiheuta terveydenhuollon palveluntarjoajille merkittäviä lisätoimenpiteitä.

Juoma- ja jätevesi

NIS2-direktiivin soveltamisalaan kuuluvat juomaveden toimittajat ja jakelijat sekä jätevettä keräävät, hävittävät ja käsittelevät yritykset. Juomaveden toimittaminen ja jakelu on ollut NIS1-direktiivin piirissä. Suomessa NIS1-sääntely on saatettu vesihuoltolain muutoksella 2018 sekä juomaveden että jäteveden osalta koskemaan vesihuoltolaitoksia, jotka toimittavat vettä tai ottavat vastaan jätevettä vähintään 5000 kuutiometriä vuorokaudessa, sekä vesihuoltolaitoksia, jotka toimittavat näille laitoksille vettä tai käsittelevät niiden jätevesiä. Sääntely koskee siten nykyisellään talousvesilaitoksia, jätevesilaitoksia ja tukkuvesihuoltolaitoksia ja toimijoita on arviolta noin 70 kpl.

Jätevesisektori on uusi säänneltävä sektori, mutta sen tuominen sääntelyn piiriin ei lisää toimijoiden määrää, sillä nykyinen NIS-sääntely vesihuoltolaissa koskee kaikkia kokorajan ylittäviä laitoksia, jotka huolehtivat jäteveden poisjohtamisesta ja käsittelystä. Valtaosa NIS1-direktiivin sääntelyn piirissä olevista laitoksista huolehtii sekä juomavedestä että jätevedestä.

Esityksen myötä kansallista soveltamisalaa rajaavasta 5000 kuutiometrin kriteeristä luovuttaisiin, ja jatkossa soveltamisalaan kuulumista määrittäisi juomaveden ja jäteveden osalta toimijatyyppi ja toimijan koko samoin kuten muillakin sektoreilla. NIS2-direktiivin ei ennakoida lisäävän juoma- ja jätevesisektorilla soveltamisalaan kuuluvien toimijoiden määrää olennaisesti. Nykyisin soveltamisalan ulkopuolella olevat alle 5000 kuution laitokset voivat olla mikro- tai pientoimijoita henkilöstön ja liikevaihtonsa vuoksi ja jäädä siten osin myös NIS2-direktiivin soveltamisalan ulkopuolelle. Soveltamisalaan kuuluvien toimijoiden määrän ennakoidaan pysyvän nykyisellä tasolla tai laskevan. Juoma- ja jätevesisektorin toimijat harjoittavat yleisesti molempien toimijatyyppien mukaista toimintaa. Soveltamisalaan kuuluvia kokokriteerin ylittäviä tai CER-direktiivin nojalla kriittiseksi määriteltäviä toimijoita arvioidaan tällä sektorilla olevan yhteensä noin 20-40 kpl ja keskeisen toimijan kokokriteerin ylittäviä toimijoita muutamia.

Valvovana viranomaisena juoma- ja jätevesisektorin osalta on toiminut elinkeino-, liikenne- ja ympäristökeskus. Jatkossa NIS2-direktiivin nojalla asetettujen velvoitteiden valvonta keskitettäisiin vesihuollon osalta Etelä-Savon elinkeino-, liikenne- ja ympäristökeskukseen, joka toimisi valvovana viranomaisena riippumatta alueesta, jolle toimija on sijoittautunut.

Digitaalinen infrastruktuuri ja digitaalisen palvelun tarjoajat

Digitaalisen infrastruktuurin ja digitaalisten palvelujen tarjoajista verkossa toimivan markkinapaikan, hakukoneen ja pilvipalvelun tarjoajat ovat kuuluneet jo NIS1-direktiivin soveltamisalaan. Suomessa toimivia verkossa toimivan markkinapaikan, hakukoneen tai pilvipalvelun tarjoajia on arvioitu olevan yhteensä noin 70-80 kappaletta, joista tosin vain osan päätoimipaikka on Suomessa. Valvovana viranomaisena on toiminut Liikenne- ja viestintävirasto.

NIS2-direktiivin myötä sääntelyn soveltamisalaan kuuluvien toimijatyyppien määrä laajenee merkittävästi digitaalisen infrastruktuurin sektorilla. Digitaalisen infrastruktuurin toimialalla uusina toimijatyyppeinä soveltamisalaan tulevat sisällönjakeluverkkojen tarjoajat (content delivery network providers), luottamuspalveluiden tarjoajat, yleisten viestintäverkkojen ja viestintäpalveluiden tarjoajat (teleyritykset) ja datakeskuspalveluiden tarjoajat, minkä lisäksi DNS-nimipalveluiden valvonta ulotettaisiin myös auktoritatiivisiin nimipalvelimiin rekursiivisten nimipalvelimien lisäksi. Lisäksi digitaalisten palvelujen tarjoajiin kuuluisivat verkkoyhteisöalustojen tarjoajat, verkossa toimivien markkinapaikkojen tarjoajat sekä verkossa toimivien hakukoneiden tarjoajat. Osa kyseisiä palveluja tarjoavista toimijoista on kuitenkin saattanut jo aiemmin kuulua NIS1-direktiivin soveltamisalaan. Esimerkiksi osa datakeskuspalvelujen tai sisällönjakelupalvelun tarjoajista on todennäköisesti myös NIS1-direktiivissä tarkoitetun pilvipalvelun tarjoajia.

Toimijatyypeistä yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat, luottamuspalvelun tarjoajat, aluetunnusrekisterit ja DNS-palveluntarjoajat kuuluisivat soveltamisalaan niiden koosta riippumatta, mikä kasvattaisi tällaisten toimijoiden lukumäärää soveltamisalassa, kun kokokriteeriä ei sovelleta. Muiden toimijatyyppien osalta kokokriteeriä sovellettaisiin myös digitaalisen infrastruktuurin toimialalla, ellei toimijoita koske jokin muu poikkeus, kuten tunnistaminen CER-direktiivin nojalla keskeiseksi toimijaksi.

Digitaalisen infrastruktuurin toimialalla soveltamisalaan kuuluvien toimijoiden määrän arvioidaan soveltamisalan laajenemisen johdosta kasvavan merkittävästi. Näillä toimijatyypeillä palveluiden tarjoaminen edellyttää palvelun tarjoajalta jo lähtökohtaisesti korkean tason riskienhallintaa kyberturvallisuudessa. Yleisten viestintäverkkojen ja viestintäpalvelujen tarjoajien sekä luottamuspalvelujen tarjoajien osalta toimijoihin on kohdistunut jaksoissa 1.1.3 ja 1.1.4 kuvatusti tietoturvavaatimuksia jo aiemmin. NIS2-direktiivin ei arvioida aiheuttavan toimijoille merkittäviä lisävelvoitteita. Soveltamisalaan kuuluvia sähköisten luottamuspalvelujen tarjoajia on arvioitu olevan yhteensä noin 30 kappaletta, joista hyväksyttyjä luottamuspalvelujen tarjoajia on yksi. Valvovana viranomaisena toimisi jatkossakin Liikenne- ja viestintävirasto.

DNS-palveluntarjoajat, aluetunnusrekisterit, pilvipalvelujen tarjoajat, datakeskuspalvelujen tarjoajat, sisällönjakeluverkkojen tarjoajat sekä verkossa toimivien markkinapaikkojen tarjoajat, verkossa toimivien hakukoneiden tarjoa-jat ja verkkoyhteisöalustojen tarjoajat kuuluisivat vain sen jäsenvaltion lainkäyttövaltaan, missä niillä on päätoimipaikka. Kyseisten toimijoiden osalta on arvioitu, että vain harva tällaisista palveluntarjoajista on sijoittautunut Suomeen, ja kansainvälistä toimivaltaa koskevien säännösten mukaisesti toimijoihin kohdistuva valvontavastuu olisi sillä jäsenvaltiolla, johon toimija on sijoittautunut. Soveltamisalaan kuuluvia, eli Suomeen sijoittautuneita DNS-palveluntarjoajia on arvioitu olevan yhteensä noin 20-30 kpl ja datakeskus- tai sisällönjakeluverkon tarjoajia on arvioitu olevan muutamia kymmeniä.

Tieto- ja viestintätekniikan palvelujen hallinta

TVT-palveluntarjoajia koskeva sektori on kokonaan uusi toimiala NIS1-direktiivin soveltamisalaan verrattuna. NIS2-direktiivistä johtuvat lain tasoiset kyberturvallisuuden riskienhallinta- ja raportointivelvoitteet olisivat uusia tämän toimialan toimijoille, jotka tulevat uutena toimijatyyppinä sääntelyn soveltamisalaan.

TVT-palveluntarjoajien (eng. ICT service providers) sektori koostuu yritysten välisistä hallintapalvelujen ja tietoturvapalvelujen tarjoajista. Edellytyksenä on yleisen kokokriteerin täyttyminen, eli yritysten olisi oltava kooltaan keskisuuria tai suurempia. Myös TVT-palveluntarjoajat kuuluvat vain sen jäsenvaltion lainkäyttövaltaan, missä niillä on päätoimipaikka. Toimijoita, joiden päätoimipaikka on Suomessa ja jotka kuuluisivat NIS2-direktiivin soveltamisalaan on arvioitu olevan yhteensä muutamia kymmeniä. NIS2-direktiivin velvoitteet olisivat kyseisille toimijoille pääosin uudenlaisia velvoitteita. Näillä toimijatyypeillä palveluiden tarjoaminen edellyttää palvelun tarjoajalta jo lähtökohtaisesti korkean tason riskienhallintaa kyberturvallisuudessa, joten riskienhallinta- ja raportointivelvoitteiden noudattamisen ei ennakoida aiheuttavan merkittäviä kustannuksia toimijoissa. Valvovana viranomaisena toimisi Liikenne- ja viestintävirasto.

Avaruus

Avaruus on uusi sektori NIS-direktiivin soveltamisalassa. Sektorin osalta sääntely koskisi maa-asematoimintaa harjoittavia toimijoita ja muita avaruuspohjaisten palvelujen tarjoamista tukevan, jäsenvaltioiden tai yksityisten tahojen omistaman, hallinnoiman ja operoiman maassa sijaitsevan infrastruktuurin ylläpitäjiä. Maainfrastruktuurin osalta keskisuuret ja isot toimijat kuuluisivat keskeisiin toimijoihin ja pienet toimijat muihin kuin keskeisiin toimijoihin. Suomessa valtaosa yrityksistä on arvion mukaan pieniä.

Maa-asemalaissa tarkoitettujen toiminnanharjoittajien osalta toimijoihin on kohdistunut jaksossa 3.9 kuvatusti tietoturvavaatimuksia jo aikaisemmin, eikä NIS2-direktiivin ole arvioitu aiheuttavan toimijoille merkittäviä lisävelvoitteita. Maa-asemista ja eräistä tutkista annetun lain

esitöissä on arvioitu velvoitteiden soveltamisalaan kuuluvan avaruussektorin toiminnan Suomessa olevan verrattain vähäistä (HE 113/2022 vp, s. 16–19).

Posti- ja kuriiripalvelut

Posti- ja kuriiripalvelut ovat uusi soveltamisala NIS-direktiivin piirissä. Posti- ja kuriiripalveluihin ei ole kohdistettu aikaisemmin kyberturvallisuusvaatimuksia, joten nyt ehdotettavat velvoitteet ovat toimijoille uusia ja toimijat ovat NIS-velvoitteiden soveltamisalassa uusi toimijajoukko. Soveltamisalaan kuuluisivat postipalvelujen tarjoajat ja kuriiripalvelujen tarjoajat. Postipalveluilla tarkoitetaan palveluja, joihin kuuluvat postilähetysten keräily, lajittelu, kuljetus ja jakelu. Postilähetyksellä taas tarkoitetaan nimenomaan yleispalvelun tarjoajan kuljetettavaa valmista lähetystä, joka on osoitettu jollekin vastaanottajalle. Nämä lähetykset voivat kirjelähetysten lisäksi olla esimerkiksi kirjoja, luetteloita, sanomalehtiä ja aikakausjulkaisuja sekä postipaketteja, jotka sisältävät joko kaupallista arvoa omaavaa tai sitä vailla olevaa tavaraa.

Posti- ja kuriirisektorin osalta NIS2-toimijoiden joukon arvioidaan olevan Suomessa pieni. Vuoden 2020 postimarkkinaselvityksessä[2] Liikenne- ja viestintävirasto totesi, että kuriiripostin arvioidaan olevan volyymiltään varsin pientä. Liikenne- ja viestintävirastolta saatujen tietojen mukaan pienten kuriiripalveluja tarjoavien toimijoiden määrä saattaa pienestä jakeluvolyymistä huolimatta olla hyvinkin suuri. Liikenne- ja viestintäviraston arvion mukaan valtaosa Suomessa toimivista kuriiri- ja jakeluyhtiöistä jää kuitenkin soveltamisalan kokorajauksen myötä todennäköisesti sääntelyn soveltamisalan ulkopuolelle. Postipalvelujen osalta soveltamisalan piiriin kuuluisi Suomesta ainakin postidirektiivin mukaisena postipalvelujen tarjoajana toimiva yleispalvelun tarjoaja, joka tällä hetkellä on Posti Oy. Soveltamisalaan arvioidaan kuuluvan Suomessa Posti Oy:n ohella vain yksittäisiä toimijoita posti- ja kuriiripalveluiden toimialalla. Valvovana viranomaisena toimisi Liikenne- ja viestintävirasto.

Jätehuolto

Jätehuolto on uusi soveltamisala NIS2-direktiivissä. Kyberturvallisuuden riskienhallintaa ja –raportointia koskevat velvoitteet ovat jätehuollon toimijoille uusia ja jätehuollon toimijat uusia valvottavia toimijoita. Jätehuollon toimijoita valvoisi Etelä-Savon elinkeino-, liikenne- ja ympäristökeskus.

Jätehuollon alalla toimii lukuisia erilaisia ja erikokoisia toimijoita. Jätehuollolla tarkoitetaan jätteen keräystä, kuljetusta, hyödyntämistä ja loppukäsittelyä, mukaan lukien tällaisen toiminnan tarkkailu ja seuranta sekä loppukäsittelypaikkojen jälkihoito ja toiminta välittäjänä.

Valtaosa Suomessa toimivista jätteenkäsittelylaitoksista sekä jätteen kuljetusyrityksistä on pieniä paikallisia tai alueellisia yrityksiä, jotka jäävät kokonsa puolesta nyt ehdotettavan sääntelyn ulkopuolelle. Aluehallintoviraston luvittamia tai ELY-keskusten valvomia jätteenkäsittelylaitoksia on arviolta noin 400 kappaletta. Jätteen kuljetusyrityksiä on hyväksyttynä jätelain mukaiseen jätehuoltorekisteriin noin 2000–3000 kappaletta. Näistä suurin osa on soveltamisalan ulkopuolelle jääviä paikallisia tai alueellisia yrityksiä, mutta joukossa on myös toimijoita, jotka täyttävät tai ylittävät soveltamisalan kokokriteerin. Jätehuollon alalla soveltamisalaan arvioidaan kuuluvan joitakin kymmeniä toimijoita kokokriteeri huomioon ottaen.

Kyberturvallisuuden riskienhallinta- ja raportointivelvoitteet olisivat jätehuollon toimijoille uusia. Jätteen käsittelyä koskevaa yleistä varautumissääntelyä on ympäristönsuojelulain 15 ja 52

[2] Postimarkkinaselvitys, Liikenne- ja viestintävirasto (2020).

§:ssä ja ympäristönsuojeluasetuksen 3, 6 ja 16 §:ssä (ennaltavarautumisvelvoite); sekä jätelain 120 §:ssä ja jäteasetuksen 41 §:ssä (jätteen käsittelyn seuranta ja tarkkailusuunnitelma). Säännösten mukaan toiminnan harjoittajien on ennalta varauduttava toimiin onnettomuuksien ja muiden poikkeuksellisten tilanteiden estämiseksi ja niiden terveydelle ja ympäristölle haitallisten seurausten rajoittamiseksi. Aluehallintoviranomaisen luvittaman toiminnanharjoittajan on laadittava riskinarviointiin perustuva varautumissuunnitelma, varattava tarpeelliset laitteet ja muut varusteet, laadittava toimintaohje, testattava laitteet ja varusteet sekä harjoiteltava toimia onnettomuuksia ja muita poikkeuksellisia tilanteita varten. Sääntely ei kuitenkaan erityisesti kohdistu verkko- ja tietoturvakysymyksiin eikä täytä NIS2-direktiivin vaatimuksia.

NIS2-direktiivin soveltamisalaan kuuluvia toimijoita olisivat keskisuuret ja suuremmat toimijat, joiden pääasiallinen toimiala on jätehuolto. Tällaisia yrityksiä Suomessa on tilastokeskuksen ja yritys- ja yhteisötietojärjestelmä YTJ:n mukaan henkilöstön määrän osalta noin 30 kappaletta. Suuriksi yrityksiksi ja siten keskeisiksi toimijoiksi henkilöstön perusteella voidaan luokitella näistä 6 yritystä. Liikevaihdon ja lopputaseen perusteella sääntelyn soveltamisalaan kuuluisi noin 30 yritystä. Joukossa on useita kuntien omistamia yrityksiä tai kuntayhtymiä. Suurimmat toimijat ovat osa yrityskonserneja, jotka voivat kuulua sääntelyn soveltamisalaan myös muun toiminnan kuin jätehuollon osalta.

Kemikaalien valmistus, tuotanto ja jakelu

Kemikaalien valmistus, tuotanto ja jakelu on uusi toimiala NIS-sääntelyn piirissä. Soveltamisalaan kuuluisivat kokokriteerin täyttävät kemikaalien valmistusta sekä niiden jakelua harjoittavat yritykset. Toimijoille lain tasolla asetettavat kyberturvallisuuden riskienhallinta- ja raportointivelvoitteet olisivat uusia ja toimijat uusi valvottava toimijajoukko valvovalle viranomaiselle. Soveltamisalaan uusina kuuluvien toimijoiden joukko olisi määrällisesti merkittävä. Valvovana viranomaisena toimisi Turvallisuus- ja kemikaalivirasto.

Elintarvikkeiden tuotanto, jalostus ja jakelu

Elintarvikkeiden tuotanto, jalostus ja jakelu on uusi toimiala NIS-sääntelyn piirissä. Soveltamisalaan kuuluisivat elintarvikeyritykset, jotka harjoittavat teollista tuotantoa tai jalostusta, jakelua, tukku- ja vähittäiskauppaa. Elintarvikesektorilla Suomessa suurten yritysten rooli on keskeinen sekä valmistavassa teollisuudessa että kaupassa. Sektori on erittäin riippuvainen tuonnista, ja keskinäisriippuvuus muista toimialoista on suurta. Elintarvikesektori on kyberturvan näkökulmasta monimutkainen kokonaisuus: toimipaikkoja on kaikissa maakunnissa, mutta jotkut toimialan yrityksistä (esim. öljyjä tuottavat yritykset) ovat alueellisesti keskittyneitä. Toisaalta pitkien etäisyyksien Suomessa ruokahuoltoa turvaavat hajautettu tuotanto ja suorat toimitukset.

Kyberturvallisuuden riskienhallintaa ja –raportointia koskevat velvoitteet ovat sektorin toimijoille uusia ja elintarvikesektorin toimijat uusia valvottavia toimijoita. Elintarvikesektorin toimijoita valvoisi NIS2-velvoitteiden osalta Ruokavirasto. Elintarvikesektorin toimijoihin kohdistuvaa muuta valvontaa on kunnissa.

Elintarvike- ja juomateollisuudessa lähes 65 %:ssa toimipaikoista työskentelee alle viisi henkilöä (LUKE tilastot). Yli 90%:ssa kaikista toimipaikoista työskentelee vähemmän kuin 20 henkilöä ja yli 200 henkilön toimipaikkoja on 32. (ETL, Tietohaarukka 2021). Näiden tietojen valossa voidaan päätellä, että NIS2-direktiivi koskisi muutamaa kymmentä teollisuusyritystä. Päivittäistavarakaupan myymälöitä on noin 2 800 (Päivittäistavarakauppa 2022). Hypermarkettien määrä on 158, tavaratalojen 88 ja isojen supermarkettien 712. Yksittäisten hypermarkettien liikevaihto ylittää 50 miljoonan euron rajan. Elintarvikesektorilla toiminnan ominaispiirteenä on

toimitus- ja tukkuketjun korostunut rooli toiminnan jatkuvuuden kannalta. Verkkokaupassa on useita toimijoita ja niiden merkitys on kasvussa.

Keskeisiä tukkutoimijoita on seitsemän. Niiden lisäksi alalla toimii useita pieniä tukkumyyjiä. Keskeisistä tukkutoimijoista viisi toimii foodservice eli ruokapalvelusektorilla. Elintarviketeollisuus toimittaa noin 30% foodservice-toimijoiden raaka-aineista. Keskeiset tukkutoimijat tulevat NIS2-soveltamisalaan joko koon perusteella tai siksi, koska ne ovat keskeisiä toimijoita CER-direktiivin perusteella.

Foodservice-toimiala palvelee sekä yksityisen että julkisen puolen ammattikeittiöitä. Suomessa on yli 16 000 ammattikeittiötä, jotka valmistavat noin 749 miljoonaa ateriaa vuodessa. Toimialalle on ominaista, että erikokoisia toimijoita on paljon. Huoltovarmuuden kannalta keskeisiä ruokapalvelutoimijoita on muutama ja niiden toiminnassa tieto- ja kyberturvallisuuden merkitys on erittäin oleellista. Foodservice-tukkureiden mukaan noin 85–90 % julkisista toimijoista tekee elintarviketilauksensa konekielisinä. Foodservice on verkostoitunutta toimintaa, jossa jokaisella on oma roolinsa, jolloin toiminta voi olla altis kyberhäiriöille.

Tarjoiluun liittyvien toimijoiden määrä on suuri, mutta suurin osa toimijoista on ravintoloita. Keskeisiä ammattikeittiöiden toimijoita, jotka perustuvat foodservice-tukkukauppaan, on noin kuusi kappaletta. Näiden lisäksi alalla toimii useita pieniä tukkumyyjiä. Elintarviketeollisuus toimittaa noin 30 % foodservice-toimijoiden raaka-aineista.

Elintarvikevalvontaviranomaisen tiedossa ja valvonnassa olevien elintarvikealan yritysten rakennetta on kuvattu taulukossa x toimipaikkojen perusteella. Elintarvikevalvontaviranomaisen rekisteri perustuu toimipaikkakohtaiseen toimintaan eikä siten ole puhtaasti yritys- tai omistajakohtainen. Elintarvikkeiden tuotannon ja jalostuksen osalta toimipaikat ja toiminnot jaetaan eri riskiluokkiin toimintoihin liittyvien elintarviketurvallisuustekijöiden ja toiminnan volyymin eli tuotannon määrän suhteen. Tuotannon määrä korkeimman riskiluokan osalta on maitoalan laitoksissa kaksi miljoonaa litraa vastaanotettavan maidon osalta. Valtakunnallinen määrä on kaksi miljardia litraa. Liha-, kala- ja muna-alan laitoksissa korkeimman riskiluokan kohteissa tuotannon määrä on yli kymmenen miljoonaa kiloa. Muussa valmistuksessa raja on miljoona kilogrammaa tai 100 miljoonaa litraa. Ammattikeittiöiden osalta keskeisiä ovat ruokapalvelutoimijat, jotka valmistavat ruokaa sairaaloille, vanhainkoteihin ja päiväkoteihin ja jotka tulevat NIS2:n soveltamisen piiriin, koska ovat CER-direktiivin mukaisia kriittisiä toimijoita.

Myynnin osalta korkeimpaan riskiluokkaan kuuluvia kohteita (> 1000 m2) on 483. Näistä on eroteltavissa kuusi tukkuliikettä ja yksi erittäin korkean riskin vähittäismyyntikohde. Elintarvikepakkaukset ovat kriittisen tärkeitä elintarvikkeiden tuotannon, jalostuksen ja jakelun kannalta. Elintarvikevalvontaviranomaisen riskinarvioinnin mukaan korkean riskin elintarvikekontaktimateriaalitoimijoita on viisi kappaletta.

Ehdotuksen soveltamisalaan kuuluisivat yritykset, jotka ovat keskisuuria tai suurempia. Elintarvikevalvonnan viranomaisten rekisterien perusteella näitä yrityksiä arvioidaan elintarvikesektorilla olevan noin 160 kpl. Näistä keskeisten toimijoiden piiriin arvioidaan kuuluvan yhteensä 53 toimijaa.

Taulukko x. Elintarvikevalvontaviranomaisen rekisterissä vuonna 2022 olleiden toimipaikkojen perusteella tehty arvio NIS2-direktiivin mukaisista tärkeistä ja keskeisistä toimijoista

Toimiala	Arvio NIS2 tärkeistä toimijoista	Arvio NIS2 keskeisistä toimijoista
Elintarvikkeiden kuljetukset	7	2
Elintarvikkeiden varastointi ja pakastaminen	10	2
Elintarvikkeiden valmistus, muu kuin maito, liha, kala, muna ja vilja-ala	19	8
Kala-ala	62	5
Liha-ala	24	11
Maitoala	13	2
Muna-ala	7	4
Vienti ja Tuonti	6	2
Vilja-ja kasviala	4	2
Myynti	**-**	**7**
Ruokapalvelutoimijat	-	3
Elintarvikepakkausten valmistus	-	5
Yhteensä	162	53

Valmistussektori

Valmistussektori on uusi soveltamisala NIS2-direktiivissä. Soveltamisalaan kuuluisivat kokokriteerin täyttävät lain liitteessä tarkoitettujen tuotteiden valmistusta harjoittavat yritykset. Toimijoille lain tasolla asetettavat kyberturvallisuuden riskienhallinta- ja raportointivelvoitteet olisivat uusia ja toimijat uusi valvottava toimijajoukko valvovalle viranomaiselle. Soveltamisalaan uusina kuuluvien toimijoiden joukko olisi määrällisesti merkittävä. Valvovana viranomaisena toimisi osin Fimea, osin Liikenne- ja viestintävirasto ja osin Turvallisuus- ja kemikaalivirasto.

Valmistustoimialan osalta soveltamisalaan kuuluisivat keskisuuret tai suuremmat toimijat, jotka harjoittavat seuraavaa toimintaa:

Lääkinnälliset laitteet	Lääkinnällisten laitteiden ja in vitro -diagnostiikkaan tarkoitettujen lääkinnällisten laitteiden valmistus
Tietokoneiden sekä elektronisten ja optisten	NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 26 tarkoitettua taloudellista toimintaa harjoittavat yritykset: Tietokoneiden sekä elektronisten ja optisten tuotteiden valmistus Elektronisten komponenttien ja piirilevyjen valmistus

tuotteiden valmistus	Elektronisten komponenttien valmistus Kalustettujen piirilevyjen valmistus Tietokoneiden ja niiden oheislaitteiden valmistus Tietokoneiden ja niiden oheislaitteiden valmistus Viestintälaitteiden valmistus Viestintälaitteiden valmistus Viihde-elektroniikan valmistus Viihde-elektroniikan valmistus Mittaus-, testaus- ja navigointivälineiden ja -laitteiden valmistus; kellot Mittaus-, testaus- ja navigointivälineiden ja -laitteiden valmistus Kellojen valmistus Säteilylaitteiden sekä elektronisten lääkintä- ja terapialaitteiden valmistus Säteilylaitteiden sekä elektronisten lääkintä- ja terapialaitteiden valmistus Optisten instrumenttien ja valokuvausvälineiden valmistus Optisten instrumenttien ja valokuvausvälineiden valmistus Tallennevälineiden valmistus Tallennevälineiden valmistus
Sähkölaitteiden valmistus	NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 27 tarkoitettua taloudellista toimintaa harjoittavat yritykset: Sähkölaitteiden valmistus Sähkömoottorien, generaattorien, muuntajien sekä sähkönjakelu- ja valvontalaitteiden valmistus Sähkömoottorien, generaattorien ja muuntajien valmistus Sähkönjakelu- ja valvontalaitteiden valmistus Paristojen ja akkujen valmistus Paristojen ja akkujen valmistus Sähköjohtojen ja kytkentälaitteiden valmistus Optisten kuitukaapelien valmistus Muiden elektronisten ja sähköjohtojen sekä -kaapelien valmistus Kytkentälaitteiden valmistus Sähkölamppujen ja valaisimien valmistus Sähkölamppujen ja valaisimien valmistus Kodinkoneiden valmistus Sähköisten kodinkoneiden valmistus Sähköistämättömien kodinkoneiden valmistus Muiden sähkölaitteiden valmistus Muiden sähkölaitteiden valmistus
Muiden koneiden ja laitteiden valmistus	NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 28 tarkoitettua taloudellista toimintaa harjoittavat yritykset: Muiden koneiden ja laitteiden valmistus Yleiskäyttöön tarkoitettujen voimakoneiden valmistus Moottorien ja turbiinien valmistus (pl. lentokoneiden ja ajoneuvojen moottorit) Hydraulisten voimalaitteiden valmistus Pumppujen ja kompressoreiden valmistus

	Muiden hanojen ja venttiilien valmistus Laakereiden, hammaspyörien, vaihteisto- ja ohjauselementtien valmistus Muiden yleiskäyttöön tarkoitettujen koneiden valmistus Teollisuusuunien, lämmitysjärjestelmien ja tulipesäpolttimien valmistus Nosto- ja siirtolaitteiden valmistus Konttorikoneiden ja -laitteiden valmistus (pl. tietokoneet ja niiden oheislaitteet) Voimakäyttöisten käsityökalujen valmistus Muuhun kuin kotitalouskäyttöön tarkoitettujen jäähdytys- ja tuuletuslaitteiden valmistus Muualla luokittelematon yleiskäyttöön tarkoitettujen koneiden valmistus Maa- ja metsätalouskoneiden valmistus Maa- ja metsätalouskoneiden valmistus Metallin työstökoneiden ja konetyökalujen valmistus Metallin työstökoneiden valmistus Muiden konetyökalujen valmistus Muiden erikoiskoneiden valmistus Metallinjalostuskoneiden valmistus Kaivos-, louhinta- ja rakennuskoneiden valmistus Elintarvike-, juoma- ja tupakkateollisuuden koneiden valmistus Tekstiili-, vaate- ja nahkateollisuuden koneiden valmistus Paperi-, kartonki- ja pahviteollisuuden koneiden valmistus Muovi- ja kumiteollisuuden koneiden valmistus Muualla luokittelematon erikoiskoneiden valmistus
Moottoriajoneuvojen, perävaunujen ja puoliperävaunujen valmistus	NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 29 tarkoitettua taloudellista toimintaa harjoittavat yritykset: Moottoriajoneuvojen, perävaunujen ja puoliperävaunujen valmistus Moottoriajoneuvojen valmistus Moottoriajoneuvojen valmistus Moottoriajoneuvojen korien valmistus; perävaunujen ja puoliperävaunujen valmistus Moottoriajoneuvojen korien valmistus; perävaunujen ja puoliperävaunujen valmistus Osien ja tarvikkeiden valmistus moottoriajoneuvoihin Sähkö- ja elektroniikkalaitteiden valmistus moottoriajoneuvoihin Muiden osien ja tarvikkeiden valmistus moottoriajoneuvoihin
Muiden kulkuneuvojen valmistus	NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 30 tarkoitettua taloudellista toimintaa harjoittavat yritykset: Muiden kulkuneuvojen valmistus Laivojen ja veneiden rakentaminen Laivojen ja kelluvien rakenteiden rakentaminen Huvi- ja urheiluveneiden rakentaminen Raideliikenteen kulkuneuvojen valmistus Raideliikenteen kulkuneuvojen valmistus Ilma- ja avaruusalusten ja niihin liittyvien koneiden valmistus Ilma- ja avaruusalusten ja niihin liittyvien koneiden valmistus Taisteluajoneuvojen valmistus Taisteluajoneuvojen valmistus

	Muualla luokittelematon kulkuneuvojen valmistus Moottoripyörien valmistus Polkupyörien ja invalidiajoneuvojen valmistus Muiden muualla luokittelemattomien kulkuneuvojen valmistus

Valmistussektorin alaan kuuluvaa toimintaa harjoittavia yrityksiä olisi huomattava määrä. Soveltamisalaan kuuluville toimijoille lain tasolla asetettavat kyberturvallisuuden riskienhallinta- ja raportointivelvoitteet olisivat uusia. Valmistussektorin jatkuva digitalisaatio on johtanut yhä kasvavaan kyberhyökkäyspinta-alaan ja toimijoiden tarpeeseen kehittää kyberturvallisuuden riskienhallintaa ja häiriötilanteisiin varautumista oma-aloitteisesti. Valmistustoimintaa harjoittavista yrityksistä merkittävä osa on myös kooltaan pienyrityksiä siten, että ne jäävät soveltamisalan kokokriteerin alapuolelle.

Tutkimusorganisaatiot

Tutkimusorganisaatiot eivät kuuluneet NIS1-direktiivin soveltamisalaan. NIS2-direktiivin mukaan tutkimusorganisaatiolla tarkoitetaan sellaista toimijaa, jonka ensisijaisena tavoitteena on harjoittaa soveltavaa tutkimusta tai kokeellista kehitystyötä kyseisen tutkimuksen tulosten hyödyntämiseksi kaupallisiin tarkoituksiin mutta joka ei ole opetus- ja koulutusalan laitos. Määritelmän mukaiseen soveltamisalaan on kansallisesti tunnistettu kuuluvan vain yksittäisiä toimijoita. Toimijoille lain tasolla asetettavat kyberturvallisuuden riskienhallinta- ja raportointivelvoitteet olisivat uusia. Valvovana viranomaisena toimisi Liikenne- ja viestintävirasto.

Julkishallinto

Julkishallinnon toimijat tulisivat uutena toimijatyyppinä NIS-velvoitteiden soveltamisalaan, sillä julkishallinto ei ole kuulunut NIS1-direktiivin soveltamisalaan. Julkishallinnon toimijoihin ei sovellettaisi kokokriteeriä ja soveltamisala määräytyisi julkisen hallinnon tiedonhallinnasta annetussa laissa säädetyn mukaisesti. Velvoitteet olisivat julkishallinnolle uusia ja niiden valvominen uusi tehtävä. Valvovana viranomaisena toimisi Liikenne- ja viestintävirasto.

Julkishallinnon toimijoina tiedonhallintalain soveltamisalan kautta NIS2-velvoitteiden alaan tulisi yhteensä noin 160 toimijaa. Luku sisältää valtion keskushallinnon, virastot ja laitokset, valtion liikelaitokset sekä itsenäiset julkisoikeudelliset laitokset ja hyvinvointialueet ja –yhtymät mukaan luettuna Helsingin kaupungin. Jos ulkomaanedustustot lasketaan mukaan erillisinä toimijoina, julkishallinnon sektorin toimijoiden kokonaismäärä on noin 250 toimijaa.

4.2.3 Pääasialliset vaikutukset verkkotunnusvälittäjiin

Verkkotunnusten välittäminen ei kuulu NIS2-direktiivin riskienhallinta- ja raportointivelvoitteiden piiriin, ellei toimija tarjoa myös jotain muuta soveltamisalan piiriin kuuluvaa palvelua, kuten DNS-palveluja. Verkkotunnusvälittäjille asetetaan kuitenkin eräitä muita velvoitteita, joilla on vaikutuksia niiden toimintaan, joista keskeisimpänä velvollisuus laatia ja julkaista verkkotunnusrekisterin tietojen oikeellisuuden varmistamista sekä verkkotunnusten rekisteröintitietojen luovuttamista koskevat toimintaperiaatteet ja menettelyt. Lisäksi verkkotunnusvälittäjien olisi asetettava julkisesti saataville muut verkkotunnuksen rekisteröintitiedot kuin henkilötiedot sekä vastattava rekisteritietoihin pääsyä pyytävälle ilman aiheetonta viivytystä ja viimeistään 72 tunnin kuluessa siitä, kun verkkotunnusvälittäjä on vastaanottanut lainmukaisen ja asianmukaisesti perustellun pyynnön.

Velvoite julkaista verkkotunnuksen rekisteröintitietoja voi edellyttää toimijoilta järjestelmäkehitystä rekisteritietojen julkaisemisen tekniseksi toteuttamiseksi. Verkkotunnusrekisterin tietojen oikeellisuuden varmistamiseen liittyvillä ehdotuksilla ei arvioida olevan merkittäviä vaikutuksia verkkotunnusvälittäjiin, sillä toimijoilla on jo nykyään laissa säädetty velvollisuus merkitä verkkotunnusrekisteriin verkkotunnuksen käyttäjää koskevat oikeat, ajantasaiset ja yksilöivät tiedot. Ehdotuksilla voi kuitenkin olla erityisesti kertaluonteisia vaikutuksia sääntelyn soveltamisen alkaessa.

4.3 Taloudelliset vaikutukset

Vaikutukset yrityksiin

Esityksellä katsotaan olevan taloudellisia vaikutuksia soveltamisalaan kuuluville yrityksille erityisesti riskienhallinta- ja raportointivelvoitteiden sekä toimijaluetteloon ilmoittautumisen kautta. Esitys lisää soveltamisalan toimijoiden kustannuksia ja hallinnollista taakkaa, mutta kyberturvallisuuden parantumisella nähdään olevan myös positiivisia vaikutuksia sekä yritysten liiketoimintaedellytyksille, että kansantaloudelle ja yhteiskunnan kriisinkestävyydelle. Kyberturvallisuuden riskienhallintaan investoiminen parantaa soveltamisalaan kuuluvien yritysten toimintavarmuutta ja edistää liiketoimintaa digitalisoituvassa yhteiskunnassa. Kyberturvallisuushäiriöiden vähentyminen säästäisi toimijoita häiriöiden haitallisista vaikutuksista aiheutuvilta kustannuksilta.

Esityksellä katsotaan olevan kustannusvaikutuksia yrityksille erityisesti riskienhallintaa koskevan velvoitteen kautta. Riskienhallintavelvoitteista aiheutuvien kustannuksien lisäksi toimijoille aiheuttavat vähäisiä kustannuksia raportointivelvoite merkittävistä poikkeamista ja ilmoittautumisvelvoite valvovan viranomaisen ylläpitämään toimijaluetteloon. Näistä aiheutuvat kustannukset arvioidaan kokonaisuudessaan vähäiseksi suhteessa riskienhallintaan ja riskienhallintatoimenpiteiden toteuttamiseen. Kustannuksia yrityksille voi aiheutua myös valvovan viranomaisen yritykseen kohdistamista valvontatoimenpiteistä.

Riskienhallinnasta ja riskienhallintatoimenpiteistä aiheutuvat kustannukset voidaan jakaa kertaluonteisiin ja jatkuviin kustannuksiin. Esityksestä aiheutuvien kustannuksien määrään vaikuttavat yrityksessä ennalta toteutetun kyberturvallisuuden riskienhallinnan taso, toiminnan laatu ja laajuus sekä toiminnassa käytettävien viestintäverkkojen ja tietojärjestelmien määrä ja laatu.

Yleisesti IT-kustannukset ovat keskimäärin n. 4−5 % yrityksen liikevaihdosta. Vaihteluväli on toimijan koosta, kybermaturiteetista ja sektorista riippuen 1,5−5%. Esimerkiksi elintarvikesektorilla arvioitiin kyberturvallisuuskustannuksiksi keskimäärin 0,28 % vuotuisesta liikevaihdosta ja valmistussektorilla 0,69 % vuotuisesta liikevaihdosta.[3] Komission arvion mukaan kyberturvallisuuskustannusten on arvioitu olevan keskimäärin eri toimialoilla 0,52 % vuotuisesta liikevaihdosta.

[3] [3] Insta (2023) Selvitys kyberturvallisuusdirektiivin (NIS2-direktiivi) riskienhallintavelvoitteiden taloudellisista vaikutuksista elintarvike- ja valmistussekotoreille

Komission arvion mukaan NIS2-direktiivin mukaisilla velvoitteilla arvioidaan olevan ensimmäisten toimeenpanovuosien aikana soveltamisalaan kuuluvan toimijan nykyisiä kyberturvallisuuteen liittyviä IT-kustannuksia keskimäärin 12–22 % korottava vaikutus riippuen siitä, onko velvoitteiden kohteena oleva toimija kuulunut NIS1-direktiivin soveltamisalaan.[4]

Kyberturvallisuuden varmistamisen kustannukset lukeutuvat useimmiten laajemmin toimijoiden ICT-kokonaiskustannuksiin, jolloin puhtaasti kyberturvallisuuteen liittyviä kustannuksia on vaikea erotella ja erotteleminen on usein tulkinnanvaraista. Kyberturvallisuuskustannuksiin voidaan lukea laajasti erilaisia menolajeja, kuten laitteistot, ohjelmistot ja tietoliikenneyhteydet. Muita kyberturvallisuutta edistäviä kustannuksia voi olla hallinnolliset kulut, henkilöstökulut, erilaiset auditoinnit ja koulutukset. Lisäksi on huomioitava direktiivin velvoitteet huolehtia verkko- ja tietojärjestelmien fyysisestä turvallisuudesta, josta voi aiheutua esimerkiksi erilaisten laitteistojen ja kaapeleiden asennus- ja ylläpitokuluja. Kyberhyökkäyksillä ja –häiriöillä sekä muilla tietoturva- tai tietosuojaloukkauksilla voi olla merkittäviä negatiivisia taloudellisia vaikutuksia sekä tietojärjestelmän tai viestintäverkon välityksellä palveluja tarjoavalle yritykselle että palveluja käyttäville tahoille. Kyberhäiriöistä aiheutuvia kustannuksia voidaan arvioida karkeasti sen pohjalta, mitä tosiasialliset kyberhäiriötilanteet ovat toimijoille kustantaneet. Häiriötilanteiden kustannuksiin vaikuttavat monet eri tekijät, kuten häiriön laatu, laajuus, vaikutukset toimijan ja sektorin toiminnan jatkuvuuteen sekä miten nopeasti toimija toipuu häiriöstä. Häiriötilanteista voi aiheutua sekä suoria selvitys- ja korjauskustannuksia, että epäsuoria kustannuksia esimerkiksi toiminnan keskeytymisen tai mainehaitan vuoksi. Eksponentiaalisesti lisääntyneiden kyberhäiriöiden vuoksi niiden aiheuttamat kustannukset ovat myös kokonaisuudessaan kasvaneet. Esimerkiksi vuonna 2019 Lahden kaupunkiin kohdistuneen kyberhyökkäyksen suorat kustannukset olivat 685 670 euroa.[5] Vuonna 2020 SolarWinds –yrityksen Orion Platform hallintatyökaluun kohdistunut haittaohjelma levisi tuhansiin organisaatioihin. Kyberhyökkäyksen vaikutukset olivat keskimäärin 11 % vuotuisesta liikevaihdosta tai noin 12 miljoonaa dollaria yritystä kohden. [6] Solarwinds -yritykselle koitui tapauksesta vuoden 2021 aikana ainakin 40 miljoonan dollarin kustannukset. Tämän lisäksi yritykselle arvioitiin aiheutuvan merkittävä mainehaitta, joten kustannusten voidaan arvioida olevan paljon suuremmat.[7] Voidaan karkeasti todeta, että erilaisista kyberhäiriöistä aiheutuvat kustannukset olisivat yleisesti merkittävästi suurempia kuin puhtaasti esityksen velvoitteiden mukaisesta kyberturvallisuuden riskienhallinnasta aiheutuvat kustannukset. Mikäli yritys torjuu kyberturvallisuuden riskienhallinnan avulla kyberturvallisuushäiriöstä aiheutuvia haitallisia vaikutuksia, on tällä positiivinen taloudellinen vaikutus yritykselle. Komissio on arvioinut EU:n tasolla kyberturvallisuushäiriöistä ja –kriiseistä aiheutuneiksi kustannuksiksi yhteensä 118 miljardia euroa kymmenen vuoden ajanjakson aikana.

Esityksellä voidaan nähdä olevan yritysten kilpailukykyä positiivisesti edistäviä vaikutuksia, kun esitys velvoittaa direktiivin piiriin kuuluvia yrityksiä ylläpitämään korkeaa kyberturvallisuuden tasoa. Esityksellä velvoitetaan yrityksiä myös huomioimaan toimitusketjujen kybertur-

[4] Kooste komission vaikutusarvioinnista NIS2-direktiivin antamisen yhteydessä: SWD(2020) 344 final https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2020:0344:FIN:EN:PDF
[5] YLE (2019) Kyberhyökkäys on maksanut Lahden kaupungille lähes 690 000 euroa https://yle.fi/a/3-10914550
[6] Cybersecurity Impact Report 2021 https://www.ironnet.com/resource-library/2021-cybersecurity-impact-report
[7] Cybersecurity Dive (2021) One year later: has SolarWinds changed how industry builds software? https://www.cybersecuritydive.com/news/solarwinds-1-year-later-cyber-attack-orion/610990/

vallisuus, jolloin kyberturvallisuudestaan riittävällä tasolla huolehtiva yritys on todennäköisempi yhteistyökumppani ja kuluttajan valinta. Esimerkiksi SolarWinds –yritykseen kohdistunut haittaohjelma vaikutti yhtiön toimintaketjussa myös muihin toimijoihin, joihin kohdistui myös korjaustoimenpiteistä aiheutuvia kustannuksia.

Liikenne- ja viestintäministeriö hankki esityksen valmistelun yhteydessä selvityksen NIS2-direktiivin 21 artiklan mukaisen riskienhallintavelvoitteen kustannuksista suomalaisille yrityksille. Selvityksen kohteena oli arvioida direktiivin mukaisen riskienhallintavelvoitteen kustannuksia elintarvike- ja valmistussektoreilla, koska näillä toimialoilla yritykset eivät olleet kuuluneet NIS1-direktiivin soveltamisalaan ja toimialoilla huomattava lukumäärä esityksen myötä soveltamisalaan uutena tulevia yrityksiä. Selvityksen toteutti Insta Advance Oy (jäljempänä ”Insta”). Selvitys on saatavilla valtioneuvoston hankeikkunasta hanketunnuksella LVM0044:00/2022 (linkki: https://valtioneuvosto.fi/hanke?tunnus=LVM044:00/2022).

Selvitys on toteutettu perustuen NIS2-direktiivin 21 artiklaan riskienhallinnassa ja riskienhallintatoimenpiteissä huomioitavista osa-alueista. Kyberturvallisuuden riskienhallinnassa annetussa laissa ehdotetun 7–9 §:n nojalla riskienhallinnassa huomioitavat osa-alueet vastaavat NIS2-direktiivin 21 artiklaa.

Selvityksen perusteella riskienhallintavelvoitteesta aiheutuu elintarvike- ja valmistussektorin yrityksille yrityskohtaisesti kertaluontoisia kustannuksia keskimäärin noin 320.000 euroa, joista 27 % on työkustannuksia ja 73 % muita kustannuksia. Jatkuvaluonteisia kustannuksia aiheutuu keskimäärin noin 214.000 euroa, joista 26 % on työkustannuksia ja 74 % muita kustannuksia. Elintarvikesektorilla kustannuksia arvioitiin olevan keskimäärin vähemmän kuin valmistussektorilla. Elintarvikesektorilla kertaluonteisia kustannuksia arvioitiin olevan 274.000 euroa ja jatkuvaluonteisia kustannuksia 148.000 euroa. Valmistussektorilla kertaluonteisia kustannuksia arvioitiin olevan 367.000 euroa ja jatkuvaluonteisia kustannuksia 279.000 euroa.

Riskienhallinnassa huomioitavista osa-alueista kustannuksia arvioitiin liittyvän riskienhallinnassa huomioitaviin osa-alueisiin riskianalyysejä ja tietojärjestelmien turvallisuutta koskevista politiikoista, poikkeamien käsittelystä, toimitusketjun turvallisuuden varmistamisesta sekä viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuudesta. Kustakin riskienhallinnassa huomioitavasta osa-alueesta arvioitiin aiheutuvan kertaluontoisia kustannuksia vaihteluvälillä 12.100 – 52.900 euroa ja jatkuvia kustannuksia vaihteluvälillä 4.500 – 39.500 euroa.

Selvityksessä pyrittiin arvioimaan myös riskienhallintavelvoitteista aiheutuvia kustannushyötyjä yrityksille. Selvityksen perusteella mahdollisten kustannushyötyjen euromääräiseen arviointiin liittyy niin suuria epävarmuuksia, etteivät yritykset pääosin kyenneet esittämään niistä arvioita. Yritysten vastauksissa toistui kuitenkin näkemys siitä, että kyberturvallisuustason paranemisella on väistämättä merkittäviä positiivisia liiketaloudellisia vaikutuksia ja kyberturvallisuuteen liittyvät vaatimukset näkyvät yritysten mukaan liiketoiminnassa monin tavoin. Kustannushyötyjen nähtiin liittyvän erityisesti asiakkaiden luottamuksen lisääntymiseen ja kyberhyökkäyksien vaikeutumiseen ja niistä aiheutuvien haitallisten vaikutusten vähentymiseen.

Ehdotuksen mukaan toimijoiden olisi tunnistettava kaikki vaaratekijät huomioivan lähestymistavan mukaisesti viestintäverkkoihin ja tietojärjestelmiin ja niiden fyysiseen ympäristöön kohdistuvat riskit sekä toteutettava ajantasaiset, oikeasuhtaiset ja riittävät riskienhallintatoimenpiteet. Toimijalla olisi oltava käytössään riskienhallinnan toimintamalli ja toimintamallissa sekä siihen perustuvissa hallintatoimenpiteissä olisi huomioitava ja ylläpidettävä ajantasaisena vähintään NIS2-direktiivin 21 artiklan mukaiset osa-alueet. Toimenpiteiden riittävyyttä olisi arvioitava suhteessa toimintaan kohdistuviin riskeihin, toimijan kokoon ja yleiseen alistumiseen

kyberturvallisuusriskeille eli poikkeamien esiintymisen todennäköisyydelle sekä vakavuudelle ottaen huomioon niiden yhteiskunnalliset ja taloudelliset vaikutukset. Riskienhallinnassa ei edellytetä kaikilta toimijoilta samanlaisia toimenpiteitä, vaan niitä on arvioitava riskiperusteisesti.

Seuraavaksi kuvataan NIS2-direktiivin 21 artiklan mukaisten riskienhallinnan osa-alueiden mukaisesti jaoteltuna riskienhallinnasta arvioituja kustannuksia toimijoille elintarvike- ja valmistussektoreilla.

1. Riskianalyysi ja tietojärjestelmien turvallisuus

NIS2-direktiivin 21 artiklan 2 kohdan a alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteisiin on sisällytettävä riskianalyyseja sekä tietojärjestelmien turvallisuutta koskevat politiikat. Direktiivissä ei määritellä yksityiskohtaisesti, mitä politiikkoja yritysten on vähintään laadittava.

Selvityksen mukaan elintarvikesektorilla yritysten arvio velvoitteen sopeutumiseen käytettävistä kertaluonteisia henkilötyöpäivistä oli 10-20 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen sopeutumiseen kertaluonteisesti käytettävien muiden kustannusten määrän olevan 30 001-50 000 euroa. Jatkuvaluonteisia muita kustannuksia arvioitiin olevan korkeintaan 5 000- 15 000 euroa, mutta monet yritykset arvioivat myös, että jatkuvaluonteisia muita kustannuksia ei velvoitteen täyttämisestä synny. Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 32 000 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 11 400 euroa vuosittain tämän jälkeen.

Selvityksen mukaan valmistussektorilla yritysten arvio velvoitteen sopeutumiseen käytettävistä kertaluonteisia henkilötyöpäivistä oli 21-50 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan 10-20 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen sopeutumiseen kertaluonteisesti käytettävien muiden kustannusten määrän olevan 5 000-30 000 euroa. Jatkuvaluonteisia muita kustannuksia arvioitiin olevan korkeintaan 5 000- 30 000 euroa. Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 52 900 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 36 900 euroa vuosittain tämän jälkeen.

Esitetyt luvut perustuvat yritysten omaan arvioon tarvittavan dokumentaation laajuudesta. Toimialasta, liiketoimintaympäristöstä ja dokumentoinnin nykytilasta riippuen tarvittavan työmäärän ja kustannusten arvioissa voi olla merkittäviä eroja eri yritysten välillä.

2. Poikkeamien käsittely

NIS2-direktiivin 21 artiklan 2 kohdan b alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteisiin on sisällytettävä poikkeamien käsittely, joilla tunnistetaan poikkeamariskit, ehkäistään, havaitaan ja hallitaan poikkeamia, palaudutaan niistä ja lievennetään niiden vaikutuksia. Poikkeamalla tarkoitetaan tapahtumaa, joka vaarantaa verkko- ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden.

Asiantuntijoiden arvion mukaan tavoitteen täyttämisessä voidaan sääntelyn kohteena olevan toimijan riskianalyysin mukaisesti ottaa huomioon erilaisia teknisiä ratkaisuja havainnointikyvykkyyden parantamiseksi, kuten keskitetty lokienhallinta, poikkeamien tunnistamiseen käytettävät SIEM-järjestelmät (Security Information and Event Management) ja päätelaitteiden suojausratkaisut, kuten EDR (Endpoint Detection and Response). Lisäksi yrityksen tulisi tunnistaa käytössään olevat verkot, niihin liitetyt ICT-palvelut, -tuotteet ja -laitteet sekä niiden kautta kulkeva liikenne. Yrityksellä tulisi olla käytössä poikkeama- ja häiriötilanteisiin prosessit, jotka kattavat näiden tilanteiden tunnistamisen ja niiden aikana toimimisen sekä toimintatavat poikkeamista viestimiseen sisäisesti, asiakkaille ja viranomaisille (Insta 2023).

Selvityksen mukaan elintarvikesektorilla yritysten arvio velvoitteen sopeutumiseen käytettävistä kertaluonteisia henkilötyöpäivistä oli 10-20 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen sopeutumiseen kertaluonteisesti käytettävien muiden kustannusten määrän olevan 30 001-50 000 euroa. Jatkuvaluonteisia muita kustannuksia arvioitiin olevan korkeintaan 5 000- 15 000 euroa.

Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 47 200 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 19 700 euroa vuosittain tämän jälkeen.

Selvityksen mukaan valmistussektorilla yritysten arvio velvoitteen sopeutumiseen käytettävistä kertaluonteisia henkilötyöpäivistä oli 21-50 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan 10-20 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen sopeutumiseen kertaluonteisesti käytettävien muiden kustannusten määrän olevan 5 000-15 000 euroa. Jatkuvaluonteisia muita kustannuksia arvioitiin olevan korkeintaan 15 001- 30 000 euroa. Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 43 200 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 39 500 euroa vuosittain tämän jälkeen.

3. Toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu sekä kriisinhallinta

NIS2-direktiivin 21 artiklan 2 kohdan c alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteisiin on sisällytettävä toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisinhallinta.

Asiantuntijoiden arvion mukaan toiminnan jatkuvuuden hallinnan sekä kriisinhallinnan hallintatoimenpiteisiin voi sisältyä muun muassa ICT-tuotteet ja -palvelut kattavat jatkuvuus ja toipumissuunnitelmat, ICT-tuotteiden ja -palveluiden palautumisen testauksen määrittäminen osaksi edellisiä suunnitelmia sekä ICT-tuotteiden ja -palveluiden palautumisen ja kyberturvallisuuspoikkeamien aikaisen toiminnan säännöllinen harjoitteleminen.

Selvityksen mukaan elintarvikesektorilla yritysten arvio velvoitteen sopeutumiseen käytettävistä kertaluonteisia henkilötyöpäivistä oli 10-20 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen sopeutumiseen kertaluonteisesti käytettävien muiden kustannusten määrän olevan 15 001-30 000 euroa. Jatkuvaluonteisia muita kustannuksia arvioitiin olevan korkeintaan 5 000- 15 000 euroa.

Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 31 200 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 19 400 euroa vuosittain tämän jälkeen.

Selvityksen mukaan valmistussektorilla yritysten arvio velvoitteen sopeutumiseen käytettävistä kertaluonteisia henkilötyöpäivistä oli 10-20 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan 10-20 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen sopeutumiseen kertaluonteisesti käytettävien muiden kustannusten määrän olevan 5 000-15 000 euroa. Jatkuvaluonteisia muita kustannuksia arvioitiin olevan korkeintaan 15 001- 30 000 euroa.

Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 32 100 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 29 500 euroa vuosittain tämän jälkeen.

4. Toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat

NIS2-direktiivin 21 artiklan 2 kohdan d alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteissä on otettava huomioon toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat.

NIS2-direktiivin johdanto-osan 85 kohdan mukaan yritysten olisi arvioitava ja otettava huomioon toimittajiensa tuotteiden ja palveluntarjoajiensa palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet ja toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt, mukaan lukien tuotekehityksen suojausmenettelyt. Keskeisiä ja tärkeitä toimijoita olisi erityisesti kannustettava sisällyttämään kyberturvallisuusriskien hallintatoimenpiteitä sopimusjärjestelyihin, joita ne tekevät välittömien toimittajiensa ja palveluntarjoajiensa kanssa. Kyseiset toimijat voisivat käsitellä myös alemman tason toimittajistaan ja palveluntarjoajistaan johtuvia riskejä.

Täyttääkseen toimitusketjujen turvallisuutta koskevan velvoitteen yritysten tulisi asiantuntijoiden arvion mukaan yrityksen toimintaympäristö huomioiden määritellä roolit, vastuut ja valtuudet kyberturvallisuudelle sekä yrityksen sisällä, että koko toimitusketjussa. Lisäksi yritysten tulisi ylläpitää toimitusketjusta kuvausta, joka sisältää riippuvuudet, haavoittuvuudet, uhat ja riskien vaikutukset. Kuvauksen tulisi kattaa myös palveluntarjoajien ja toimittajien keskeiset alihankkijat. Yritysten tulisi myös valvoa ICT-tuotteiden ja –palveluiden kyberturvallisuutta koko niiden elinkaaren ajan sekä tehdä yhteistyötä sisäisten ja ulkoisten sidosryhmien kanssa jakamalla tietoa sekä parhaita käytänteitä. (Insta 2023).

Selvityksen mukaan elintarvikesektorilla yritysten arvio velvoitteen sopeutumiseen käytettävistä kertaluonteisia henkilötyöpäivistä oli 10-20 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen sopeutumiseen kertaluonteisesti käytettävien muiden kustannusten määrän olevan 5 000-15 000 euroa. Jatkuvaluonteisia muita kustannuksia velvoitteen ei arvioitu aiheuttavan.

Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 39 100 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 23 200 euroa vuosittain tämän jälkeen.

Selvityksen mukaan valmistussektorilla yritysten arvio velvoitteen sopeutumiseen käytettävistä kertaluonteisia henkilötyöpäivistä oli 10-100 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen sopeutumiseen kertaluonteisesti käytettävien muiden kustannusten määrän olevan 5 000-15 000 euroa. Jatkuvaluonteisia muita kustannuksia arvioitiin olevan korkeintaan 5 000-15 000 euroa, mutta yhtä monet myös arvioivat, että jatkuvaluonteisia kustannuksia ei synny tai niiden summa on alle 5 000 euroa.

Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 46 500 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 31 700 euroa vuosittain tämän jälkeen.

5. Verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen

NIS2-direktiivin 21 artiklan 2 kohdan e alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteisiin on sisällytettävä verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen.

NIS2-direktiivin johdanto-osan 80 kohdan mukaan jäsenvaltioiden olisi edistettävä asiaa koskevien eurooppalaisten ja kansainvälisten standardien käyttöä keskeisten ja tärkeiden toimijoiden keskuudessa tai ne voivat vaatia toimijoita käyttämään sertifioituja TVT-tuotteita, TVT-palveluja ja TVT-prosesseja. Lisäksi johdanto-osan 78 kohdan mukaan verkko- ja tietojärjestelmien turvallisuuden olisi katettava säilytettävien, siirrettävien ja käsiteltävien tietojen turvallisuus. Kyberturvallisuusriskien hallintatoimenpiteisiin olisi kuuluttava järjestelmäanalyysi, jossa otetaan huomioon inhimilliset tekijät, jotta saadaan täydellinen kuva verkko- ja tietojärjestelmän turvallisuudesta.

Asiantuntija-arvion mukaan yritysten tulisi ottaa huomioon, onko niillä käytössä hankintojen vaatimusmäärittely ja seurataanko toimittajien vaatimustenmukaisuutta säännöllisesti. Yritysten tulisi ottaa huomioon toimittajien sertifikaatit sekä ICT-tuotteiden ja palveluiden kohdalla tietoturvaan liittyvät viitekehykset, kun ne arvioivat toimittajia sekä ICT-tuotteita ja –palveluita.

Verkko- ja tietojärjestelmien turvallisuutta arvioitaessa tulisi Instan asiantuntijoiden arvion mukaan huomioida myös inhimilliset uhkatekijät esimerkiksi käytettävyystestauksen, käyttötapauskuvausten ja tehtävien eriyttämisen kautta. Lisäksi velvoitteen täyttämiseen vaikuttaa se, saadaanko ja seurataanko toimittajilta sekä ICT-tuotteista ja -palveluista saatuja tietoturvapoikkeamatiedotteita. Verkko- ja tietojärjestelmien kehittämisen kannalta yrityksellä tulisi olla käytössä turvallisen ohjelmistokehityksen prosessi ja sitä tulisi valvoa.

Selvityksen mukaan elintarvikesektorilla yritysten arvio velvoitteen sopeutumiseen käytettävistä kertaluonteisia henkilötyöpäivistä oli 10-20 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat, että velvoitteen sopeutumisesta ei aiheudu kertaluonteisia tai jatkuvaluonteisia muita kustannuksia.

Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 30 800 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 21 900 euroa vuosittain tämän jälkeen.

Selvityksen mukaan valmistussektorilla yritysten arvio velvoitteen sopeutumiseen käytettävistä kertaluonteisia henkilötyöpäivistä oli 10-20 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan korkeintaan 10-20 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen sopeutumiseen kertaluonteisesti käytettävien muiden kustannusten määrän olevan 5 000-30 000 euroa, mutta monet arvioivat myös, että velvoitteen täyttämisestä ei aiheudu muita kertaluonteisia kustannuksia. Jatkuvaluonteisia muita kustannuksia ei arvioitu aiheutuvan.

Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 34 200 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 25 100 euroa vuosittain tämän jälkeen.

6. Toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta

NIS2-direktiivin 21 artiklan 2 kohdan f alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteisiin on sisällytettävä toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta.

Asiantuntijoiden arvion mukaan tämän velvoitteen täyttäminen vaatii yrityksen toiminnasta riippuen sekä yleisiä että hallintakeinokohtaisia mittareita, joilla tietoturvan tehokkuutta voidaan mitata. Yrityksen olisi myös seurattava mittareita säännöllisesti. Lisäksi mittaustulokset tulisi arvioida ja raportoida johdolle. Hallintatoimenpiteiden tehokkuuden arvioinnin toimintaperiaatteisiin ja menettelyihin liittyvät myös jatkuvan parantamisen käytänteet, joiden avulla suunnitellaan ja toteutetaan kehittämistoimenpiteitä mittaustulosten pohjalta. Yritysten tulisi myös arvioida ja ottaa huomioon toiminnassaan hallintatoimenpiteiden toteuttamisen jälkeinen jäännösriski. (Insta 2023).

Selvityksen mukaan elintarvikesektorilla yritysten arvio velvoitteen sopeutumiseen käytettävistä kertaluonteisia henkilötyöpäivistä oli alle 10 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen sopeutumiseen kertaluonteisesti käytettävien muiden kustannusten määrän olevan 5 000-15 000 euroa. Jatkuvaluonteisia muita kustannuksia velvoitteen ei arvioitu aiheuttavan.

Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 12 100 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 4 500 euroa vuosittain tämän jälkeen.

Selvityksen mukaan valmistussektorilla yritysten arvio velvoitteen sopeutumiseen käytettävistä kertaluonteisia henkilötyöpäivistä oli 10-50 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan 10-20 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen sopeutumiseen kertaluonteisesti käytettävien muiden kustannusten määrän olevan 5 000-50 000 euroa, mutta monet arvioivat myös, että velvoitteen täyttämisestä ei aiheudu muita kertaluonteisia kustannuksia. Jatkuvaluonteisia muita kustannuksia ei arvioitu aiheutuvan.

Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 34 700 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 27 600 euroa vuosittain tämän jälkeen.

7. Perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus

NIS2-direktiivin 21 artiklan 2 kohdan g alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteisiin on sisällytettävä perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus. NIS2-direktiivin johdanto-osan 89 kohdan mukaan yritysten olisi otettava käyttöön monenlaisia perustason kyberhygieniakäytäntöjä, kuten nollaluottamuksen periaate, ohjelmistopäivitykset, laitteiden konfigurointi, verkon segmentointi, identiteetin- ja pääsynhallinta ja käyttäjien tietoisuuden lisääminen, ja järjestettävä henkilöstölleen koulutusta kyberuhkista, verkkourkinnasta ja käyttäjän manipuloinnista.

Instan tekemissä haastatteluissa havaittiin, että NIS2-direktiivissä luetellaan esimerkkeinä perustason kyberhygieniakäytännöistä joitakin sellaisia menettelytapoja, jotka saattavat olla haasteellisia toteuttaa etenkin direktiivin soveltamisalaan kuuluvissa pienemmissä yrityksissä. Esimerkkinä tällaisista menettelyistä mainittiin erityisesti nollaluottamuksen periaate eli ns. Zero Trust.

Selvityksen mukaan elintarvikesektorilla yritykset arvioivat, että velvoitteeseen sopeutumisesta ei aiheudu kertaluonteisia henkilötyöpäiviä. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen sopeutumiseen kertaluonteisesti käytettävien muiden kustannusten määrän olevan korkeintaan 30 001-50 000 euroa. Kuitenkin useat arvioivat myös, että kertaluonteisia muita kustannuksia ei velvoitteen täyttämisestä aiheudu. Jatkuvaluonteisia muita kustannuksia arvioitiin koituvan korkeintaan 15 001-30 000 euroa, mutta monet arvioivat myös kustannuksiksi alle 5 000 euroa.

Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 21 900 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 19 500 euroa vuosittain tämän jälkeen.

Selvityksen mukaan valmistussektorilla yritysten arvio velvoitteen sopeutumiseen käytettävistä kertaluonteisia henkilötyöpäivistä alle 10 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan 10-20 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen sopeutumiseen kertaluonteisesti käytettävien muiden kustannusten olen korkeintaan 5 000-15 000 euroa, mutta monet arvioivat myös, että velvoitteen täyttämisestä ei aiheudu muita kertaluonteisia kustannuksia. Jatkuvaluonteisia muita kustannuksia arvioitiin koituvan 5 000- 15 000 euroa.

Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 37 100 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 26 700 euroa vuosittain tämän jälkeen.

8. Toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä

NIS2-direktiivin 21 artiklan 2 kohdan h alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteisiin on sisällytettävä toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä.

Asiantuntijoiden arvion mukaan tämän velvoitteen arvioinnissa yritykset voivat ottaa erityisesti huomioon, onko niillä dokumentoidut kryptografian ja salauksen toimintaperiaatteet, jotka ottavat huomioon aitouden, eheyden sekä luottamuksellisuuden näkökulmat. Lisäksi yritykset voivat arvioida, onko algoritmien, protokollien, avainten pituuksien sekä salaustuotteiden valinnat tehty voimassa olevien suositusten mukaisesti, ja onko avainten ja sertifikaattien hallinta ja suojaaminen dokumentoitu.

Selvityksen mukaan elintarvikesektorilla yritykset arvioivat, että velvoitteeseen sopeutumisesta aiheutuu alle 10 henkilötyöpäivää ja monet arvioivat, että velvoitteesta ei aiheudu kertaluonteisia henkilötyöpäiviä. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää. Velvoitteista ei arvioitu aiheutuvan kertaluontoisia tai jatkuvia muita kustannuksia.

Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 23 000 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 10 200 euroa vuosittain tämän jälkeen.

Selvityksen mukaan valmistussektorilla yritysten arvio velvoitteen sopeutumiseen käytettävistä kertaluonteisia henkilötyöpäivistä oli 10-20 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää. Velvoitteista ei arvioitu aiheutuvan kertaluontoisia tai jatkuvia muita kustannuksia.

Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 30 900 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 23 500 euroa vuosittain tämän jälkeen.

9. Henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta

NIS2-direktiivin 21 artiklan 2 kohdan i alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteisiin on sisällytettävä henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta. NIS2-direktiivin johdanto-osan 79 kohdan mukaan toimijoiden olisi käsiteltävä kyberturvallisuusriskien hallintatoimenpiteissään myös henkilöstöturvallisuutta ja otettava käyttöön asianmukaiset pääsynhallintaperiaatteet. Näiden toimenpiteiden olisi oltava direktiivin (EU) 2022/2557 mukaisia. Direktiivin 2022/2557 (CER-direktiivi) 13 artiklan 1 kohdan e alakohdan mukaan kriittisten toimijoiden tulee ottaa käyttöön toimenpiteitä, jotka ovat tarpeen asianmukaisen henkilöstöturvallisuuden hallinnan varmistamiseksi, ottaen asianmukaisesti huomioon sellaiset toimenpiteet kuin kriittisiä tehtäviä hoitavien henkilöstöryhmien määrittäminen, pääsyoikeuksien vahvistaminen tiloihin, kriittiseen infrastruktuuriin ja arkaluonteisiin tietoihin pääsemiseksi, taustatarkastuksia koskevien menettelyjen käyttöönottaminen 14 artiklan mukaisesti ja sellaisten henkilöryhmien määrittäminen, joilta tällaisia taustatarkastuksia vaaditaan, sekä asianmukaisten koulutusvaatimusten ja pätevyyksien vahvistaminen.

Edellisten lisäksi asiantuntijoiden arvioiden mukaan pääsynhallintaperiaatteissa tulisi ottaa huomioon oikeuksien myöntäminen, muuttaminen ja poistaminen sekä asianmukainen valvonta. Pääsynhallintaperiaatteiden tulisi kattaa koko yrityksen kriittinen infrastruktuuri ja tilat sekä arkaluonteiset tiedot. Omaisuudenhallinnan tulisi kattaa sekä fyysinen että aineeton omaisuus. Lisäksi yrityksellä tulisi olla periaatteet koskien salassapito- ja vaitiolositoumuksia.

Kyselytutkimuksessa havaittiin, että vaatimus omaisuudenhallinnasta on osittain tulkinnanvarainen, koska NIS2-direktiivissä ei määritellä omaisuudenhallinta-termiä tarkasti. Yrityksiä

haastateltaessa kävi ilmi, että omaisuudenhallintaa tarkasteltiin usein ISO 27001-standardin tavoin kaikki tieto-omaisuus ja siihen liittyvät muut omaisuuserät huomioiden. Suppeasti tarkasteltuna omaisuudenhallinta olisi mahdollista tässä yhteydessä kuitenkin ymmärtää esimerkiksi henkilöstön hallussa olevan omaisuuden, kuten työvälineiden, hallinnoinniksi. Laaja tulkinta voisi sisältää kaiken omaisuuden, jolla on yritykselle arvoa. On syytä huomioida, että omaisuudenhallinnan kehittämiseen liittyvän työn ja muiden kustannusten määrä vaihtelee merkittävästi riippuen siitä, missä laajuudessa omaisuudenhallintaan liittyviä toimenpiteitä toteutetaan. Haastatteluissa omaisuudenhallinnan osalta käytettiin ISO 27001 -standardin mukaista määritelmää.

Selvityksen mukaan elintarvikesektorilla yritykset arvioivat, että velvoitteeseen sopeutumisesta aiheutuu alle 10 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää, mutta monet arvioivat, että vuosittain aiheutuvia toistuvia henkilötyöpäiviä ei velvoitteen täyttämisestä aiheudu. Velvoitteista ei arvioitu aiheutuvan kertaluontoisia tai jatkuvia muita kustannuksia.

Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 12 000 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 8 500 euroa vuosittain tämän jälkeen.

Selvityksen mukaan valmistussektorilla yritysten arvio velvoitteen sopeutumiseen käytettävistä kertaluonteisia henkilötyöpäivistä oli korkeintaan 10-20 henkilötyöpäivää, mutta monet arvioivat velvoitteen täyttämisen aiheuttavan alle 10 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää. Velvoitteista ei arvioitu aiheutuvan kertaluontoisia tai jatkuvia muita kustannuksia.

Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 18 000 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 11 00 euroa vuosittain tämän jälkeen.

10. Tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa

NIS2-direktiivin 21 artiklan 2 kohdan j alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteisiin on sisällytettävä tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa. Monivaiheisen tunnistautumisen käyttöönotto kaikissa suurten yritysten järjestelmissä saattaisi aiheuttaa kohtuuttoman suuria kustannuksia. Käyttöönotto voi vaatia esimerkiksi kalliimpien lisenssien käyttöönottoa pilvipalveluissa ja vanhemmissa järjestelmissä monivaiheinen tunnistautumisen käyttöönotto voi olla vaikeaa. Käyttöönotto perustuu kuitenkin riskiarviointiin, eikä sen käyttö ole pakollista kaikissa ympäristöissä, vaan tarvittaessa. Monivaiheinen tunnistautumisen katsotaan olevan myös yritykselle hyödyllinen varsinkin, kun käyttöönotto perustuu riskiarviointiin.

Esityksen riskienhallintavelvoitteiden täyttämisestä johtuvien taloudellisten vaikutusten tasoon vaikuttavat muun muassa toimialojen ja toimijoiden yleinen kybermaturiteettitaso ja kyvykkyydet, jotka vaihtelevat tällä hetkellä niin eri sektoreiden kuin toimijoiden välillä. Arviointiin vaikuttaa lisäksi sektori- ja toimijakohtaiset riskiarvioinnit. Mitä haitallisempia ja laajakantoisempia vaikutuksia mahdollinen kyberhäiriö voi aiheuttaa tietylle toimijalle, sitä enemmän mahdollisia investointeja direktiivin vaatimusten mukaisuuden osoittaminen voi edellyttää, riippuen

toimijan kybermaturiteetin tasosta. Mahdolliset kustannusvaikutukset tulee myös suhteuttaa toimijan kokoon. Ensimmäisen verkko- ja tietoturvadirektiivin soveltamisalaan kuuluvalle toimijalle kohdistuu lähtökohtaisesti vähemmän suoraan tämän esityksen velvoitteista aiheutuvia kustannuksia, koska toimijat ovat olleet jo kyberturvallisuusvelvoitteiden piirissä ja kyberturvallisuutta vahvistavia toimenpiteitä on jo tehty.

Selvityksen mukaan elintarvikesektorilla yritykset arvioivat, että velvoitteeseen sopeutumisesta aiheutuu korkeintaan 10-20 henkilötyöpäivää. Monet arvioivat kuitenkin, että velvoitteeseen sopeutumisesta ei aiheudu henkilötyöpäiviä. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan korkeintaan alle 10 henkilötyöpäivää, mutta monet arvioivat, että vuosittain aiheutuvia toistuvia henkilötyöpäiviä ei velvoitteen täyttämisestä aiheudu. Velvoitteista ei arvioitu aiheutuvan kertaluontoisia tai jatkuvia muita kustannuksia.

Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 24 700 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 10 100 euroa vuosittain tämän jälkeen.

Selvityksen mukaan valmistussektorilla yritysten arvio velvoitteen sopeutumiseen käytettävistä kertaluonteisia henkilötyöpäivistä oli 10-20 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan korkeintaan alle 10 henkilötyöpäivää. Monet arvioivat, että toistuvia henkilötyöpäiviä ei velvoitteen täytöstä aiheudu. Kertaluonteisia muita kustannuksia arvioitiin aiheutuvan alle 5000 euroa. Vuosittain aiheutuvia jatkuvaluonteisia kustannuksia arvioitiin aiheutuvan alle 5000 euroa.

Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille valmistussektorin yrityksille aiheutuu kertakustannuksena keskimäärin 37 300 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 27 700 euroa vuosittain tämän jälkeen.

Riskienhallinnan osa-alue	Elintarvikesektori		Valmistussektori	
	kertakustannukset	vuosittaiset kustannukset	kertakustannukset	vuosittaiset kustannukset
1. Riskianalyysi ja tietojärjestelmien turvallisuus	32 200 €	11 400 €	52 900 €	36 900 €
2. Poikkeamien käsittely	47 200 €	19 700 €	43 200 €	39 500 €
3. Toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu sekä kriisinhallinta	31 200 €	19 400 €	32 100 €	29 500 €
4. Toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat	39 100 €	23 200 €	46 500 €	31 700 €
5. Verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen	30 800 €	21 900 €	34 200 €	25 100 €

6. Toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta	12 100 €	4 500 €	34 700 €	27 600 €
7. Perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus	21 900 €	19 500 €	37 100 €	26 700 €
8. Toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä	23 000 €	10 200 €	30 900 €	23 500 €
9. Henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta	12 000 €	8 500 €	18 000 €	11 000 €
10. Tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa	24 700 €	10 100 €	37 300 €	27 700 €
Yhteensä	**274 000 €**	**148 000 €**	**367 000 €**	**279 000 €**

Selvityksen mukaan suurimmat kustannukset koituvat seuraavista velvoitteista: riskianalyysi ja tietojärjestelmän turvallisuus, poikkeamien käsittely sekä toimitusketjujen turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuuskohdat. Huomioitavaa on, että tarkasteluun valitut sektorit eivät ole olleet NIS-sääntelyn piirissä, joten lukujen voidaan arvioida olevan eräänlaisia maksimeja sääntelystä koituvista kustannuksista. Huoltovarmuuskeskus on arvioinut sekä elintarviketeollisuudessa että teollisuudessa kybermaturiteetin olevan alle perustason ja nykytilan vaativan kehittämistä nykyiseen uhka- ja riskitilanteeseen vastaamiseksi. Elintarvikesektorilla erityisesti heikkoudeksi tunnistettiin kyberriskien hallinnan prosessien puutteet ja sen vaikutukset päätöksenteon riskilähtöisyyteen sekä kyberturvallisuuden tilannekuvan puutteet esimerkiksi lokitietojen hyödyntämisen osalta. Teollisuudessa havaittiin erityisiksi puutteiksi toimittajahallinnan kehittäminen ja sidonnaisuuksien tunnistaminen, riskienhallinta sekä johdon tuen ja kiinnostuksen puutteen vaikutukset.

Muille sektoreille kuin elintarvike- ja valmistussektoreille ei pystytä tekemään samankaltaista euromääräistä arviota. Esityksen taloudellisten vaikutusten tasoon vaikuttavat muun muassa toimialojen ja toimijoiden yleinen kybermaturiteettitaso ja kyvykkyydet, jotka vaihtelevat tällä hetkellä niin eri sektoreiden kuin toimijoiden välillä. Arviointiin vaikuttaa lisäksi sektori- ja toimijakohtaiset riskiarvioinnit. Mitä haitallisempia ja laajakantoisempia vaikutuksia mahdollinen kyberhäiriö voi aiheuttaa tietylle toimijalle, sitä enemmän mahdollisia investointeja direktiivin vaatimusten mukaisuuden osoittaminen voi edellyttää, riippuen toimijan kybermaturiteetin tasosta. Mahdolliset kustannusvaikutukset tulee myös suhteuttaa toimijan kokoon. Lähtökohtaisesti kustannuksien määrään vaikuttaa myös se, onko toimija kuulunut NIS1-direktiivin velvoitteiden soveltamisalaan. Koska elintarvike- ja valmistussektorin toimijat eivät pääosin ole kuuluneet NIS1-direktiivin soveltamisalaan, riskienhallinnassa huomioitavien osa-alueiden osalta kustannuksien voidaan yleisesti arvioida vastaavan esitettyjä arvioita toimijakohtaisten vaihteluiden välillä.

Toimialojen kybermaturiteettia on selvitetty Suomessa Huoltovarmuuskeskuksen toimesta.[8] Selvityksessä jokaiselle toimialalle määritettiin myös arvio uhkatason vaikutuksesta toimialalle. Vuonna 2022 kybermaturiteetin taso oli korkein teleliikenne-, ICT ja ohjelmisto-, finanssi-toimialoilla, jotka ovat perinteisesti olleet kyberrikollisuuden kohteena ja tästä johtuen jo pitkään säänneltyjä toimialoja, myös NIS1-direktiivin soveltamisalassa. Toimialat ovat kyenneet kehittämään kyberturvallisuuttaan liiketoiminta- ja riskilähtöisesti. Näille toimialoille on arvioitu, että ne kykenevät vahvan kypsyystason ansiosta vastaamaan nykyiseen riski- ja uhkakuvaan. Näille toimialoille arvioidaan koituvan tämän johdosta pienemmät kustannukset NIS2-velvoitteiden täyttämisestä, sillä direktiivin vaatimia toimia tehdään jo pitkälti vaatimusten mukaisesti.

Energia- ja terveydenhuolto toimialat ylittivät myös keskiarvomaturiteetiksi määritetyn perustason, mutta alojen osalta uhka- ja riskitason vaikutus on arvioitu merkittäväksi eli aloilla on paljon toimintoja, jotka voidaan arvioida riskilähtöisesti merkittäviksi. Energiatoimialalla NIS2-direktiivin soveltamisalan piiriin tulee paljon uusia toimijoita. Näitä uusia toimijoita ovat sähköverkonhaltijat, sähköntuottajat, sähkönmyyjät, sähköpörssit, maakaasuverkonhaltijat, LNG-terminaalin operaattorit (pelkästään verkkoon liitetyt tai myös muut), maakaasuntoimittajat, LNG-toimittajat, vetytoimijat, kaukolämpö/-kylmätoimijat, öljyn jalostus ja öljyn varastointi. Energia-alalla uhkatason merkitys toimialalle arvioidaan nousevaksi. Kypsyystaso arvioidaan yleisesti hyväksi ja erilaisiin uhkiin on varauduttu. Ala jakautuu kuitenkin korkean ja matalan kypsyystason toimijoihin ja tietoturvakulttuuri on vaihtelevaa toimijoiden välillä. Lisäksi on tunnistettu, että suuremmalla maantieteellisellä alueella toimivat organisaatiot ovat investoineet kyberturvallisuuteen paikkakuntakohtaisia toimijoita enemmän. NIS2-direktiivin velvoitteiden täyttäminen voi täten johtaa joillekin toimijoille suurempiin kustannusvaikutuksiin erityisesti sääntelyn piiriin tulevilla uusilla toimijoilla.

Terveydenhuolto toimialalla NIS2-direktiivin soveltamisalan piiriin kuuluvat julkiset hyvinvointialueet ja uusina direktiivin soveltamisalaan kuuluvat myös jotkin tutkimuslaitokset ja laboratoriot. Tietosuojaan liittyvät toimenpiteet ovat terveydenhuoltoalaan kohdistuvan regulaation myötä hoidettu, mutta kyberturvallisuuden osalta monen toimijan kohdalla arvioitiin tarvittavan järjestelmällisempiä toimenpiteitä. Erityisesti kriittisten palveluiden suojaaminen sekä toimitusketjut, joissa palveluntarjoajien kyberturvallisuuden tason seuraaminen ja sopimusvelvoitteiden asettaminen arvioitiin heikoksi. Toimialan heikkoudeksi arvioitiin myös hybridiuhkiin varautuminen osana jatkuvuussuunnittelua sekä säännöllistä harjoittelua. Erityisesti näillä osa-alueilla NIS2-direktiivin velvoitteiden täyttämisen voidaan arvioida aiheuttavan kustannuksia, vaikka muutoksia ei arvioida NIS1-toimijoiden kohdalla merkittäviksi.

Selvityksessä hieman perustason maturiteetin alle jäivät NIS2-toimialoista logistiikka, elintarviketeollisuus, teollisuus, vesihuolto, kauppa ja jakelu sekä satamat ja merenkulku. Näille toimialoille arvioidaan kohdistuvan kustannuksia NIS2-velvoitteiden täyttämisestä.

Vesihuollossa uhkatason merkitys toimialalle arviointiin nousevaksi. Kokonaiskypsyys jää alle hyvän perustason ja alan keskeinen rooli yhteiskunnan toimivuudessa arvioidaan merkittävästi. Tämän johdosta arvioidaan, että investointeja kyberturvallisuuteen tulee toimialalla tehdä, jotta nykyisiin uhkakuviin on tarpeeksi varauduttu. Erityisesti heikkoudeksi tunnistettiin kyberturvallisuuden kokonaishallinnan puutteet, heikko näkyvyys kumppanien toimintaan kehitystyössä ja korkea riippuvuussuhde IT-palveluntoimittajiin. Vesihuolto on kuitenkin ollut NIS-direktiivin piirissä, joten kyberturvallisuusregulaatiota on jo kohdistunut toimijoihin. Vesihuolto on

[8] Huoltovarmuuskeskus (2022) Toimialojen kyberkypsyyden selvitys 2022.

kuitenkin yhteiskunnan toiminnan kannalta kriittinen palvelu, ja suuremmat poikkeustapahtumat voivat eskaloitua paikallisiksi katastrofeiksi, jonka johdosta riskit ovat suuremmat ja täten toimialalle voi syntyä suurempia kustannuksia NIS2-direktiivin täytäntöönpanosta.

Logistiikka-alalla uhkatason merkitys arvioitiin nousevaksi. Toimiala on jatkuvasti kehittyvä ja altis kilpailulle sekä toimitusketjuissa tapahtuville muutoksille, mikä tarkoittaa, että kyberturvallisuuden kokonaisvaltaiseen hallintaan tulee kiinnittää erityistä huomiota. Toimialan heikkoudeksi tunnistettiin muun muassa puutteet lokihallinnan politiikkojen ja linjausten määrityksessä ja jalkautuksessa, järjestelmätason sekä OT-ympäristöjen valvonnan kattavuudessa ja varmistamisessa. Tämän lisäksi heikkoudeksi arvioitiin kolmansien osapuolten ja toimintojen välisten riippuvuuksien tunnistaminen.

Kauppa ja jakelun uhkatason merkitys arviointiin neutraaliksi. Kaupan ja jakelun toimialan kokonaiskypsyys jää alle hyvän perustason, jolloin varautuminen kyberuhkiin ei ole kattavaa. Maturiteettitasossa oli paljon hajontaa eri toimijoiden välillä. Toimialan heikkoudeksi tunnistettiin kyberriskienhallintakulttuurin puute ja sen vaikutus riskilähtöisen päätöksenteon haasteisiin sekä kyberturvallisuusnäkökulman heikompi huomioiminen operatiiviseen jatkuvuuteen verrattuna muun muassa seuraavissa osa-alueissa: tapahtumien ja häiriöiden hallinta, haavoittuvuuksien hallinta, omaisuudenhallinta ja kriittisten palveluiden suojaaminen.

Satamat ja merenkulku toimialalle uhkatason merkitys arvioitiin neutraaliksi. Toimialan kypsyys oli kuitenkin matala ja arvioitiin vaativan merkittäviä toimenpiteitä, jotta toimiala pystyisi hyvin vastaamaan nykyiseen uhkatasoon. Toimialalla on korostunut rooli kansallisen huoltovarmuuden ylläpidossa poikkeustilanteessa. Toimialan heikkoudeksi havaittiin johdon tuen puute, joka estää kehittämistarpeiden läpiviennin, jolloin kyberturvallisuusinvestointien läpivienti on estynyttä. Lisäksi havaittiin puutteita kyberturvallisuuden hallinnan perustason määrittelyssä. Tämän johdosta toimialalle arvioidaan koituvan enemmän kustannuksia NIS2-velvoitteiden täyttämisestä. Muiden liikenteen toimijoiden kybermaturiteetin tasosta ei ole tietoa. Sektorille on kuitenkin kohdistunut NIS-velvoitteita aikaisemminkin, joten sektorilla on toimijoita, joille ei kohdistu niin suuria kustannuksia velvoitteiden täyttymisestä. Sektorille on kuitenkin tulossa paljon uusia toimijoita sääntelyn piiriin, joten kustannukset ovat näille toimijoille todennäköisesti suurempia.

Muiden NIS2-sektoreiden osalta kybermaturiteetin tasoa ei ole tutkittu Suomessa.

Vaikutukset kansantalouteen

Esityksellä pyritään parantamaan kriittisten toimialojen kyberturvallisuutta ja tätä kautta parantavan markkinoiden luottamusta ja kansantaloutta. Esityksen vaikutukset kansantalouteen ovat välillisiä.

Esityksellä on vaikutuksia julkistaloudelle, jotka koostuvat uusista viranomaistehtävistä sekä laajenevasta valvottavien toimijoiden joukosta. Julkistaloudelliset vaikutukset kuvataan jaksossa 4.4.

Esityksen tuoma suurempi sääntelytaakka tarkoittaa, että toimijat joutuvat käyttämään lisää resursseja kyberturvallisuuteen. Tämä voi pienentää yrityksillä lyhyellä aikavälillä voittoja, ja on myös mahdollista, että tietoturvaan ja tietosuojaan kohdennetut lisäresurssit ovat pois muusta toiminnasta. Hyvästä tietoturvasta ja tietosuojan tasosta huolehtiminen voi tarjota kuitenkin yri-

tyksille esimerkiksi maine-edun ja auttaa siten liiketoiminnan menestymistä. Oletetusti kyberturvallisuuteen panostaminen vähentää tietoturvahäiriöitä, jolloin riski kyberturvallisuuden murtumisesta pienenee ja tästä johtuvia kustannuksia pystytään ainakin osin välttämään koko kansantalouden tasolla.

Kriittisten toimialojen tietoturvan ja tietosuojan kansantaloudellinen merkitys on suuri. Tietoturvan ja tietosuojan murtumisesta aiheutuneet häiriöt vaikuttaisivat suoraan toimialojen palkansaajiin ja bruttokansantuotteen kehitykseen. Kriittisten toimialojen kohdalla tietoturvan ja tietosuojan murtuminen vaikuttaisi kuitenkin myös muita vaikutusketjuja pitkin kansantalouden toimintaan ja kehitykseen. Toimialojen väliset keskinäisriippuvuudet ja epäsuorat kustannukset ovat vaikutuksista olennaisimpia. Tietoturvan tai tietosuojan murtumisen kustannukset kertautuvat muihin toimialoihin keskinäisriippuvuuksien kautta.

Tietoturvan ja tietosuojan murtumisella voi olla laajempia vaikutuksia yritysten toimintaedellytyksiin ja kansantalouden toimintaan, jos esimerkiksi tietomurto vaikuttaa kansalaisten luottamukseen yhteiskunnan toimivuudesta tai yritysten odotuksiin. Yrityksille toiminnan keskeytyminen tietoturvan tai tietosuojan häiriötilanne aiheuttaa kustannuksia sekä tuotannon tai palveluntarjonnan keskeytymisen sekä häiriön haitallisten vaikutusten poistamisen vuoksi. Lisäksi kyberturvan pettäminen voi johtaa epäsuoriin kustannuksiin, jos asiakkaiden luottamus yritykseen järkkyy, mikä taas johtaa pienentyneisiin asiakasmääriin ja pienentyneeseen myyntiin.

Tietoturvan murtumisella voi olla seurauksia kotitalouksien luottamukselle, mikä voi johtaa digitaalisen talousjärjestelmän toiminnan järkkymiseen. Myös instituutioita kohtaan koettu epäluottamus voi lisääntyä, jos tietosuojan ja tietoturvan nähdään olevan yhteiskunnassa heikosti hoidettua. Kotitalouksien kannalta tietosuojan ja tietoturvan murtuminen aiheuttaa yleisellä tasolla suoria kustannuksia, jos hyödykkeitä joudutaan hankkimaan toista kautta tietoturvan pettäessä tai pääsy hyödykkeisiin katkeaa. Suoriin kustannuksiin kuuluvat myös kansalaisen kohdistamat lisäresurssit esimerkiksi uuden palvelutarjoajan etsimiseen tai oman tietoturvan ja tietosuojan tason parantamiseen.

Säännösten yhdenmukaistaminen parantaa EU:n sisämarkkinoiden toimintaa ja madaltaa yritysten maasta toiseen laajentumisen kustannuksia. NIS1-direktiivin yhteydessä komission tekemän arvion mukaan yksittäiselle yritykselle aiheutuu noin 9000 € lisäkulu liiketoiminnan laajentamisesta toiseen EU-maahan. Digitaalisten sisämarkkinoiden toteutuminen täydellisesti voisi mahdollistaa 415 miljardia euroa kasvua EU:n bruttokansantuotteeseen, joten kasvunpotentiaali on yhteisten säännösten myötä merkittävä.

4.4 Vaikutukset viranomaisten toimintaan

Vaikutukset viranomaisten tehtäviin ja julkistalouteen

Esityksen vaikutukset viranomaisille koostuvat uusien viranomaistehtävien suorittamisesta aiheutuvista vaikutuksista ja sääntelyn noudattamisesta julkishallinnolle aiheutuvista vaikutuksista. Tässä alaluvussa kuvataan esityksen vaikutuksia viranomaisille viranomaistoiminnan osalta. Sääntelyn noudattamisesta julkishallinnon toimijoille aiheutuvia vaikutuksia käsitellään seuraavassa alaluvussa.

Esityksellä on uusien tehtävien hoitamisesta aiheutuvia taloudellisia vaikutuksia Liikenne- ja viestintävirastolle. Liikenne- ja viestintävirasto huolehtisi ehdotuksen mukaan CSIRT-yksikön tehtävistä, kansallisten kyberkriisinhallintaviranomaisten välisen koordinaattorin tehtävästä, valvovan viranomaisen tehtävästä eräillä sektoreilla, NIS2-direktiivin mukaisen kansallisen yhteyspisteen tehtävästä sekä eräistä seuraamusmaksulautakuntaan liittyvistä tehtävistä. Koska

Liikenne- ja viestintäviraston tehtävien määrä lisääntyisi NIS2-direktiivin toimeenpanon myötä, Liikenne- ja viestintävirasto edellyttäisi lisäresursointia uusista tehtävistä aiheutuvien kustannuksien kattamiseksi.

Esityksellä on uusien valvontatehtävien hoitamisesta aiheutuvia taloudellisia vaikutuksia Energiavirastolle, Turvallisuus- ja kemikaalivirastolle, Sosiaali- ja terveysalan lupa- ja valvontavirastolle, Etelä-Savon ELY-keskukselle, Ruokavirastolle, Lääkealan turvallisuus- ja kehittämiskeskukselle sekä Finanssivalvonnalle, jotka toimisivat sektorikohtaisesti valvovina viranomaisina. Lisäksi valvontayhteistyöstä edellä mainittujen viranomaisten kanssa seuraisi suoria taloudellisia vaikutuksia tietosuojavaltuutetulle. Valvonnasta aiheutuvien kustannuksien määrään vaikuttaa kullakin sektorilla soveltamisalassa olevien toimijoiden määrä ja laatu sekä sellaisten toimijoiden määrä, jotka eivät ole kuuluneet NIS1-direktiiviä täytäntöönpanevan sääntelyn soveltamisalaan. Valvovan viranomaisen tehtävä olisi uusi Turvallisuus- ja kemikaalivirastolle, Etelä-Savon ELY-keskukselle, Ruokavirastolle ja Lääkealan turvallisuus- ja kehittämiskeskukselle. Lisäksi suhteessa NIS1-direktiivin toimeenpanoon Suomessa, NIS2-direktiivin voimaantulon myötä soveltamisala laajenee ja valvovilta viranomaisilta edellytetään laajempaa kyvykkyyttä, mikä aiheuttaa lisäkustannuksia jokaisessa valvovassa viranomaisessa.

Toisaalta NIS1-direktiivissä omaksutusta kriittisten toimijoiden identifiointiprosessista luovuttaisiin ja velvoitteiden soveltamisala määriteltäisiin jatkossa toimijoiden toimialan ja koon perusteella. Toimijaluettelon keräämisessä hyödynnettäisiin toimijoiden omia ilmoituksia sekä olemassa olevia rekisteritietoja. Näiden tekijöiden arvioidaan vähentävän viranomaisille aiheutuvaa hallinnollista taakkaa verrattuna NIS1-direktiivin nojalla tapahtuvaan valvontaan. Valvovalla viranomaisella olisi lisäksi mahdollisuus kohdentaa valvontaa riskiperusteisesti sekä asettaa tehtäviään tärkeysjärjestykseen, mikä vaikuttaisi valvonnasta aiheutuviin kustannuksiin viranomaisessa. Toisaalta yleisesti sovellettaviin sektorisäännöksiin verrattuna NIS2-sääntelyn keskittäminen uuteen yleislakiin voi lisätä velvoitteiden soveltamisalaa koskevan neuvonnan tarvetta.

Valvontatehtävä edellyttäisi lisäresursseja jokaisessa valvovassa viranomaisessa, koska valvottavien toimijoiden määrä kasvaa kunkin valvovan viranomaisen valvontatoimialalla ja viranomaiselta edellytetään NIS1-direktiivin valvontaa pidemmälle menevää kyvykkyyttä valvontatoimintaan. Sektoreilla, jotka eivät ole kuuluneet NIS1-sääntelyn piiriin ja valvovalla viranomaisella ei ole ollut NIS1-direktiiviä täytäntöönpanevan sääntelyn valvontatehtävää ennestään, NIS2-direktiivin valvontaa ei pystyttäisi suorittamaan ilman uusia resursseja. Jaksossa 5.1 käsitellään toteuttamisvaihtoehtoa valvonnan keskitetystä järjestämisestä, jonka on arvioitu aiheuttavan hajautettua valvontamallia suuremman kustannusvaikutuksen julkiselle taloudelle.

Seuraavassa taulukossa esitetään arvio valvontatehtävästä aiheutuvasta lisäresurssitarpeesta kullekin valvovalle viranomaiselle ja tietosuojavaltuutetulle.

Viranomainen	**Valvottava toimiala**	**Arvio lisäresurssitarpeesta**	**NIS1-valvova viranomainen**
Liikenne- ja viestintävirasto	Ilmaliikenne, raideliikenne, vesiliikenne, tieliikenne, avaruus, digitaalinen infrastruktuuri, TVT-palvelujen hallinta, kuriiri- ja postipalvelun tarjoajat, digitaalisen palvelun tarjoajat, valmistus	8,5 htv ja tietojärjestelmäinvestoinnit 0,4 M€ vuodelle 2024 ja 0,15 M€ vuodesta 2025 alkaen	Kyllä

	(moottoriajoneuvojen, perävaunujen ja puoliperävaunujen valmistusta harjoittavat toimijat, muiden kulkuneuvojen valmistusta harjoittavat toimijat), tutkimusorganisaatiot, julkishallinto.		
Energiavirasto	Sähkö, kaukolämmityksen tai kaukojäähdytyksen haltijat, kaasu (jakelu- ja siirtoverkonhaltijat)	Täydentyy myöhemmin	Kyllä
Turvallisuus- ja kemikaalivirasto	Kaasu (maakaasun toimittajat, varastointilaitteiston haltijat, maakaasun käsittelylaitteiston haltijat, maakaasualan yritykset sekä maakaasun jalostus- ja käsittelylaitteistojen haltijat), öljy, vedyn tuotantoa, varastointia ja siirtoa harjoittavat toimijat, aineiden valmistusta ja aineiden tai seosten jakelua harjoittavat yritykset ja yritykset, jotka tuottavat esineitä aineista tai seoksista, valmistus (tietokoneiden sekä elektronisten ja optisten tuotteiden valmistusta harjoittavat toimijat, sähkölaitteiden valmistusta harjoittavat toimijat ja muiden koneiden ja laitteiden valmistusta harjoittavat toimijat).	5 htv + tietojärjestelmäinvestoinnit 0,2 M€ vuodelle 2024 ja 0,06 M€ vuodesta 2025 alkaen.	Ei
Sosiaali- ja terveysalan lupa- ja valvontavirasto	Terveys	2 htv sekä tietojärjestelmäinvestoinnit kertaluontoisesti noin 0,15 M€ ja 10 000 – 20 000 euroa vuosittain 2025 alkaen.	Kyllä
Etelä-Savon ELY-keskus	Jätehuolto	2,5 htv sekä noin 40.000 kertaluontoinen kustannus sekä tietojärjestelmäkustannus 0,05 M€ vuodesta 2025 alkaen.	Ei

Etelä-Savon ELY-keskus, Vesihuoltopalvelut-yksikkö	Juomavesi ja jätevesi	3 htv sekä noin 100.000 eur ostopalvelumääräraha.	Kyllä
Ruokavirasto	Elintarvikeyritykset, jotka harjoittavat tukkukauppaa, teollista tuotantoa tai jalostusta	5 htv sekä tietojärjestelmäkustannus 0,54 M€ vuodelle 2024 ja 0,05 M€ vuodesta 2025 alkaen	Ei
Lääkealan turvallisuus ja kehittämiskeskus	Lääkinnällisiä laitteita valmistavat toimijat ja In vitro –diagnostiikkaan tarkoitettuja lääkinnällisiä laitteita valmistavat toimijat	Täydentyy myöhemmin	Ei
Finanssivalvonta	Pankkitoiminta ja finanssimarkkinoiden infrastruktuuri	Ei vaikutuksia	Kyllä
Tietosuojavaltuutettu	-	2,5 htv.	-
Yhteensä			

Kyberturvallisuusosaajista on Suomessa pulaa, joten sekä viranomaisissa että sääntelyn kohteena olevissa toimijoissa lisääntyvä tarve alan osaajille saattaa aiheuttaa rekrytointihaasteita. Ehdotuksessa on pyritty luomaan edellytyksiä viranomaisten väliselle tiiviille yhteistyölle, jonka avulla voidaan kehittää kyberturvallisuusosaamista sektorirajat ylittävästi.

Ehdotus sisältää myös eräitä lisävelvoitteita sähköisen viestinnän palveluista annetun lain mukaisille verkkotunnusvälittäjille. Liikenne- ja viestintävirasto valvoo verkkotunnusvälittäjien toimintaa, ja uusien velvoitteiden myötä valvontatehtävä laajenee kattamaan nyt ehdotettujen velvoitteiden noudattamisen. Uusien verkkotunnusvälittäjiin kohdistuvien valvontatehtävien on arvioitu edellyttävän edellä kuvatun taulukon lisäksi 0,5 henkilötyövuoden lisäresurssin Liikenne- ja viestintävirastolle.

Liikenne- ja viestintävirasto

Valvontatehtävien lisäksi Liikenne- ja viestintävirastolle esitettäisiin myös muita viranomaistehtäviä, joista aiheutuu lisäresursointitarpeita. Liikenne- ja viestintävirasto on toiminut NIS1-direktiivissä mainittuna CSIRT-yksikkönä jo aiemmin, mutta NIS2-direktiivin myötä yksikön tehtävät lisääntyvät merkittävästi. Uudet tehtävät edellyttävät uudenlaisten toimintojen perustamista sekä olemassa olevien toimintojen sekä tietojärjestelmien kehittämistä. Keskeisiä CSIRT-yksikölle ehdotettavia tehtäviä olisivat tietoturvaloukkauksiin reagoiminen ja toimijan avustaminen, kansainväliseen yhteistyöhön osallistuminen, haavoittuvuustietojen analysointi sekä haavoittuvuustiedon julkaisemisprosessin koordinointi. CSIRT-yksikölle ehdotettujen uusien

tehtävien sekä Liikenne- ja viestintävirastolle osoitettavien valvontatehtävien on arvioitu edellyttävän lisäresursseja yhteensä 8 – 17 henkilötyövuotta sekä järjestelmäkehitykseen vuonna 2024 yhteensä 400 000 euroa ja sen jälkeen vuosittain 150 000 euroa.

Liikenne- ja viestintävirasto nimeäisi myös seuraamusmaksujen määräämistä varten perustettavan seuraamusmaksulautakunnan puheenjohtajan ja varapuheenjohtajan. Lisäksi Liikenne- ja viestintävirasto toimisi koordinaattorina laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallinnassa sekä vastaisi laajamittaisten kyberturvallisuuspoikkeamien ja –kriisien hallintasuunnitelman laatimisesta yhteistyössä muiden viranomaisten kanssa. Tehtävät olisivat Liikenne- ja viestintävirastolle uusia, ja edellyttäisivät yhteensä 0,5 henkilötyövuoden lisäresurssin. Lisäksi Liikenne- ja viestintävirasto jatkaisi NIS1- ja NIS2-direktiiveissä tarkoitettuna keskitettynä yhteyspisteenä. Keskitetty yhteyspiste muun muassa edistää valvovien viranomaisten välistä yhteistyötä ja koordinaatiota. Tehtävä voitaisiin arvion mukaan toteuttaa nykyisillä resursseilla.

Liikenne- ja viestintävirastolle edellä kuvatut uudet tehtävät aiheuttaisivat yhteensä vähintään 8,5 htv:n lisäresurssitarpeen. Lisäksi Liikenne- ja viestintävirastolle aiheutuisi kustannuksia tehtävien toteuttamiseksi tarpeellisista järjestelmäinvestoinneista 0,4 M€ vuodelle 2024 ja 0,15 M€ vuodesta 2025 alkaen. Tällä resurssitasolla Liikenne- ja viestintävirasto suoriutuisi NIS2-direktiivin toimeenpanon edellyttämistä keskeisimmistä tehtävistä vähimmäistasolla hyödyntäen mahdollisuuksia tehostaa nykyisiä toimintoja ja kohdentaa olemassa olevia resursseja uudelleen viraston sisällä.

Liikenne- ja viestintävirasto suoriutuisi yllä kuvatuilla lisäresursseilla vähimmäistasolla viraston vastuulle kuuluvien sektoreiden valvontatehtävistä, sääntelyn mukaisten ilmoitusten käsittelystä, ilmoituksiin vastaamisesta ja uuden ilmoitusmenettelyn teknisestä toteuttamisesta, sääntelyn edellyttämästä teknisestä skannauskyvykkyydestä, haavoittuvuuskoordinaatiosta ja seuraamusmaksulautakunnan tehtävistä. Sääntely asettaa uusia tehtäviä ja vaatimuksia myös verkkotunnusten rekisteröintipalveluille, viranomaisten analyysi- ja forensiikkakyvylle, kriittisten toimialojen tukemiselle, kansainväliselle yhteistyölle, sertifiointia ja standardisointia koskeviin tehtäviin sekä ICT-kyvykkyyksien ja automaation kehittämiselle. Edellä mainitut tehtäväkokonaisuudet ja vaatimukset kuuluvat myös liikenne- ja viestintävirastolle. Liikenne- ja viestintävirasto ei kuitenkaan kykene edistämään viimeksi mainittuja tehtäväkokonaisuuksia esitetyllä resurssitasolla ja niiden edistäminen edellyttäisi lisäresursointia.

Vuoden 2024 talousarviossa Liikenne- ja viestintävirastolle on myönnetty rahoitus NIS2-direktiivin toimeenpanoon liittyviin uusiin tehtäviin 8,5 htv ja tietojärjestelmäinvestoinnit 0,4 M€ vuodelle 2024 ja 0,15 M€ vuodesta 2025 alkaen. Liikenne- ja viestintävirastolle aiheutuvat edellä kuvatut lisäkustannukset katetaan momentin 31.01.02 Liikenne- ja viestintäviraston toimintamenot määrärahojen puitteissa vuodesta 2024 lukien.

Tietosuojavaltuutettu

Esityksellä olisi taloudellisia vaikutuksia tietosuojavaltuutetulle. Tietosuojavaltuutetulle seuraisi lisätyötä ensinnäkin 1. lakiehdotuksen 46 §:ssä säädettävästä valvovien viranomaisten, CSIRT-yksikön ja keskitetyn yhteyspisteen velvollisuudesta tehdä tarvittaessa yhteistyötä muun muassa tietosuojavaltuutetun kanssa. Toiseksi lisätyötä seuraisi henkilötietoturvaloukkausten käsittelyä koskevien ilmoitusten käsittelystä sekä mahdollisista samanaikaisista valvontamenettelyistä. Tietosuojavaltuutettu käsittelee EU:n yleisen tietosuoja-asetuksen ja henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018) perusteella tehtyjä ilmoituksia henkilötietojen tietoturvaloukkauksista. Kaikilla 1.

lakiehdotuksen nojalla valvottavilla toimijoilla, jotka ovat tietosuojalainsäädännössä tarkoitettuja rekisterinpitäjiä tai henkilötietojen käsittelijöitä, on jo nykyisin velvollisuus tehdä ilmoituksia. Esityksen 1. lakiehdotuksen mukaisesti valvontaviranomaisilla olisi velvollisuus ilmoittaa tietosuojavaltuutetulle, jos sille ilmoitetun poikkeaman yhteydessä on tapahtunut henkilötietojen tietoturvaloukkaus tai jos laissa säädettyjen velvoitteiden laiminlyönti voi johtaa tai on johtanut yleisessä tietosuoja-asetuksessa tarkoitettuun henkilötietojen tietoturvaloukkaukseen. Ottaen huomioon sen, että NIS2-direktiivin täytäntöönpanon myötä direktiivin soveltamisala laajenee, ja myös rekisterinpitäjillä ja henkilötietojen käsittelijöillä on vastaava ilmoitusvelvollisuus suoraan tietosuojalainsäädännön nojalla, on odotettavissa, että ilmoitusten määrä lisääntyy ja toisaalta sääntelystä voi seurata päällekkäisiä henkilötietojen tietoturvaloukkauksia ilmoituksia.

Ehdotettu sääntely voi olla osittain päällekkäistä tietosuojalainsäädäntöön perustuvan henkilötietojen käsittelyyn liittyvien tietoturvallisuusvelvoitteiden noudattamisen valvonnan kanssa. Tämä tarkoittaisi myös, että yksittäiseen valvontaviranomaisen toteamaan laiminlyöntiin liittyen voisi olla vireillä samanaikaisesti myös tietosuojavaltuutetun käynnistämiä valvontatoimenpiteitä, mikä tarkoittaisi lisätyötä tietosuojavaltuutetulle. Siltä osin kuin 1. lakiehdotuksessa tarkoitettuja valvontatoimenpiteitä ja tietosuojavaltuutetun valvontatoimenpiteitä olisi vireillä samanaikaisesti, viranomaisten yhteistyössä olisi erityisesti varmistuttava 1. lakiehdotuksen 41 §:n mukaisesti siitä, että seuraamusmaksua määrätä samasta teosta kummassakin valvontamenettelyssä.

Sääntelystä seuraisi henkilöstövaikutuksia ja vaikutuksia tiedonhallintaan. Tietojärjestelmämuutoksesta seuraavat kertaluonteiset kustannukset olisi katettava valtion talouden kehyspäätösten ja valtion talousarvion mukaisista määrärahoista. Tietosuojavaltuutetun osalta ehdotetusta sääntelystä aiheutuva pysyvä lisärahoitustarve olisi yhteensä vähintään 2,5 henkilötyövuotta, joka olisi katettava viimeistään vuoden 2025 talousarviossa (momentti 25.01.03). Koska lainsäädännön soveltaminen käynnistyisi lokakuussa 2024 ja uusi sääntely edellyttäisi valmistautumista valvontayhteistyöhön, osa vaikutuksista syntyisi viimeistään loppuvuodesta 2024. Täysimääräisesti lisätyövaikutukset toteutuisivat vuonna 2025.

Energiavirasto (Täydentyy myöhemmässä vaiheessa)

Turvallisuus- ja kemikaalivirasto

Turvallisuus- ja kemikaalivirasto (Tukes) olisi toimivaltainen viranomainen keskeisiltä ja merkittäviltä osin NIS2-direktiivin toimeenpanoa. Turvallisuus- ja kemikaalivirasto toimii kuuden eri ministeriön hallinnon alalla, ja virastoon on keskitetty kemikaalituotteisiin sekä tuotteisiin, laitteistoihin ja laitoksiin liittyviä teknisen turvallisuuden ja luotettavuuden lupa- ja valvontatehtäviä sekä Suomen arviointi- ja akkreditointipalvelut (FINAS). NIS2-direktiivin toimivaltaisen viranomaisen tehtävät ovat Tukesille uusia, eikä virastossa ole aikaisempaa osaamista ja resursseja tehtäväalueella. Toimialueet ja toimijakenttä ovat virastolle osittain tuttuja. Ehdotetut uudet tehtävät ovat elinkeinoelämän ja viraston kannalta merkittäviä ja edellyttävät virastolta uuden osaamisen hankintaa rekrytoinneilla ja uudelleen kouluttautumisella. Kyberturvauhkiin liittyvän osaamisen kehittäminen ja keskittäminen Tukesiin on perusteltua, sillä viraston lupa- ja valvontatehtävät kohdistuvat merkittäviltä osin yhteiskunnan ja turvallisuuden kannalta tärkeisiin ja kriittisiin toimialoihin, kuten vaarallisten kemikaalien valmistus, teollinen käsittely ja

varastointi (laitokset, jotka voivat aiheuttaa suuronnettomuusvaaraa), sähkötuotteet ja sähkölaitteistot, painelaitteet ja painelaitteiden käytönaikainen valvonta, mittauslaitteet ja mittausten luotettavuus, kaivostoiminta sekä energia-ala, kuten maa- ja biokaasut sekä vety. Pitkällä aikavälillä kyberturvallisuuteen liittyvien tehtävien yhdistäminen Tukesin nykyisiin tehtäviin on yhteiskunnan ja tärkeiden toimialojen turvallisuuden kannalta tarkoituksenmukaista sekä kriittisen osaamisen kehittämisen että kustannustehokkuuden kannalta.

Kokonaisresurssitarve uusiin lakisääteisiin viranomaistehtäviin arvioidaan olevan vuosina 2024–2026 viisi asiantuntijahenkilötyövuotta (5 htv) säädösmuutosten toimeenpanemiseksi sekä uusien viranomaisvalvontamenettelyjen kehittämiseksi. Määrärahaa arvioidaan uudelleen vuonna 2026, kun kokemusta toimijakentän laajuudesta ja valvontakentän haastavuudesta on karttunut.

Turvallisuus- ja kemikaalivirastolle esitetään lisäresursseja vuodesta 2024 (32.01.08) eteenpäin yhteensä 510 000 euroa (5 htv 450 000 ja 60 000 Vallu-järjestelmän ylläpitokustannuksiin). Lisäksi esitetään kertaluonteisesti vuodelle 2024 Vallu-järjestelmän uudistamiseen 200 000 euroa.

Taulukko (tuhatta euroa)

	2024	2025	2026	2027
Henkilöstökulut (5 htv)	450	450	450 (+mahdollinen lisä-htv tarve)	450 (+mahdollinen lisä-htv tarve)
Investointimenot (VALLU)	200 (kertaluontoinen)	0	0	0
Edelliseen liittyvät ylläpitokustannukset	0	60	60	60
TAE-lisäys yhteensä	650	510	510 (+lisä-htv-tarve)	510 (+lisä-htv-tarve?)

Etelä-Savon ELY-keskus

Etelä-Savon ELY-keskuksen osalta vesihuollon, eli juomavesi- ja jätevesilaitosten valvontaviranomaisen tehtävästä aiheutuvat vaikutukset koostuvat pysyvästä valvontatarpeesta, 1. lakiehdotuksen 29 §:n mukaisiin tarkastuksiin tarvittavasta ostopalvelusta sekä kertaluonteisista investoinneista. NIS2-direktiivin viranomaisvalvonta integroidaan osaksi vesihuollon varautumissuunnitelmien valvontaa, jota tehostettaisiin. NIS2-direktiivin soveltamisalaan kuuluvilta vesihuoltolaitoksilta vaadittaisiin selvitys lain vaatimusten täyttämisestä ja kyseiset asiat tulisi sisällyttää vesihuoltolain mukaiseen varautumissuunnitelmaan, joka toimitetaan valvovalle viranomaiselle tietyin väliajoin. Lain 29 § mukaisissa tarkistuksissa tarkastuksissa käytetään apuna ulkopuolisen tietotekniikan asiantuntijoiden palveluita mm tarvittavien testien ja mittausten toteutukseen. Kertaluonteiset investoinnit koostuvat vesihuollon tietojärjestelmään tehtävistä tarvittavista muutoksista valvontatoiminnallisuuksiin. Soveltamisalaan kuuluvia valvottavia laitoksia arvioidaan olevan yhteensä ainakin noin 20-40 kpl. Etelä-Savon ELY-keskuksen

valvontatehtäviin tarvittava pysyvä lisävoimavara on 3 htv. Vastaavasti esitetään pysyvää määrärahaa 100 000 euroa per vuosi asiantuntijapalveluiden ostopalveluihin. Momentille esitetään tarvittavien tietojärjestelmien kehittämiseen 100 000 euroa vuodelle 2025.

NIS2-direktiivin soveltamisalan keskeisiin toimijoihin, joihin valvontaa ainakin kohdistetaan, kuuluu 3 § 1 momentin 1 kohdan mukaan suoraan 2 vesihuoltolaitosta. CER-direktiivin toimeenpanosta tulevasta soveltamisalasta riippuen NIS2-direktiivin mukaan valvottavia laitoksia arvioidaan olevan yhteensä ainakin noin 20-40 kpl. Etelä-Savon ELY-keskuksen valvontatehtäviin tarvittava pysyvä lisävoimavara on 3 htv. Vastaavasti esitetään pysyvää määrärahaa 100 000 euroa / vuosi asiantuntijapalveluiden ostopalveluihin. Momentille esitetään tarvittavien tietojärjestelmien kehittämiseen 100 000 euroa vuodelle 2025.

Etelä-Savon ELY-keskukselle jätehuollon valvonnan osalta kyse olisi kokonaan uusista tehtävistä. Nykytilanteessa ns. Y-alustan järjestelmät, kuten ympäristölupien valvontajärjestelmä, jätehuoltorekisteri, ym., joita käytetään ympäristölupavalvonnan ja jätehuoltorekisteriasioiden käsittelyyn ja raportointiin eivät sellaisenaan sovellu NIS2-direktiivin toimeenpanoon tai valvottavien toimijoiden seulontaan. Järjestelmissä ei käsitellä yritysten taloustietoja tai tietoja yritysten henkilöstömääristä, jotka ovat tarpeellisia toimijoiden seulonnassa. Lisäksi Y-alustan järjestelmissä ei voida käsitellä turvaluokiteltuja asiakirjoja, joita turvallisuusjärjestelyihin liittyvät asiakirjat ovat. Y-alustan asiakirjojen arkistointi tehdään USPA-asianhallintajärjestelmässä.

Etelä-Savon ELY-keskuksen arvion mukaan direktiivin velvoitteiden täytäntöönpano edellyttäisi jätehuollon osalta järjestelmien päivittämistä ja jatkokehittämistä sekä väliaikaista ja pysyvää henkilöstöresurssien tarvetta. Järjestelmien kehitys edellyttäisi kertaluonteista 0,2M€ suuruista kustannusta. Järjestelmien vuosittaisiksi ylläpitokustannuksiksi arvioitaisiin 0,05 M€ vuodesta 2025 alkaen, koska järjestelmät kuuluisivat vain osin olemassa olevien ylläpitosopimusten piiriin. Toimeenpanon valmistelussa ja alussa edellytettäisiin 1 htv (80 000€) kertaluonteista henkilöstöresurssin tarvetta ja pysyvää 1,5 htvn (120 000€) lisäresurssitarvetta. Alussa edellytettäisiin siis yhteensä 2,5 htv:n (200 000€) lisäresurssitarvetta. Erityisesti toiminnan alkaessa tarve tiedottamiselle, neuvonnalle sekä kouluttamiselle korostuu, mikä edellyttäisi noin 40 000€ kertaluonteista kustannusta. Edellä mainituilla lisäresursseilla Etelä-Savon ELY-keskus suoriutuisi direktiivin toimeenpanon edellyttämistä tehtävistä vähimmäistasolla. Lisämäärärahatarpeet kohdistuisivat työ- ja elinkeinoministeriön pääluokkaan momentille 32.01.02 Elinkeino- liikenne ja ympäristökeskusten toimintamenot.

Ruokavirasto

Ruokavirastolle uudet tehtävät aiheuttaisivat yhteensä 5 htv:n lisäresurssitarpeen hallituksen esityksen mukaisiin toimeenpanotehtäviin. Lisäksi Ruokavirastolle aiheutuisi kustannuksia tehtävien toteuttamiseksi tarpeellisista tietojärjestelmäinvestoinneista 0,54 M€ vuodelle 2024 ja 0,05 M€ vuodesta 2025 alkaen. Tällä resurssitasolla Ruokavirasto suoriutuisi NIS2-direktiivin toimeenpanon edellyttämistä tehtävistä vähimmäistasolla hyödyntäen mahdollisuuksia tehostaa nykyisiä toimintoja ja kohdentaa olemassa olevia resursseja uudelleen viraston sisällä. Vuoden 2024 osalta määrärahan lisäysesitys on tarkoitus tehdä momentille 30.20.01 (Ruokaviraston toimintamenot) kevään lisätalousarviossa ja muutoin normaalin kehys- ja talousarviovalmistelun yhteydessä.

Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira

Sosiaali- ja terveysalan lupa- ja valvontavirasto Valviralle esitys toisi uusia valvontatehtäviä. NIS2-direktiivin mukaiseen valvontaan ei Valvirassa ole tällä hetkellä osoittaa henkilöresurssia. Valviralla tulisi olla valmius arviolta vähintään kymmeniin vuosittaisiin NIS2-tarkastuksiin,

NIS-häiriöilmoitusten nykyistä nopeampaan käsittelyyn ja NIS-organisaatiorekisterin ylläpitoon. Valviran arvion mukaan velvoitteiden täytäntöönpano edellyttäisi 2 htv:n lisäresurssitarpeen valvontaa varten sekä tietojärjestelmien osalta kertaluontoista investointia n. 0,15 M€ ja jatkuvia kustannuksia noin 10 000 – 20 000 euroa vuodessa.

Lääkealan turvallisuus- ja kehittämiskeskus Fimea (Täydentyy myöhemmin)

Muut viranomaiskustannukset

Finanssivalvonnalle ei aiheutuisi esityksestä aiheutuvia uusia resurssitarpeita.

Riskienhallinta- ja raportointivelvoitteiden lisäksi sääntelyssä esitetään verkkotunnusrekisterin ylläpitäjälle eräitä uusia velvoitteita. Suomessa rekisteriä fi-maatunnukseen päättyvistä verkkotunnuksista ylläpitää Liikenne- ja viestintävirasto. Liikenne- ja viestintävirastolle asetettaisiin velvollisuus julkaista verkkotunnusrekisterin tiedot sähköisessä palvelussa sekä vastata rekisterin sisältämiä henkilötietoja koskeviin tietopyyntöihin ilman aiheetonta viivytystä ja viimeistään 72 tunnin kuluessa pyynnön vastaanottamisesta. Liikenne- ja viestintäviraston olisi lisäksi julkaistava käytössään olevat toimintaperiaatteet ja menettelyt käyttäjätietojen oikeellisuuden varmentamisesta sekä verkkotunnusten rekisteröintitietojen luovuttamisesta. Liikenne- ja viestintävirastolle aiheutuisi näistä tehtävistä kustannuksia.

Lisäksi viranomaiskustannuksia aiheutuisi vähäisissä määrin kyberturvallisuusstrategian laatimisesta sekä laajamittaisten kyberturvallisuuskriisien ja –poikkeamien hallintasuunnitelman laatimisesta ja näiden ajantasaisena pitämisestä. Kuvatut kustannukset katetaan asianomaisten viranomaisten olemassa olevien määrärahojen puitteissa.

Vaikutukset julkishallinnon toimijoille riskienhallinta- ja raportointivelvoitteiden kohteena

Riskienhallinta- ja raportointivelvoitteita olisi sovellettava myös julkishallinnon toimijoissa NIS2-direktiivin toimeenpanemiseksi. Näin ollen soveltamisen kohteena oleville julkishallinnon toimijoille aiheutuisi esityksestä vaikutuksia myös velvoitteiden noudattamisesta. Velvoitteista ja niiden soveltamisalasta ehdotetaan säädettäväksi tiedonhallintalaissa.

Hallituksen esityksessä ehdotetaan tiedonhallintalakiin uutta 4 a lukua, jossa säädettäisiin NIS2-direktiivin mukaisista kyberturvallisuutta koskevista velvoitteista luvun soveltamisalaan kuuluville valtion virastoille ja laitoksille, valtion liikelaitoksille, itsenäisille julkisoikeudellisille laitoksille sekä hyvinvointialueille, hyvinvointiyhtymille ja Helsingin kaupungille niiden hoitaessa laissa hyvinvointialueiden hoidettavaksi säädettyjä tehtäviä.

Esityksessä ehdotetaan, että soveltamisalaan kuuluvan tiedonhallintayksikön olisi ilmoittauduttava Liikenne- ja viestintävirastolle kyseisen sääntelyn mukaiseksi toimijaksi. Direktiivin sääntelyn mukaisesti tiedonhallintayksikön olisi tunnistettava, arvioitava ja hallittava sen toiminnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen kohdistuvia riskejä, ylläpidettävä kyberturvallisuuden riskienhallinnan toimintamallia sekä toteutettava kyberturvallisuuden riskienhallintatoimenpiteitä. Tiedonhallintayksikön johto vastaisi kyberturvallisuuden riskienhallinnan toteuttamisesta ja valvonnasta sekä hyväksyisi kyberturvallisuuden riskienhallinnan toimintamallin. Tiedonhallintayksikön johdolla tulisi olla riittävä perehtyneisyys kyberturvallisuuden riskienhallintaan.

Tiedonhallintalain 4 luvussa säädetään tietoturvallisuuteen liittyvistä tiedonhallintayksikköä ja viranomaisia koskevista velvoitteista ja vaatimuksista. Lisäksi lain 4 §:n 2 momentissa on säädetty tiedonhallintayksikön johdon vastuista. Mainittua sääntelyä sovelletaan myös ehdotetun sääntelyn soveltamisalaan kuuluviin viranomaisiin ja tiedonhallintayksiköihin. Kuten nykytilaa koskevassa jaksossa 3.16 on kuvattu, voimassa oleva tiedonhallintalain sääntely kattaa osin jo nykyisellään kyseiset direktiivin mukaiset velvoitteet. Vaikka direktiivin mukainen sääntely edellyttää nimenomaista sääntelyä kyberturvallisuuden osalta, siitä ei aiheutuisi viranomaisille ja tiedonhallintayksiköille sellaisia uusia velvoitteita ja vaatimuksia, jotka lisäisivät niiden työtä olennaisesti siitä, mihin jo voimassa oleva tiedonhallintalain sääntely velvoittaa. Lähinnä kyse olisi kyberturvallisuutta koskevien riskien huomioimisesta omana kokonaisuutenaan, kun nykysääntelyn nojalla kyberturvallisuus on tullut ottaa huomioon osana tietoturvallisuutta. Myöskään tiedonhallintayksikön johdon vastuut eivät lisääntyisi merkittävästi nykyisestä.

Tiedonhallintalain 4 a luvun soveltamisalaan kuuluvalla tiedonhallintayksiköllä olisi velvollisuus ilmoittaa merkittävistä poikkeamista Liikenne- ja viestintävirastolle. Ilmoitusvelvollisuus jakautuisi 24 tunnin kuluessa tehtävään ensi-ilmoitukseen, 72 tunnin kuluessa tehtävään jatkoilmoitukseen sekä kuukauden kuluessa toimitettavaan loppuraporttiin. Jos poikkeama on edelleen meneillään, kun loppuraportti pitäisi toimittaa, olisi loppuraportin sijaan toimitettava edistymisraportti. Direktiivin mukaiset määräajat alkavat kulua, kun tiedonhallintayksikkö on tullut tietoiseksi poikkeamasta.

Mainitun ensi- ja jatkoilmoituksen ei tarvitsisi olla sisällöltään laajoja. Lähtökohtaisesti ilmoitusvelvollisuuden täyttää lyhyt kuvaus poikkeamasta ja arvio siitä, epäilläänkö merkittävän poikkeaman johtuvan lainvastaisista tai vihamielisistä teoista ja voiko sillä olla rajat ylittäviä vaikutuksia. Loppuraportin laatiminen vaatisi viranomaiselta mainittuja ilmoituksia enemmän työtä. Toisaalta sen työstämiseen olisi aikaa kuukausi ilmoitusvelvollisuuden alkamisesta. On epätodennäköistä, että viranomaisella olisi jatkuvaluonteisesti työstettävänään sääntelyssä tarkoitettuja loppuraportteja, vaan kysymys olisi toisinaan tapahtuvasta työstä, joka olisi toteutettavissa olemassa olevilla resursseilla. Direktiivin sääntely ei myöskään edellytä jatkuvan valvonnan tai muiden vastaavien toimien järjestämistä poikkeamien havaitsemiseksi. Viranomaisen/tiedonhallintayksikön tulisikin arvioida riskiarvionsa mukaisesti, miten se olemassa olevilla resursseillaan järjestää tarvittavat toimet poikkeamien havaitsemiseksi ja niistä ilmoittamiseksi.

Soveltamisalaan kuuluvan viranomaisen olisi mahdollista saada sääntelyn mukaisten velvoitteiden toteuttamiseen tukea sääntelyä valvovalta Liikenne- ja viestintävirastolta, jonka tehtävään kuuluisi tiedonhallintalain 4 a lukua koskeva yleinen ohjaus- ja neuvontavelvoite. Liikenne- ja viestintävirasto antaisi myös ohjeita ja neuvoja poikkeamien käsittelyssä. Kyberturvallisuuden riskienhallinnalla tiedonhallintayksikköjen ja viranomaisten toiminnan kyberturvallisuus myös paranee ja tämä todennäköisesti ennalta ehkäisee poikkeamia ja niiden haitallisia vaikutuksia. Soveltamisalaan kuuluvat viranomaiset ovat kehittäneet kyberturvallisuuden tasoaan osana nykyistä varautumista ja nykyisten tehtävien hoitaminen edellyttää kyberturvallisuuden riskienhallinnasta huolehtimista. NIS2-direktiivin toimeenpanemiseksi tiedonhallintalakiin ehdotettavien muutosten ei siten katsota aiheuttavan kaikille viranomaisille merkittäviä lisäresurssitarpeita, jotka aiheutuisivat viranomaisille NIS2-direktiivin edellyttämien velvoitteiden kohteena olemisesta. Osalla viranomaisista ehdotettu sääntely kuitenkin voisi edellyttää valmiustason nostamista sekä tietojärjestelmämuutoksia. Sääntelyn noudattamisesta aiheutuvat kustannukset olisi katettava valtion talouden kehyspäätösten ja valtion talousarvion mukaisista määrärahoista.

Esityksessä ehdotetaan lisäksi, että tiedonhallintalain 18 §:ssä säädetty asiakirjojen turvallisuusluokitteluvelvoite koskisi myös Suomen Erillisverkot Oy:tä ja sen kokonaan omistamaa tytäryhtiötä niiden hoitaessa julkisen hallinnon turvallisuusverkkolaissa tarkoitettuja tehtäviä. Mai-

nituilla toimijoilla on olemassa valmiudet asiakirjojen turvallisuusluokitteluun ja turvallisuusluokiteltujen asiakirjojen käsittelyyn eikä ehdotetulla velvoitteella siten olisi erityisiä vaikutuksia niiden toimintaan. Turvallisuusverkkotoiminnassa tapahtuvassa tiedonvaihdossa ja yhteistyössä asiakirjojen käsittely niitä turvallisuusluokittelevien viranomaisten kanssa on myös selkeämpää, kun on olemassa yhtenäiset laissa säädetyt vaatimukset asiakirjojen merkitsemisestä ja niiden käsittelyssä noudatettavista menettelyistä.

4.5 Muut ihmisiin kohdistuvat ja yhteiskunnalliset vaikutukset

Vaikutukset turvallisuuteen

Yhteiskuntien digitaalinen kehitys, jota muun muassa COVID-19 –pandemia on vauhdittanut, on muuttanut oleellisesti nykyistä toimintaympäristöä ja tuonut mukanaan uusia haasteita. Viestintäverkkojen ja tietojärjestelmien määrä ja niiden merkitys osana yhteiskunnan toiminnan edellyttämien palveluiden tuottamista ja yhteiskunnan kriittisen infrastruktuurin toimintaa kasvaa jatkuvasti. Kyberuhkien ja -hyökkäyksien määrä on kasvanut ja kyberhyökkäykset kehittyvät jatkuvasti teknologian kehittyessä. Yhteiskunnan kannalta kriittiset toiminnot ovat entistä riippuvaisempia tietojärjestelmistä ja viestintäverkoista, joissa esiintyvällä kyberhäiriöllä voi olla merkittäviä haitallisia vaikutuksia paitsi häiriön kohteena olevaan toimijaan, myös yhteiskuntaan laajemmin. Myös ulko- ja turvallisuuspolitiikan muutokset ovat heijastuneet kyberympäristöön. Palvelunestohyökkäysten, murtautumisten, haittaohjelmien ja valtiollisen toiminnan riski on kasvanut ja uhkataso noussut. Kyberhyökkäyksiä käytetään osana yhteiskuntaan kohdistuvaa hybridivaikuttamista.

Esityksellä vahvistettaisiin yhteiskunnan yleistä kyberturvallisuustasoa ja kriisinkestävyyttä. Kyberturvallisuusosaamisen ja kyberturvallisuuden riskienhallintatoimien parantuessa haitallisten vaikutusten aiheuttaminen yhteiskunnan toiminnan kannalta keskeisille palveluille vaikeutuu ja kallistuu. Esitykseen sisältyvillä ehdotuksilla kansallisen kyberturvallisuusstrategian sekä laajamittaisen kyberkriisinhallintasuunnitelman laatimisesta pyritään kehittämään koko yhteiskunnan kyberturvallisuutta kokonaisuutena sekä valmiutta vastata laajamittaisiin ja jäsenvaltioiden rajat ylittäviin kyberpoikkeamiin.

Esityksellä parannettaisiin yhteiskunnan toiminnan kannalta keskeisten toimijoiden toiminta-edellytyksiä muuttuneessa toimintaympäristössä. Ehdotus yhdenmukaistaisi kyberturvallisuuden riskienhallinta- ja raportointivaatimuksia eri toimialoilla ja laajentaisi kyberturvallisuussääntelyn kattamaan useampia toimijoita. Esityksessä painotetaan varautumista ja ennaltaehkäiseviä toimenpiteitä, jotta kybertoimintaympäristön muutoksiin, häiriöihin ja haavoittuvuuksiin voidaan vastata entistä ennakoivammin. Tavoitteena on välttää kyberhäiriöiden aiheuttamia keskeytyksiä yhteiskunnan toiminnan kannalta keskeisten palveluiden tai toimintojen jatkuvuudessa, sillä häiriö kriittisen palvelun tarjonnassa voi aiheuttaa yhteiskunnalle merkittävää vahinkoa. Yhdessä yhteiskunnan kriittisessä toiminnossa (esimerkiksi energiantuotannossa tai viestintäverkkojen toiminnassa) tapahtunut häiriö voi merkittävästi vaikuttaa myös muiden kriittisten palvelujen tarjoamiseen sekä aiheuttaa laajamittaisia haitallisia vaikutuksia yhteiskunnassa. Lisäksi vaikutukset eräiden kriittisten palvelujen jatkuvuuteen voivat aiheuttaa paitsi taloudellisia menetyksiä, myös esimerkiksi kansalaisten henkeen ja terveyteen kohdistuvia uhkia. Riskienhallinnassa olisi huomioitava myös kyberturvallisuusuhkien poikkisektorisuus ja toimitusketjujen merkitys. Esityksen velvoitteet ovat investointi yhteiskunnan toimintavarmuuteen ja kyberkestävyyteen.

Merkittävistä poikkeamista raportointi erityisesti loppuraportoinnin osalta parantaisi tiedonkulkua keskeisille viranomaisille ja siten yhteisen tilannekuvan muodostamista merkittävistä poikkeamista ja niiden syistä yhteiskunnassa. Yhdistettynä vastaaviin velvoitteisiin muissa EU-jäsenvaltioissa NIS2-direktiivin toimeenpano lisää viranomaisten ENISA:n kautta kyberhäiriöistä saamien tietojen määrää. Lisäksi esitys sisältää useita ehdotuksia, joilla vahvistetaan yhteistyötä ja tietojenvaihtoa viranomaisten ja velvoitteiden piiriin kuuluvien toimijoiden välillä.

Viestintäverkot ja tietojärjestelmät ovat globaalisti sidoksissa toisiinsa ja myös toiseen jäsenvaltioon kohdistuvalla kyberhyökkäyksellä tai -häiriöllä voi olla heijastevaikutuksia Suomeen. NIS2-direktiivin toimeenpano EU:n jäsenvaltioissa parantaa yleistä kyberhäiriöiden sietoisuuden ja niihin varautumisen tasoa koko EU:n laajuisesti yhdenmukaistamalla kriittisten sektoreiden kyberturvallisuusvaatimuksia sekä parantamalla jäsenvaltioiden yhteistyötä rajat ylittävissä kyberhäiriötilanteissa. Ehdotus vähentäisi myös sisämarkkinoiden fragmentoituneisuutta ja tasaisi toimijoiden toimintaedellytyksiä. Kyberturvallisuushäiriöt vaikeuttavat sisämarkkinoiden toimintaa, aiheuttavat taloudellisia menetyksiä ja heikentävät käyttäjien luottamusta unionin talous- ja yhteiskuntaelämään. Tehokkaalla kyberturvallisuuden riskienhallinnalla voidaan vähentää kyberturvallisuushäiriöiden määrää sekä niistä aiheutuvia vaikutuksia.

Vaikutukset tietoyhteiskuntaan ja tietosuojaan

Esityksellä olisi myönteisiä vaikutuksia tietoyhteiskunnan kehitykseen, sillä se edistäisi tietoturvallisten palvelujen ja käytänteiden käyttöönottoa ja siten loisi kysyntää tällaisille palveluille sekä kyberturvallisuuden ammattilaisille. Kyberturvallisuustason parantuminen vähentäisi palvelujen käytössä esiintyviä häiriöitä ja edistäisi yleistä luottamusta digitaalisiin palveluihin.

Sääntelyn edellyttämien koulutusvaatimusten arvioidaan myös lisäävän henkilöstön tietoisuutta ja ymmärrystä tietoturvasta etenkin sellaisissa organisaatioissa, joissa tällaista koulutusta ei ole aikaisemmin tarjottu. Kansallisen kyberturvallisuuden parantaminen edellyttää paitsi kyberturvallisuuden huippuosaajia, myös entistä parempaa tietoturvaosaamista kansalaisten ja yritysten arjessa. Esitys nostaisi kyberturvallisuuden riskienhallinnan osaamisen kysyntää ja kasvattaisi kyberturvallisuuden riskienhallinnan osaamista soveltamisalaan kuuluvissa toimijoissa.

Esityksen on arvioitu parantavan myös viranomaisten kyberturvallisuusosaamista. Ehdotettu sektorikohtainen valvontamalli edistäisi sektorikohtaisen kyberturvallisuusosaamisen kehittymistä sektorikohtaisissa valvovissa viranomaisissa. Lisäksi raportointivelvollisuuden laajentaminen useammille sektoreille ja toimijoihin lisää myös viranomaisten ymmärrystä toimijoihin kohdistuvista kyberuhista.

Tietojärjestelmissä ja viestintäverkoissa käsiteltävien tietojen tietosuoja edellyttää järjestelmien tietoturvaominaisuuksien kehittämistä. Toimenpiteet tietojärjestelmien ja viestintäverkkojen kyberturvallisuuden parantamiseksi vaikuttavat niissä käsiteltävien tietojen tietosuojaan sitä parantavasti.

Esityksellä olisi tiedonhallintalain 8 §:n 2 momentissa tarkoitettuja vaikutuksia tietoaineistoihin ja tietojärjestelmiin. Esitystä täydennetään tiedonhallinnan muutosvaikutusten arvioinnilla.

Ympäristövaikutukset

Esityksellä ei ole tunnistettu olevan merkittäviä ympäristövaikutuksia.

Esitys edesauttaisi viimeisimmän sukupolven ICT-infrastruktuurin ja –palvelujen parempaa hyödyntämistä, jotka olisivat ympäristön kannalta kestävämpiä. Esityksellä vahvistetaan sellaisten kriittisten sektoreiden kyberturvallisuutta, joihin kohdistuvat kyberturvallisuusriskit ja merkittävät poikkeamat voisivat toteutuessaan aiheuttaa sekä välittömiä että välillisiä vakavia seurauksia ympäristölle. Tältä osin erityisen merkityksellisiä sektoreita olisivat energia-ala, jätehuolto ja vesihuolto. Esitys edesauttaisi välillisesti merkittävistä poikkeamista aiheutuvien ympäristölle haitallisten seurausten torjumista parantamalla toimijoiden kyberturvallisuuden riskienhallintaa ympäristölle merkityksellisillä toimialoilla.

5 Muut toteuttamisvaihtoehdot

5.1 Vaihtoehdot ja niiden vaikutukset

5.1.1 Riskienhallinta- ja raportointivelvoitteiden kansalliset laajennukset

NIS2-direktiivin kansallinen täytäntöönpano edellyttää direktiivin asettamista velvoitteista säätämistä lain tasolla. NIS2-direktiivin velvoitteissa on pääosin kyse yksityiskohtaisesta ja vähimmäisharmonisoivasta sääntelystä. Kansallista liikkumavaraa ei pääosin liity NIS2-direktiivin vähimmäissoveltamisalaan tai velvoitteiden sisältöön. Kansallinen liikkumavara on kuvattu edellä jaksossa 2.10.

NIS2-direktiivin täytäntöönpanossa vaihtoehtoina on arvioitu vähimmäistason mukaista täytäntöönpanoa suhteessa kansallisesti korkeatasoisempien riskienhallinta- ja raportointivelvoitteiden asettamiseen tai soveltamisalan laajentamiseen. EU:n sisämarkkinoilla toimivien yrityksien näkökulmasta NIS2-direktiiviä täytäntöönpanevan kansallisen sääntelyn yhteismitallisuus Suomessa suhteessa muihin jäsenvaltioihin olisi tavoiteltavaa, jotta NIS2-direktiivin vaatimukset soveltamisalaan kuuluvalle toimijalle olisivat mahdollisimman yhteismitalliset jäsenvaltioissa. NIS2-direktiiviä täytäntöönpanevan sääntelyn yhteismitallisuuden vuoksi suhteessa muihin jäsenvaltioihin esityksen lähtökohdaksi on valikoitunut riskienhallinta- ja raportointivelvoitteiden vähimmäistaso direktiivin asettamalla tasolla.

5.1.2 Sääntelymalli muuten kuin julkishallinnon toimialalla

Esityksen valmistelussa on arvioitu sääntelyn toteuttamista joko ehdotetussa muodossa eli yhdellä eräiden toimijoiden kyberturvallisuuden riskienhallinnasta annettavalla lailla tai ottamalla NIS2-direktiivin täytäntöönpanosäännökset osaksi sektorikohtaista lainsäädäntöä. NIS1-direktiivin täytäntöönpanossa päädyttiin lisäämään direktiivin täytäntöönpanosäännökset osaksi sektorikohtaista lainsäädäntöä. NIS1-direktiivin edellyttämät riskienhallinta- ja raportointivelvoitteet olivat kuitenkin huomattavasti yleisluonteisempia ja avoimempia kuin NIS2-direktiivin vastaavat velvoitteet. NIS1-direktiivin täytäntöönpanon yhteydessä katsottiinkin, etteivät kyseiset velvoitteet eronneet muusta toimijan riskienhallinnasta sillä tavoin, että siitä olisi ollut aiheellista säätää eri laissa (HE 192/2017 vp). NIS2-direktiivissä asetettavat riskienhallinta- ja raportointivelvoitteet ovat kuitenkin huomattavasti yksityiskohtaisempia, eikä esimerkiksi toimijalle asetetun yleisen varautumis- tai riskienhallintavelvoitteen voida enää katsoa vastaavan NIS2-direktiivin velvoitteita. Valittavaan sääntelytapaan vaikuttaa vahvasti myös kyberturvallisuuden merkityksen kasvu viimeisen viiden vuoden aikana. Suomi oli poikkeus EU:ssa NIS1-direktiivin täytäntöönpanossa noudatetun hajautetun sääntelytavan osalta. Merkittävä osa muista jäsenvaltioista otti käyttöön jo viimeistään NIS1-direktiivin täytäntöönpanon yhteydessä yhden ns. kyberturvallisuuslain.

Yhden lain malli on kannatettava vaihtoehto myös siksi, että se täyttäisi paremmin NIS2-direktiivin tavoitteen, eli osoittaisi kyberturvallisuusvelvoitteiden vähimmäistason. Nyt ehdotetun eräiden toimijoiden kyberturvallisuuden riskienhallinnasta annettavan lain tarkoituksena olisi toimia paitsi yhteiskunnan toiminnan kannalta kriittisten toimijoiden kyberturvallisuussääntelynä, myös yleisenä esimerkkinä kyberturvallisuusvelvoitteiden sääntelykehikosta. Näin ollen yhden lain malli myös selkeyttäisi kansallista kyberturvallisuussääntelyä, joka on Suomessa hajautettu lukuisiin sektorikohtaisiin säädöksiin ja kyberturvallisuutta koskeviin yksittäisiin säännöksiin. Valintaa puoltaa myös se, että NIS2-direktiivin soveltamisala on huomattavasti laajempi kuin NIS1-direktiivin soveltamisala, eikä kaikkea soveltamisalaan kuuluvaa toimintaa toimijatyyppien ja toimialojen osalta ole säännelty ennestään. Näin ollen velvoitteista säätäminen sektorikohtaisesti hajauttaen edellyttäisi lisäyksiä lukuisiin sektorilakeihin sekä kokonaan uuden lain tai muun ratkaisun niiden toimijoiden osalta, joita koskevaa sektorikohtaista sääntelyä ei ole. On huomattava, että NIS2-direktiivin soveltamisalaan kuuluu hieman yli kaksinkertainen määrä sektoreita verrattuna NIS1-direktiiviin. NIS2-direktiivin sääntely toimijoihin kohdistuvien velvoitteiden ja niiden valvonnan osalta on myös NIS1-direktiivin sääntelyä tarkempaa ja yksityiskohtaisempaa, mikä aiheuttaisi sektorikohtaisesti hajauttaen useaan sektorilakiin merkittävän määrän toisiaan vastaavia uusia säännöksiä, joiden soveltamisala voisi poiketa lain muiden säännösten soveltamisalasta. Tätä ei voida pitää sääntelyn selkeyden ja sääntelytaakan näkökulmasta tavoiteltavana. Täytyy myös huomioida, että yhden lain mallia tulisi todennäköisesti täydentää kyberturvallisuuden korkean tason varmistamiseksi eri sektoreiden alakohtaisella alemman tason sääntelyllä, jossa voidaan tarvittaessa määrätä yksityiskohtaisemmalla tasolla kyberturvallisuuden varmistamisesta soveltamisalaan kuuluvien toimijoiden toiminnassa. Tällä tavalla toteutettuna kaikilla sektoreilla olisi yhteiset velvoitteet ja tavoitteet uudessa yleislaissa, jonka vaatimuksia voitaisiin tarkentaa sektorikohtaisesti.

5.1.3 Julkishallinnon toimialan NIS2 -erityislaki ja soveltaminen julkishallinnon toimialalla

Julkishallinnon toimiala puhtaasti julkishallinnon toiminnan harjoittamisen ominaisuudessa on NIS2-direktiivissä uutta sääntelyä suhteessa NIS1-direktiiviin. Julkishallinnon toimialaan liittyy direktiivissä useita säännöksiä, joihin sisältyy kansallista harkintaa ja liikkumavaraa. Nämä säännökset liittyvät muun muassa soveltamisalaan kuuluviin toimijoihin ja käsiteltäviin tietoihin, joiden osalta direktiivin ulkopuolelle on rajattu muun muassa kansalliseen turvallisuuteen, yleiseen turvallisuuteen tai puolustukseen liittyvät tiedot. Lisäksi poikkeuksia sisältyy toimijoiden valvontaa ja seuraamuksia koskeviin säännöksiin. Tietojen käsittelyn rajoitukset koskevat myös muiden toimialojen piiriin kuuluvaa toimintaa, mutta liittyvät erityisesti julkishallinnon toimialaan.

Julkishallinnon tietoturvallisuutta koskee yleislain tasoinen laki eli tiedonhallintalaki, jonka sisältämä sääntely kattaa NIS2-direktiivin sääntelyn jaksossa 3.16 kuvatuilta osin. NIS2-direktiivin edellyttämä sääntely on julkishallinnon toimialan kansallisen liikkumavaran ja sen erityispiirteiden vuoksi katsottu tarkoituksenmukaiseksi sijoittaa tiedonhallintalakiin, jolloin julkishallinnon toimialan toimijoiden yleislain tasoiset tietoturvallisuuteen liittyvät velvoitteet olisivat kootusti yhdessä laissa. NIS2-säännöksillä tiedonhallintalaissa olisi muusta soveltamisesta poikkeava soveltamisala ja sääntely koottaisiin tästä syystä yhteen lukuun, jossa velvoitteet ja niiden valvonta olisi järjestetty julkishallinnon toimialan osalta. Sektorikohtaisen valvonnan ja julkishallinnon tilannetietoisuuden osalta on myös tarkoituksenmukaista, että julkishallinnon toimijoilla on erikseen säädetty valvonta ja valvova viranomainen suhteessa muihin toimialoihin, joilla toimii myös julkisia toimijoita. Julkinen toimija voi harjoittamansa toiminnan osalta kuulua eräiden toimijoiden kyberturvallisuuden riskienhallinnasta annetun lain soveltamisalaan (esim. hyvinvointialueiden ja hyvinvointiyhtymien terveydenhuolto). Julkinen toimija voisi myös kuulua yksinomaan eräiden toimijoiden kyberturvallisuuden riskienhallinnasta annetun

lain soveltamisalaan, koska tiedonhallintalakia ei sovellettaisi esimerkiksi kuntiin ja kuntayhtymiin (pois lukien Helsingin kaupunki tietyiltä osin) eikä muihin kuin viranomaisiin, jotka hoitavat julkista hallintotehtävää. Näiden julkisten toimijoiden asema NIS2-direktiivin suhteen määräytyisi eräiden toimijoiden kyberturvallisuuden riskienhallinnasta annetun lain perusteella, jos ne harjoittavat toimintaa jollain muulla NIS2-direktiivin liitteissä I ja II mainitulla toimialalla. Esimerkkinä tällaisesta toimijasta voidaan mainita kuntayhtymä Helsingin seudun ympäristöpalvelut HSY, joka harjoittaa toimintaa muun muassa vesi- ja jätehuollon alalla. Sektorikohtaisen valvonnan ja tilannetiedon keruun vuoksi on tärkeää, että direktiivin muulla (kuin julkishallinnon toimialan) toimialalla toimiva julkinen toimija kuuluu myös kyseisen erityistoimialan valvonnan piiriin ja sitä koskee kyseisen erityistoimialan valvonta ja ilmoitusvelvollisuus.

Julkishallinnon toimialalla direktiivin velvoitteita ei katsottu tarkoituksenmukaiseksi soveltaa kansallisesti laajemmalle, kuin on välttämätöntä. Julkishallinnon toimialalla on voimassa olevaa tietoturvallisuuteen liittyvää sääntelyä. Tiedonhallintalain 4 luvun riskienhallintaa korostava tietoturvallisuussääntely soveltuu kaikkiin julkishallinnon toimijoihin mukaan lukien yksityisiin henkilöihin tai yhteisöihin, jotka hoitavat julkista hallintotehtävää. Tietoturvallisuuteen liittyviä velvoitteita sisältyy myös yleiseen tietosuoja-asetukseen. Näkökulmana on otettu myös huomioon, että tietosuoja-asetuksen nojalla on jo olemassa valvontaviranomainen, jonka tehtäviin kuuluu myös julkishallinnon toimialan valvonta. Kyberturvallisuuden osalta NIS2-direktiivissä edellytetään, että myös julkishallinnon velvoitteiden noudattamista on valvottava. Valvovan viranomaisen resurssien kohdentamiseksi on tarkoituksenmukaista kohdentaa velvoitteet vain niihin, jotka myös direktiivin valmistelussa on katsottu kriittisiksi toimijoiksi. Lisäksi ehdotetussa sääntelyssä korostetaan, että muutkin julkishallinnon toimijat voivat ilmoittaa kyberuhkista, poikkeamista ja läheltä piti-tilanteista valvovalle viranomaiselle, mikä sinänsä on ollut tähänkin asti mahdollista. Ehdotetun sääntelyn johdosta Liikenne- ja viestintävirastolla olisi kuitenkin entistä selkeämpi rooli julkishallinnon ilmoitusten käsittelyssä ja tilannekuvan kokoamisessa sekä viranomaisten välisessä tiedonvaihdossa. Myös CSIRT-yksikölle ehdotetut toimivaltuudet tukevat monessa suhteessa myös julkishallinnon tieto- ja kyberturvallisuuden parantamista.

Direktiivin 2 artiklan 5 kohdan nojalla jäsenvaltiot voivat säätää, että direktiiviä sovelletaan paikallistason julkishallinnon toimijoihin tai opetus- ja koulutusalan laitoksiin, etenkin kun niissä harjoitetaan olennaisen tärkeää tutkimustoimintaa. Vaikka direktiivi sinänsä mahdollistaisi soveltamisalan laajentamisen kuntiin ja opetus- ja koulutusalan toimijoihin, näitä ei ehdoteta kuuluvaksi ehdotetun tiedonhallintalain 4 a luvun soveltamisalaan, lukuunottamatta Helsingin kaupunkia sen hoitaessa laissa hyvinvointialueiden järjestämisvastuulle säädettyjä tehtäviä.

Kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla toimiviin viranomaisiin sekä turvallisuusverkon palvelutuottajiin ja palvelujen käyttöön puolestaan liittyy edellä mainittujen lisäksi sekä tarkoituksenmukaisuusharkintaan että käsiteltävän tiedon sensitiivisyyteen liittyviä syitä, joiden vuoksi näiden toimijoiden ei ehdoteta kuuluvan sääntelyn soveltamisalaan. Mainitut toimijat ovat tiedonhallintalain velvoitteiden lisäksi jo esimerkiksi toiminnan laadun, kansainvälisten tietoturvallisuusvelvoitteiden sekä turvallisuusverkkolain ja sen nojalla annetun asetuksen sekä valtiovarainministeriön määräysten johdosta velvollisia huolehtimaan kyberturvallisuudesta varsin kattavasti. Ehdotetulla lailla ei myöskään rajoiteta mahdollisuuksia noudattaa 4 a luvun sääntelyä myös näissä viranomaisissa. Myös ne voivat ottaa huomioon ehdotetut kyberturvallisuuden riskienhallintavelvoitteet yhtenä tietoturvallisuuden tarkistuslistana. Mainitut toimijat voivat myös vapaaehtoisesti ja haluamassaan laajuudessa ilmoittaa Liikenne- ja viestintävirastolle poikkeamista sekä tehdä muuta yhteistyötä kuten tähänkin asti.

Voimassa oleva lainsäädäntö mahdollistaa tietyssä laajuudessa Liikenne- ja viestintäviraston tarkastusoikeuden myös turvallisuusverkon palveluihin (laki sähköisen viestinnän palveluista 325 § 2 momentti). Lisäksi Liikenne- ja viestintävirastolle on lainsäädännössä säädetty tehtäviä liittyen viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arviointiin ja hyväksyntään (esim. laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista ja laki kansainvälisistä tietoturvallisuusvelvoitteista). Useissa laeissa on myös säädetty virka-avusta, esimerkiksi turvallisuusverkkolain 23 §:n mukaan Puolustusvoimat, poliisi, Rajavartiolaitos ja Liikenne- ja viestintävirasto ovat valtiovarainministeriön pyynnöstä velvollisia mahdollisuuksiensa mukaan antamaan turvallisuusverkon palveluntuottajille virka-apua turvallisuusverkon palvelutuotannon häiriöttömän toiminnan takaamiseksi. Myös tässä hallituksen esityksessä CSIRT-yksiköllе ehdotetut tehtävät sekä viranomaisten välinen yhteistyö tukevat osaltaan myös näiden lain soveltamisalan ulkopuolelle jäävien kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla toimivien viranomaisten kyberturvallisuuden riskienhallintaa.

5.1.4 Valvonnan järjestäminen

Esityksen valmistelussa on arvioitu toimijoihin kohdistuvien velvoitteiden valvonnan järjestämisen osalta vaihtoehtoina joko keskitettyä tai sektorikohtaisesti hajautettua valvontamallia. NIS1-direktiiviä täytäntöönpanevan sääntelyn valvontavastuu on osoitettu niille viranomaisille, jotka valvovat toimialansa muitakin turvallisuusriskienhallintavelvoitteita sektorikohtaisen erityissääntelyn nojalla, johon NIS1-direktiivin velvoitteet on sisällytetty. Esityksen valmistelussa on siten arvioitu vaihtoehtoina, jatketaanko NIS2-direktiivin toimeenpanon yhteydessä NIS1-direktiivin aikaista valvontamallia, eli valvontavastuun jakamista sektorikohtaisesti viranomaisille, jotka valvovat toimialaansa kohdistuvia muitakin turvallisuus- ja riskienhallintavelvoitteita, vai olisiko valvonta perusteltua keskittää yhdelle toimivaltaiselle viranomaiselle, joka valvoisi NIS2-direktiivin mukaisia velvoitteita kaikilla toimialoilla.

Valmistelussa ei ole tunnistettu olemassa olevaa viranomaista, jolle olisi säädetty voimassa olevassa laissa NIS2-direktiivin vähimmäistason edellyttämät valvontatoimivaltuudet NIS2-sektoria koskien tai viranomaista, jonka nykyisiin valvontatehtäviin NIS2-direktiivin velvoitteiden valvonta olisi luontevasti sopiva osa. Valmistelussa on tunnistettu, että ehdotettujen valvontatehtävien tapaisia tehtäviä on osoitettu useille eri viranomaisille, eikä nykyisistä viranomaisista yhdelläkään ole ehdotetun sääntelyn edellyttämää laaja-alaista osaamista eri toimialojen erityispiirteistä ja kyberturvallisuudesta. Valvonnan keskittämisen näkökulmasta vaihtoehtoina on arvioitu tehtävien keskittämistä uudelle valvontataholle tai Liikenne- ja viestintäviraston Kyberturvallisuuskeskukselle, jonka erityisiin tehtäviin sisältyy yleisiä tietoturvallisuuden edistämiseen liittyviä tehtäviä ja joka tukee, ohjaa ja valvoo tietoturvallisuutta ja yksityisyyden suojan toteutumista sähköisessä viestinnässä sekä ylläpitää kansallisen kyberturvallisuuden tilannekuvaa. Valmistelussa on arvioitu, että Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen osalta rooli samanaikaisesti sekä keskitettynä valvovana viranomaisena jokaisella sektorilla että tietoturvaloukkauksia tutkivana ja ohjaavana CSIRT-yksikkönä yhdistettynä Kyberturvallisuuskeskuksen nykyisiin tehtäviin loisi laajan tehtäväkokonaisuuden, joka olisi epätarkoituksenmukainen sekä soveltamisalaan kuuluville toimijoille että viranomaiselle. Samalla tehtäväkokonaisuus aiheuttaisi haittaa Kyberturvallisuuskeskuksen nykyisten tehtävien hoitamiselle. Mikäli valvonta keskitettäisiin, olisi näin ollen perustettava uusi valvontaa suorittava viranomaistaho tai itsenäinen yksikkö olemassa olevan viranomaisen yhteyteen. Ottaen huomioon valvottavien toimijoiden määrä ja soveltamisalan laajuus sekä valvonnassa edellytetyn sektorikohtaisen osaamisen tarve, uuden valvontatahon perustaminen aiheuttaisi ennakoitavasti korkeampia kustannuksia, kuin valvonnan hajauttaminen sektorikohtaisesti.

NIS2-sektoreilla on olemassa olevia valvontaviranomaisia, jotka valvovat niille sektorikohtaisessa lainsäädännössä määritettyjä kokonaisuuksia tai osa-alueita muun ohella turvallisuuden ja riskienhallinnan osalta. Mikäli viranomaistehtävät keskitettäisiin jatkossa vain yhdelle viranomaiselle, se voisi aiheuttaa päällekkäisiä valvontatoimivaltuuksia sekä päällekkäisiä raportointivelvollisuuksia toimijoille. Valvonnan järjestämistä sektorikohtaisesti puoltaa myös se, ettei kyberturvallisuus ole valvottavan toimijan muusta toiminnasta erillinen osa, vaan yhteiskunnan digitalisoituessa kyberturvallisuus hahmotetaan toiminnan kokonaisturvallisuuden osa-alueena. Toimijan näkökulmasta erilaisten riskien hallinta hahmotetaan tyypillisesti yhtenä kokonaisuutena, eikä kyberturvallisuusriskien hallintaa tai sen valvontaa ole lähtökohtaisesti perusteltua eriyttää tai tarkastella muusta riskien hallinnasta erillisenä kokonaisuutena. Palveluun kohdistuva häiriö voi aiheutua tietojärjestelmiin kohdistuvasta häiriöstä tai muuhun turvallisuuteen liittyvästä häiriöstä. Lisäksi häiriöillä voi kyberturvallisuuden lisäksi olla todennäköisesti vaikutuksia toimijan muuhun toimintaan ja sen turvallisuuteen sektorikohtaisine erityispiirteineen. Esimerkiksi liikennesektorilla kyberhäiriö voi vaikuttaa merkittävästi myös liikenneturvallisuuteen tai terveyssektorilla asiakas- tai potilasturvallisuuteen. Näin ollen myös toimijan näkökulmasta olisi lähtökohtaisesti selkeämpi ja vähemmän hallinnollista taakkaa aiheuttava ratkaisu, ettei erilaisten riskien hallintaan tai toiminnan turvallisuuteen ja jatkuvuuteen liittyvien velvoitteiden valvontaa ja häiriöiden raportointia ole hajautettu useille viranomaisille, vaan toimijaa valvoisi lähtökohtaisesti yksi viranomainen toimintaan kohdistuvien turvallisuus- ja riskienhallintavelvoitteiden osalta.

Toimialakohtaisella lähestymistavalla ja valvonnan järjestämisellä pystytään huomioimaan sektorikohtaisia erityispiirteitä sekä ottamaan paremmin huomioon muu sektorikohtainen sääntely. Riippumatta valittavasta valvontamallista kyberturvallisuuteen liittyvää osaamista tulisikin vahvistaa joka tapauksessa kaikissa viranomaisissa niiden nykyisten valvontatehtävien toteuttamiseksi, jotta viranomaiset kykenisivät aiempaa paremmin ymmärtämään kyberturvallisuuden merkityksen valvomassaan toiminnassa. Myös valvovan viranomaisen näkökulmasta on arvioitu tarkoituksenmukaiseksi arvioida valvottavan toiminnan turvallisuutta kokonaisuutena.

Keskitetyn valvontamallin hyötynä olisi valvontamallin selkeys sellaisille toimijoille, jotka harjoittavat toimintaa usealla soveltamisalaan kuuluvalla toimialalla. Keskitetty valvontamalli keskittäisi myös kyberturvallisuuden riskienhallintavelvoitteisiin liittyvää osaamista viranomaisessa. Toisaalta keskittäminen edellyttäisi uuden, itsenäisen valvontatoiminnon tai –viranomaisen perustamista tai olemassa olevan valvontatoiminnon merkittävää laajentamista, koska olemassa olevaa viranomaista, jonka nykyisten tehtävien yhteyteen poikkihallinnollisen valvontatoiminnon voisi luontevasti yhdistää, ei ole tunnistettu. Keskitetyssä valvontamallissa valvovalle viranomaiselle tulisi huomattava määrä valvottavia toimijoita ja laaja tehtävä eri toimialoilla soveltamisalaan toimivien toimijoiden tunnistamiseksi ja valvomiseksi. Mikäli valvontatehtäviä keskitettäisiin yhdelle viranomaiselle jokaisen toimialan osalta, muodostuisi valvontakentästä huomattavan laaja.

Keskitetty valvontamalli on katsottu perustelluimmaksi vaihtoehdoksi yleisen tietosuoja-asetuksen ja sen täytäntöönpanemiseksi annetun sääntelyn valvonnassa. Toisin kuin tietosuojasääntelyssä, NIS2-direktiivin soveltamisalaan kuuluvat vain direktiivissä säädetyt kriteerit täyttävät toimijat säädetyillä toimialoilla. Toimijoiden määrä ja laatu sekä toiminnan yhteiskunnallinen merkittävyys vaihtelevat toimialakohtaisesti, mikä puoltaa valvontamallia, jossa toimialakohtaiset erityispiirteet sekä toimialakohtaisen muuta kuin kyberturvallisuutta koskevan turvallisuuden ja riskienhallinnan sääntely voidaan yhteensovittaa mahdollisimman hyvin NIS2-valvontaan. Useilla toimialoilla on tunnistettu NIS2-direktiiviä täydentävää tietoturvasääntelyä tai muuta riskienhallintaan, turvallisuuteen tai toiminnan jatkuvuuteen liittyvää olemassa olevaa sääntelyä, jolloin tällaisten valvontatehtävien keskittämisestä samaan viranomaiseen voidaan

saavuttaa synergiaetuja ja välttää päällekkäisiä valvontatoimivaltuuksia tai epäselvyyksiä toimivaltuuksien osalta.

On myös huomattava, että NIS2-direktiivin riskienhallintavelvoite on sisällöltään sellainen, että sen valvonta edellyttää valvontamallista riippumatta valvovalta viranomaiselta sekä kyseisen toimialan markkinatuntemusta, että sektorikohtaisten erityispiirteiden, kuten muun relevantin lainsäädännön ja parhaiden käytäntöjen tuntemusta. Valvovan viranomaisen olisi tunnettava valvottavaa toimialaa ja markkinaa hyvin, sillä kyberturvallisuusriskien hallinta, kuten muukin riskienhallinta, on hyvin organisaatio- ja toimialakohtaista. Erilaisiin organisaatioihin kohdistuu erilaisia riskejä, ja myös toteutuneilla häiriötilanteilla voi olla hyvin erilaiset vaikutukset yhteiskuntaan riippuen siitä, minkä sektorin toimijaan häiriö kohdistuu. NIS2-direktiivissä asetetut velvoitteet ovat luonteeltaan vähimmäissääntelyä, ja tieto- ja kyberturvallisuussääntelyssä on myös merkittäviä sektorikohtaisia eroja. Joillakin NIS2-direktiivin soveltamisalaan kuuluvilla sektoreilla on voimassa NIS2-direktiiviä täydentävää tieto- tai kyberturvallisuussääntelyä, jolla tavoitellaan NIS2-direktiiviä korkeampaa kyberturvallisuuden tasoa tai asetetaan yksityiskohtaisempia velvoitteita.

Edellä esitetyt seikat huomioiden valmistelun aikana on vaihtoehtoarvioinnin lopputuloksena päädytty siihen, että kunkin sektorin osalta valvonta olisi syytä osoittaa yhdelle sektorikohtaiselle viranomaiselle valvonnan tarkoituksenmukaiseksi järjestämiseksi ja toimivaltaan liittyvien epäselvyyksien välttämiseksi. Valvonnan yhteensovittamisen ja tehokkuuden johdosta valvontatehtävä olisi perusteltua osoittaa nykyistä valvontamallia jatkaen sille viranomaiselle, joka jo voimassa olevan lainsäädännön perusteella valvoo toimialan toimijoita tai niihin kohdistuvia turvallisuusriskienhallintavelvoitteita. Sektorikohtaisilla viranomaisilla on paras tuntemus kyseisen toimialan erityispiirteistä ja muusta toimintaa koskevasta sääntelystä, jolloin kyseisellä valvovalla viranomaisella on paras osaaminen ja ymmärrys toimialan riskienhallintaan liittyvistä seikoista. Sektorikohtaisilla viranomaisilla on myös paras markkinaymmärrys kyseisen toimialan osalta, ja sitä kautta paremmat mahdollisuudet arvioida sääntelyn piiriin kuuluvia toimijoita sekä niihin kohdistuvien riskien tai poikkeamien merkittävyyttä ja vaikutuksia. Valmistelun aikana on kuitenkin tunnistettu, että nyt ehdotettavien valvontatehtävien suorittaminen edellyttää myös valvovalta viranomaiselta uudenlaista erityisosaamista. Tällaisen valvonnan järjestäminen voi olla haastavaa etenkin sellaisissa viranomaisissa, joiden tehtäviin ei ole aikaisemmin kuulunut nyt ehdotettavien valvontatehtävien tapaisia tehtäviä. Toisaalta digitalisoituva yhteiskunta edellyttää viranomaista kehittämään kyberturvallisuutta koskevaa ymmärrystä myös muiden kuin kyberturvallisuutta koskevien turvallisuusvelvoitteiden valvomiseksi, nykyisten tehtävien mukaisesti. Lisäksi valvonnan keskittäminen yhdelle viranomaiselle edellyttäisi vastaavasti riittävän osaamisen ja resurssien hankkimista sille viranomaiselle, jolle tehtävä osoitettaisiin, mikä aiheuttaisi kustannuksia erityisesti laajan soveltamisalan ja sektorikohtaisten erityispiirteiden tuntemuksen osalta. Resursoinnin näkökulmasta onkin katsottu tarkoituksenmukaiseksi, että kyberturvallisuusvelvoitteita valvoisivat sektorikohtaisesti samat viranomaiset, jotka valvovat sääntelyn kohteena olevia toimijoita muiltakin osin. Uuden valvontaa toteuttavan keskitetyn viranomaistahon arvioidaan noin 20–50 % hajautettua mallia korkeammat kokonaiskustannukset valvontatoiminnan järjestämiseksi samalla tasolla kuin hajautetussa mallissa vastaavalla tasolla.

Edellä esitetyn lisäksi NIS1-direktiivin täytäntöönpanossa omaksuttu sektorikohtainen valvontamalli on koettu pääosin toimivaksi, ja nykyisten valvovien viranomaisten ja valvonnan kohteena olevien toimijoiden välille on muodostunut luottamussuhteita ja yhteistyötä, jonka tarkoituksena on parantaa kyberturvallisuuden tasoa, riskienhallintaa ja kriisinkestävyyttä. Kansallisesti olemassa oleva viranomaisten keskinäinen sekä yritysten välinen yhteistyö on kehittynyt vuosien aikana pääosin toimivaksi, eikä tätä yhteistyötä ole tarkoituksenmukaista kaventaa NIS2-direktiivin täytäntöönpanon yhteydessä.

Julkishallinnon toimialan valvova viranomainen

Esityksessä ehdotetaan, että direktiivin mukainen julkishallinnon toimialan toimivaltainen, valvova viranomainen olisi Liikenne- ja viestintävirasto. Valmistelun aikana on arvioitu eri vaihtoehtoja toimivaltaiseksi viranomaiseksi. Valtiovarainministeriö haastatteli muun ohessa tämän selvittämiseksi helmi-maaliskuussa 2023 eri julkishallinnon organisaatioita sekä NIS1valvontaviranomaisten edustajia. Haastattelujen perusteella suurinta kannatusta toimivaltaiseksi viranomaiseksi sai Liikenne- ja viestintäviraston alainen Kyberturvallisuuskeskus. Haastatteluissa nostettiin esiin Kyberturvallisuuskeskuksen ennestään olemassa oleva kyvykkyys ja osaaminen valvontaan. Lisäksi keskitetyn valvonnan todettiin tuottavan synergioita suhteessa siihen, että julkishallinnon toimialan valvonta hajautettaisiin useille viranomaisille. Esiin tuotiin myös kyberturvallisuusalan osaamispula, jonka takia uuden toimijan synnyttäminen tai valvontatehtävän osoittaminen toiselle viranomaiselle ei olisi perusteltua. Lisäksi haastatteluissa todettiin, ettei valvonnasta olisi myöskään kannattavaa tehdä liian moniportaista monimutkaisuuden välttämiseksi, ja olisi selkeää, että yksi taho valvoisi kaikkia direktiivin mukaiseen tiedonhallintalain sääntelyn alaan kuuluvia julkishallinnon toimijoita. Oikeusministeriö ja liikenne- ja viestintäministeriö nostivat esille kysymyksen valvovan viranomaisen mahdollisuudesta valvoa hierarkiassaan yläpuolellaan olevaa tahoa, jonka takia toimijan tulisi mahdollisesti olla valtioneuvostotasoinen riippumaton toimija. Toisaalta haastatteluissa todettiin Liikenne- ja viestintäviraston omaavan jo tällä hetkellä esimerkiksi kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseen liittyviä tehtäviä, jotka kohdistuvat myös ministeriötasolle.

Muina mahdollisina toimivaltaisina viranomaisina nousivat esiin aluehallintovirastot ja tietosuojavaltuutetun toimisto. Myös Valtiontalouden tarkastusvirastoa ehdotettiin yhdessä haastattelussa toimivaltaiseksi viranomaiseksi. Haastatteluissa tuotiin kuitenkin esiin, ettei mainituilla toimijoilla olisi nykyisellään kyvykkyyttä tehtävän hoitamiseen ilman lisäresursointia. Yhtenä vaihtoehtona esitettiin myös uuden itsenäisen ja riippumattoman viranomaisen perustamista.

Haastattelujen lisäksi julkishallinnon sektoriin keskittyvän alatyöryhmän jäseniltä kysyttiin näkemystä toimivaltaisesta viranomaisesta. Liikenne- ja viestintäministeriön mukaan ministeriöitä valvovan viranomaisen tehtävä tulisi lähtökohtaisesti olla valtioneuvostotasoisella toimijalla ja olla mahdollisimman keskitetty. Oikeusministeriön mukaan soveltuvin osin tulisi hyödyntää keskittämistä, mutta samalla tulisi huomioida keskittämisen riskit. Työ- ja elinkeinoministeriö kysyi, pitäisikö aluehallinnossa ja paikallishallinnossa olla joku keskitetty ”väliporras”, joka toimisi tietojen kerääjänä ja asioiden koordinoija omalla alueellaan sekä välittäisi omalta alueeltaan tiedot keskitetysti Liikenne- ja viestintävirastolle. Ympäristöministeriön mukaan, mikäli viranomaistehtäviä lähdettäisiin keskittämään alue- tai paikallistasolle, voitaisiin arvioida mallia, jossa ELY-keskukset hoitaisivat asiaa tai asiat keskitettäisiin yhdelle ELY-keskukselle, kuten NIS1-direktiivin toimeenpanossa vesihuollon osalta tehtiin. Sisäministeriön mukaan paras olisi yhden viranomaisen malli, jolle poikkeamailmoitukset aina lopuksi toimitettaisiin (esim. Liikenne- ja viestintävirasto), jolle tulisi säätää oikeus tai velvollisuus luovuttaa tieto kansallista turvallisuutta koskevasta tietoturvatapahtumasta kansallisen turvallisuuden viranomaisille. Ulkoministeriön mukaan toimivaltaisena viranomaisena tulisi olla joko Liikenne- ja viestintävirasto tai Digi- ja väestötietovirasto. Valtiovarainministeriön mukaan valvonta olisi tarkoituksenmukaista keskittää yhdelle toimijalle, eikä jakaa useille eri toimijoille. Toimivaltaisena viranomaisena valtionhallintotasolla tulisi olla sellaisen organisaation, jonka osaaminen ja tehtävät tukevat kyberturvallisuutta koskevien velvoitteiden täyttämistä.

Kuten mainituissa haastatteluissa ja vastauksissa on tuotu esiin, Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksella olisi parhaimmat edellytykset ja asiantuntemus toimia direktiivin mukaisena julkishallinnon toimialan valvovana viranomaisena. Tehtävää kuitenkin ehdotetaan tiedonhallintalain sääntelyssä Liikenne- ja viestintävirastolle, koska tehtävään liittyisi sellaista

julkisen vallan käyttöä, josta viranomaisen on vastattava. Liikenne- ja viestintävirastossa tehtävä voitaisiin kuitenkin osoittaa Kyberturvallisuuskeskuksen henkilöstölle. Vaikka Kyberturvallisuuskeskuksella on jo entuudestaan kyberturvallisuuden valvontaan liittyvää erityisosaamista ja asiantuntemusta, edellyttää esityksessä ehdotettu tehtävä myös kyseisen toimijan lisäresursointia. Lisäresursoinnin tarve olisi tällöin kuitenkin vähäisempi verrattuna siihen, että tehtävä osoitettaisiin jollekin muulle viranomaiselle.

Myöskään valvontatehtävän jakaminen useammalle viranomaiselle ei olisi tarkoituksenmukaista. Vaikka haastatteluissa ja vastauksissa on todettu olevan ongelmallista, että ministeriöitä valvoisi hierarkkisesti alemmalla tasolla oleva virasto, valmistelussa on arvioitu, ettei tämä olisi esteenä valvonnan toteuttamiseksi esityksessä ehdotetulla tavalla. Direktiivin mukaisen valvonnan luonne ja tarkoitus huomioon ottaen valvontatehtävän osoittaminen keskitetysti myös ministeriöiden osalta Liikenne- ja viestintävirastolle on tarkoituksenmukaisinta. Virastolla on paras asiantuntemus ja kyvykkyys suoriutua tehtävästä, mitä on pidettävä painavampana perusteena kuin sitä, että valvonta hajautettaisiin hallinnon rakenteellisten syiden vuoksi ministeriöiden osalta jollekin valtioneuvostotason toimijalle. Tällainen hajauttaminen lisäisi kustannuksia, minkä lisäksi valvonnan laatu ja yhdenmukainen toteutus vaarantuisivat.

5.1.5 Seuraamusmaksu

Esityksessä ehdotetaan, että seuraamusmaksun NIS2-direktiivin velvoitteiden vastaisesta toiminnasta määräisi Liikenne- ja viestintäviraston yhteydessä toimiva seuraamuslautakunta, joka koostuisi valvovien viranomaisten nimeämistä jäsenistä.

Perustuslakivaliokunta on kiinnittänyt huomattavan korkeiden seuraamusmaksujen osalta huomiota oikeusturvaa koskeviin näkökohtiin. Perustuslakivaliokunta on pitänyt ongelmallisena sitä, että yksittäinen virkamies voisi määrätä itsenäisesti erittäin korkean hallinnollisen seuraamusmaksun. Perustuslakivaliokunnan kannan mukaisesti huomattavan suurien hallinnollisten seuraamusmaksujen päättäminen tulisi perustuslain 21 §:ään lukeutuvista oikeusturvasyistä säätää monijäsenisen toimielimen tehtäväksi (PeVL 14/2018 vp, s. 19). NIS2-direktiivin 34 artikla edellyttää jäsenvaltioita säätämään hallinnollisten seuraamusmaksujen enimmäismäärän vähimmäistasoksi keskeisille toimijoille 10 miljoonaa euroa tai 2 % toimijan maailmanlaajuisesta liikevaihdosta ja muille kuin keskeisille toimijoille 7 miljoonaa euroa tai 1,4 % toimijan maailmanlaajuisesta liikevaihdosta sen mukaan, kumpi on suurempi. Koska NIS2-direktiivin rikkomisen tai laiminlyönnin johdosta tulisi voida määrätä korkeitakin seuraamusmaksuja ei perustuslain oikeusturvaan liittyvien näkökohtien johdosta ole perusteltua säätää hallinnollisen seuraamusmaksun määräämistä muun kuin monijäsenisen toimielimen tehtäväksi. Jos hallinnollisen seuraamusmaksun määräisi kukin valvova viranomainen omalla toimialallaan, se edellyttäisi tavanomaisesta hallintopäätöksestä poikkeavasta päätöksentekomenettelystä, kuten kollegiaalisesta päätöksenteosta säätämistä.

Seuraamusmaksun määräämistoimivallan osalta vaihtoehtoina on arvioitu seuraamusmaksun määräämistä tuomioistuimen toimesta, seuraamusmaksun määräämistoimivallan keskittämistä Liikenne- ja viestintävirastolle tai seuraamusmaksulautakuntaa, joka koostuisi valvovista viranomaisista. Olemassa olevaa monijäsenistä toimielintä, jonka tehtäviin seuraamusmaksun määräämisen toimivalta luontevasti sopisi, ei ole tunnistettu, minkä johdosta kuvattuihin vaihtoehtoihin on päädytty.

Hallinnollisen seuraamusmaksun määrääminen tuomioistuimen toimesta ensiasteena on poikkeuksellista. Myös perustuslakivaliokunta on suhtautunut varauksellisesti siihen, että hallinnollisten seuraamusmaksujen määräämiseen liittyviä tehtäviä annettaisiin tuomioistuimille (PeVL

12/2019 vp). Muutoksenhaun yksiportaisuuden vuoksi toimivallan osoittamista hallintotuomioistuimelle ei voida pitää perusteltuna. Seuraamusmaksulautakunnan ja toimivallan keskittämisen keskeisenä menettelyllisenä erona olisi, että seuraamusmaksulautakunta koostuisi kunkin valvovan viranomaisen nimeämistä jäsenistä, kun keskitetyssä mallissa seuraamusmaksua koskevaan päätöksentekoon osallistuisi vain Liikenne- ja viestintäviraston tai sille seuraamusmaksun määräämistä esittelevän valvovan viranomaisen virkamiehiä. Ehdotetussa valvontamallissa, jossa toimijoiden valvonta olisi hajautettu sektorikohtaisesti eri valvoville viranomaisille NIS1-direktiivin täytäntöönpanoa jatkavan mallin mukaisesti, seuraamusmaksulautakunnan hyötynä suhteessa toimivallan keskittämiseen olisi toimialakohtaisen asiantuntemuksen hyödyntäminen ja jokaisen valvovan viranomaisen nimeämän edustajan osallistaminen seuraamusmaksuja määrättäessä, mikä johtaisi korkeaan toimialakohtaiseen asiantuntemukseen sekä seuraamuskäytännön ennakoitavuuteen ja yhdenmukaisuuteen eri toimialojen välillä. Seuraamustoimivallan keskittäminen yhdelle valvovalle viranomaiselle ei olisi johdonmukaista, kun valvonta muutoin on sektorikohtaisesti hajautettua. Seuraamusmaksutoimivallan keskittämisen etuna suhteessa seuraamuslautakuntaan olisi sen hallinnollisesti kevyempi rakenne. Seuraamuslautakunnan toiminnan järjestämisestä ei kuitenkaan aiheutuisi olennaisesti suurempia hallinnollisia kustannuksia, sillä se perustettaisiin olemassa olevan viranomaisen eli Liikenne- ja viestintäviraston yhteyteen ja kokoontuisi vain tarvittaessa. Seuraamusmaksujen määräämiselle ennakoidaan olevan tarvetta harvoin, sillä valvovalla viranomaisella olisi käytössään useita toimivaltuuksia toimijoiden ohjaamiseksi ja velvoittamiseksi lain vastaisen toiminnan oikaisemisesta. Näin ollen seuraamusmaksujen määräämisen toimivallan osoittaminen seuraamusmaksulautakunnalle arvioidaan esillä olleista vaihtoehdoista perustelluimmaksi, kun valvonta on järjestetty toimialakohtaisesti ja lautakunnassa on edustettuna jokainen valvova viranomainen

5.2 Muiden jäsenvaltioiden suunnittelemat tai toteuttamat keinot

5.2.1 Ruotsi

Ruotsin kansallinen verkko- ja tietoturvasääntely sisältyy yhteiskunnan toiminnan kannalta keskeisten palvelujen ja digitaalisten palvelujen tietoturvallisuutta koskevaan lakiin (lagen om informationssäkerhet för samhällsviktiga och digitala tjänster 2018:1174), joka pohjautuu NIS1-direktiivin velvoitteisiin. Lain nojalla on lisäksi annettu sitä täydentävä asetus (2018:1175).

NIS2-direktiivin pohjalta Ruotsissa valmistellaan julkinen valtiollinen selvitys kansallisesti keskeisistä kysymyksistä (statens offentliga utredningar), jonka tarkoituksena on toimia valmisteluasiakirjana ennen lakiehdotuksen laatimista. Selvityksen on tarkoitus valmistua viimeistään 23.2.2024. Lähtökohdat julkiselle valtiolliselle selvitykselle määritellään täytäntöönpanomuistiossa, joka on julkaistu 2.3.2023 (Kommittédirektiv: Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft, jäljempänä *täytäntöönpanomuistio*).

Täytäntöönpanomuistion mukaan sääntelyn lähtökohtana on velvoitteiden valvonnan osalta jatkaa NIS1-direktiivin pohjalta osoitettuja viranomaisyksiköitä. Tietoturvavelvoitteiden valvonta on Ruotsissa hajautettu sektorikohtaisille viranomaisille (Statens energimyndigheten (energia), Transportstyrelsen (liikenne), Finansinspektionen (pankkiala ja finanssimarkkinoiden infrastruktuuri), Inspektionen för vård och omsorg (terveydenhuolto), Livsmedelsverket (juomaveden toimittaminen ja jakelu) sekä Post- och telestyrelsen (digitaalinen infrastruktuuri ja digitaalisten palveluiden tarjoajat)). NIS2-direktiivin myötä verkko- ja tietoturvasääntelyn piiriin tuleville uusille toimialoille on kohdistettava valvontaviranomaiset.

Valvonnan koordinoinnista on vastannut huoltovarmuudesta vastaava kansallinen viranomainen MSB (Myndigheten För Samhällsskydd och Beredskap), joka on toiminut verkko- ja tietoturvallisuuden keskitettynä yhteyspisteenä, edustanut Ruotsia jäsenvaltioiden välisessä yhteistyöryhmässä sekä toiminut CSIRT-yksikkönä. Täytäntöönpanomuistion mukaan vastaavat tehtävät halutaan säilyttää MSB:n vastuulla NIS2-direktiivin täytäntöönpanon myötä ja MSB:tä pidetään tarkoituksenmukaisena Ruotsin edustajana Euroopan kyberkriisien yhteysorganisaatioiden verkostossa.

Ruotsin kansallinen tieto- ja kyberturvallisuusstrategia (Nationell strategi för samhällets informationsoch cybersäkerhet 2016/17:213) on valmistunut vuonna 2016. Strategian tavoitteena on tarjota toimijoille edellytykset parantaa tieto- ja kyberturvallisuuttaan sekä lisätä koko yhteiskunnan kattavaa tietoisuutta ja osaamista tieto- ja kyberturvallisuuden alalla. Strategiaa on päivitetty vuonna 2018 lisäämällä strategian yhteyteen liitteen tieto- ja kyberturvallisuusstrategian päivityksestä (Uppdatering om genomförandet av Nationell strategi för samhällets informations- och cybersäkerhet).

5.2.2 Viro

Virossa NIS1-direktiivi pantiin kansallisesti toimeen yleislailla kyberturvallisuudesta (Küberturvalisuse seadus). NIS2-direktiivin kansallisen täytäntöönpanon valmistelusta vastaa talous- ja viestintäministeriö (Majandus- ja Kommunikatsiooniministeerium), jonka tarkoituksena on tehdä kyberturvallisuuden kansalliseen yleislakiin uuden direktiivin vaatimat muutokset. Viron kansallista kyberturvallisuuslakia on muutettu vuonna 2022 lailla kyberturvallisuuslain ja muiden lakien muuttamisesta (Küberturvalisuse seaduse ja teiste seaduste muutmise seadus). Muutoshankkeen taustalla oli tarve tarkastaa kansallista sääntelyä EU-lainsäädännön pohjalta ja sen keskeinen tavoite oli vahvistaa julkisen sektorin tietoturvastandardia ja laajentaa standardi koskemaan kaikkia verkko- ja tietoturvajärjestelmiä korvaamalla ISKE (Infosüsteemide turvameetmete süsteem) uudella E-ITS –standardilla (Eesti infoturbestandard).

Kyberturvallisuuden yleislain toisen muutoshankkeen päätavoitteena on saattaa NIS2-direktiivin velvoitteet osaksi kansallista sääntelyä.

NIS1-direktiivin mukaiset valvonta- ja yhteistyövelvoitteet on järjestetty keskitetysti. Kansallisena yhteyspisteenä, toimivaltaisena viranomaisena ja CSIRT-yksikkönä on toiminut Viron tietojärjestelmävirasto (Riigi Infosüsteemi Amet). Viimeisin Viron julkaisema kyberturvallisuutta koskeva kansallinen strategia (Küberturvalisuse strateegia) sijoittuu vuosille 2019-2020. Strategia määrittelee kansallisesti keskeiset kyberturvallisuustavoitteet, joiden avulla Viron kyberturvallisuutta voidaan kehittää.

5.2.3 Tanska

Tanskassa NIS1-direktiivin velvoitteet on pantu täytäntöön lailla verkkotunnusjärjestelmien ja tiettyjen digitaalisten palvelujen verkko- ja tietoturvasta (Lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester, jäljempänä *NI1S-laki*). Laki asettaa tietoja verkkoturvallisuusvaatimuksia keskeisten palvelujen tarjoajille sekä säätää toimijoiden valvomisesta. NIS1-lain mukaisena keskitettynä yhteyspisteenä ja CSIRT-toimijana Tanskassa toimii Kyberturvallisuuskeskus (Center for Cybersikkerhed) ja viranomaisvalvonta on keskitetty Elinkeinovirastolle (Erhvervsstyrelse). Toimijoiden tulee raportoida lain velvoitteiden nojalla kyberturvallisuusloukkauksista Kyberturvallisuuskeskukselle ja Elinkeinovirastolle.

Tanskan kansallinen kyberturvallisuusstrategia vuosille 2022-2024 on julkaistu joulukuussa 2021 (National strategi for cyber- og informationssikkerhed 2022-2024).

NIS2-direktiivin täytäntöönpanosta vastaa Tanskan puolustusministeriö.

5.2.4 Saksa

NIS1-direktiivi pantiin kansallisesti täytäntöön lailla verkko- ja tietoturvadirektiivin täytäntöönpanosta (Gesetz zur Umsetzung der NIS-Richtlinie). Direktiivin velvoitteiden pohjalta laki laajensi BSI:n (Bundesamt für Sicherheit in der Informationstechnik) valvonta- ja täytäntöönpanovaltuuksia. BSI on toiminut Saksassa NIS1-direktiivin mukaisena keskitettynä yhteyspisteenä ja kansallisena CSIRT-yksikkönä. Myös viranomaisvalvonta on järjestetty keskitetysti. NIS1-direktiivin mukaisena valvovana viranomaisena toimii BSI. NIS1-direktiivin täytäntöönpano ei edellyttänyt suuria muutoksia kansalliseen sääntelyyn, sillä vuodesta 2015 voimassa ollut tietoturvalaki (IT-Sicherheitsgesetz) on edellyttänyt kriittisten infrastruktuurien toimijoiden (KRITIS) riskienhallinta- ja raportointitoimia kyberturvallisuuden parantamiseksi.

Saksassa NIS2 –direktiivi suunnitellaan toimeenpantavaksi tietoturvalain 3.0 (IT-Sicherheitsgesetz 3.0) kautta. Uudella lailla on tarkoitus muokata tietoturvalain edellistä versiota (IT-Sicherheitsgesetz 2.0), joka tuli voimaan vuonna 2021. IT-Sicherheitsgesetz 2.0 perustuu KRITIS –toimijoihin, jotka toimivat kriittiseksi määritellyn toimialan sisällä. Toimijat tulevat sääntelyn piiriin silloin, kun lain määrittelemät kynnysarvot täyttyvät. Kynnysarvo on pääsääntöisesti 500 000 ihmistä tarjottavan palvelun piiriissä. NIS2 –sääntelyn raja-arvot poikkeavat Saksan sääntelystä, sillä NIS2 edellyttää 50 työntekijää ja 10 miljoonan euron liikevaihtoa. Koska kansallisesti voimassa olevan sääntelyn soveltamisala poikkeaa NIS2-direktiivin mukaisesta soveltamisalasta, on direktiivin kansallisen täytäntöönpanon yhteydessä on päätettävä, miten soveltamisala tulee jatkossa määritellä.

NIS2 menee velvoitteissaan nykyistä Saksan kansallista sääntelyä pidemmälle suojatoimenpiteiden, raportointivelvoitteiden, valvontatoimien, hallinnollisten seuraamusten ja rekisteröintivelvoitteiden osalta. Myös EU-jäsenmaiden sisäinen tiedonvaihto ja yhteistyö tulevat uusien NIS2 –velvoitteiden kautta lisääntymään.

5.2.5 Ranska

Ranskassa NIS1-direktiivi toimeenpantiin osana lakia, jolla kansallinen turvallisuussääntely pyrittiin yhdenmukaistamaan Euroopan unionin sääntelyyn (LOI n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité). NIS1-direktiivin mukaisena keskitettynä kansallisena yhteyspisteenä toimii Ranskassa ANSSI (Agence nationale de la sécurité des systèmes d’information) ja CSIRT-yksikkönä tietoturvallisuuden tilannekeskus CERT-FR, joka on sijoitettu ANSSI:n yhteyteen.

Kriittistä infrastruktuuria koskevaan sääntelyyn on kansallisesti sisällytetty tietoturvallisuusvelvoitteita lakiuudistuksen kautta (CIIP, loi n° 2013-1168 du 18 décembre 2013). Lain tarkoituksena on säätää tietoturvallisuutta koskevista riskienhallinta- ja raportointivelvoitteista kansallisille toimijoille. Lain edellyttämä raportointi tulee tehdä Ranskan kansalliselle kyberturvallisuusviranomaiselle ANSSI:lle.

Digitaalisen turvallisuuden strategia (Stratégie nationale pour la sécurité du numérique) on julkaistu vuonna 2015, ja sen tavoitteena on edistää tietojärjestelmien vakautta, taloudellista kehitystä sekä kansalaisten luottamusta tietojärjestelmiin.

6 Lausuntopalaute

[Täydennetään lausuntokierroksen jälkeen]

7 Säännöskohtaiset perustelut

7.1 Laki kyberturvallisuuden riskienhallinnasta

1 §. *Soveltamisala*. Lailla pantaisiin täytäntöön NIS2-direktiivi säätämällä direktiivin soveltamisalan edellyttämällä tavalla eräiden yhteiskunnan toiminnan kannalta kriittisten toimijoiden kyberturvallisuuden riskienhallinta- ja raportointivelvoitteista sekä niiden noudattamisen valvonnasta. Lain soveltamisalaan kuuluvat toimijat määriteltäisiin 3 §:ssä.

Laissa säädettäisiin NIS2-direktiivin täytäntöönpanemiseksi lisäksi NIS2-direktiivin 10 artiklassa tarkoitetusta tietoturvaloukkauksiin reagoivasta ja niitä tutkivasta yksiköstä eli CSIRT-yksiköstä (Computer Security Incident Response Team), sen tehtävistä ja toiminnalle asetettavista vaatimuksista sekä eräistä muista seikoista liittyen viranomaisten yhteistyöhön kyberturvallisuuspoikkeamien ja –riskien hallitsemiseksi.

2 §. *Määritelmät*. Säännöksessä säädettäisiin laissa käytetyistä määritelmistä. Määritelmät vastaisivat pääosin NIS2-direktiivin määritelmiä.

Pykälän *1 kohdassa* säädettäisiin aluetunnusrekisterin määritelmästä NIS2-direktiivin 6 artiklan 21 kohtaa vastaavasti. Aluetunnusrekisterillä tarkoitettaisiin toimijaa, jolle on myönnetty oikeus hallinnoida tiettyä aluetunnusta ja joka kyseistä aluetunnusta hallinnoidessaan vastaa muun muassa verkkotunnusten rekisteröinnistä kyseisen aluetunnuksen alle sekä kyseisen aluetunnuksen teknisestä toiminnasta, myös siihen liittyvien nimipalvelinten toiminnasta, sen tietokantojen ylläpidosta ja aluetunnuksen vyöhyketiedostojen jakelusta nimipalvelimille, riippumatta siitä, suorittaako toimija kyseiset toiminnot itse vai ulkoistaako se ne, ja lukuun ottamatta tilanteita, joissa rekisteri käyttää aluetunnuksia vain omiin tarkoituksiinsa.

Pykälän *2 kohdassa* määriteltäisiin CER-direktiivi, jolla tarkoitettaisiin Euroopan parlamentin ja neuvoston direktiiviä (EU) 2022/2557 kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta.

Pykälän *3 kohdassa* säädettäisiin datakeskuspalvelun määritelmästä. Määritelmä vastaisi sisällöllisesti NIS2-direktiivin 6 artiklan 31 kohtaa. Datakeskuspalvelulla tarkoitettaisiin palvelua, joka käsittää rakenteita tai rakenteiden ryhmiä, jotka on tarkoitettu datan tallennus-, käsittely- ja siirtopalveluja tarjoavien tietoteknisten ja verkkolaitteiden keskitettyyn ylläpitoon, yhteenliittämiseen ja ohjaukseen yhdessä kaikkien tarvittavien sähkönjakeluun ja toimintaolosuhteiden säätelyyn tarkoitettujen laitteiden ja infrastruktuurien kanssa. NIS2-direktiivin 35 resitaalissa täydennetään 6 artiklan 31 kohdan määritelmää. Resitaalin mukaan käsite kattaa sellaiset datakeskuspalvelujen tarjoajat, jotka eivät ole osa pilvipalveluinfrastruktuuria.

Pykälän *4 kohdassa* säädettäisiin DNS-palveluntarjoajan määritelmästä. Määritelmä vastaisi sisällöllisesti NIS2-direktiivin 6 artiklan 20 kohtaa. DNS-palveluntarjoajalla tarkoitettaisiin toimijaa, joka tarjoaa yleisesti saatavilla olevia rekursiivisia verkkotunnusten selvityspalveluja internetin loppukäyttäjille tai auktoritatiivisia verkkotunnusten selvityspalveluja kolmansille osapuolille, lukuun ottamatta juurinimipalvelimia.

Pykälän 5 *kohdassa* määriteltäisiin DORA-asetus, jolla tarkoitettaisiin finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU) N:o 600/2014, (EU) N:o 909/2014 ja (EU) 2016/1011 muuttamisesta annettua Euroopan parlamentin ja neuvoston asetusta (EU) 2022/2554.

Pykälän *6 kohdassa* määriteltäisiin eIDAS-asetus, jolla tarkoitettaisiin sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta annettua Euroopan parlamentin ja neuvoston asetusta (EU) N:o 910/2014.

Pykälän *7 kohdassa* säädettäisiin haavoittuvuuden määritelmästä. Haavoittuvuuden määritelmä vastaisi sisällöllisesti NIS2-direktiivin 6 artiklan 15 kohtaa. Haavoittuvuudella tarkoitettaisiin kyberturvallisuusasetuksen (EU) 2019/881 2 artiklan 12 alakohdassa määritellyn tieto-ja viestintätekniikan tuotteen tai kyberturvallisuusasetuksen 2 artiklan 13 alakohdassa määritellyn tieto- ja viestintätekniikan palvelun heikkoutta, alttiutta tai vikaa, jota kyberuhka voi hyödyntää.

Pykälän *8 kohdassa* säädettäisiin hallintapalvelun tarjoajan määritelmästä. Määritelmä vastaisi sisällöllisesti NIS2-direktiivin 6 artiklan 39 kohtaa. Hallintapalvelun tarjoajalla tarkoitettaisiin toimijaa, joka tarjoaa TVT-tuotteiden, verkkojen, infrastruktuurin, sovellusten tai muiden viestintäverkkojen ja tietojärjestelmien asentamiseen, hallintaan, käyttöön tai ylläpitoon liittyviä palveluja joko asiakkaan tiloissa tai etäyhteyden välityksellä toteutettavan tuen tai aktiivisen ylläpidon muodossa.

Pykälän *9 kohdassa* säädettäisiin hyväksytyn luottamuspalvelun tarjoajan määritelmästä. Hyväksytyllä luottamuspalvelun tarjoajalla tarkoitettaisiin eIDAS-asetuksen 3 artiklan 20 alakohdassa määriteltyä hyväksyttyä luottamuspalvelun tarjoajaa eli sellaista eIDAS-asetuksen mukaista luottamuspalvelun tarjoajaa, joka tarjoaa yhtä tai useampaa hyväksyttyä luottamuspalvelua ja jolle valvontaelin on myöntänyt hyväksytyn aseman.

Pykälän *10 kohdassa* säädettäisiin keskisuuren toimijan määritelmästä. Keskisuuri toimija voisi olla joko julkinen tai yksityinen organisaatio, joka täyttää komission suosituksen 2003/361/EY liitteessä olevan 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset. Määritelmä määräytyisi komission suosituksessa 2003/361/EY tarkoitetun keskisuuren yrityksen määritelmän mukaisesti, mutta kuitenkin niin, että suosituksen liitteessä olevaa 3 artiklan 4 kohtaa, eli julkisyhteisön tai –laitoksen omistus- tai äänioikeudelle asetettuja rajoituksia ei tässä yhteydessä sovellettaisi. Keskisuuren toimijan määritelmän täyttymistä tai ylittymistä tulisi arvioida suhteessa komission suosituksen kynnysarvoihin ja niiden tulkintaan.

Komission suosituksessa 2003/361/EY säädetään mikroyrityksen, pienen yrityksen ja keskisuuren yrityksen enimmäiskoosta. Toimija täyttäisi keskisuuren yrityksen määritelmän silloin, kun se ylittää pienen yrityksen määritelmän reunaehdot, mutta ei ylitä pk-yrityksille asetettuja enimmäiskynnysarvoja. Toimija täyttäisi siten keskisuuren toimijan määritelmän, kun sen palveluksessa on vähintään 50 työntekijää taikka sen vuotuinen liikevaihto ja tase ylittävät 10 miljoonaa euroa. Jos toimijan palveluksessa on alle 50 työntekijää, mutta sekä liikevaihto että tase ylittävät 10 miljoonaa, toimija täyttäisi keskisuuren toimijan määritelmän. Jos toimijan palveluksessa on alle 50 työntekijää ja joko liikevaihto tai tase, mutta ei molemmat, ylittää 10 miljoonaa euroa, toimija ei täyttäisi keskisuuren toimijan määritelmää. Toimija ylittäisi keskisuuren toimijan määritelmän silloin kun se ylittää komission suosituksen mukaiset pk-yritysten määritelmän enimmäiskynnysarvot.

Mikäli toimija toimii usealla eri toimialalla ja vain osa sen toiminnasta on liitteessä I tai II tarkoitettua toimintaa, kokorajoitusta arvioidaan toimijan kokonaistoiminnan perusteella. Näin ollen liikevaihtoa, tasetta ja henkilöstömäärää arvioidaan koko toimijan osalta eikä arviointia tule rajata vain liitteessä I tai II tarkoitetun toiminnan laajuuteen. Arviointi tehdään toimijakohtaisesti.

Pykälän *11 kohdassa* säädettäisiin NIS2-direktiivin 6 artiklan 3 kohtaa vastaavasti kyberturvallisuuden käsitteestä. Kyberturvallisuudella tarkoitettaisiin kyberturvallisuutta siten kuin se on määritelty Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta annettua Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 (jäljempänä *kyberturvallisuusasetus*) 2 artiklan 1 kohdassa. Kyberturvallisuudella tarkoitettaisiin siten toimia, joita tarvitaan viestintäverkkojen ja tietojärjestelmien, tällaisten järjestelmien käyttäjien ja muiden asianosaisten henkilöiden suojaamiseksi kyberuhilta. Määritelmä ei rajoittaisi toimien muotoa tai laatua, vaan kysymykseen voisi tulla sekä teknisiä että muita suojaamiseksi tarpeellisia toimia niiden muodosta ja laadusta riippumatta. Viestintäverkkojen ja tietojärjestelmien käyttäjien ohella muita asianosaisia henkilöitä olisivat esimerkiksi henkilöt, joihin liittyvää tai joiden omistamaa tietoa viestintäverkossa ja tietojärjestelmässä käsitellään.

Pykälän *12 kohdassa* säädettäisiin NIS2-direktiivin 6 artiklan 10 kohtaa vastaavasti kyberuhkan määritelmästä. Kyberuhkalla tarkoitettaisiin kyberuhkaa siten kuin se on määritelty kyberturvallisuusasetuksen 2 artiklan 8 alakohdassa. Kyberuhkalla tarkoitettaisiin potentiaalista tilannetta, tapahtumaa tai toimintaa, joka voi vahingoittaa tai häiritä viestintäverkkoja tai tietojärjestelmiä, tällaisten järjestelmien käyttäjiä ja muita henkilöitä tai muulla tavoin vaikuttaa näihin haitallisesti.

Pykälän *13 kohdassa* säädettäisiin luottamuspalvelun tarjoajan määritelmästä. Luottamuspalvelun tarjoajalla tarkoitettaisiin eIDAS-asetuksen 3 artiklan 19 alakohdassa määriteltyä luottamuspalvelun tarjoajaa. Tämän asetuksen 3 artiklan 19 alakohdan mukaan luottamuspalvelun tarjoajalla tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, joka tarjoaa yhtä tai useampaa luottamuspalvelua joko hyväksyttynä tai ei-hyväksyttynä luottamuspalvelun tarjoajana. Luottamuspalvelulla tarkoitetaan eIDAS-asetuksen 3 artiklan 16 alakohdan mukaan sähköistä palvelua, jota yleensä tarjotaan vastiketta vastaan ja joka koostuu joko sähköisten allekirjoitusten, sähköisten leimojen tai sähköisten aikaleimojen, sähköisten rekisteröityjen jakelupalvelujen ja kyseisiin palveluihin liittyvien varmenteiden luomisesta, tarkastamisesta ja validoinnista tai verkkosivustojen todentamisen varmenteiden luomisesta, tarkastamisesta ja validoinnista tai sähköisten allekirjoitusten, leimojen tai kyseisiin palveluihin liittyvien varmenteiden säilyttämisestä.

Pykälän *14 kohdassa* säädettäisiin läheltä piti –tilanteen määritelmästä. Määritelmä vastaisi sisällöllisesti NIS2-direktiivin 6 artiklan 5 kohtaa. Läheltä piti –tilanteella tarkoitettaisiin tapahtumaa, joka olisi voinut vaarantaa viestintäverkoissa ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden mutta jonka toteutuminen onnistuttiin estämään tai joka ei toteutunut satunnaisen syyn vuoksi.

Pykälän *15 kohdassa* säädettäisiin pilvipalvelun määritelmästä NIS2-direktiivin 6 artiklan 30 kohtaa ja johdantokappaletta 33 vastaavasti. Pilvipalvelulla tarkoitettaisiin digitaalista palvelua, joka tarjoaa laajaan etäkäyttöön skaalattavan ja joustavan joukon jaettavissa olevia ja tarveperusteisesti ohjattavia tietoteknisiä resursseja, myös sijainniltaan hajautettuja resursseja. NIS2-direktiivin pilvipalvelun määritelmää tarkennetaan sen johdantokappaleessa 33. Pilvipalvelun määritelmää tulisi tulkita yhdenmukaisesti NIS2-direktiivin pilvipalvelun määritelmän kanssa.

Tietotekninen resurssi voisi tarkoittaa siten esimerkiksi verkkoja, palvelimia ja muuta tietoteknistä infrastruktuuria, käyttöjärjestelmiä, ohjelmistoja, tallennustilaa, sovelluksia ja palveluja. Tarveperusteisella ohjauksella tarkoitettaisiin pilvipalvelun käyttäjän kykyä käyttää yksipuolisesti ja oma-aloitteisesti tietojenkäsittelyvalmiuksia ilman pilvipalveluntarjoajan inhimillistä panosta. Laajalla etäkäytöllä tarkoitettaisiin sitä, että resursseja tarjotaan verkossa ja niitä pääsee käyttämään erilaisten päätelaitteiden käytön mahdollistavien järjestelyjen ansiosta. Skaalautuvuus viittaa tietoteknisiin resursseihin, joita pilvipalvelujen tarjoaja voi teknisesti jakaa joustavasti kysynnän vaihtelun mukaan resurssien maantieteellisestä sijainnista riippumatta. Joustavaa joukolla tarkoitetaan tietoteknisiä resursseja, joita tarjotaan ja vapautetaan käyttöön kysynnän mukaan niin, että resursseja voidaan nopeasti lisätä ja vähentää kuormituksen perusteella. Jaettavissa olevalla kuvataan tietoteknisiä resursseja, joita tarjotaan useille käyttäjille, joilla on yhteinen pääsy palveluun, jossa prosessointi on kuitenkin käyttäjäkohtaista, vaikka palvelu tarjotaan saman sähköisen laitteiston kautta. Hajautetulla viitataan tietoteknisiin resursseihin, jotka sijaitsevat erillisissä verkotetuissa tietokoneissa tai laitteissa ja jotka viestivät ja koordinoivat toimintaansa keskenään rakenteisella viestinvaihdolla. Pilvipalvelujen palvelu- ja toimintamalleilla tarkoitettaisiin NIS2-direktiivin johdantokappaletta 33 vastaavasti samaa kuin standardissa ISO/IEC 17788:2014 määritellyillä palvelu- ja toimintamalleilla.

Pykälän *16 kohdassa* säädettäisiin poikkeaman määritelmästä. Määritelmä vastaisi sisällöllisesti NIS2-direktiivin 6 artiklan 6 kohtaa. Poikkeamalla tarkoitettaisiin tapahtumaa, joka vaarantaa viestintäverkoissa tai tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden.

Pykälän *17 kohdassa* määriteltäisiin poikkeaman käsittely. Määritelmä vastaisi sisällöllisesti NIS2-direktiivin 6 artiklan 8 kohtaa. Poikkeaman käsittelyllä tarkoitettaisiin mitä tahansa toimia ja menettelyjä, joilla pyritään ehkäisemään ja havaitsemaan poikkeama, analysoimaan, rajoittamaan tai hallitsemaan sitä ja palautumaan siitä.

Pykälän *18 kohdassa* säädettäisiin riskin määritelmästä. Riskillä tarkoitettaisiin laissa NIS2-direktiivin 6 artiklan 9 kohdan määritelmää vastaavasti sitä, kuinka todennäköinen viestintäverkossa ja tietojärjestelmässä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden ja luottamuksellisuuden vaarantava tapahtuma olisi ja toisaalta millaisen häiriön se toteutuessaan aiheuttaisi. Riskin vakavuutta arvioitaessa olisi otettava huomioon riskin toteutumisen todennäköisyys sekä riskin toteutumisesta aiheutuvan häiriön tai menetyksen suuruus ja merkitys. Riskistä aiheutuvan menetyksen merkitystä tulisi arvioida suhteessa samoihin seikkoihin, jotka ovat merkityksellisiä merkittävän poikkeaman eli poikkeamailmoituksen kynnyksen kannalta, ja niihin kohdistuvien vaikutusten kautta. Näitä seikkoja ovat palvelujen toimintahäiriöt, asianomaisen toimijan taloudelliset tappiot sekä muihin luonnollisiin henkilöihin tai oikeushenkilöihin vaikuttavat aineelliset tai aineettomat vahingot. Näihin seikkoihin tulisi myös lukea verkko- tai tietojärjestelmässä käsiteltävien tietojen määrä ja laatu sekä riskin toteutumisesta aiheutuvat haitalliset vaikutukset tietojen luottamuksellisuudelle ja henkilötietojen suojalle.

Pykälän *19 kohdassa* säädettäisiin sisällönjakeluverkon määritelmästä. Määritelmä vastaisi sisällöllisesti NIS2-direktiivin 6 artiklan 32 kohtaa. Sisällönjakeluverkolla tarkoitettaisiin maantieteellisesti hajautettujen palvelimien verkkoa, jonka tarkoituksena on varmistaa digitaalisen sisällön ja digitaalisten palvelujen hyvä saatavuus, käytettävyys ja nopea jakelu internetin käyttäjille sisällön ja palvelujen tarjoajien puolesta.

Pykälän *20 kohdassa* säädettäisiin teledirektiivin määritelmästä. Teledirektiivillä tarkoitettaisiin Eurooppalaisesta sähköisen viestinnän säännöstöstä annettua Euroopan parlamentin ja neuvoston direktiiviä (EU) 2018/1972.

Pykälän *21 kohdassa* säädettäisiin NIS2-direktiivin 6 artiklan 40 kohtaa vastaavasti tietoturvapalveluntarjoajan määritelmästä. Tietoturvapalveluntarjoajalla tarkoitettaisiin 8 kohdassa tarkoitettua hallintapalvelun tarjoajaa, joka toteuttaa kyberturvallisuusriskien hallintatoimia tai antaa tukea niitä varten.

Pykälän *22 kohdassa* säädettäisiin TVT-palvelun määritelmästä. TVT-palvelun määritelmä vastaa sisällöllisesti kyberturvallisuusasetuksen (EU) 2019/881 2 artiklan 13 alakohdassa määriteltyä tieto- ja viestintätekniikan palvelua. TVT-palvelulla tarkoitettaisiin mitä tahansa palvelua, jonka sisältönä on kokonaan tai pääasiassa tiedon välittäminen, tallentaminen, hakeminen tai käsittely viestintäverkkojen ja tietojärjestelmien avulla.

Pykälän *23 kohdassa* säädettäisiin TVT-tuotteen määritelmästä. TVT-tuotteen määritelmä vastaisi sisällöllisesti kyberturvallisuusasetuksen (EU) 2019/881 2 artiklan 12 alakohdassa määriteltyä tieto- ja viestintätekniikan tuotetta. TVT-tuotteella tarkoitettaisiin mitä tahansa viestintäverkkojen ja tietojärjestelmien elementtiä ja elementtien ryhmää.

Pykälän *24 kohdassa* säädettäisiin valvovan viranomaisen määritelmästä. Valvovalla viranomaisella tarkoitettaisiin kullakin toimialalla tämän lain 26 §:n nojalla toimivaltaista valvovaa viranomaista, jonka tehtävänä järjestää tämän lain, sen nojalla annettujen määräysten ja NIS2-direktiivin nojalla annettujen säädösten valvonta toimialalla. Valvovalla viranomaisella tarkoitettaisiin NIS2-direktiivin 8 artiklan 1 kohdan mukaista toimivaltaista viranomaista.

Pykälän *25 kohdassa* säädettäisiin NIS2-direktiivin 6 artiklan 33 kohtaa vastaavasti verkkoyhteisöalustan määritelmästä. Verkkoyhteisöalustalla tarkoitettaisiin alustaa, jonka avulla loppukäyttäjät voivat olla yhteydessä toisiinsa, jakaa sisältöä, hakea tietoa ja viestiä keskenään monenlaisilla päätelaitteilla, erityisesti pikaviestikeskustelujen, julkaisujen, videoiden ja suositusten muodossa.

Pykälän *26 kohdassa* säädettäisiin verkossa toimivan hakukoneen määritelmästä. Määritelmä vastaisi sisällöllisesti oikeudenmukaisuuden ja avoimuuden edistämisessä verkossa toimivien välityspalvelujen yrityskäyttäjiä varten annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/1150 2 artiklan 5 kohtaa. Verkossa toimivalla hakukoneella tarkoitettaisiin digitaalista palvelua, joka antaa käyttäjille mahdollisuuden suorittaa kyselyjä hakujen tekemiseksi periaatteessa kaikilta verkkosivustoilta tai kaikilta tietynkielisiltä verkkosivustoilta mitä tahansa aihetta koskevan hakusanan, äänikomennon, lausekkeen tai muun syöttötiedon muodossa tehdyn kyselyn perusteella ja joka antaa missä tahansa muodossa tuloksia, joista voi saada pyydettyyn sisältöön liittyvää tietoa. Määritelmä vastaisi NIS2-direktiivin 6 artiklan 29 kohdan määritelmää. Lain liitteessä tarkoitetulla verkossa toimivien hakukoneiden tarjoajalla viitattaisiin määritelmän mukaista palvelua tarjoavaan toimijaan.

Pykälän *27 kohdassa* säädettäisiin verkossa toimivan markkinapaikan määritelmästä. Määritelmällä tarkoitettaisiin kuluttajansuojalain (38/1978) 6 luvun 8 §:n 4 kohdan mukaisesti palvelua, jossa tarjotaan kuluttajalle mahdollisuutta tehdä etäsopimuksia muiden elinkeinonharjoittajien kuin markkinapaikan tarjoajan kanssa taikka yksityishenkilöiden kanssa ja jossa hyödynnetään markkinapaikan tarjoajan käyttämää tai hänen puolestaan käytettyä verkkosivustoa, sovellusta tai muuta ohjelmaa tai sen osaa. Määritelmä vastaisi NIS2-direktiivin 6 artiklan 28 kohdan määritelmää. Lain liitteessä tarkoitetulla verkossa toimivien markkinapaikkojen tarjoajalla viitattaisiin määritelmän mukaista palvelua tarjoavaan toimijaan.

Pykälän *28 kohdassa* säädettäisiin viestintäverkon ja tietojärjestelmän määritelmästä. Määritelmä vastaisi sisällöllisesti NIS2-direktiivin 6 artiklan 1 kohtaa. NIS1- ja NIS2-direktiivien suomennoksissa käytetyn ”verkko- ja tietojärjestelmän”-käsitteen sijaan kansallisessa laissa käytettäisiin NIS1-direktiivin kansallisessa täytäntöönpanosääntelyssä ja sähköisen viestinnän palveluista annetussa laissa vakiintunutta käsitettä ”viestintäverkko ja tietojärjestelmä”. Viestintäverkon ja tietojärjestelmän käsitteestä säädettäisiin laissa vastaavasti kuin NIS2-direktiivissä säädetään verkko- ja tietojärjestelmän käsitteestä.

Viestintäverkolla ja tietojärjestelmällä tarkoitettaisiin eurooppalaisesta sähköisen viestinnän säännöstöstä annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2018/1972 (ns. teledirektiivi) 2 artiklan 1 kohdassa määriteltyä sähköistä viestintäverkkoa; laitetta taikka yhteen kytkettyjen tai toisiinsa yhteydessä olevien laitteiden ryhmää, joista yksi tai useampi suorittaa ohjelman avulla digitaalisten tietojen automaattista käsittelyä; tai digitaalisia tietoja, joita em. järjestelmissä säilytetään, käsitellään, haetaan tai siirretään näiden järjestelmien toimintaa, käyttöä, suojausta tai ylläpitoa varten. Viestintäverkon ja tietojärjestelmän käsitettä olisi tulkittava yhdenmukaisesti suhteessa tulkintaan NIS2-direktiivin verkko- ja tietojärjestelmän määritelmästä.

Pykälän *29 kohdassa* säädettäisiin NIS2-direktiivin 6 artiklan 2 kohtaa vastaavasti viestintäverkon ja tietojärjestelmän turvallisuuden määritelmästä. Viestintäverkon ja tietojärjestelmän turvallisuudella tarkoitettaisiin viestintäverkon ja tietojärjestelmän kykyä suojautua tapahtumilta, jotka vaarantavat viestintäverkossa ja tietojärjestelmässä olevien tietojen saatavuutta, aitoutta, eheyttä ja luottamuksellisuutta sekä sitä, että tiedot ja palvelut ovat niiden käyttöön oikeutettujen hyödynnettävissä. Määritelmä kattaisi siten tietoturvan elementit siitä, että tietoturvallisessa järjestelmässä tiedon tulisi olla vain niiden käyttöön oikeutettujen saatavilla, tietoja eivät voisi muuttaa muut kuin siihen oikeutetut sekä että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä.

Pykälän *30 kohdassa* määriteltäisiin yleinen tietosuoja-asetus, jolla tarkoitettaisiin luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annetun Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679.

Pykälän *31 kohdassa* säädettäisiin yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajan määritelmästä. Yleisesti saatavilla oleva sähköinen viestintäpalvelu vastaisi sisällöllisesti sähköisen viestinnän palveluista annetun lain (917/2014) 3 §:n 1 momentin 37 kohdassa tarkoitettua viestintäpalvelua. Lain 3 §:n 1 momentin 37 kohdan mukaan viestintäpalvelulla tarkoitetaan palvelua, joka muodostuu kokonaan tai pääosin viestin siirtämisestä viestintäverkossa sekä siirto- ja lähetyspalvelua joukkoviestintäverkossa ja henkilöiden välisen viestinnän palvelua.

Pykälän *32 kohdassa* säädettäisiin yleisten sähköisten viestintäverkkojen tarjoajan määritelmästä. Palvelun määritelmä vastaisi sisällöllisesti sähköisen viestinnän palveluista annetun lain (917/2014) 3 §:n 1 momentin 34 kohdassa tarkoitettua verkkopalvelua. Lain 3 §:n 1 momentin 34 kohdan mukaan verkkopalvelulla tarkoitetaan palvelua, jossa teleyritys (verkkoyritys) tarjoaa omistamaansa tai muulla perusteella hallussaan olevaa viestintäverkkoa käytettäväksi viestien siirtoon tai jakeluun.

3 §. *Toimijat*. Pykälässä säädettäisiin lain soveltamisalaan kuuluvista toimijoista. Toimijan määritelmä olisi kaksiosainen liittyen toimijan toiminnan laatuun tai tyyppiin ja toimijan kokoon. Lisäksi eräissä poikkeustapauksissa lain soveltamisalaan voisi kuulua toimija sen koosta riippumatta ja esimerkiksi CER-direktiivin nojalla määritellyt kriittiset toimijat kuuluisivat aina

lain soveltamisalaan. Lain soveltamisalan ja toimijan käsitteen olisi tarkoitus vastata NIS2-direktiivin 2 artiklan 1–4 kohtia ja 3 artiklan 1 ja 2 kohtia siten että se kattaisi kaikki NIS2-direktiivin vähimmäissoveltamisalaan kuuluvat keskeiset ja tärkeät toimijat.

Ehdotetussa *1 momentissa* säädettäisiin siitä, mitkä tahot olisivat laissa tarkoitettuja ja siten lain soveltamisalaan kuuluvia toimijoita ylittäessään yleisen kokoedellytyksen. Toimijalla tarkoitettaisiin lain liitteissä I ja II tarkoitettua toimintaa harjoittavia tai niissä tarkoitettua toimijatyyppiä olevia luonnollisia tai oikeushenkilöitä, jotka täyttävät tai ylittävät keskisuuren toimijan määritelmän. Keskisuuren toimijan määritelmästä säädettäisiin 2 §:n 15 kohdassa. Keskisuurella toimijalla tarkoitettaisiin julkista tai yksityistä toimijaa, joka täyttää komission suosituksen 2003/361/EY liitteessä olevan 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset ja jotka tarjoavat palvelujaan tai harjoittavat toimintaansa unionissa. Suosituksen liitteessä olevan 3 artiklan 4 kohtaa ei sovellettaisi keskisuuren toimijan määrittelyssä. Toimijan määritelmän kannalta ei olisi merkitystä yksikön tai organisaation oikeudellisella muodolla, vaan ainoastaan sillä, että toimija harjoittaa liitteessä I tai II tarkoitettua toimintaa ja täyttää toimijatyyppiä koskevan kokoedellytykset.

Tässä laissa tarkoitettuja toimijoita olisivat siten lähtökohtaisesti vain keskisuuret toimijat tai sitä suuremmat toimijat. Ehdotetussa 2 momentissa säädettäisiin kuitenkin eräistä poikkeuksista kokorajoitukseen, eli tilanteista, joissa toimija olisi laissa tarkoitettu toimija sen koosta riippumatta. Yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat, luottamuspalvelun tarjoajat, aluetunnusrekisterit sekä DNS-palveluntarjoajat olisivat laissa tarkoitettuja toimijoita niiden koosta riippumatta. Lisäksi CER-direktiivin nojalla määritellyt kriittiset toimijat olisivat tässä laissa tarkoitettuja toimijoita niiden koosta riippumatta.

Liitteen I *kohdissa 1-4* määriteltäisiin lain soveltamisalaan kuuluvat toimijat liikennesektorin osalta. Ilmaliikenteen osalta soveltamisalaan kuuluisivat kaupallisen lentoliikenteen harjoittajat, eräät lentoaseman pitäjät sekä lennonjohtopalvelun tarjoajat. Raideliikenteen osalta soveltamisalaan kuuluisivat rataverkon haltijat ja liikenteenohjauspalvelua tarjoavat yhtiöt, rautatieyritykset sekä palvelupaikan ylläpitäjät. Vesiliikenteen osalta soveltamisalaan kuuluisivat matkustaja- ja rahtiliikennettä hoitavat yhtiöt, satamanpitäjät ja toimijat, jotka huolehtivat rakenteista ja varusteista sataman alueella sekä VTS-palveluntarjoajat. Sataman alueella rakenteista ja varusteita huolehtivat toimijat voivat olla edellä mainittuja satamanpitäjiä tai muita toimijoita, jotka satamanpitäjä eli sataman alueen ylläpitäjä on sopimuksen perusteella oikeuttanut toimimaan alueella ja tarjoamaan palvelua. Aiemmin satamayhtiöt eli satamanpitäjät omistivat ylläpitämällään alueella olevat varastot ja muut rakenteet sekä erilaiset lastinkäsittelylaitteet. Nykyisin satamanpitäjä hallinnoi usein vain kyseistä aluetta ja osaa tai kaikkia satamapalvelun tarjoamiseen liittyvistä toimista voi toteuttaa sopimukseen perustuen muu toimija tai useat muut toimijat. Tällaisia satamatoimintoihin liittyviä palveluita voivat olla esimerkiksi alusten kiinnitys- ja irrotuspalvelu, hinaajapalvelu, lastinkäsittely, lastinkäsittelylaitteiden ja niitä käyttävän henkilöstön toimittaminen, lastitietojen käsittelyyn liittyvien toimien hoitaminen, satama-alueen vartiointipalvelut sekä kulunvalvontaan ja kulkulupiin liittyvät palvelut, jos kyseiset palvelut ovat sataman toiminnan kannalta merkityksellisiä. Tieliikenteen osalta soveltamisalaan kuuluisivat liikenteenhallinnasta vastaavat tieviranomaiset eräin poikkeuksin, sekä älykkäiden liikennejärjestelmien ylläpitäjät. Soveltamisala vastaisi liikennesektorin osalta sisällöllisesti NIS2-direktiivin Liitteen I kohdassa 2 määriteltyä vähimmäissoveltamisalaa.

Liitteen I *kohdassa 5* määriteltäisiin lain soveltamisalaan kuuluvat toimijat avaruussektorin osalta. NIS2-direktiivin soveltamisala kattaisi direktiivin liitteen I kohdan 11 mukaisesti avaruuspohjaisten palvelujen tarjoamista tukevan, jäsenvaltioiden tai yksityisten tahojen omista-

man, hallinnoiman ja operoiman maassa sijaitsevan infrastruktuurin ylläpitäjät, lukuun ottamatta yleisten sähköisten viestintäverkkojen tarjoajia. Määritelmän on katsottu sisältävän ainakin maa-asemalain 2 §:n 1 momentin 5 kohdassa tarkoitetut toiminnanharjoittajat. Lain soveltamisalaan kuuluisivat siten ainakin sellaiset toiminnanharjoittajat, jotka harjoittavat tai jonka on tarkoitus harjoittaa maa-asema- tai tutkatoimintaa tai jotka tosiasiallisesti vastaavat tällaisesta toiminnasta. Myös muut NIS2-direktiivin liitteen I kohdan 11 määritelmän täyttävät avaruussektorin toimijat kuin maa-asemalain mukaiset toiminnanharjoittajat kuuluisivat lain soveltamisalaan. Soveltamisala vastaisi avaruussektorin osalta sisällöllisesti NIS2-direktiivin liitteen I kohdassa 11 määriteltyä vähimmäissoveltamisalaa.

Liitteen I *kohdassa 6* määriteltäisiin lain soveltamisalaan kuuluvat toimijat digitaalisen infrastruktuurin osalta. Soveltamisalaan kuuluisivat internetin yhdysliikennepisteiden ylläpitäjät, DNS-palveluntarjoajat, aluetunnusrekisterit, pilvipalvelun tarjoajat, datakeskuspalvelun tarjoajat, sisällönjakeluverkon tarjoajat, luottamuspalvelun tarjoajat, yleisten sähköisten viestintäverkkojen tarjoajat sekä yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat. Toimijatyypit määriteltäisiin tarkemmin 2 §:n kohdissa 1, 3, 4, 13, 15, 19, 31 ja 32. Soveltamisala vastaisi digitaalisen infrastruktuurin osalta sisällöllisesti NIS2-direktiivin liitteen kohdassa 8 määriteltyä vähimmäissoveltamisalaa.

Liitteen I *kohdassa 7* määriteltäisiin lain soveltamisalaan kuuluvat toimijat TVT-palvelujen hallinnan osalta. Soveltamisalaan kuuluisivat hallintapalvelun tarjoajat ja tietoturvapalveluntarjoajat. Toimijatyypit määriteltäisiin tarkemmin 2 §:n kohdissa 8 ja 21. Soveltamisala vastaisi TVT-palvelujen hallinnan osalta NIS2-direktiivin liitteen I kohdassa 9 määriteltyä vähimmäissoveltamisalaa.

Liitteen I *kohdissa 8-12* määriteltäisiin lain soveltamisalaan kuuluvat toimijat energiasektorin osalta. Sähköalan osalta soveltamisalaan kuuluisivat sähkön toimittajat, jakeluverkonhaltijat, kantaverkonhaltijat, sähköntuottajat, sähkömarkkinaoperaattorit, aggregoinnin, kulutusjouston tai energian varastoinnin tarjoajat sekä latauspisteiden operaattorit. Lisäksi soveltamisalaan kuuluisivat kaukolämmityksen tai kaukojäähdytyksen haltijat, eli kaukolämmityksen ja -jäähdytyksen jakelijat. Kaukolämmön tai -jäähdytyksen tuottajat, joilla ei ole ollenkaan jakelutoimintaa jäisivät soveltamisalan ulkopuolelle. Kaasualan osalta lain soveltamisalaan kuuluisivat maakaasun toimittajat, jakeluverkonhaltijat, siirtoverkonhaltijat, varastointilaitteiston haltijat, nesteytetyn maakaasun käsittelylaitteiston haltijat, eräät maakaasualan yritykset sekä maakaasun jalostus- ja käsittelylaitteistojen haltijat. Öljyalan osalta soveltamisalaan kuuluisivat öljynsiirtoputkistojen haltijat, öljyn tuotanto-, jalostus- ja käsittelylaitteistojen haltijat, öljyn varastointia ja siirtoa hoitavat operaattorit sekä keskusvarastointiyksiköt. Vetyalan osalta soveltamisalaan kuuluisivat vedyn tuotantoa, varastointia ja siirtoa harjoittavat toimijat. Soveltamisala vastaisi energiasektorin osalta sisällöllisesti NIS2-direktiivin liitteen I kohdassa 1 määriteltyä vähimmäissoveltamisalaa.

Liitteen I *kohdassa 13* määriteltäisiin lain soveltamisalaan kuuluvat toimijat terveyssektorin osalta. Soveltamisalaan kuuluisivat terveydenhuollon tarjoajat, EU:n vertailulaboratoriot, lääkkeiden tutkimusta ja kehitystä harjoittavat toimijat, lääkeaineiden ja lääkkeiden valmistusta harjoittavat toimijat sekä eräiden lääkinnällisten laitteiden valmistajat. Soveltamisala vastaisi terveyssektorin osalta NIS2-direktiivin liitteen I kohdassa 5 määriteltyä vähimmäissoveltamisalaa.

Liitteen I *kohdassa 14* määriteltäisiin lain soveltamisalaan kuuluvat toimijat juomaveden osalta. Soveltamisalaan kuuluisivat sekä ihmisten käyttöön tarkoitetun veden toimittajat, että jakelijat. Soveltamisala vastaisi juomaveden osalta NIS2-direktiivin liitteen I kohdassa 6 määriteltyä vähimmäissoveltamisalaa.

Liitteen I *kohdassa 15* määriteltäisiin lain soveltamisalaan kuuluvat toimijat jäteveden osalta. Soveltamisalaan kuuluisivat yhdyskuntajätevettä, talousjätevettä tai teollisuusjätevettä keräävät, hävittävät tai käsittelevät yritykset. Soveltamisala vastaisi jäteveden osalta NIS2-direktiivin liitteen I kohdassa 7 määriteltyä vähimmäissoveltamisalaa.

Liitteen II *kohdassa 1* määriteltäisiin lain soveltamisalaan kuuluvat toimijat posti- ja kuriiripalvelujen osalta. Soveltamisalaan kuuluisivat sekä kuriiripalvelun tarjoajat, että postipalvelun tarjoajat. Soveltamisala vastaisi posti- ja kuriiripalvelujen osalta sisällöllisesti NIS2-direktiivin liitteen II kohdassa 1 määriteltyä vähimmäissoveltamisalaa.

Liitteen II *kohdassa 2* määriteltäisiin lain soveltamisalaan kuuluvat toimijat digitaalisen palvelun tarjoajien osalta. Soveltamisalaan kuuluisivat verkossa toimivien markkinapaikkojen tarjoajat, verkossa toimivien hakukoneiden tarjoajat sekä verkkoyhteisöalustojen tarjoajat. Toimijatyypit määriteltäisiin tarkemmin 2 §:n kohdissa 25-27. Soveltamisala vastaisi digitaalisen palvelun tarjoajien osalta NIS2-direktiivin liitteen II kohdassa 6 määriteltyä vähimmäissoveltamisalaa.

Liitteen II *kohdassa 3* määriteltäisiin lain soveltamisalaan kuuluvat toimijat moottoriajoneuvojen, perävaunujen ja puoliperävaunujen valmistuksen osalta. Soveltamisalaan kuuluisivat NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 29 tarkoitettua valmistusta harjoittavat yritykset. Soveltamisala vastaisi moottoriajoneuvojen, perävaunujen ja puoliperävaunujen valmistuksen osalta NIS2-direktiivin liitteen II kohdan 5 alakohdassa e määriteltyä vähimmäissoveltamisalaa.

Liitteen II *kohdassa 4* määriteltäisiin lain soveltamisalaan kuuluvat toimijat muiden kulkuneuvojen valmistuksen osalta. Soveltamisalaan kuuluisivat NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 30 tarkoitettua valmistusta harjoittavat yritykset. Soveltamisala vastaisi muiden kulkuneuvojen valmistuksen osalta NIS2-direktiivin liitteen II kohdan 5 alakohdassa f määriteltyä vähimmäissoveltamisalaa.

Liitteen II *kohdassa 5* määriteltäisiin lain soveltamisalaan kuuluvat tutkimusorganisaatiot. Soveltamisalaan kuuluisivat tutkimusorganisaatiot, joiden ensisijaisena tavoitteena on harjoittaa soveltavaa tutkimusta tai kokeellista kehitystyötä kyseisen tutkimuksen tulosten hyödyntämiseksi kaupallisiin tarkoituksiin. Lakia ei kuitenkaan sovellettaisi korkeakouluihin tai muihin opetus- ja koulutusalan laitoksiin. Tutkimusorganisaatioihin olisi luettava toimijat, joiden toiminnasta olennainen osa on Taloudellisen yhteistyön ja kehityksen järjestön vuonna 2015 laaditussa, tutkimus- ja kehittämistoiminnan tietojen keräämis- ja raportointiohjeita koskevassa Frascati-käsikirjassa tarkoitettua soveltavaa tutkimusta tai kokeellista kehitystyötä, joiden tuloksia ne hyödyntävät kaupallisiin tarkoituksiin, kuten tuotteen valmistamiseen tai kehittämiseen tai prosessiin, palvelun tarjoamiseen tai sen markkinointiin. Tutkimusorganisaatiot, jotka jakavat ja hyödyntävät tutkimustuloksia kaupallisiin tarkoituksiin, voivat olla tärkeitä osia arvoketjuissa, mikä tekee niiden viestintäverkkojen ja tietojärjestelmien turvallisuudesta merkityksellisen EU:n sisämarkkinoiden kyberturvallisuuden kannalta. Tutkimusorganisaation määritelmä vastaisi NIS2-direktiivin 6 artiklan 41 kohdan määritelmää ja johdantokappaletta 36. Lain soveltamisala vastaisi tutkimusorganisaatioiden osalta NIS2-direktiivin liitteen II kohdassa 7 määriteltyä vähimmäissoveltamisalaa.

Liitteen II *kohdassa 6* määriteltäisiin lain soveltamisalaan kuuluvat toimijat kemikaalisektorin osalta. Soveltamisalaan kuuluisivat kemikaalien valmistusta, tuotantoa tai jakelua. Soveltamisala vastaisi kemikaalisektorin osalta NIS2-direktiivin liitteen II kohdassa 3 määriteltyä vähimmäissoveltamisalaa.

Liitteen II *kohdassa 7* määriteltäisiin lain soveltamisalaan kuuluvat toimijat elintarvikesektorin osalta. Soveltamisalaan kuuluisivat elintarvikeyritykset, jotka harjoittavat tukkukauppaa, teollista tuotantoa tai jalostusta. Yrityksen ei tarvitsisi toimia kaikilla mainitusta toimialan osista, vaan riittäisi että se harjoittaisi jotakin niistä. Soveltamisala vastaisi elintarvikesektorin toimijoiden osalta sisällöllisesti NIS2-direktiivin liitteen II kohdassa 4 määriteltyä vähimmäissoveltamisalaa.

Liitteen II *kohdassa 8* määriteltäisiin lain soveltamisalaan kuuluvat toimijat jätehuoltosektorin osalta. Soveltamisalaan kuuluisivat jätehuoltoa harjoittavat yritykset. Soveltamisala vastaisi jätehuoltosektorin osalta NIS2-direktiivin liitteen II kohdassa 2 määriteltyä vähimmäissoveltamisalaa.

Liitteen II *kohdassa 9-10* määriteltäisiin lain soveltamisalaan kuuluvat toimijat lääkinnällisten laitteiden valmistuksen osalta. Soveltamisalaan kuuluisivat ns. MD-asetuksen soveltamisalaan kuuluvien lääkinnällisten laitteiden sekä in vitro –diagnostiikkaan tarkoitettujen lääkinnällisten laitteiden valmistajat. Vakavan kansanterveysuhan aikana kriittisiksi katsottuja lääkinnällisiä laitteita valmistavat toimijat kuuluisivat kuitenkin edellä kuvatulla tavalla Liitteen I kohdassa 13 tarkoitettuihin terveyssektorin toimijoihin. Soveltamisala vastaisi lääkinnällisten laitteiden valmistuksen osalta NIS2-direktiivin liitteen II kohdan 5 alakohdassa a määriteltyä vähimmäissoveltamisalaa.

Liitteen II *kohdassa 11* määriteltäisiin lain soveltamisalaan kuuluvat toimijat tietokoneiden sekä elektronisten ja optisten tuotteiden valmistuksen osalta. Soveltamisalaan kuuluisivat NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 26 tarkoitettua valmistusta harjoittavat yritykset. Soveltamisala vastaisi tietokoneiden sekä elektronisten ja optisten tuotteiden valmistuksen osalta NIS2-direktiivin liitteen II kohdan 5 alakohdassa b määriteltyä vähimmäissoveltamisalaa.

Liitteen II *kohdassa 12* määriteltäisiin lain soveltamisalaan kuuluvat toimijat sähkölaitteiden valmistuksen osalta. Soveltamisalaan kuuluisivat NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 27 tarkoitettua valmistusta harjoittavat yritykset. Soveltamisala vastaisi sähkölaitteiden valmistuksen osalta NIS2-direktiivin liitteen II kohdan 5 alakohdassa c määriteltyä vähimmäissoveltamisalaa.

Liitteen II *kohdassa 13* määriteltäisiin lain soveltamisalaan kuuluvat toimijat muiden koneiden ja laitteiden valmistuksen osalta. Soveltamisalaan kuuluisivat NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 28 tarkoitettua valmistusta harjoittavat yritykset. Soveltamisala vastaisi muiden koneiden ja laitteiden valmistuksen osalta NIS2-direktiivin liitteen II kohdan 5 alakohdassa d määriteltyä vähimmäissoveltamisalaa.

Ehdotuksella pantaisiin täytäntöön NIS2-direktiivin 2 artiklan 1–4 kohdat, 3 artiklan 1–2 kohdat ja 6 artiklan 38 kohta, pois lukien 2 artiklan 2 kohdan b–e alakohdat.

Pykälän *2 momentissa* säädettäisiin lain soveltamisesta liitteessä I tai II tarkoitettuun toimijaan sen koosta riippumatta, eli silloin, kun toimija ei täytä keskisuuren toimijan kynnysarvoa.

NS2-direktiivin 2 artiklan 2 kohdan b–e alakohdissa edellytetään, että soveltamisala kattaisi koosta riippumatta toimijat liitteissä I ja II tarkoitetuilla toimialoilla b – e alakohdissa tarkoitetuissa tilanteissa.

Ehdotetun 2 momentin nojalla lain soveltamisesta tällaisiin toimijoihin säädettäisiin valtioneuvoston asetuksella. Lainsäädäntövallan siirto olisi lakiteknisesti tarpeen, sillä kysymys olisi hyvin yksityiskohtaisesta toimijoiden määrittämisestä, jotka toiminnan erityisen laadun vuoksi kuuluisivat poikkeuksellisesti lain ja NIS2-direktiivin velvoitteiden soveltamisalaan toimijan koosta riippumatta. Ottaen huomioon NIS2-direktiivin 2 artiklan 2 kohdan b–e alakohdissa tarkoitettujen kriteerien laatu, soveltamisala näitä toimijoita koskien olisi myös altis muutoksille jatkossa, jos toimijoiden toiminnan laatu tai koko muuttuvat tai tiettyjen sektorien kannalta kriittiset toimijat vaihtuvat.

Ehdotetulla asetuksenantovaltuudella siirrettäisiin valta säätää lain soveltamisesta koosta riippumatta sellaisiin liitteissä I tai II tarkoitettua toimintaa harjoittaviin toimijoihin, joihin lakia ei muutoin sovellettaisi, koska ne eivät täyttäisi 1 momentissa tarkoitettua keskisuuren toimijan määritelmää. Edellytyksenä olisi lisäksi, että toimijassa olisi kyse jostakin 1–4 kohdassa tarkoitetusta tilanteesta. Ehdotetut 1–4 kohdat vastaisivat NIS2-direktiivin 2 artiklan 2 kohdan b–e alakohtia ja luettelo olisi tyhjentävä. Asetuksella ei voitaisi säätää lain soveltamisesta muulla kuin 1 – 4 kohdassa tarkoitetulla perusteella taikka muihin kuin liitteissä I tai II tarkoitettua toimintaa harjoittaviin toimijoihin. Jos toimija saatetaan asetuksella lain soveltamisalaan, olisi asetuksella samalla määriteltävä, onko toimijaa pidettävä 27 §:ssä tarkoitettuna keskeisenä toimijana.

Ehdotettu 2 momentti koskisi muita kuin niitä toimijoita, jotka kuuluvat koosta riippumatta lain soveltamisalaan 1 momentin 2 tai 3 alakohdan nojalla.

Ehdotuksella pantaisiin täytäntöön NIS2-direktiivin 2 artiklan 2 kohdan b–e alakohdat soveltamisalasta.

4 §. *Soveltamisalan rajaukset.* Pykälässä säädettäisiin eräistä poikkeuksista lain soveltamisalaan.

Pykälän *1 – 3 momentilla* otettaisiin käyttöön NIS2-direktiivin 2 artiklan 7–9 kohtien mukainen kansallinen liikkumavara soveltamisalasta.

Pykälän *1 momentissa* säädettäisiin poikkeus riskienhallinta- ja raportointivelvoitteiden soveltamisesta toimintaan tai palveluihin, joita tarjotaan maanpuolustuksen, kansallisen turvallisuuden, yleisen järjestyksen ja turvallisuuden taikka rikosten ennalta estämisen, rikostutkinnan ja syytetoimien toteuttamiseksi. Toimijaa koskisi edelleen 39 §:ssä tarkoitettu velvoite ilmoittautua toimijaluetteloon.

Pykälän *2 momentissa* säädettäisiin poikkeus koko lain soveltamisesta toimijaan, joka tarjoaa ainoastaan 1 momentissa tarkoitettua toimintaa tai palvelua.

Pykälän *3 momentin* nojalla toimija kuuluisi lain soveltamisalaan 1 ja 2 momentissa säädetystä poiketen silloin kun toimija on luottamuspalvelun tarjoaja.

Pykälän *4 momentissa* säädettäisiin poikkeus koko lain soveltamisesta toimijaan, johon DORA-asetusta ei sovelleta sen 2 artiklan 4 kohdan nojalla. Ehdotetulla 4 momentilla rajattaisiin lain soveltamisala NIS2-direktiivin 2 artiklan 10 kohdan mukaisesti.

Pykälän *5 momentissa* säädettäisiin selkeyden vuoksi NIS2-direktiivin 2 artiklan 11 kohtaa vastaavasta rajauksesta sille, ettei laissa velvoiteta sellaisen tiedon antamiseen, jonka luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin siihen liittyvää

tärkeää etua. Tällaisessa tilanteessa tiedon luovuttamiselle ei olisi velvollisuutta tämän lain nojalla. Säännöksellä ei rajattaisi tahoja, joiden välillä tällainen tiedon luovuttaminen voisi tulla kyseeseen, vaan merkityksellistä olisi luovutettavan tiedon laatu. Säännös voisi tulla poikkeuksellisessa tilanteessa sovellettavaksi esimerkiksi luovutettaessa tietoja keskitetyltä yhteyspisteeltä Euroopan komissiolle, NIS-yhteistyöryhmälle tai Euroopan unionin kyberturvallisuusvirasto ENISA:lle.

5 §. *Suhde muuhun lainsäädäntöön.* Pykälässä säädettäisiin lain suhteesta muuhun kyberturvallisuuden riskienhallinta- ja raportointivelvoitteita koskevaan lainsäädäntöön. Koska lakia sovellettaisiin horisontaalisesti eri sektoreilla, olisi tämän johdosta tarpeen selkeyttää lain suhdetta muihin säädöksiin ehdotetulla säännöksellä, joka ilmentäisi lain luonnetta yleislakina suhteessa sellaiseen sektorikohtaisiin sääntelyyn, jolla pyritään saavuttamaan kyberturvallisuuden korkeampi taso.

Laissa asetettaisiin horisontaalisesti kyberturvallisuuden riskienhallinnan ja poikkeamaraportoinnin yleiset vähimmäisvelvoitteet kaikille NIS2-direktiivin soveltamisalaan kuuluville toimijoille siten, että laissa säädettäisiin NIS2-direktiivin vähimmäistason edellyttämistä riskienhallinta- ja raportointivelvoitteista kullekin toimialalle. Sektorikohtaisesti on kuitenkin mahdollista, että kansallisessa laissa tai EU-sääntelyssä asetetaan tietylle toimialalle tai toimijatyypille yksityiskohtaisempia tai tarkempia velvoitteita, joilla pyritään varmistamaan NIS2-direktiivin mukaisia yleisvelvoitteita korkeampi kyberturvallisuuden taso. Tällaiset velvoitteet voivat sisältää esimerkiksi ehdotettuun lakiin verrattuna yksityiskohtaisempia säännöksiä riskienhallinnassa huomioitavista osa-alueista, edellyttää tietyn standardin tai sertifioinnin käyttämisestä taikka edellyttää tiiviimpää tai nopeampaa raportointia valvovalle viranomaiselle. Sektorikohtaista sääntelyä tulisi soveltaa tämän lain lisäksi siltä osin kuin sillä pyrittäisiin kyberturvallisuuden korkeamman tason turvaamiseen.

Pykälän *1 momentissa* säädettäisiin lain suhteesta muussa kansallisessa laissa oleviin säännöksiin. NIS2-direktiivi on sen 5 artiklan mukaisesti vähimmäisvelvoittava, eli NIS2-direktiivillä ei estetä jäsenvaltiota antamasta tai pitämästä voimassa säännöksiä, joilla varmistetaan kyberturvallisuuden korkeampi taso, edellyttäen, että tällaiset säännökset ovat unionin oikeudessa säädettyjen jäsenvaltioiden velvoitteiden mukaisia. Jos muussa laissa olisi tällaisia säännöksiä, joilla varmistettaisiin kyberturvallisuuden korkeampi taso, niitä sovellettaisiin sen lisäksi, mitä tässä laissa säädetään.

Pykälän *2 momentissa* säädettäisiin lain suhteesta toimialakohtaisissa unionin säädöksissä asetettaviin edellytyksiin toimijalle. Ehdotuksella pantaisiin täytäntöön NIS2-direktiivin 4 artikla. Sektorikohtaisia vaatimuksia kyberturvallisuudesta on unionin alakohtaisissa säädöksissä ainakin finanssimarkkinoihin ja ilmaliikenteeseen liittyen.

NIS2-direktiivin 4 artiklan 2 kohdan mukaisesti vaatimusten tulisi katsoa olevan vaikutukseltaan vastaavia, kun kyberturvallisuusriskien hallintatoimenpiteet ovat vaikutukseltaan vähintään NIS2-direktiivin 21 artiklan 1 ja 2 kohdassa säädettyjä toimenpiteitä vastaavia; tai alakohtaisessa unionin säädöksessä säädetään tämän NIS2-direktiivin mukaisten CSIRT-yksiköiden, toimivaltaisten viranomaisten tai keskitettyjen yhteyspisteiden välittömästä, tarvittaessa automaattisesta ja suorasta, pääsystä poikkeamailmoituksiin, jos merkittävistä poikkeamista ilmoittamista koskevat vaatimukset ovat vaikutukseltaan vähintään tämän direktiivin 23 artiklan 1–6 kohdassa säädettyjä vaatimuksia vastaavia. Mikäli sektorikohtainen sääntely katsotaan vaikutuksiltaan vastaavaksi kuin tässä laissa säädetyt velvoitteet, ei toimijaan sovellettaisi tämän lain 2 luvun tai 43 §:n velvoitteita eikä 4 ja 5 luvun säännöksiä valvonnasta ja seuraamusmaksun määräämisestä. Sektorikohtaisesta sääntelystä huolimatta kaikki tässä laissa tarkoitetut sektorit,

toimialat ja toimijatyypit tulisi huomioida kansallisten kyberturvallisuusstrategian ja laajamittaisten kyberturvallisuuspoikkeamien ja –kriisien hallintasuunnitelman valmistelussa ja CSIRT-yksikön toiminnassa.

Komissio on julkaissut tarkempaa ohjeistusta sektorikohtaisen unionin sääntelyn arvioimisesta suhteessa NIS2-sääntelyyn ja, mikäli sektorikohtainen sääntely katsotaan NIS2-sääntelyä vastaavaksi, NIS2-sääntelyn soveltumisesta tällaisen sektorikohtaisen sääntelyn alaan kuuluviin toimijoihin. Komission ohjeet NIS2-direktiivin 4 artiklan 1 ja 2 kohdan soveltamisesta on annettu tiedonantona 2023/C 328/02.

6 §. *Lainkäyttövalta ja alueellisuus.* Pykälässä säädettäisiin Suomen lainkäyttövallasta kansainvälisten toimijoiden osalta NIS2-direktiivin 26 artiklan mukaisella tavalla.

Pykälän *1 momentin* nojalla Suomen lakia sovellettaisiin toimijaan, joka on sijoittautunut Suomeen NIS2-direktiivin 26 artiklan 1 kohdan pääsäännön mukaisesti. Suomen lainkäyttövaltaan ja Suomen lain soveltamisalaan kuuluvat siten pääsääntöisesti toimijat, jotka ovat sijoittautuneet Suomeen. Mikäli Suomessa NIS2-direktiivin soveltamisalaan kuuluvaa toimintaa harjoittaisi tai palveluja tarjoaisi toimija, joka on sijoittautunut toiseen EU-jäsenvaltioon, kuuluisi toimija pääsääntöisesti ja vastaavasti sijoittautumisvaltionsa lainsäädännön ja -valvonnan alaan. Julkishallinnon toimija kuuluisi NIS2-direktiivin 26 artiklan 1 kohdan c alakohdan mukaisesti aina sen jäsenvaltion lainkäyttövaltaan, joka toimijan on perustanut.

Pykälän *2 momentissa* säädettäisiin poikkeuksesta 1 momentin pääsääntöön eräiden toimijoiden osalta NIS2-direktiivin 26 artiklan 1 kohdan a alakohtaa vastaavasti. Riippumatta valtiosta, johon toimija on sijoittautunut, yleisen sähköisen viestintäverkon tarjoaja ja yleisesti saatavilla olevan sähköisen viestintäpalvelun tarjoaja kuuluisi sen jäsenvaltion lainkäyttövallan piiriin, jossa se tarjoaa palvelujaan. Näin ollen mainittuja palveluita Suomessa tarjoavat toimijat kuuluisivat Suomen lainkäyttövaltaan. Jos yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoaja tarjoaa yleisesti saatavilla olevaa rekursiivista DNS-palvelua ainoastaan internetyhteyspalvelun osana, kyseinen toimija kuuluisi kunkin jäsenvaltion lainkäyttövaltaan, joissa se tarjoaa palvelujaan, jäsenvaltiossa tarjottavan palvelun osalta.

Pykälän *3 momentissa* säädettäisiin poikkeuksesta 1 momentin pääsääntöön eräiden toimijoiden osalta NIS2-direktiivin 26 artiklan 1 kohdan b alakohtaa ja 26 artiklan 2-5 kohtia vastaavasti. Momentissa tarkoitetut toimijat kuuluisivat NIS2-direktiivissä tarkoitettujen velvoitteiden osalta sen jäsenvaltion lainkäyttövaltaan, jossa sijaitsee toimijan NIS2-direktiivin 26 artiklan 2 kohdassa tarkoitettu päätoimipaikka. Lainkäyttövalta näiden toimijoiden osalta kuuluisi siten vain yhdelle jäsenvaltiolle. NIS2-direktiivin 26 artiklan 2 kohdan mukaisesti toimijan päätoimipaikan katsotaan olevan siinä jäsenvaltiossa, jossa kyberturvallisuuden riskienhallinnan toimenpiteisiin liittyvät päätökset pääsääntöisesti tehdään. Jos tällaista jäsenvaltiota ei voida määrittää tai jos tällaisia päätöksiä ei tehdä unionissa, päätoimipaikan katsotaan sijaitsevan jäsenvaltiossa, jossa kyberturvallisuustoiminnot toteutetaan. Jos tällaista jäsenvaltiota ei voida määrittää, päätoimipaikan katsotaan sijaitsevan jäsenvaltiossa, jossa asianomaisella toimijalla on eniten työntekijöitä työllistävä toimipaikka unionissa.

Jos toimijan päätoimipaikka sijaitsisi Euroopan unionin ulkopuolella mutta se tarjoaisi palvelujaan Euroopan unionin alueella, toimijan edellytetään nimeävän edustaja Euroopan unioniin NIS2-direktiivin 26 artiklan 3 kohdan mukaisesti. Tällöin toimija kuuluisi sen jäsenvaltion lainkäyttövallan piiriin, jossa toimijan nimetty edustaja sijaitsee. Jos Euroopan unionin ulkopuolelle sijoittautunut toimija ei ole asettanut toimijalta edellytettyä ja NIS2-direktiivin 26 artiklan 3

kohdassa tarkoitettua nimettyä edustajaa Euroopan unionissa ja toimija tarjoaa palveluita Suomessa, toimija kuuluisi Suomen lainkäyttövaltaan ja lain soveltamisalaan.

Euroopan unionin ulkopuolelle sijoittuneen toimijan katsotaan tarjoavan palveluja Euroopan unionin alueella, jos se aikoo tarjota palveluja henkilöille yhdessä tai useammassa jäsenvaltiossa. Esimerkiksi yhdessä tai useammassa jäsenvaltiossa yleisesti käytettävän kielen tai rahayksikön käyttäminen ja mahdollisuus tilata palveluja kyseisellä kielellä taikka unionissa olevien asiakkaiden tai käyttäjien mainitseminen voivat osoittaa toimijan aikomusta tarjota palveluja unionin jäsenvaltiossa oleville henkilöille. Toisaalta yksin verkkosivuston tai sähköpostiosoitteen tai muiden yhteystietojen saatavuus unionissa ei yleensä riitä osoittamaan, että toimija aikoo tarjota palvelujaan Euroopan unionissa.

Nimetyn edustajan olisi toimittava toimijan puolesta, ja toimivaltaisten viranomaisten tai CSIRT-yksiköiden olisi voitava ottaa yhteyttä edustajaan. Edustaja olisi nimettävä nimenomaisesti toimijan antamalla kirjallisella valtuutuksella hoitamaan tämän puolesta tässä direktiivissä säädetyt velvoitteet, myös poikkeamista raportointi. Edustajan nimeäminen ei kuitenkaan rajoittaisi jäsenvaltioiden mahdollisuutta panna vireille oikeustoimia toimijaa itseään vastaan.

Pykälän *4 momentissa* säädettäisiin valvovan viranomaisen mahdollisuudesta kohdistaa valvonta- ja täytäntöönpanotoimia sellaiseen toimijaan, joka on sijoittautunut toiseen Euroopan unionin jäsenvaltioon, mutta joka tarjoaa palveluja Suomessa tai jolla on viestintäverkko tai tietojärjestelmä Suomessa. Valvova viranomainen voisi suorittaa toiseen Euroopan unionin jäsenvaltioon sijoittautuneeseen toimijaan kohdistuvia valvonta- ja täytäntöönpanotoimia Suomessa laissa säädetyllä tavalla, jos sijoittautumisvaltion toimivaltainen viranomainen sitä pyytää. Edellytyksenä on lisäksi, että toimija tarjoaa palveluja Suomessa tai sillä on viestintäverkko tai tietojärjestelmä Suomen alueella ja valvovalla viranomaisella olisi oikeus suorittaa pyydetty toimi tämän lain nojalla.

Jäsenvaltioiden viranomaisten keskinäisestä yhteistyöstä säädetään NIS2-direktiivin 37 artiklassa, joka valvovan viranomaisen tulisi yhteistyötä toteuttaessa huomioida. NIS2-direktiivin 37 artiklan 1 kohdan toisen kappaleen nojalla valvova viranomainen ei saisi kieltäytyä pyynnöstä, paitsi jos sillä ei ole lain nojalla toimivaltaa antaa pyydettyä apua, pyydetty apu ei ole oikeassa suhteessa valvovan viranomaisen valvontatehtäviin tai pyyntö koskee sellaisia tietoja tai käsittää sellaisia toimintoja, joiden paljastaminen tai toteuttaminen olisi vastoin Suomen kansalliseen turvallisuuteen, yleiseen turvallisuuteen tai puolustukseen liittyviä etuja. Ennen pyynnöstä kieltäytymistä valvovan viranomaisen olisi kuultava muita asianomaisia toimivaltaisia viranomaisia sekä, jos jokin jäsenvaltioista sitä pyytää, Euroopan unionin komissiota ja ENISAa.

7 §. *Kyberturvallisuuden riskienhallintavelvoite*. Pykälässä säädettäisiin soveltamisalaan kuuluvien toimijoiden yleisestä velvoitteesta tunnistaa, arvioida ja hallita riskejä, joita sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen kohdistuu.

Pykälän *1 momentin* nojalla toimijoiden velvollisuutena olisi varmistua riskienhallinnan keinoin siitä, että toiminnassa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuustaso ja riskienhallintatoimenpiteiden taso on riittävä ja oikeasuhtainen riskeihin ja viestintäverkon tai tietojärjestelmän merkitykseen nähden. Riskienhallinnalla tarkoitettaisiin toiminnan tai palveluntarjonnan kannalta merkityksellisiin viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien tunnistamista, riskien vakavuuksien arvioimista sekä riittävien toimenpiteiden toteuttamista riskien hallitsemiseksi.

NIS2-direktiivin johdantokappaleen 77 mukaisesti riskienhallintakulttuuria toimijoissa tulisi edistää ja kehittää, ja siihen tulisi sisältyä riskinarviointi ja riskeihin suhteutettujen kyberturvallisuusriskien hallintatoimenpiteiden toteuttaminen.

Pykälän *2 momentin* nojalla toimijan tulisi toteuttaa turvallisuus- ja riskienhallintatoimenpiteet, jotka ovat ajantasaisia, oikeasuhtaisia ja riittäviä suhteessa toiminnassa käytettäville viestintäverkoille ja tietojärjestelmille aiheutuville riskeille sekä viestintäverkon tai tietojärjestelmän merkitykselle toimijan toiminnan ja palveluntarjonnan kannalta. Tunnistetun riskin merkityksen määrittely on sekä subjektiivista toimijan omien liiketoiminta- tai palveluintressien perusteella, että objektiivista toimijan viestintäverkon ja tietojärjestelmän luotettavuudesta riippuvaisen palvelun yleisen ja yhteiskunnallisen merkittävyyden ja tärkeyden perusteella. Objektiiviset perusteet kuvataan tarkemmin 9 §:ssä ja sen perusteluissa. Riskienhallinnan tarkoituksena on estää tai minimoida viestintäverkkojen ja tietojärjestelmien poikkeamien vaikutusta toimintaan, palvelujen vastaanottajiin ja muihin palveluihin häiriötilanteessa häiriön syystä riippumatta. Riskienhallinnalla on siten pyrittävä turvaamaan toiminnan jatkuvuus tilanteissa, joissa viestintäverkkojen ja tietojärjestelmien toiminta häiriintyisi joko pahantahtoisen toiminnan vuoksi tai muusta syystä.

Velvoite kyberturvallisuuden riskienhallinnasta olisi luonteeltaan jatkuvaa, sillä viestintäverkkojen ja tietojärjestelmien turvallisuuteen kohdistuvat riskit muuttuvat ja turvallisuustoimet kehittyvät ajan myötä. Riskienhallinnassa toteutettavien toimenpiteiden tulisi ennen kaikkea olla ajantasaisia, eli vastata ajantasaista teknologista kehitystä ja tunnettuja parhaita käytänteitä siitä, kuinka kyberturvallisuusriskeiltä voidaan suojautua tai niiden vaikutuksia minimoida. Riskienhallinnan riittävyyttä ja oikeasuhtaisuutta arvioitaessa tulisi huomioida muun ohella viestintäverkon tai tietojärjestelmän merkitys toimijan toiminnan tai palveluntarjonnan kannalta, viestintäverkossa tai tietojärjestelmässä käsiteltävien tietojen laatu sekä muiden toimijoiden riippuvuus toimijan toiminnasta, palveluntarjonnasta, viestintäverkosta tai tietojärjestelmästä sekä erityisesti sen merkitys yhteiskunnan kriisinkestävyyden kannalta.

Kyberturvallisuuden riskienarvioinnin tarkoituksena olisi edistää ja kehittää riskienhallintakulttuuria, johon sisältyy riskienarviointi ja riskeihin suhteutettujen kyberturvallisuusriskien hallintatoimenpiteiden toteuttaminen ja seuranta. Mitä merkittävämpiä vaikutuksia riskillä toteutuessaan olisi ja mitä merkittävämpi sen toteutumisen todennäköisyys on, sitä tehokkaampia, korkeatasoisempia ja korkeampia kustannuksia aiheuttavia hallintatoimenpiteitä edellytettäisiin oikeasuhtaiselta riskienhallinnalta.

Riskin määritelmästä säädettäisiin 2 §:n 18 kohdassa.

Ehdotetuilla 7–10 §:llä pantaisiin täytäntöön NIS2-direktiivin artiklat 20–22.

8 §. *Kyberturvallisuuden riskienhallinnan toimintamalli*. Pykälässä säädettäisiin toimijan velvoitteesta pitää käytössään ajantasainen kyberturvallisuuden riskienhallinnan toimintamalli säädetyn riskienhallintavelvoitteen toteuttamiseksi. Kyberturvallisuuden riskienhallinnan toimintamallissa tulisi tunnistaa toimijan käytössä oleviin tai palveluntarjontaan vaikuttaviin viestintäverkkoihin ja tietojärjestelmiin sekä niiden fyysiseen ympäristöön kohdistuvat riskit sekä tunnistaa ja kuvata riskienhallinnan toimenpiteet ja menettelyt, joilla viestintäverkkoja ja tietojärjestelmiä sekä niiden fyysistä ympäristöä suojataan riskien ja poikkeamien toteutumiselta tai haitallisilta vaikutuksilta. Toimija voisi luoda kyberturvallisuuden riskienhallinnan toimintamallin itse tai hankkia sen ulkoistetusti. Kyberturvallisuuden riskienhallinnan toimintamalli voisi olla myös osa toimijan laajempaa riskienhallintasuunnitelmaa, jossa huomioidaan myös muita toimintaan kohdistuvia riskejä tai osa muuta turvallisuusvarautumista.

Kyberturvallisuuden riskienhallinnan toimintamalli tulisi luoda kaikki vaaratekijät huomioivan lähestymistavan (all-hazard approach) mukaisesti kattamaan sekä viestintäverkot ja tietojärjestelmät että niiden fyysinen ympäristö. Tarkoituksena on suojata viestintäverkkojen ja tietojärjestelmien sekä niiden avulla harjoitettua toimintaa tai tarjottavia palveluita tietoturvaloukkauksilta, järjestelmähäiriöiltä, inhimillisiltä virheiltä, vihamielisiltä teoilta ja luonnonilmiöiltä. Kaikki vaaratekijät huomioivassa lähestymistavassa tulisi siis huomioida kaikki kohtuudella ennakoitavissa olevat viestintäverkkoihin ja tietojärjestelmiin kohdistuvat uhkatekijät, olivat ne sitten tietoturvauhkien, luonnon tai ihmisen aiheuttamia, onnettomuuksia tai tahallaan aiheutettuja.

Kaikki vaaratekijät huomioivan lähestymistavan tulisi kattaa viestintäverkkojen ja tietojärjestelmien tietoturvallisuusriskit kuten hallinnollisen, henkilöstö-, laitteisto- ja ohjelmisto-, tietoaineisto- sekä käyttöturvallisuuden riskit ja niiden fyysisen ympäristön, toimitilojen ja välttämättömien resurssien osalta sellaisia tapahtumia, kuten varkaus, tulipalo, tulva, televiestintähäiriö tai sähkökatko, luvaton fyysinen pääsy toimijan tietoihin tai tietojenkäsittely-ympäristöön sekä vahinko ja häirintä, joka vaarantaisi viestintäverkoissa ja tietojärjestelmissä tai niiden välityksellä käsiteltävien tietojen tai palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden.

Riskienhallinnassa olisi otettava huomioon se, missä määrin toimija on riippuvainen viestintäverkosta ja tietojärjestelmistä. Mitä merkittävämmästä järjestelmästä palveluntuotannon kannalta on kyse ja mitä merkittävämpiä haitallisia vaikutuksia riski toteutuessaan järjestelmälle aiheuttaisi, sitä korkeampitasoista riskienhallintaa olisi tältä osin edellytettävä.

Kyberturvallisuuden riskienhallinnan toimintamalli ja siihen perustuvat hallintatoimenpiteet olisi päivitettävä ja pidettävä ajantasaisena osana 7 §:ssä tarkoitettua jatkuvaa riskien tunnistamista ja arviointia.

9 §. *Kyberturvallisuuden riskienhallinnan toimenpiteet*. Toimijoiden olisi toteutettava oikeasuhtaiset toimenpiteet viestintäverkkojen ja tietojärjestelmien turvallisuudelle kohdistuvien riskien hallitsemiseksi, ehkäisemiseksi ja haitallisten vaikutusten estämiseksi tai minimoimiseksi. Näiden toimenpiteiden oikeasuhteisuutta arvioitaessa on otettava asianmukaisesti huomioon se, missä määrin toimija altistuu riskeille, toimijan koko ja poikkeamien esiintymisen todennäköisyys ja niiden vakavuus, mukaan lukien niiden yhteiskunnalliset ja taloudelliset vaikutukset.

Pykälän *2 momentissa* säädettäisiin NIS2-direktiivin 21 artiklan 2 kohtaa vastaavasti osa-alueista, jotka olisi vähintään huomioitava kyberturvallisuuden riskienhallinnan toimintamallin luomisessa ja tarpeellisten riskienhallintatoimenpiteiden määrittelyssä. Osa-alueiden yksilöinnin tarkoitus alakohdissa on määritellä vaatimukset toisaalta mahdollisimman tarkasti, jotta ne ovat toimijoille ennakoitavia ja toisaalta teknologianeutraalisti, jotta ne soveltuvat kaikille toimialoille ja jatkuvasti muuttuvaan kyberturvallisuusympäristöön. Vaatimusten määrittely edesauttaa myös sitä, että valvovan viranomaisen perusteet valvontatoimenpiteille ovat selkeät ja ennakoitavat. Pykälässä käytettävät termit on pyritty sovittamaan yhteen teknisen toimialan terminologian kanssa. Toimintaperiaatteilla tarkoitetaan toimijan yleisen tason periaatteita ja päämäärien määrittelyä eli politiikkoja (policy). Menettelyillä tarkoitetaan erilaisia prosesseja ja teknisiä menettelytapoja (procedures, processes). Käytännöillä tarkoitetaan toimintatapoja (practises). Termien välinen rajanveto ei ole tarkkarajaista ja teknisissä lähteissä kuten standardeissa niitä voidaan käyttää eri merkityksissä.

Kohdassa 1 tarkoitettaisiin kyberturvallisuuden riskienhallinnan toimintaperiaatteita ja riskienhallinnan toimenpiteiden vaikuttavuuden arviointia. Kohdalla pantaisiin täytäntöön NIS2-direktiivin 21 artiklan 2 kohdan f alakohta sekä osin a alakohta. Kyberturvallisuuden riskienhallinnan

toimintaperiaatteilla tarkoitetaan organisaation ylimmän tason suunnittelua, jolla tunnistetaan, arvioidaan ja käsitellään järjestelmällisesti organisaatioon tai sen toimintaan kohdistuvia riskejä, asetetaan päämäärät ja seurataan niiden toteutumista. Toimijalla tulisi olla kattava kyberturvallisuuden riskienhallinnan toimintamalli, jolla tunnistetaan, analysoidaan, arvioidaan ja käsitellään viestintäverkkoihin ja tietojärjestelmiin sekä niiden fyysiseen ympäristöön kohdistuvia riskejä säännöllisesti. Riskienhallinnan tulisi olla luonteeltaan jatkuvaa ja osana organisaation toimintaa, minkä toteutuminen edellyttää toimintaperiaatteiden ja toimenpiteiden vaikuttavuuden arvioinnin sisällyttämistä hallintatoimenpiteisiin. Kyberturvallisuuden riskienhallinnan toimintaperiaatteiden ja toimintamallin olisi suositeltavaa perustua ajantasaisiin toimialalla omaksuttuihin parhaisiin käytänteisiin ja standardeihin.

Riskienhallinnassa tulisi noudattaa kaikki vaaratekijät huomioivaa lähestymistapaa ja varmistaa, että yrityksen hallintotapa ja riskienhallintaprosessit ottavat huomioon kyberturvallisuusriskit. Riskienhallinnan lähtökohtana tulisi olla tunnistaa luottamuksellisuuteen, eheyteen, saatavuuteen ja aitouteen liittyvät tarpeet sekä toimintojen kannalta keskeiset palvelut, järjestelmät, prosessit ja henkilöt. Tätä tunnistamista tarkennetaan omaisuudenhallintaa koskevassa kohdassa 5. Lisäksi tulisi tunnistaa toimijaan kohdistuvat uhat ja arvioida näiden todennäköisyydet sekä vaikutukset. Riskienhallinnan tavoitteena tulisi olla riskien käsittely niin, että niiden todennäköisyys tai vaikutus on minimoitu, poistettu tai ulkoistettu. Riskien käsittelyn lopputuloksena muodostuneet jäännösriskit tulisi hyväksyä perustellusti. Riskienhallinnan vaikuttavuutta olisi arvioitava säännöllisesti sopivin mittarein niin, että valittujen toimenpiteiden toimivuutta voitaisiin mitata ja tarvittaessa parantaa. Arvioinnin voisi tehdä esimerkiksi itsearviointina tai riippumattomia tietoturvapalveluntarjoajia hyödyntäen.

Kohdassa 2 tarkoitettaisiin viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevia toimintaperiaatteita ja menettelyitä. Kohdalla pantaisiin täytäntöön NIS2-direktiivin 21 artiklan 2 kohdan a alakohta. Viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevilla toimintaperiaatteilla tarkoitetaan toimijan näkemystä tietoturvan päämääristä, periaatteista ja toteutuksesta koko elinkaaren ajan. Nämä voivat koskea hallinnollista, henkilöstö-, laitteisto-, ohjelmisto-, viestintäverkko- ja tietoaineistoturvallisuutta sekä operoinnin ja fyysisen ympäristön turvallisuutta. ISO 27001 -standardin yhteydessä vastaavista toimintaperiaatteista käytetään termiä tietoturvapolitiikka. Toimijalla tulisi olla kirjalliset viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet ja menettelyt. Näiden tulisi olla oikeasuhtaisia toimijan tarpeisiin nähden ja ajantasaisesti ylläpidettyjä. Toimijan henkilöstön tulisi tuntea käytössä olevat turvallisuusmenettelyt ja sitoutua niiden noudattamiseen. Sopivien menettelyiden valinnassa voitaisiin huomioida liiketoiminnalliset tarpeet ja tunnistetut kyberturvallisuusriskit.

Kohdassa 3 tarkoitettaisiin viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuutta sekä menettelyjä haavoittuvuuksien käsittelyssä ja julkistamisessa. Kohdalla pantaisiin täytäntöön NIS2-direktiivin 21 artiklan 2 kohdan e alakohta. Toimijan tulisi ylläpitää viestintäverkkojen ja tietojärjestelmien turvallisuutta koko niiden elinkaaren ajan. Hankittavien järjestelmien olisi oltava toiminnan tarpeiden perusteella riittävän turvallisia muun muassa eheyden, saatavuuden ja luottamuksellisuuden suhteen ja niiden olisi kyettävä suojautumaan tavallisimpia hyökkäyksiä vastaan. Järjestelmien turvallinen konfiguraatio tulisi määritellä, dokumentoida ja ylläpitää koko elinkaaren ajan, ja tämä tulisi huomioida erityisesti päivitysten aikana. Konfiguraatio- ja ohjelmistopäivitysten tulisi olla dokumentoituja, muutoshallintaprosessien mukaisesti suunniteltuja, kattavia sekä kohteen ominaispiirteiden ja päivitysten kriittisyyden kannalta oikea-aikaisia. Luvattomien tai haitallisten muutosten tekeminen tulisi estää. Turvallisuuden kannalta kriittisimmät kohteet tulisi tunnistaa ja näiden turvallisuudesta tulisi huolehtia lisäksi esimerkiksi tarkastelemalla säännöllisesti prosesseja tai teknisillä testauksilla. Jos toimija tuottaa viestintäverkko- tai tietojärjestelmäpalveluita, olisi toimijan huo-

lehdittava näiden turvallisuudesta. Toimijan olisi varmistettava, että näiden turvallinen konfiguraatio on mahdollista ja niille tuotetaan turvallisuuspäivityksiä. Löydettyjä haavoittuvuuksia varten olisi oltava olemassa raportointikanava sekä ennalta määritellyt menettelytavat ja käytännöt ilmoitusten käsittelyä varten. Toimijan tulisi varmistua siitä, että tuotteet on kehitetty käyttäen tunnettuja hyviä käytäntöjä niin, että prosessi kattaa koko kehityksen elinkaaren. Jos toimija ei tuota viestintäverkko- tai tietojärjestelmäpalveluja itse, ei sen tarvitsisi myöskään itse käsitellä haavoittuvuusilmoituksia tai julkistaa haavoittuvuuksia. Viestintäverkkojen osalta olisi huolehdittava verkon turvallisesta rakenteesta. Toiminnoille kriittiset kohteet tulisi tunnistaa ja tarvittaessa suojata ajantasaisin teknisin keinoin, esimerkiksi vyöhykkeistämällä. Mahdollinen haitallinen tekninen liikenne tulisi kyetä havaitsemaan ja estämään.

Kohdassa 4 tarkoitettaisiin toimitusketjun, toimittajien tuotteiden ja palveluntarjoajien palvelujen yleisestä laatua ja häiriönsietokykyä, tuotteisiin ja palveluihin sisällytettyjä kyberturvallisuusriskien hallintatoimenpiteitä sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytäntöjä. Kohdalla pantaisiin täytäntöön NIS2-direktiivin 21 artiklan 2 kohdan d alakohta ja 21 artiklan 3 kohta. Toimijalla tulisi olla ajantasainen tieto kaikista toimintaan ja palveluntarjontaan vaikuttavista välittömistä toimittajista ja palveluntarjoajista. Toimijan tulisi riskienhallinnassaan ottaa huomioon toimitusketjuhäiriön vaikutus sen omaan toimintaan sekä varautua mahdolliseen toimitushäiriöön. Toimijan olisi otettava turvallisuusnäkökohdat huomioon suhteessa toimitusketjunsa välittömiin laite- tai palvelutoimittajiin. Riskien hallintatoimenpiteitä harkitessa tulisi ottaa huomioon välittömälle toimittajalle ja palveluntarjoajalle ominaiset haavoittuvuudet, tuotteiden ja palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt. Nämä voisivat sisältää erilaisia turvallisuuteen liittyviä vaatimuksia esimerkiksi saatavuuden, ylläpidettävyyden ja sopimusten osalta. Tässä laissa säädettyjen vaatimusten kannalta toimija vastaa itse siitä, että se hankkii omaan toimintaansa sellaisia tuotteita ja palveluita, että toimijan riskienhallinnan vaatimukset täyttyvät. Lain vaatimukset eivät siis koske alihankkijaa, ellei se itsekin ole toimija, jonka toimintaa sääntely koskee. Tällöinkin alihankkija vastaa sääntelyn kannalta siihen itseensä kohdistuvien vaatimusten täyttämisestä ja siltä palveluita tai tuotteita hankkivan toimijan suhteen siitä, mitä alihankinnassa on sovittu. Toimijat voisivat hallita toimitusketjujen kyberturvallisuusriskiä sisällyttämällä kyberturvallisuusriskien hallintatoimenpiteitä sopimusjärjestelyihin, joita ne tekevät välittömien toimittajiensa ja palveluntarjoajiensa kanssa. NIS2-direktiivin 85 johdantokappaleen mukaisesti toimitusketjusta ja suhteesta toimittajiin aiheutuviin riskeihin puuttuminen olisi erityisen tärkeää toimijalle toimitusketjujen merkityksen vuoksi.

NIS yhteistyöryhmä, Euroopan komissio ja ENISA laativat NIS2-direktiivin 22 artiklan mukaisesti yhteistyössä riskiarviointeja tietyistä toimitusketjuista. Siltä osin, kuin tällaisia riskiarviointeja on laadittu, toimijoiden olisi hyödynnettävä riskiarvioita soveltuvin osin.

Kohdassa 5 tarkoitettaisiin omaisuudenhallintaa ja turvallisuuden kannalta tärkeiden toimintojen tunnistamista. Kohdalla pantaisiin täytäntöön NIS2-direktiivin 21 artiklan 2 kohdan i alakohta osittain. Omaisuudenhallinnalla tarkoitetaan niitä menettelyjä ja toimenpiteitä, joilla toimija hallinnoi toiminnan kannalta olennaista laite-, ohjelmisto- ja tieto-omaisuuttaan. Omaisuudenhallinta on kyberturvallisuusriskien hallinnassa keskeinen keino, jonka huolellinen hoitaminen ennalta ehkäisee riskien toteutumista ja auttaa riskienhallinnassa. Toimijalla olisi oltava säännölliset ja dokumentoidut omaisuudenhallinnan menettelyt ja ohjeet, jotka pitävät sisällään toimintojen, prosessien ja tietojen tunnistamisen. Omaisuudella tarkoitetaan esimerkiksi tiloja, laitteita, ohjelmistoja, palveluita, henkilöitä, aineetonta omaisuutta ja resursseja kuten immateriaalioikeuksia tai IP-osoitteita. Viestintäverkkoon ja tietojärjestelmään liittyvä omaisuus tulisi tunnistaa ja luokitella suojaustarpeiden perusteella. Omaisuudesta tulisi ylläpitää ajantasaista luetteloa. Omaisuudenhallinnan tulisi olla olennainen osa henkilöstön, ulkoisten toimijoiden ja

tietojärjestelmien muutoksia sekä laitteiden elinkaaren hallintaa niiden käyttöönotosta turvalliseen poistamiseen asti.

Kohdassa 6 tarkoitettaisiin henkilöstöturvallisuutta ja kyberturvallisuuskoulutusta. Kohdalla pantaisiin täytäntöön NIS2-direktiivin 21 artiklan 2 kohdan i alakohta osittain ja g alakohta. Henkilöstöturvallisuudella tarkoitetaan menettelyjä, joilla varmistetaan henkilöiden tietoturvavastuut ja velvollisuudet, tietoturvaosaaminen ja taustatarkastukset sekä avainhenkilöriskien hallinta. Lisäksi nämä menettelyt kattavat väärinkäytösten estämistä, kuten vaarallisten työyhdistelmien tunnistamista ja välttämistä, työtehtäväkiertoa, sekä työsuhteen tai sopimuksen päättymisen. Toimijalla tulisi olla henkilöstöön liittyvät menettelytavat, joissa huomioidaan myös ulkoiset toimijat, kuten alihankkijat. Menettelytapojen tulisi huomioida myös työsuhteen päättymisen ja työtehtävien muutoksien jälkeiset vastuut ja velvollisuudet. Henkilöstöä ja ulkoisia toimijoita olisi tiedotettava heidän työtehtäviensä ja tarjoamiensa palveluiden turvallisuuteen liittyvistä vastuista ja velvoitteista, esimerkiksi salassapitoon liittyen. Jos työtehtävien ja vastuiden katsotaan vaativan erityistä luotettavuutta, henkilölle voitaisiin esimerkiksi tehdä esimerkiksi tarkoituksenmukainen taustatarkistus.

Toimijan olisi huolehdittava siitä, että henkilöstöllä on kyvykkyys toimia tavalla, joka vastaa kyberturvallisuuden hallintamallia ja hallintatoimenpiteitä. Tämän saavuttamiseksi henkilöstölle tulisi järjestää koulutusta, jolla pyritään tietoisuuden parantamiseen yleisesti kyberturvallisuudesta, ajantasaisten menettelyiden ja käytäntöjen tuntemuksesta sekä tunnetuista kyberturvallisuusriskeistä. Koulutuksella tai muulla vastaavalla tavalla tulisi varmistua, että henkilöstöllä on työtehtäviinsä nähden riittävä osaaminen viestintäverkon ja tietojärjestelmän suojaamisesta, kyberturvallisuusriskien tunnistamisesta, riskienhallintakäytännöistä ja niiden vaikutusten arvioinnista toimijan tarjoamiin palveluihin liittyen, ja että tätä osaamista myös ylläpidetään riittävällä tasolla. Toimijan johdon velvollisuudesta ylläpitää riittävää perehtyneisyyttä kyberturvallisuuden riskienhallintaan säädettäisiin 10 §:ssä.

Kohdassa 7 tarkoitettaisiin pääsynhallinnan ja todentamisen menettelyitä. Kohdalla pantaisiin täytäntöön NIS2-direktiivin 21 artiklan 2 kohdan alakohta i osittain ja alakohta j osittain. Pääsynhallinnalla ja todentamisella tarkoitetaan menettelyjä, joilla varmistetaan käyttäjien, laitteiden, sovellusten ja järjestelmien tunnistaminen sekä toteutetaan pääsy tietoturvallisuutta koskevien vaatimusten mukaisesti. Pääsynhallinnan ja todentamisen menettelyiden tulisi koskea sekä luonnollisia käyttäjiä kuten henkilöstöä ja ulkoisia toimijoita, että järjestelmätunnuksia kuten laitteiden, ohjelmistojen, rajapintojen ja muiden oleellisten resurssien käyttämiä tunnuksia. Pääsynhallinnan tulisi koskea sekä ohjelmistolla todennettavaa pääsyä, että fyysistä pääsyä. Menettelyiden tulisi perustua liiketoimintavaatimuksiin sekä tietoverkkoja ja tietojärjestelmiä koskeviin vaatimuksiin järjestelmien erityispiirteet huomioon ottaen.

Toimijalla tulisi olla pääsynhallintaan liittyvät määrittelyt ja käytännöt, joilla varmistetaan kattavasti luotettava tunnistaminen ja joilla sallitaan pääsy vain tarvittaviin viestintäverkkoihin ja tietojärjestelmiin, suojattaviin tietoihin sekä muihin resursseihin. Toimijalla tulisi olla menettelyt käyttäjätunnusten ja käyttöoikeuksien koko elinkaaren ajalle ja käyttöoikeuksia olisi hallittava niiden mukaisesti. Käyttöoikeuksia ja niiden käyttöä tulisi valvoa. Käyttöoikeuksista ja käyttöoikeusrooleista olisi pidettävä ajantasaista kirjaa ja käyttäjille on annettava vain ne oikeudet, jotka ovat työtehtävien suorittamisen vuoksi välttämättömiä (vähimpien oikeuksien periaate). Toimijoilla tulisi olla menettelyt vahvojen oikeuksien käyttäjätilien ja pääkäyttäjätilien hallintaan. Pääkäyttäjäoikeudet tulisi rajoittaa mahdollisimman pienelle käyttäjäjoukolle ja näitä tunnuksia on suojattava vahvoin menetelmin. Pääkäyttäjäoikeuksien käyttöä tulisi valvoa.

Valittavien todentamiskäytäntöjen ja -tekniikoiden tulisi perustua tietojen saatavuutta koskeviin vaatimuksiin ja todentamisen menettelyihin. Todennusmenetelmien olisi oltava riittävän turvallisia niin, että oikeudeton käyttö on mahdollisuuksien mukaan estetty. Tarvittaessa todennusmenetelmänä tulisi käyttää vahvaa tunnistusta, monivaiheista todentamista (MFA) tai jatkuvaa todentamista, mikäli niiden käyttö on mahdollista.

Kohdassa 8 tarkoitettaisiin salausmenetelmien käyttämistä koskevia toimintaperiaatteita ja menettelyitä. Kohdalla pantaisiin täytäntöön NIS2-direktiivin 21 artiklan 2 kohdan h alakohta ja j alakohta osittain. Salausmenetelmillä tarkoitetaan kryptografisia menetelmiä, joilla tieto muutetaan sellaiseen muotoon, ettei ulkopuolinen voi saada sen sisältöä selville. Toimijan olisi luotava kryptografian käyttöön liittyvät toimintaperiaatteet ja menettelyt, joilla suojataan tarvittaessa tiedon luottamuksellisuutta, aitoutta ja eheyttä. Tiedon salaaminen voi olla tarpeen esimerkiksi silloin, jos sitä siirretään avoimessa tietoverkossa tai säilötään ilman riittävää fyysistä suojaa. Tällöin on valittava salaustekniikka, joka on suojaukseltaan riittävä salattavan tiedon laatuun, salausluokitukseen, suojausaikaan ja suorituskykyvaatimuksiin nähden. Salaustekniikan osalta olisi huomioitava algoritmien, käyttötapojen ja avainvahvuuksien lisäksi myös avaimen saatavuus sekä turvallinen säilytys, luonti ja hallinta. Käytetyn salausmenetelmän vaatimusten tulisi olla ajantasaisia koko järjestelmän elinkaaren ajan, jolloin esimerkiksi salausalgoritmin tulisi olla vaihdettavissa (kryptoketteryys).

Kohdassa 9 tarkoitettaisiin poikkeamien havainnointia ja käsittelyä turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi. Alakohdalla pantaisiin täytäntöön NIS2-direktiivin 21 artiklan 2 kohdan b alakohta. Poikkeamalla tarkoitettaisiin 2 §:n määritelmän mukaisesti tapahtumaa, joka vaarantaa viestintäverkossa ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden. Poikkeaman käsittelyllä tarkoitettaisiin NIS2-direktiivin artiklan 6 kohdan 1 alakohdan 8 mukaisesti mitä tahansa toimia ja menettelyjä, joilla pyritään ehkäisemään ja havaitsemaan poikkeama, analysoimaan, rajoittamaan tai hallitsemaan sitä ja palautumaan siitä. Turvallisuuden palauttamisella tarkoitetaan järjestelmän palauttamista turvalliseen tilaan erityistilanteen tai häiriötilan jälkeen. Toimintavarmuuden ylläpitämisellä tarkoitetaan menettelyjä, joilla parannetaan järjestelmän toimintavarmuutta sekä kykyä toimia erityistilanteessa ja toipua häiriötilasta. Poikkeamien käsittelyä varten toimijalla tulisi olla ennalta dokumentoidut menettelyt, roolit ja vastuut poikkeamien ehkäisemistä, havainnoimista, analysointia, hallitsemista ja palautumista sekä raportointia varten. Poikkeamien havainnointia varten toimijalla tulisi olla raportointikanavat sisäisille ja ulkoisille toimijoille. Toimijalla tulisi olla työkaluja ja prosesseja tapahtumien kirjaamiseen ja havainnointiin.

Havainnointi- ja analysointikyvyn kannalta on välttämätöntä, että toimijalla on kerättynä ja käytettävissä riittävät lokitiedot esimerkiksi ylläpidosta, muutoksista, käytöstä ja virheistä. Toimijan tulisi arvioida tapahtumat sen selvittämiseksi, aiheuttavatko ne poikkeaman. Toimijalla tulisi olla käytännöt, joilla poikkeaman vakavuus ja vaikutukset voitaisiin arvioida ja tarvittaessa luokitella. Poikkeaman käsittelyssä tulisi olla käytännöt myös niihin reagoimiseksi, sekä tarvittaessa poikkeaman rajoittamiseksi, selvittämiseksi ja vaikutusten poistamiseksi. Poikkeaman jälkeen tulisi arvioida poikkeamaan johtaneet syyt ja oppia sen kokemuksista, jotta vastaavan poikkeaman uhkaan voidaan varautua jatkossa paremmin. Vakaviin ja muihin toimijoihin ulottuviin poikkeamiin tulisi olla olemassa menettelyt, vastuut ja kommunikointikanavat muiden toimijoiden varoittamiseksi. Poikkeamien käsittelyn tulisi sisältää myös menettelyt tiedon jakamiseen niin, ettei se vaaranna toimijaa tai muuta organisaatiota. Poikkeamien käsittelyn menettelyjä tulisi ylläpitää ja kehittää koko elinkaaren ajan, ja niitä tulisi päivittää esimerkiksi kokemusten perusteella.

Kohdassa 10 tarkoitettaisiin varmuuskopiointia, palautumissuunnittelua, kriisinhallintaa ja muuta toimivuuden jatkuvuuden hallintaa ja tarvittaessa suojattujen varaviestintäjärjestelmien käyttöä toimijan toiminnassa. Kohdalla pantaisiin täytäntöön NIS2-direktiivin 21 artiklan 2 kohdan c alakohta ja alakohta j osittain. Varmuuskopioinnilla tarkoitetaan tiedon kopiointia turvalliseen paikkaan. Palautumissuunnittelulla tarkoitetaan prosesseja ja menetelmiä, joilla järjestelmä saadaan takaisin toimintakuntoon esimerkiksi varajärjestelyin tai varmuuskopioista. Toiminnan jatkuvuuden hallinnalla tarkoitetaan prosesseja ja menettelyjä, joilla organisaatio varautuu hallitsemaan häiriötilanteet ja jatkamaan toimintaa ennalta määritellyllä hyväksyttävällä tasolla. Suojatuilla varaviestintäjärjestelmillä tarkoitetaan viestintäkanavia, jotka eivät ole riippuvaisia muusta järjestelmästä ja joissa on riittävä toimintavarmuus sekä luottamuksellisuus.

Toimijalla tulisi olla dokumentoidut menettelyt toiminnan jatkuvuuden ja häiriötilanteista palautumisen osalta. Jatkuvuus olisi varmistettava ja sen voisi tehdä esimerkiksi riskienhallinnan perusteella luodulla jatkuvuussuunnitelmalla sekä toipumissuunnitelmalla. Suunnitelmat voisivat sisältää esimerkiksi olosuhteet, joissa niiden käyttö aktivoidaan sekä tarvittavia rooleja, resursseja, toimenpiteitä ja viestintäkanavia koskevat suunnitelmat sekä tarvittavat suojatut varaviestintäjärjestelmät. Suunnitelmien tulisi sisältää vähintään kriisinhallintamenettelyt erittäin vakavien poikkeamien varalta. Muun riskienhallinnan mukaisesti suunnitelmia tulisi ylläpitää ja kehittää säännöllisesti sekä niiden mukaista toimintaa harjoitella.

Varmuuskopioinnin osalta toimijan olisi määritettävä esimerkiksi se, miltä osin varmuuskopioita on otettava ja järjestelmistä sekä varajärjestelmistä. Toimija voisi määrittää käytäntöjä varmuuskopioinnin tiheydestä, varmuuskopioiden säilytysajasta, varmuuskopioiden suojauksesta ja palautuksen testaamisesta tilanteessa, jossa alkuperäinen järjestelmä ei olisi käytettävissä.

Tarve suojattujen varaviestintäjärjestelmien käytölle voisi perustua esimerkiksi siihen, että riskiarviossa on todettu välttämättömäksi varmistaa viestintäkanavat myös silloin, kun tavanomaisesti käytössä olevat järjestelmät (esim. puhelin, sähköposti, pikaviestimet) eivät ole käytettävissä. Tällöin olisi määriteltävä käytettävät varaviestintäjärjestelmät ja niiden tarve sekä tapa käyttöönotolle.

Kohdassa 11 tarkoitettaisiin perustason kyberhygieniakäytäntöjä toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi. Kohdalla pantaisiin täytäntöön NIS2-direktiivin 21 artiklan 2 kohdan g alakohta osittain. Toimijan tulisi suojata viestintäverkkonsa ja tietojärjestelmänsä perustason kyberhygieniakäytännöin. Toimijan tulisi varmistaa, että perustason kyberhygieniakäytännöt on toteutettu ja että työntekijät noudattavat niitä. Näiden käytäntöjen taso tulisi mitoittaa riittäväksi perustuen toimintojen kriittisyyteen. Valittujen toimenpiteiden tulisi perustua yleisiin hyviin käytäntöihin sekä riskienarviointiin.

Kyberhygieniakäytännöillä tarkoitetaan yleisiä hyviä tietoturvatoimenpiteitä, joilla varmistetaan järjestelmien, ohjelmien ja palveluiden turvallisen käytön perustaso. Kyberhygieniakäytännöillä tarkoitettaisiin perustason teknisiä ja muita toimenpiteitä kohdassa kuvattujen kohteiden turvallisuuden varmistamiseksi. Kyberhygieniakäytännöt voisivat sisältää muun muassa viestintäverkon rakenteellista turvallisuutta, haitallisen liikenteen havainnointia ja estämistä, toimintojen jäljitettävyyttä ja monitorointia, laitteiden ja ohjelmistojen turvallista konfigurointia, ohjelmistojen päivityksiä, kattavaa ja luotettavaa tunnistamista sekä käyttäjien osaamisen parantamista ja tietoisuuden lisäämistä. Perustason kyberhygieniakäytäntöihin voidaan lukea esimerkiksi luottamattomuuden periaate (zero-trust), ajantasaiset ohjelmistopäivitykset, laitteiden ja ohjelmistojen turvallinen konfigurointi, verkon segmentointi, identiteetin- ja pääsynhallinta sekä käyttäjien osaamisen parantaminen ja tarvittaessa viestintäverkkojen ja tietojärjestelmien turvallisuutta parantavien teknologioiden käyttöönotto tarpeellisilta osin. Kohta olisi osin

päällekkäinen muiden kohtien edellyttämien seikkojen kanssa, mutta selkeyden ja merkityksen vuoksi kuvattaisiin myös erillisenä.

Kohdassa 12 tarkoitettaisiin toimenpiteitä viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön ja tilaturvallisuuden sekä välttämättömien resurssien varmistamiseksi. Kohdalla pantaisiin täytäntöön NIS2-direktiivin 21 artiklan 2 kohdan johtolause viestintäverkkojen ja tietojärjestelmien fyysistä ympäristöä suojaavien toimenpiteiden osalta. NIS2-direktiivin johdantokappaleen 79 mukaan näiden toimenpiteiden olisi oltava CER-direktiivin mukaisia. CER-direktiivin artikla 13 koskee kriittisten toimijoiden toimenpiteitä häiriönsietokyvyn varmistamiseksi. Artiklassa säädetään muun muassa tilojen fyysisestä suojauksesta kuten aidoista, esteistä, ilmaisulaitteista, kulunvalvonnasta, hälytyskäytännöistä sekä poikkeamista palautumiseksi vaihtoehtoisten toimitusketjujen kartoittamisesta.

Fyysisellä turvallisuudella tarkoitetaan fyysisten ja teknisten turvatoimien toteuttamisesta siten, että järjestelmiä, tiloja, verkkoja ja muita resursseja suojataan luvattomalta pääsyltä sekä muilta vahingoilta ja häiriöiltä. Välttämättömillä resursseilla tarkoitetaan tunnistettuja toiminnan kannalta kriittisiä tukitoimintoja, -palveluita ja -järjestelmiä, joiden saatavuus olisi varmistettava. Toimijan tulisi tunnistaa fyysisen ympäristön tekijät, joiden turvallisuus on viestintäverkkojen ja tietojärjestelmien toiminnan kannalta tärkeää ja suojata näitä toimintaan vaikuttavien uhkien vaikutukselta ja häiriöiltä. Toimijan tulisi huomioida myös viestintäverkkoihin ja tietojärjestelmiin vaikuttavat fyysiset ympäristöt, jotka voivat olla hyvin erilaisia ja esimerkiksi maantieteellisesti laajoja tai suppeita. Fyysisiä uhkia ovat ympäristötekijät ja pahantahtoiset toimijat. Viestintäverkkoja ja tietojärjestelmiä tulisi valvoa ja niitä tulisi suojata luvattomalta fyysiseltä pääsyltä, vahingoilta ja häiriöiltä. Lisäksi on suojauduttava luonnollisilta ja yhteiskunnallisilta tapahtumilta, kuten tulipaloilta, tulvilta ja levottomuuksilta. Toimijan tulisi varautua välttämättömien resurssien, kuten sähkönjakelun, tietoliikenneyhteyksien ja jäähdytyksen häiriöihin ja estää viestintäverkkojen ja tietojärjestelmien tuhoutuminen, vahingoittuminen tai toimijan kriittisten toimintojen keskeytyminen välttämättömien resurssien puutteen tai häiriön vuoksi.

Ehdotetussa *3 momentissa* säädettäisiin toimijalta edellytettyjen toimenpiteiden suhteellisuuden tasosta. Kyberturvallisuuden riskienhallinnan toimenpiteiden olisi oltava oikeassa suhteessa riskiin, eli haitallisten vaikutusten toteutumisen todennäköisyydelle ja seurauksille, joita riskin toteutumisesta olisi. Momentissa säädettäisiin perusteista, joiden mukaisesti toimija voi suhteuttaa riskienhallintatoimenpiteidensä oikean tason.

Toimenpiteet tulisi suhteuttaa toiminnan laatuun ja laajuuteen, sillä toiminnan laatu ja laajuus ovat välittömässä yhteydessä sekä toimijan resursseihin torjua kyberuhkia että toimijan tarjoamien palveluiden merkitykseen yhteiskunnan toimintojen kannalta. Toimenpiteet tulisi suhteuttaa niihin kohtuudella ennakoitavissa oleviin välittömiin vaikutuksiin, joita ennakoidusta uhkasta voisi aiheutua sen toteutuessa. Vaikutuksia tulisi arvioida erityisesti yhteiskunnalle merkityksellisten toimintojen näkökulmasta, ja mitä merkittävämpiä vaikutuksia uhkan toteutumisella voitaisiin arvioida olevan yhteiskunnan tai talouden näkökulmasta, sitä merkittävämpiä hallintatoimenpiteitä olisi tarpeen toteuttaa. Vaikutuksia tulisi siten arvioida toimijan itsensä ohella myös niille, jotka käyttävät tai ovat riippuvaisia toimijan palveluista. Toimenpiteet tulisi suhteuttaa myös toimijan viestintäverkkojen ja tietojärjestelmien riskialttiuteen. Tiettyihin teknisiin ratkaisuihin voi liittyä tunnettuja tietoturvauhkia ja lisäksi toimijan toiminnan luonne, laatu tai toimijan rooli vaikuttaa siihen, kuinka houkuttelevaa toiminta on pahantahtoiselle toimijalle toiminnan kohteeksi valikoitumiselle. Toimenpiteet tulisi suhteuttaa myös poikkeaman syntymisen todennäköisyyteen ja sen toteutumisen vakavuuteen, mikä liittyy kokonaisarvioon uhkan laadusta ja luonteesta ja riskin määritelmään. Lisäksi toimenpiteet tulisi suhteuttaa viimeaikainen kehitys huomioon ottaen ajantasaisiin käytettävissä oleviin teknisiin mahdollisuuk-

siin torjua tunnistettuja uhkia. Viimeaikaisella kehityksellä viitattaisiin erityisesti tekniseen kehitykseen teknisten hallintatoimenpiteiden ja riskienhallintakeinojen kehitykseen sekä tunnettujen riskienhallintakeinojen kehitykseen esimerkiksi tunnettujen uhkatyyppien, uhkatoimijoiden, hyökkäystapojen ja uusien teknologioiden osalta.

Pykälän *4 momentin* nojalla valvova viranomainen voisi antaa tarkempia teknisiä määräyksiä siinä esitetyistä seikoista valvontatoimialallaan. Viranomaisen määräyksenantovaltuus koskisi 2 momentissa tarkoitettujen velvoitteiden tarkentamista ja täsmentämistä. Tarkemmat määräykset voisivat kuitenkin koskea vain teknisiä seikkoja, eli niillä ei saisi laajentaa 9 §:ssä säädettyjä velvoitteita. Määräysten olisi oltava teknologianeutraaleja. NIS2-direktiivissä on annettu komissiolle toimivalta antaa täytäntöönpanosäädöksiä, joissa vahvistetaan toimenpiteiden tekniset ja menetelmiin liittyvät vaatimukset sekä tarvittaessa alakohtaiset vaatimukset. Komission täytäntöönpanosäädöksiä sovellettaisiin ensisijaisesti suhteessa valvovan viranomaisen määräyksiin. Siltä osin kuin komissio on käyttänyt sille annettua toimivaltaa ja antanut NIS2-direktiiviä tarkentavia täytäntöönpanosäädöksiä, olisi valvovien viranomaisten huomioitava ne määräysvalmistelussa ja huolehdittava antamiensa määräysten yhteensovittamisesta komission täytäntöönpanosäädösten kanssa.

Pykälän *5 momentin* nojalla riskienhallinnan toimintamallissa ja hallintatoimenpiteissä on noudatettava lisäksi NIS2-direktiivin 21 artiklan 5 kohdan nojalla annettavia Euroopan komission täytäntöönpanosäädöksiä. Sektorikohtaisia yksityiskohtaisempia NIS2-direktiivin nojalla säädettyjä vaatimuksia voisivat olla esimerkiksi NIS2-direktiivin 21 artiklan 5 kohdan ensimmäisen alakohdan nojalla Euroopan komission hyväksymät täytäntöönpanosäädökset teknisiin ja menetelmiin liittyvistä vaatimuksista, jotka koskevat DNS-palveluntarjoajia, aluetunnusrekistereitä, pilvipalvelujen tarjoajia, datakeskuspalvelujen tarjoajia, sisällönjakeluverkkojen tarjoajia, hallintapalvelun tarjoajia, tietoturvapalveluntarjoajia, verkossa toimivien markkinapaikkojen tarjoajia, verkossa toimivien hakukoneiden tarjoajia, verkkoyhteisöalustojen tarjoajia ja luottamuspalvelun tarjoajia. Lisäksi sektorikohtaisempia yksityiskohtaisempia NIS2-direktiivin nojalla säädettyjä vaatimuksia voisivat olla saman artiklan 5 kohdan toisen alakohdan nojalla Euroopan komission hyväksymät täytäntöönpanosäädökset, joilla vahvistetaan riskienhallintatoimenpiteiden tekniset ja menetelmiin liittyvät vaatimukset sekä tarvittaessa alakohtaiset vaatimukset, jotka koskevat muita kuin edellä tarkoitettuja toimijoita.

10 §. *Johdon vastuu*. Toimijan ylin johto olisi vastuussa viestintäverkkojen ja tietojärjestelmien kyberturvallisuutta koskevan riskienhallinnan toteuttamisesta ja valvonnasta toimijassa. Vastuu tarkoittaisi viimesijaista vastuuta järjestää ja resursoida riskienhallinta asianmukaisesti, sekä valvoa sen toimintaa. Toimijan johto hyväksyisi kyberturvallisuuden riskienhallinnan toimintamallin sekä valvoisi riskienhallinnan toteuttamista, resursointia, toimenpiteitä, riskiarvioiden ajantasaisuutta ja toimenpiteiden vaikuttavuutta. Toimijan johdolla tulisi niin ikään olla riittävä ja ajantasainen perehtyneisyys kyberturvallisuuden riskienhallintaan, mikä edellyttäisi perehtyneisyyden hankkimista joko kouluttautumalla tai muulla vastaavalla tavalla säännöllisin väliajoin. Osana 9 §:ssä tarkoitettuja hallintatoimenpiteitä johto huolehtii myös henkilöstön kyberturvallisuuskoulutuksen järjestämisestä.

Johdolla tarkoitettaisiin toimijan hallitusta, hallintoneuvostoa, toimitusjohtajaa tai muussa niihin rinnastettavassa asemassa olevaa, joka tosiasiallisesti johtaa toimijan toimintaa. Tällaisessa asemassa voisi olla esimerkiksi avoimen yhtiön yhtiömies, kommandiittiyhtiön vastuunalainen yhtiömies, eurooppalaisen taloudellisen etuyhtymän henkilöjäsen tai yksityinen elinkeinonharjoittaja. Johdolla tarkoitettaisiin myös toimitusjohtajan välittömään alaisuuteen kuuluvaa tahoa, jos se hoitaa toimijan ylimpiä johtotehtäviä, joissa tosiasiallisesti johdetaan sen toimintaa.

Ehdotuksella pantaisiin täytäntöön NIS2-direktiivin 20 artiklan 1 ja 2 kohdat.

11 §. *Poikkeamailmoitukset viranomaiselle*. Pykälässä säädettäisiin toimijoiden velvollisuudesta ilmoittaa merkittävästä poikkeamasta valvovalle viranomaiselle. Ehdotetuilla 11 – 13 §:llä pantaisiin täytäntöön NIS2-direktiivin 23 artiklan 1–4 kohdat. Ilmoitusvelvollisuus koskisi vain merkittäviä poikkeamia.

Merkittävällä poikkeamalla tarkoitettaisiin poikkeamaa, joka on aiheuttanut tai voi aiheuttaa palvelujen vakavan toimintahäiriön tai asianomaiselle toimijalle taloudellisia tappioita taikka jos poikkeama on vaikuttanut tai voisi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa. Mikäli toimija havaitsee merkittävän poikkeaman jonkun muun, esimerkiksi välittömän alihankkijan toiminnassa, olisi toimijan ilmoitettava tällaisesta poikkeamasta silloin, jos kyseinen poikkeama on aiheuttanut tai voi aiheuttaa vakavan toimintahäiriön toimijan omissa palveluissa taikka jos se on aiheuttanut tai voi aiheuttaa huomattavaa aineellista tai aineetonta vahinkoa toimijalle. Toimijan alustavassa arvioinnissa poikkeaman merkittävyydestä olisi otettava huomioon ainakin viestintäverkot ja tietojärjestelmät, joihin poikkeama vaikuttaa, ja erityisesti niiden merkitys toimijan palvelujen tarjoamisessa, kyberuhkan vakavuus ja tekniset ominaisuudet sekä mahdolliset taustalla olevat haavoittuvuudet, joita käytetään hyväksi, sekä toimijan kokemukset samanlaisista poikkeamista. Indikaattorit, kuten palvelun häiriintymisen laajuus, poikkeaman kesto tai niiden palvelun vastaanottajien lukumäärä, joihin poikkeama vaikuttaa, voivat olla tärkeitä määritettäessä, onko palvelun toimintahäiriö vakava.

Ilmoitusvelvollisuus olisi kolmivaiheinen, eli toimijan olisi toimitettava valvovalle viranomaiselle 24 tunnin kuluessa poikkeaman havaitsemisesta ensi-ilmoitus ja 72 tunnin kuluessa poikkeaman havaitsemisesta jatkoilmoitus. Poikkeamatilanteen päätyttyä toimijan olisi toimitettava valvovalle viranomaiselle vielä 13 §:ssä tarkoitettu loppuraportti. Kolmivaiheisen ilmoitusvelvollisuuden tavoitteena on toisaalta varmistaa poikkeamien nopea ilmoittaminen ja ajantasaisen tilannekuvan muodostaminen ja toisaalta mahdollistaa toimijan resurssien suuntaaminen ensisijaisesti poikkeamien käsittelyyn liittyviin toimintoihin. Toimija voisi tehdä ensi- ja jatkoilmoitukset myös kerralla, mikäli sillä olisi ensi-ilmoituksen määräajassa, eli viipymättä ja viimeistään 24 tunnin kuluessa poikkeaman havaitsemista saatavilla molempien ilmoitusten edellyttämät tiedot.

Ensi-ilmoitus olisi tehtävä viipymättä ja viimeistään 24 tunnin kuluessa siitä, kun toimija on havainnut poikkeaman. Ensi-ilmoituksen vähimmäissisältö koostuisi merkittävän poikkeaman havaitsemisesta, alustavasta arviosta siitä, epäilläänkö merkittävän poikkeaman johtuvan rikoksesta tai muusta lainvastaisesta tai vihamielisestä teosta, sekä alustavasta arviosta siitä, voiko havaitulla merkittävällä poikkeamalla olla vaikutuksia muihin EU-jäsenvaltioihin sekä tällaisten rajat ylittävien vaikutusten todennäköisyys. Ensi-ilmoituksessa olisi lisäksi ilmoitettava muut mahdolliset tiedot, joiden avulla toimivaltainen viranomainen voi määrittää poikkeaman mahdolliset rajatylittävät vaikutukset.

Jatkoilmoitus olisi tehtävä viipymättä ja viimeistään 72 tunnin kuluessa poikkeaman havaitsemisesta. Jatkoilmoituksessa toimijan olisi esitettävä alustava arvio merkittävästä poikkeamasta, sen vakavuudesta ja vaikutuksista sekä vaarantumista kuvaavat indikaattorit (Indicator of Compromise) eli IoC-tieto, jos sellaisia on saatavilla. Lisäksi toimijan olisi päivitettävä ensi-ilmoituksessa annetut tiedot, mikäli niihin on tullut muutoksia tai tarkennuksia.

Pykälän *5 momentin* nojalla valvova viranomainen voisi tarvittaessa antaa omalla toimialallaan tarkentavia määräyksiä siitä, milloin 1 momentissa tarkoitettu poikkeama on merkittävä, loppuraportissa ilmoitettavista tiedoista sekä merkittävien poikkeamien ja 12-13 §:ssä tarkoitettujen tietojen ilmoittamismenettelystä. NIS2-direktiivissä on annettu komissiolle toimivalta antaa

täytäntöönpanosäädöksiä, joissa täsmennetään poikkeamailmoitusten tietosisältö, muoto ja ilmoitusmenettely sekä tapaukset, joissa poikkeama katsotaan merkittäväksi. Komission täytäntöönpanosäädöksiä sovellettaisiin ensisijaisesti suhteessa valvovan viranomaisen määräyksiin. Siltä osin kuin komissio on käyttänyt sille annettua toimivaltaa ja antanut NIS2-direktiiviä tarkentavia täytäntöönpanosäädöksiä, olisi valvovien viranomaisten huomioitava ne määräysvalmistelussa ja huolehdittava antamiensa määräysten yhteensovittamisesta komission täytäntöönpanosäädösten kanssa.

Pykälän *6 momentin nojalla* luottamuspalvelun tarjoajien olisi tehtävä myös jatkoilmoitus viimeistään 24 tunnin kuluessa merkittävän poikkeaman havaitsemisesta 2 momentissa säädetystä määräajasta poiketen.

12 §. *Poikkeaman väliraportti*. Pykälässä säädettäisiin toimijan velvollisuudesta antaa valvovalle viranomaiselle lisätietoja tai väliraportti poikkeaman tilannepäivityksistä. Ensi- ja jatkoilmoituksen lisäksi toimijan olisi annettava valvovan viranomaisen pyynnöstä lisätietoja tai väliraportti asian tilannepäivityksistä ja käsittelyn edistymisestä. Jos poikkeama on pitkäkestoinen, eli poikkeaman käsitteleminen ei ole päättynyt alle kuukauden kuluessa jatkoilmoituksen toimittamisesta, milloin muusta kuin pitkäkestoisesta poikkeamasta olisi toimitettava loppuraportti, toimijan olisi annettava valvovalle viranomaiselle oma-aloitteisesti väliraportti poikkeaman käsittelyn etenemisestä. Väliraportti olisi annettava oma-aloitteisesti viimeistään kuukauden kuluessa jatkoilmoituksesta. Väliraportin tarkoituksena olisi kuvata poikkeaman käsittelyn etenemistä, poikkeaman vaikutuksia ja muita asian vaikutukseen liittyviä olennaisia tekijöitä sekä muutoksia ensi- ja jatkoilmoituksen tietoihin. Toimijan olisi valvovan viranomaisen pyynnöstä annettava lisätietoja poikkeamasta ja sen käsittelystä tai uusi väliraportti poikkeaman tilannepäivityksistä ja käsittelyn etenemisestä.

13 §. *Poikkeaman loppuraportti*. Pykälän *1 momentin* nojalla toimijan olisi annettava valvovalle viranomaiselle loppuraportti, kun poikkeaman käsittely on päättynyt. Loppuraportti olisi annettava viimeistään kuukauden kuluttua siitä, kun jatkoilmoitus on toimitettu. Jos kyse on pitkäkestoisesta poikkeamasta, jonka käsittely on kestänyt yli kuukauden jatkoilmoituksen toimittamisesta, olisi toimijan annettava loppuraportin sijaan 12 §:ssä tarkoitettu väliraportti asian tilannepäivityksistä ja käsittelyn etenemisestä. Tällöin loppuraportti olisi toimitettava viimeistään kuukauden kuluessa poikkeaman käsittelyn päättymisestä.

Pykälän *2 momentissa* säädettäisiin loppuraportin vähimmäissisällöstä. Loppuraportin tarkoituksena olisi selvittää toimijalle itselleen sekä valvovalle viranomaiselle poikkeaman todennäköisesti aiheuttanut uhka tai syy, kuvaus poikkeaman laadusta, vakavuudesta ja vaikutuksista sekä toimenpiteet, joilla poikkeaman haitallisia vaikutuksia lievennettiin tai pyrittiin lieventämään. Lisäksi loppuraportissa tulisi kuvata merkittävän poikkeaman rajat ylittävät vaikutukset, mikäli poikkeamasta niitä aiheutui. Loppuraportoinnin tavoitteena olisi selventää toimijalle sen kokemukset ja havainnot poikkeaman syistä, vaikutuksista ja käsittelystä sekä siten parantaa poikkeamien jälkiarvioinnin kautta sekä poikkeaman kohteena olleen toimijan että muiden toimijoiden sietoisuutta kyberhäiriöille ja –hyökkäyksille tulevaisuudessa. Loppuraportin tarkoituksena olisi tarjota keino poikkeaman syiden, seurausten ja hyvien oppien saamiselle siten, että vastaavia merkittäviä poikkeamia voidaan jatkossa ennaltaehkäistä vastaisuuden varalle. Loppuraportin tarkoituksena ei olisi kohdistaa seuraamuksia tai muita sanktioita toimijalle.

14 §. *Poikkeamasta ja kyberuhasta ilmoittaminen muulle kuin viranomaiselle*. Toimijoiden olisi *1 momentin* mukaan ilmoitettava viipymättä merkittävästä poikkeamasta myös niille palvelujensa vastaanottajille, joihin merkittävä poikkeama todennäköisesti vaikuttaa. Lisäksi toimijoiden olisi *2 momentin* mukaisesti ilmoitettava viipymättä palvelujensa vastaanottajille sellaisesta

merkittävästä kyberuhkasta, joka saattaa vaikuttaa niihin. Toimijan olisi ilmoitettava palvelujensa vastaanottajille kyberuhkan olemassaolosta sekä kaikista toimenpiteistä tai korjaavista toimista, joita palvelun vastaanottajat voivat toteuttaa uhkan hallitsemiseksi tai lieventääkseen siitä johtuvia riskejä. Ehdotetussa 2 momentissa tarkoitettu ilmoittaminen ei kuitenkaan vaikuttaisi toimijan velvollisuuteen toteuttaa asianmukaisia ja välittömiä toimenpiteitä uhkien ehkäisemiseksi tai korjaamiseksi ja palvelun normaalin turvallisuustason palauttamiseksi. Merkittäviä kyberuhkia koskevat tiedot olisi annettava palvelun vastaanottajille maksutta, ja ne olisi ilmaistava helppotajuisesti.

Merkittävällä kyberuhkalla tarkoitettaisiin 2 §:n 10 kohdassa määriteltyä kyberuhkaa, jonka voidaan sen teknisten ominaisuuksien perusteella olettaa vaikuttavan mahdollisesti vakavasti toimijan viestintäverkkoihin ja tietojärjestelmiin tai toimijan palvelujen käyttäjiin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa.

Jos poikkeamasta ilmoittaminen yleisölle on yleisen edun mukaista, valvova viranomainen voisi velvoittaa toimijan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.

Ehdotetulla säännöksellä pannaan täytäntöön NIS2-direktiivin 23 artiklan kohdat 1, 2 ja 7.

15 §. *Vapaaehtoinen ilmoittaminen.* Pykälässä säädettäisiin mahdollisuudesta tehdä vapaaehtoinen ilmoitus muista kuin merkittävistä poikkeamista, kyberuhkista ja läheltä piti –tilanteista. Lain soveltamisalaan kuuluvia toimijoita kannustetaan tekemään vapaaehtoisia ilmoituksia kyberuhkista, jotta kyberuhkien toteutuminen poikkeamina voitaisiin estää. Kyberturvallisuuden edistämiseksi on kuitenkin tärkeää, että myös sellaiset toimijat tai yksityishenkilöt, jotka eivät kuulu tämän lain soveltamisalaan ilmoittaisivat vapaaehtoisesti poikkeamista, kyberuhkista ja läheltä piti -tilanteista.

Toimijoille asetettavan ilmoitusvelvollisuuden tarkoituksena ei olisi estää vapaaehtoista ilmoittamista. Vapaaehtoisia ilmoituksia voisi tehdä muutenkin kuin ehdotuksessa säädetyllä tavalla tai ehdotuksessa säädetyistä asioita. NIS2-direktiivin täytäntöön panemiseksi olisi kuitenkin tarpeen ottaa lain tasolle säännös eräistä vapaaehtoisista ilmoituksista, joita valvovan viranomaisen on vähintään otettava vastaan ja joihin valvovan viranomaisen on reagoitava samalla tavalla kuten ilmoitukseen, jonka tekemiseen tässä laissa tarkoitetulla toimijalla on velvollisuus.

Pykälässä säädettäisiin myös valvovan viranomaisen velvollisuudesta ottaa yleisesti vastaan toimialallaan vapaaehtoisia poikkeamailmoituksia merkittävistä poikkeamista, kyberuhkista ja läheltä piti –tilanteista. Vapaaehtoisia ilmoituksia olisi otettava vastaan myös muilta kuin sellaisilta toimijoilta, joihin sovelletaan NIS2-direktiivissä tarkoitettuja riskienhallinta- ja raportointivelvoitteita. Valvovan viranomaisen tulisi käsitellä vapaaehtoisia poikkeamailmoituksia noudattaen 16-17 §:n mukaista menettelyä. Valvova viranomainen voisi asettaa pakollisten ilmoitusten käsittelyn etusijalle vapaaehtoisten ilmoitusten käsittelyyn nähden.

Säännöksen tarkoituksena ei olisi rajata vapaaehtoista ilmoittamista vain säännöksen mukaisiin tilanteisiin tai säännöksen mukaiseen menettelyyn. Kysymys olisi NIS2-direktiivin täytäntöönpanemiseksi vähimmäissäännöksestä, jossa määriteltäisiin valvovan viranomaisen velvollisuus ottaa vastaan vähintään kuvattuja ilmoituksia. Vapaaehtoisia ilmoituksia kyberhäiriöistä, -uhkista, läheltä piti –tilanteista ja muista kyberturvallisuuden ylläpitämiseksi olennaisista havainnoista voitaisiin tehdä viranomaiselle jatkossa myös muuten kuin säännöksessä kuvatulla tavalla.

Toimijoihin, jotka vapaaehtoisesti ilmoittavat merkittävistä poikkeamista, kyberuhkista ja läheltä piti –tilanteista, ja joihin ei sovelleta tämän lain mukaisia riskienhallinta- ja raportointivelvoitteita, ei sovelleta vapaaehtoisen ilmoituksen johdosta tätä lakia muilta osin.

Valvovan viranomaisen olisi toimitettava 18 §:ssä tarkoitetulle keskitetylle yhteyspisteelle tieto myös vapaaehtoisuuteen perustuvista ilmoituksista, jotka sille on toimitettu.

Ehdotetulla säännöksellä pannaan osittain täytäntöön NIS2-direktiivin 30 artikla.

16 §. *Poikkeamailmoituksen vastaanottaminen.* Pykälän *1 momentissa* säädettäisiin valvovan viranomaisen velvollisuudesta vastata poikkeamailmoituksiin. Vastaamisvelvoite koskisi sekä 11 §:ssä tarkoitettuja poikkeamailmoituksia että 15 §:ssä tarkoitettuja vapaaehtoisia ilmoituksia.

Valvovan viranomaisen olisi vastattava poikkeamailmoituksen tehneelle taholle viivytyksettä saatuaan siltä 11 tai 15 §:ssä tarkoitettu poikkeamailmoitus. Vastaus tulisi antaa viivytyksettä ja mahdollisuuksien mukaan 24 tunnin kuluessa, mutta kuitenkin virka-aikojen puitteissa. Valvovalta viranomaiselta ei siten edellytettäisi esimerkiksi valmiutta päivystää viikonloppuisin, öisin tai arkipyhinä. Vastaukseen tulee sisällyttää alustava palaute merkittävästä poikkeamasta sekä ohjeet merkittävän poikkeaman ilmoittamisesta esitutkintaviranomaiselle, jos asiassa epäillään rikosta. Alustavalla palautteella tarkoitettaisiin valvovan viranomaisen näkemystä poikkeaman merkittävyydestä sekä muista poikkeaman hallitsemiseksi tarpeellisista seikoista. Valvova viranomainen voisi sisällyttää vastaukseen myös muita tarpeelliseksi katsomiaan seikkoja, kuten yleisiä ohjeita tai neuvoja vaikutuksia lieventävistä toimenpiteistä.

Pykälän *2 momentin* nojalla valvova viranomainen voisi asettaa pakollisiin ilmoituksiin vastaamisen ja niiden 17 §:n mukaisen käsittelyn etusijalle vapaaehtoisten ilmoitusten käsittelyyn nähden. Ilmoituksien käsittelyn järjestäminen tärkeysjärjestykseen olisi oltava mahdollista esimerkiksi tilanteessa, jossa vapaaehtoisia ilmoituksia tulisi niin merkittävä määrä käytettävissä oleviin resursseihin nähden, että ilmoitusvelvollisuuden alaan kuuluvien ilmoituksien käsittely viivästyisi tai vaarantuisi sen johdosta. Ilmoitusvelvollisuuden alaan kuuluvien ilmoitusten käsittelyn tulisi olla ensisijaista valvovalle viranomaiselle ja CSIRT-yksikölle merkittävistä poikkeamista aiheutuvien haitallisten vaikutusten minimoimiseksi.

Ehdotetulla säännöksellä pannaan täytäntöön osittain NIS2-direktiivin 23 artiklan 5 kohta sekä 30 artiklan 2 kohta.

17 §. *Poikkeamailmoitusten käsittely*. Pykälässä säädettäisiin poikkeamailmoitusten käsittelystä, eli siitä, mihin toimenpiteisiin valvovan viranomaisen olisi poikkeamailmoituksen johdosta ryhdyttävä 16 §:ssä säädetyn vastaamisvelvoitteen lisäksi.

Pykälän *1 momentin* nojalla valvovan viranomaisen olisi toimitettava 11 – 13 §:ssä sekä 15 §:ssä tarkoitetut ilmoitukset ja raportit CSIRT-yksikölle, jotta CSIRT-yksikkö voi antaa täydentävää ohjeistusta ja teknistä tukea toimijalle sen pyynnöstä yhteistyössä valvovan viranomaisen kanssa. CSIRT-yksikkö antaisi toimijan pyynnöstä ohjeita tai operatiivisia neuvoja poikkeamaa lieventävistä toimenpiteistä siitä aiheutuvien haitallisten vaikutusten minimoimiseksi. Tarvittaessa ohjeita tai neuvoja voitaisiin antaa myös valvovan viranomaisen ja CSIRT-yksikön yhteistyönä.

Pykälän *2 momentin* nojalla valvovan viranomaisen tulisi toimittaa CER-direktiivin mukaisille toimivaltaisille viranomaisille tietoa merkittävistä poikkeamista, kyberuhkista ja läheltä piti –tilanteista, joista CER-direktiivin nojalla määritellyt kriittiset toimijat ovat ilmoittaneet.

Pykälän *3 momentin* nojalla silloin, jos poikkeamasta olisi aiheutunut yleisen tietosuoja-asetuksen 33 artiklassa tarkoitettu henkilötietojen tietoturvaloukkaus, josta olisi tehtävä ilmoitus yleisen tietosuoja-asetuksen nojalla toimivaltaiselle, henkilötietojen suojaa valvovalle viranomaiselle, valvovan viranomaisen olisi tiedotettava poikkeaman havaitsemisesta tietosuojavaltuutettua. Ilmoitus tehtäisiin Suomessa tapahtuvan valvonnan yhteydessä havaitusta seikasta tietosuojavaltuutetulle, vaikka yleisen tietosuoja-asetuksen nojalla tilanteessa toimivaltainen valvontaviranomainen olisi sijoittautunut toiseen EU-jäsenvaltioon. Tietosuojavaltuutettu harkitsisi yleisen tietosuoja-asetuksen ja tietosuojalain nojalla tilanteessa tarpeelliset toimenpiteet.

Pykälän *4 momentin* nojalla silloin, jos merkittävällä poikkeamalla olisi vaikutuksia muihin EU-jäsenvaltioihin, valvovan viranomaisen olisi tiedotettava merkittävästä poikkeamasta keskitettyä yhteyspistettä sekä toimittaa keskitetylle yhteyspisteelle merkittävää poikkeamaa koskevat ilmoitukset ja raportit. Keskitetystä yhteyspisteestä säädettäisiin 18 §:ssä.

Keskitetyn yhteyspisteen tulisi tiedottaa ilman aiheetonta viivytystä merkittävästä poikkeamasta Euroopan unionin kyberturvallisuusvirasto ENISA:aa ja niitä jäsenvaltioita, joihin poikkeama vaikuttaa. Jäsenvaltioiden tiedottaminen tapahtuisi kunkin jäsenvaltion NIS2-direktiivin nojalla nimetyn keskitetyn yhteyspisteen kautta. Keskitetyllä yhteyspisteellä olisi tässä tarkoituksessa oikeus toimittaa tietoja poikkeamailmoituksista sekä väli- ja loppuraporteista toisen EU-jäsenvaltion keskitetylle yhteyspisteelle ja ENISA:lle. Keskitetyn yhteyspisteen olisi annettava muille jäsenvaltioille sekä ENISA:lle erityisesti sellaisia tietoja, joiden avulla on mahdollista määrittää poikkeaman vaikutuksia siinä toisessa jäsenvaltiossa, johon vaikutukset kohdistuvat, sekä rajat ylittäviä vaikutuksia Euroopan unionin tasolla. Keskitetyn yhteyspisteen olisi huomioitava toimijaan liittyvien tietojen luottamuksellisuus sekä turvallisuus- ja kaupalliset edut ja pidättäydyttävä näiden etujen tarpeettomasta vaarantamisesta sekä tarpeettomasta tietojen luovuttamisesta. Keskitetyn yhteyspisteen ilmoitusvelvoitteeseen ei kuuluisi edellä 4 §:n 5 momentin nojalla sellaisten tietojen antaminen, joiden luovuttaminen olisi vastoin Suomen keskeisiä kansalliseen turvallisuuteen, yleiseen turvallisuuteen tai maanpuolustukseen liittyviä intressejä.

Ehdotetulla säännöksellä pantaisiin täytäntöön NIS2-direktiivin 23 artiklan 1 ja 5 kohta osittain, 23 artiklan 6, 8 ja 10 kohta sekä 13 artiklan 2 ja 3 kohdat.

18 §. *Keskitetty yhteyspiste.* Pykälässä säädettäisiin NIS2-direktiivin 8 artiklan 3 kohdassa tarkoitetusta keskitetystä yhteyspisteestä. Keskitettynä yhteyspisteenä Suomessa ehdotetaan toimivaksi Liikenne- ja viestintäviraston Kyberturvallisuuskeskus, jolla on ollut vastaava tehtävä NIS1-direktiivin täytäntöönpanon myötä.

Keskitetyn yhteyspisteen ensisijaisena tehtävänä olisi NIS2-direktiivin mukainen yhteydenpito suhteessa muihin EU-jäsenvaltioihin ja Euroopan unionin kyberturvallisuusvirasto ENISA:an. Keskitetty yhteyspiste vastaisi niistä tehtävistä, joita sille NIS2-direktiivissä on säädetty, sekä ilmoitusten vastaanottamisen, että lähettämisen osalta. Keskitetyn yhteyspisteen roolista poikkeamailmoitusten käsittelyssä on säädetty edellä 17 §:n 5 momentissa.

Keskitetyn yhteyspisteen tehtävänä olisi myös edistää kansallisten valvovien viranomaisten välistä yhteistyötä niille tässä laissa säädettyjen tehtävien toteuttamiseksi. Keskitetty yhteyspiste voisi edistää valvovien viranomaisten välistä yhteistyötä ja tiedonvaihtoa sekä antaa suosituksia valvoville viranomaisille tämän lain mukaisten vaatimusten ja valvonnan yhteensovittamiseksi.

Keskitetyllä yhteyspisteellä olisi lisäksi keskeinen rooli yhteydenpidossa muihin EU-jäsenvaltioihin ja ENISA:an. Sen lisäksi keskitetyn yhteyspisteen olisi toimitettava ENISA:lle kolmen kuukauden välein yhteenvetoraportti Suomessa ilmoitetuista merkittävistä poikkeamista, poikkeamista, kyberuhkista ja läheltä piti –tilanteista.

Pykälällä pantaisiin täytäntöön NIS2-direktiivin 8 artiklan 3-4 kohdat sekä 23 artiklan 9 kohta.

19 §. *CSIRT-yksikön tehtävät.* Pykälässä säädettäisiin NIS2-direktiivin 10 ja 11 artiklassa tarkoitetusta tietoturvaloukkauksiin reagoivasta ja niitä tutkivasta yksiköstä, eli CSIRT-yksiköstä.

Pykälän *1 momentin* nojalla Suomessa CSIRT-yksikkö olisi Liikenne- ja viestintäviraston toiminto, jonka toiminta olisi järjestettävä erilliseksi eri toimijoita valvovista viranomaisista. CSIRT-yksikön tehtävänä olisi seurata ja analysoida kyberuhkia, haavoittuvuuksia ja poikkeamia sekä kerätä tietoja niistä ja antaa ennakkovaroituksia toimijoille yhteiskunnassa sekä muut ehdotetun 2 momentin mukaiset operatiivisen ja teknisen tason viranomaistehtävät, jotka liittyvät kyberturvallisuuden riskienhallintaan yhteiskunnassa. CSIRT-yksikön tehtävänä olisi tarjota toimijoille operatiivisen ja teknisen tason tukea ja ohjeita merkittävien poikkeamien ja riskien ehkäisemiseksi, havaitsemiseksi ja hallitsemiseksi sekä niiden vaikutusten lieventämiseksi, jos se on tarpeellista, toimija sitä pyytää, ja CSIRT-yksikkö voi resurssiensa puitteissa tukea antaa. CSIRT-yksikön tehtävänä ei olisi valvoa tässä laissa tarkoitettuja toimijoita, minkä johdosta toiminta olisi järjestettävä erilliseksi valvontatoiminnosta Liikenne- ja viestintävirastossa. CSIRT-yksikön olisi lisäksi täytettävä NIS2-direktiivin 11 artiklan 1 kohdassa tarkoitetut vaatimukset, eli sen olisi huolehdittava muun muassa viestintäkanaviensa saatavuudesta, toimitilojensa ja tietojärjestelmiensä sijoittamisesta suojattuihin paikkoihin sekä henkilöstönsä riittävyydestä ja asianmukaisesta koulutuksesta.

Pykälän *2 momentissa* säädettäisiin tarkemmin CSIRT-yksikön tehtävistä. Pykälän 2 momentin *1 kohdan* mukaan CSIRT-yksikkö seuraa ja analysoi kyberuhkia, haavoittuvuuksia ja poikkeamia kansallisella tasolla. Lisäksi se voi kerätä niitä koskevia tietoja sekä tiedottaa niistä tilanteen mukaan esimerkiksi antamalla havaittua haavoittuvuutta koskevia ennakkovaroituksia, hälytyksiä, ilmoituksia ja tietoja. Kyse olisi yleisluonteisesta tiedottamisesta, joka kohdistuisi esimerkiksi tässä laissa tarkoitettuihin keskeisiin tai tärkeisiin toimijoihin tai valvoviin viranomaisiin taikka muihin sidosryhmiin, kuten erilaisiin verkostoihin tai yleisöön. Tehtävää tulisi toteuttaa mahdollisuuksien mukaan koordinoidusti sähköisen viestinnän palveluista annetun lain 304 §:n 7 kohdassa Liikenne- ja viestintävirastolle säädetyn tehtävän kanssa.

Pykälän 2 momentin *2 kohdan* mukaan CSIRT-yksikön tehtävänä olisi pyynnöstä avustaa viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden reaaliaikaisessa tai lähes reaaliaikaisessa seurannassa. Avustaminen voisi tarkoittaa tapauskohtaisesti esimerkiksi ohjeita, neuvoja tai teknistä avustamista. CSIRT-yksikkö voisi tarjota palvelua tai avustaa ja neuvoa sekä tässä laissa tarkoitettuja, että muita toimijoita hankkimaan kolmannen osapuolen palvelua seurantaa varten. Seurannan toteuttamisessa olisi otettava huomioon, mitä henkilötietojen käsittelystä ja luottamuksellisen viestinnän suojasta erikseen säädetään. CSIRT-yksikön tehtävänä olisi erityisesti ohjaava ja neuvova rooli, joka ei vaikuttaisi toimijalla olevaan velvollisuuteen huolehtia sen käytössä olevien viestintäverkkojen ja tietojärjestelmien turvallisuudesta.

Pykälän 2 momentin *3 kohdan* mukaan CSIRT-yksikkö reagoi poikkeamailmoituksiin ja tarvittaessa avustaa poikkeamasta ilmoittanutta tahoa poikkeaman käsittelyssä. Lähtökohtaisesti kuka tahansa voisi tehdä CSIRT-yksikölle ilmoituksen tietoturvapoikkeamasta, ja CSIRT-yksikön tehtävänä olisi reagoida näihin ilmoituksiin. CSIRT-yksikkö reagoisi poikkeamailmoituksiin tarkoituksenmukaisella tavalla esimerkiksi vastaamalla siihen, ohjeistamalla ja neuvomalla ilmoituksen tehnyttä tahoa, koordinoimalla poikkeamaan vastaamista, tutkimalla ilmoitettua poikkeamaa tai tarjoamalla tarvittavaa teknistä tukea. CSIRT-yksikkö reagoisi siis myös muiden kuin tässä laissa tarkoitettujen keskeisten tai tärkeiden toimijoiden tekemiin ilmoituksiin ja tarvittaessa avustaisi niitä poikkeaman käsittelyssä. Vastuu poikkeaman käsittelystä ja tarvittavien toimenpiteiden suorittamisesta olisi pääasiallisesti kuitenkin ilmoituksen tehneellä taholla itsellään.

Pykälän 2 momentin *4 kohdan* mukaan CSIRT-yksikön tehtävänä olisi kerätä ja analysoida uhkatietoja ja tietoturvaloukkausten tutkintaa koskevia tietoja eli forensisia tietoja. Forensisilla tiedoilla tarkoitetaan tietoturvaloukkauksen jättämää digitaalista todistusaineistoa, näytteitä, vaarantumisindikaattoreita eli IoC-tietoja taikka muita hyökkäykseen liittyviä teknisiä tunnisteita ja jälkiä. Forensisia tietoja voitaisiin kerätä esimerkiksi laitteista, tiedoista tai lokeista. Lisäksi uhkatietoja voidaan hankkia esimerkiksi sidosryhmiltä.

Pykälän 2 momentin *5 kohdan* mukaan CSIRT-yksikön tehtävänä olisi laatia riski- ja poikkeama-analyyseja ja tukea kyberturvallisuuden tilannekuvan ylläpitämistä. Liikenne- ja viestintävirastosta annetun lain 3 §:n nojalla Liikenne- ja viestintäviraston Kyberturvallisuuskeskus ylläpitää kyberturvallisuuden tilannekuvaa. CSIRT-yksikön tehtävänä olisi tukea tilannekuvan ylläpitämistä. Riski- ja poikkeama-analyysit voisivat käsitellä joko yksittäistä tapahtumaa tai laajempia ilmiöitä ja tarvittavilta osin ne voisivat olla päivittyviä eli dynaamisia.

Pykälän 2 momentin *6 kohdan* mukaan CSIRT-yksikkö osallistuisi NIS2-direktiivin 15 artiklassa tarkoitettuun CSIRT-verkostoon. CSIRT-verkosto koostuu kaikkien EU-jäsenvaltioiden CSIRT-yksiköistä. CSIRT-verkoston tarkoituksena on edistää luottamusta sekä ripeää ja tuloksellista operatiivista yhteistyötä jäsenvaltioiden välillä. CSIRT-yksikkö voisi myös valmiuksiensa ja osaamistasonsa mukaan avustaa muita CSIRT-verkoston jäseniä niiden pyynnöstä, esimerkiksi jakamalla tietoa ajankohtaisista tapauksista, ilmiöistä ja trendeistä tai tarjoamalla teknistä apua. CSIRT-yksikön tehtävänä olisi osallistua tällaiseen yhteistyöhön sen mukaan kuin se on käytettävissä olevien resurssien puitteissa mahdollista.

Pykälän 2 momentin *7 kohdan* mukaan CSIRT-yksikkö voisi nimetä asiantuntijoita, jotka osallistuisivat NIS2-direktiivin 19 artiklassa tarkoitettuihin vertaisarviointeihin. NIS2-direktiivin 19 artiklassa tarkoitetun vertaisarvioinnin suorittavat kyberturvallisuusasiantuntijat, joiden nimeäminen tehdään erikseen vahvistettavien kriteerien perusteella. Vertaisarviointeihin osallistuminen on kuitenkin vapaaehtoista, eli CSIRT-yksikkö voisi arvioida osallistumisen tarpeellisuutta tapauskohtaisesti eikä kohdalla velvoitettaisi CSIRT-yksikköä vertaisarviointeihin osallistumiseen.

Pykälän 2 momentin *8 kohdan* mukaan CSIRT-yksikön tehtävänä olisi edistää tietoturvallisten tiedonjakovälineiden käyttöönottoa. Vaihtaessaan tietoja toimijoiden ja muiden asiaankuuluvien sidosryhmien CSIRT-yksiköllä tulisi olla käytössään asianmukainen, suojattu ja häiriönsietokykyinen viestintä- ja tietoinfrastruktuuri tietojen vaihtamiseen keskeisten ja tärkeiden toimijoiden ja muiden asiaankuuluvien sidosryhmien kanssa. Tiedonjakovälineiden tulisi täyttää tiedonhallintalain vaatimukset, ja koska niissä käsiteltävä tieto saattaa olla turvallisuusluokiteltua, myös asiakirjojen turvallisuusluokittelusta valtionhallinnossa annetun asetuksen vaatimukset. Käyttämällä tällaisia tiedonjakovälineitä CSIRT-yksikkö edistäisi niiden käyttöä yhteiskunnassa laajemminkin.

Pykälän 2 momentin *9 kohdan* mukaan CSIRT-yksikkö voisi edistää yhteistyötä yksityisen sektorin sidosryhmien kanssa antamalla ohjeita ja suosituksia esimerkiksi yhteisten tai standardoitujen käytäntöjen, luokitusjärjestelmien ja taksonomioiden hyväksymiseksi ja käyttämiseksi. CSIRT-yksikkö voisi antaa tällaisia ohjeita ja suosituksia poikkeamien käsittelemisestä, kyberturvallisuuden kriisinhallinnasta ja koordinoidusta haavoittuvuuksien julkistamisesta.

Pykälän *3 momentissa* säädettäisiin CSIRT-yksikön mahdollisuudesta asettaa tehtäviään tärkeysjärjestykseen riskiperusteisesti. Tärkeysjärjestykseen asettaminen tulisi tehdä riskiperustaista lähestymistapaa soveltaen. Riskiperusteisella lähestymistavalla tarkoitettaisiin keskittymistä ensisijaisesti sellaisiin riskeihin, uhkiin tai poikkeamiin, jotka voisivat aiheuttaa merkit-

täviä tai laaja-alaisia haitallisia vaikutuksia yhteiskunnassa taikka joiden toteutumisen todennäköisyys on huomattavan korkea. Esimerkiksi poikkeamailmoituksia voitaisiin luokitella tietoturvapoikkeaman tai kyberuhan merkittävyyden perusteella, ja tässä arvioinnissa voitaisiin huomioida esimerkiksi hyökkäystyyppi, poikkeaman tai uhan kohde sekä poikkeaman tai uhan laajuus.

Pykälän 1-3 momenteilla täytäntöönpantaisiin NIS2-direktiivin 10 artiklan kohdat 1 ja 5 sekä 3 kohdan a-d, f ja h alakohdat sekä 11 artiklan kohdat 1, 3 ja 5.

Pykälän *4 momentissa* säädettäisiin CSIRT-yksikön tehtävästä tukea kyberturvallisuustietojen vapaaehtoisia jakamisjärjestelyjä tämän lain soveltamisalaan kuuluvien toimijoiden, muiden tahojen ja CSIRT-yksikön kesken. Kyberturvallisuustietojen vapaaehtoisista jakamisjärjestelyistä säädetään 22 §:ssä. Momentilla täytäntöönpantaisiin NIS2-direktiivin 29 artikla.

Pykälän *5 momentissa* säädettäisiin CSIRT-yksikön mahdollisuudesta tuottaa tietoturvaloukkausten havainnointipalvelua, jolla voitaisiin avustaa toimijoita niiden viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden reaaliaikaisessa tai lähes reaaliaikaisessa seurannassa sekä edistää toimenpiteitä poikkeamien havaitsemiseksi, selvittämiseksi ja kyberuhkien ennalta estämiseksi. Tietoturvaloukkausten havainnointipalveluun liittyvästä tiedonkäsittelystä säädettäisiin 23 §:ssä. Säännös ei asettaisi velvoitetta palvelun tuottamiselle vaan mahdollistaisi sen, jos CSIRT-yksikkö katsoo palvelun tarjoamisen tarpeelliseksi. CSIRT-yksikkö voi tarjota tietoturvaloukkausten havainnointipalvelua suoraan sitä pyytäville toimijoille tai muille tahoille sekä sellaisille tietoturvapalveluntarjoajille, jotka tarjoavat tietoturvaloukkausten havainnointipalvelua toimijoille tai muille tahoille käytettäväksi palvelukeskuksen roolissa. Palvelu olisi CSIRT-yksikön tarjoama sen laissa säädetyn tehtävän edistämiseksi, ja olisi toimijan tai palvelun tilaajan itsensä päätettävissä, haluaako se palvelua tilata. Säännöksessä olisi kysymys tietoturvaloukkausten havainnointipalvelun tuottamista koskevan lain tasoisen toimivaltuuden täsmentämisestä. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus on tuottanut tietoturvaloukkausten havainnointipalvelua sille sähköisen viestinnän palveluista annetussa laissa säädettyjen tehtävien toteuttamiseksi. Säännöksellä selkeytettäisiin palvelun tuottamisen säädösperustaa. Lisäksi palvelun tarjoaminen edistäisi CSIRT-yksikön tehtävien hoitamista.

Pykälän *6 momentissa* säädettäisiin liikenne- ja viestintäministeriölle asetuksenantovaltuus maksuista tai niiden perusteista, joita CSIRT-yksikkö voisi periä 2 momentin 1 ja 2 kohdassa tarkoitetusta palvelusta, joka on tarjottu toimijan tai muun tahon pyynnöstä. Maksullista toimintaa voisi olla esimerkiksi pyynnöstä toteutettu 20 §:n 4 momentissa tarkoitettu kohdennettu haavoittuvuuskartoitus sekä tietoturvaloukkausten havainnointipalvelu ja muu 2 momentin 1 ja 2 kohdassa tarkoitettu palvelu, jota tarjotaan toimijan tai muun tahon pyynnöstä. Maksullisessa suoritteessa olisi kyse korvauksesta toimijalle tai muulle taholle kohdennetusta viranomaisen tuottamasta palvelusta, joka on toimijalle tai muulle taholle vapaaehtoinen.

20 §. *Yleisten viestintäverkkojen ja tietojärjestelmien verkkopohjainen haavoittuvuuskartoitus*. Pykälän säädettäisiin CSIRT-yksikön oikeudesta havainnoida yleisesti saatavilla olevia viestintäverkkoja eli niihin liitettyjä viestintäverkkoja ja tietojärjestelmiä haavoittuvuuksien havainnoimiseksi ja kartoituksen kohteen varoittamiseksi havainnoista (*haavoittuvuuskartoitus)*. Lisäksi pykälän *4 momentissa* säädettäisiin toimijan pyynnöstä toteutetusta kohdennetusta haavoittuvuuskartoituksesta. Ehdotetulla toimivaltuudella pantaisiin täytäntöön NIS2-direktiivin 11 artiklan 3 kohdan 1 alakohdan e-luetelmakohdassa ja saman artiklan 3 kohdan 2 alakohdassa CSIRT-yksikölle säädetyt tehtävät.

Haavoittuvuuskartoituksen tarkoituksena olisi haavoittuvuuksien, kyberuhkien ja turvattomasti konfiguroitujen viestintäverkkojen ja tietojärjestelmien havaitseminen sekä näistä havainnoista

asianomaisille tahoille ilmoittaminen, mikä parantaisi asianomaisten tahojen mahdollisuuksia suojautua haavoittuvuuksien hyväksikäytöltä ja kyberuhilta.

Haavoittuvuuskartoitus olisi toteutettava ennakoivalla ja ei-intrusiivisella tavalla. Ennakoivuudella tarkoitettaisiin haavoittuvuuskartoituksen yhteyttä tiedossa oleviin tai ennakoitavissa oleviin haavoittuvuuksiin tai kyberuhkiin. Ei-intrusiivisuus tarkoittaisi havainnointia viestintäverkon avulla saatavilla olevista viestintäverkoista ja tietojärjestelmistä tavalla, joka ei edellyttäisi tunkeutumista viestintäverkkoihin tai tietojärjestelmiin havaintojen tai tietojen saamiseksi. Ei-intrusiivisessa havainnoinnissa voitaisiin esimerkiksi lähettää teknisiä kyselyjä tai konekielisiä viestejä viestintäverkkoon tai tietojärjestelmään, palveluun, sen palvelimelle tai palvelimen sovellukselle, esim. portille, järjestelmässä olevien avointen porttien tai suojaamattomien teknisten ratkaisujen havaitsemiseksi. Kyselyjä voitaisiin lähettää myös tiedon keräämiseksi teknisistä ratkaisuista, kuten ohjelmistoista, joita viestintäverkoissa ja tietojärjestelmissä käytetään, sen selvittämiseksi, onko haavoittuvia tai suojaamattomia teknisiä ratkaisuja käytössä viestintäverkoissa ja tietojärjestelmissä niihin kohdistuvien haavoittuvuuksien tai kyberuhkien torjumiseksi.

Intrusiivisena ja siten kiellettynä haavoittuvuuskartoituksena olisi pidettävä ainakin sellaista toimintaa, jossa viestintäverkkoon ja tietojärjestelmään tunkeuduttaisiin ilman asianomaisen toimijan suostumusta haavoittuvuutta hyväksikäyttäen. Pykälässä erikseen edellytettäisiin myös, että kartoituksesta ei saa aiheutua haittaa asianomaisten järjestelmien tai palvelujen toiminnalle. Intrusiivista ja momentin nojalla kiellettyä olisi myös viestintäverkon ja tietojärjestelmän toimintaan vaikuttaminen haavoittuvuuskartoituksessa palvelun tavanomaisesta toiminnasta poikkeavalla tavalla tai muuten häiriötä aiheuttavalla tavalla taikka tietojen oikeudeton käsitteleminen viestintäverkossa tai tietojärjestelmässä. Haavoittuvuuskartoituksen toteuttaminen näillä tavoilla ei siten olisi ehdotuksen nojalla sallittua. Intrusiivisuutena ja siten viestintäverkkoon ja tietojärjestelmään kiellettynä tunkeutumisena ei olisi pidettävä esimerkiksi yksittäisen, tiedossa olevan tai ennalta tunnetun järjestelmän oletuskäyttäjätunnuksen ja salasanan yhdistelmän kokeilemista sen selvittämiseksi, onko järjestelmä asianmukaisesti suojattu, jos tällaisen kokeilun jälkeen toimintaa viestintäverkossa- ja tietojärjestelmässä ei jatketa tai siellä olevia tietoja käsitellä. Intrusiivisuutta ja siten kiellettyä olisi oletuskäyttäjätunnuksen ja salasanan yhdistelmän kokeileminen toistuvasti tavalla, jonka johdosta tunnukset lukittuisivat tietoturvasyistä. Intrusiivisuuden arvioinnin kannalta olennaista olisi toiminta tietojärjestelmässä. Jos haavoittuvuus havaitaan siten, että turvajärjestely avaa pääsyn tietojärjestelmään, toimintaa ei tulisi tulkita intrusiiviseksi, jos heti havainnon jälkeen yhteys tietojärjestelmään katkaistaan ja toiminta tietojärjestelmässä lopetetaan. Jos tällaisen havainnon jälkeen tietojärjestelmässä käsiteltäisiin oikeudettomasti mitä tahansa tietoja, olisi toiminta intrusiivista ja siten kiellettyä.

Haavoittuvuuskartoituksessa voitaisiin havainnoida tai kartoittaa vain viestintäverkkoja ja tietojärjestelmiä. Haavoittuvuuskartoituksella ei siten olisi sallittua hankkia ja käsitellä luottamuksellisen viestinnän suojaamia tietoja, kuten välitystietoja tai viestien sisältöä, jossa CSIRT-yksikkö ei ole viestinnän osapuolena. Haavoittuvuuskartoituksella ei siten puututtaisi luottamukselliseen viestintään. Haavoittuvuuskartoituksessa ei olisi sallittua käsitellä viestintäverkkoon tai tietojärjestelmään tallennettua henkilötietoa tällaisen käsittelyn intrusiivisuuden vuoksi. CSIRT-yksiköllä olisi oikeus haavoittamiskartoituksen toteuttamiseksi hankkia tietoja yleiseen viestintäverkkoon kytkettyjen telepäätelaitteiden ja tietojärjestelmien sekä niiden tietoliikennejärjestelyjen yksilöintitiedoista, käytetyistä ohjelmistoista ja niiden toiminnasta, teknisestä toteutuksesta ja niiden avulla tarjotuista palveluista. Haavoittuvuuskartoitus voisi kohdistua myös yleisen viestintäverkon viestintäverkkolaitteisiin, jotka kuuluisivat viestintäverkon käsitteen alaan.

CSIRT-yksikkö saisi käyttää haavoittuvuuskartoituksessa havaittuja tietoja vain haavoittuvuuskartoituksen kohteena olevalle taholle viestintäverkkoon ja tietojärjestelmään kohdistuvista haavoittuvuuksista ja riskeistä ilmoittamiseksi sekä kyberuhkien tunnistamiseksi, kyberturvallisuuden tilannekuvan ylläpitämiseksi ja haavoittuvuuksista tiedottamiseksi. Kyberuhkien tunnistaminen kattaisi myös kartoituksella kerättyjen tietojen käsittelyn aiemmin tunnistamattomien uhkien löytämiseksi. Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen tehtävästä ylläpitää kansallisen kyberturvallisuuden tilannekuvaa säädetään Liikenne- ja viestintävirastosta annetun lain (935/2018) 3 §:n 1 momentissa. Tiedottamisesta ei saisi ilmetä kartoituksen kohteeseen yhdistettävissä olevia tietoja, mutta tietoja voitaisiin käyttää esimerkiksi tiedottamisen suuntaamiseen. Tietoja voitaisiin kuitenkin luovuttaa sähköisen viestinnän palveluista annetun lain 319 §:n 2 momentin tilanteissa.

Tarpeettomat tiedot olisi poistettava viipymättä. Tällä tarkoitettaisiin, että kartoituksella saatuja tietoja tulisi säilyttää vain siltä osin kuin ne ovat tarpeen edellä mainittujen tarkoitusten toteuttamiseksi. Tämä ei estäisi sellaisten tietojen säilyttämistä, joiden ennakoidaan olevan tarpeen tulevien haavoittuvuuksien havaitsemiseksi aineistosta, jotta niihin voidaan reagoida tehokkaasti.

Ehdotetun *4 momentin nojalla* CSIRT-yksiköllä olisi oikeus suorittaa kohteen pyynnöstä sen viestintäverkossa ja tietojärjestelmissä haavoittuvuuskartoitus sellaisen haavoittuvuuden havaitsemiseksi, jolla voi olla merkittävä vaikutus viestintäverkkoon ja tietojärjestelmään tai sen avulla tarjottaviin palveluihin. Tällaisessa pyynnöstä tapahtuvassa haavoittuvuuskartoituksessa, jonka CSIRT-yksikkö toteuttaisi yhteistyössä asianomaisen tahon kanssa, voitaisiin poiketa 1–3 momentissa säädetyistä edellytyksistä. CSIRT-yksiköllä ei olisi velvollisuutta suorittaa pyynnöstä haavoittuvuuskartoitusta, vaan se voisi harkita tehtäviensä riskiperusteisen tärkeysjärjestyksen näkökulmasta, milloin erillinen pyynnöstä suoritettava haavoittuvuuskartoitus on tarkoituksenmukaista suorittaa juuri CSIRT-yksikön toimesta.

Haavoittuvuuskartoituksessa tai kohdennetussa haavoittuvuuskartoituksessa ei saisi käsitellä tietoja sähköisten viestien sisällöstä. Kohdennetussa haavoittuvuuskartoituksessa CSIRT-yksiköllä olisi kuitenkin oikeus tarkkailla ja käyttää välitystietoja, jos se on tarpeen haavoittuvuuden, kyberuhkan tai turvattoman konfiguroinnin havaitsemiseksi.

CSIRT-yksikön olisi hävitettävä haavoittuvuuskartoituksessa saamansa tiedot, kun ne eivät ole enää tarpeen haavoittuvuudesta asianomaiselle toimijalle ilmoittamiseksi tai kyberturvallisuuden tilannekuvan ylläpitämiseksi.

Henkilötietojen käsittelyperuste haavoittuvuuskartoituksessa olisi yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan e alakohta.

21 §. *Koordinoitu haavoittuvuuksien julkistaminen.* Pykälässä säädettäisiin koordinoidusta haavoittuvuuksien julkistamisprosessista. Ehdotuksella pantaisiin täytäntöön NIS2-direktiivin 12 artiklan 1 kohta.

Pykälän *1 momentin* nojalla CSIRT-yksikkö toimisi NIS2-direktiivin 12 artiklassa tarkoitettuna koordinaattorina haavoittuvuuksien koordinoitua julkistamista varten. CSIRT-yksikkö ottaisi haavoittuvuuksien julkistamista varten vastaan ilmoituksia havaituista haavoittuvuuksista. Ilmoituksen voisi tehdä CSIRT-yksikölle kuka tahansa, ja sen voisi tehdä myös nimettömänä. CSIRT-yksikön olisi varmistettava haavoittuvuudesta ilmoittavan luonnollisen henkilön tai oikeushenkilön nimettömyys aina, ellei ilmoittaja erikseen anna suostumusta henkilöllisyytensä

paljastamiseen. CSIRT-yksikkö huolehtisi myös ilmoituksen johdosta tarpeellisista jatkotoimista, kuten haavoittuvuudesta ilmoittaminen TVT-tuotteen tai –palvelun valmistajalle tai tarjoajalle sekä Euroopan haavoittuvuustietokantaan sekä siitä, että toimija toteuttaa tarpeelliset jatkotoimet havainnon johdosta. Euroopan haavoittuvuustietokantaa ylläpitää Euroopan unionin kyberturvallisuusvirasto ENISA ja sen säädösperusta on NIS2-direktiivin 12 artiklassa.

Pykälän *2 momentin* nojalla CSIRT-yksikön tehtäviin koordinaattorina kuuluisi asianomaisten toimijoiden tunnistaminen ja yhteyden ottaminen niihin, haavoittuvuudesta ilmoittavien tahojen avustaminen, julkistamisen aikataulusta neuvotteleminen ja useisiin toimijoihin vaikuttavien haavoittuvuuksien hallinta. CSIRT-yksikkö toimisi tarvittaessa myös luotettuna välittäjänä haavoittuvuudesta ilmoittavan tahon ja asianomaisen TVT-tuotteen tai –palvelun valmistajan tai tarjoajan välillä. CSIRT-yksikkö voisi lisäksi ohjata ja neuvoa asianomaisia tahoja siitä, miten Euroopan haavoittuvuustietokantaan voi ilmoittaa tietoja tai tarvittaessa hakea tietoja. CSIRT-yksiköllä olisi myös oikeus ilmoittaa itse tiedossaan olevia haavoittuvuuksia Euroopan haavoittuvuustietokantaan. CSIRT-yksikkö voisi ilmoittaa Euroopan haavoittuvuustietokantaan pykälän 3 momentissa säädetyt tiedot ilmoitettavasta haavoittuvuudesta.

Pykälän *3 momentin* nojalla, jos CSIRT-yksikkö saisi tiedon sellaisesta haavoittuvuudesta, jolla voisi olla merkittävä vaikutus muihin EU-jäsenvaltioihin, CSIRT-yksikön olisi tarvittaessa tehtävä siihen liittyen yhteistyötä CSIRT-verkostossa.

22 §. *Kyberturvallisuustietojen vapaaehtoiset jakamisjärjestelyt*. Pykälässä säädettäisiin CSIRT-yksikön koordinoimista vapaaehtoisista kyberturvallisuustietojen jakamisjärjestelyistä. Vapaaehtoisten jakamisjärjestelyjen tarkoituksena on vaihtaa kyberturvallisuustietoja niihin osallistuvien tahojen kesken sekä CSIRT-yksikön kanssa kyberuhkien ehkäisemiseksi, havaitsemiseksi, poikkeamien hallitsemiseksi ja niistä palautumiseksi tai niiden vaikutusten lieventämiseksi.

Pykälää sovellettaisiin vain CSIRT-yksikön koordinoimiin kyberturvallisuustietojen jakamisjärjestelyihin. Sen estämättä, mitä 1 momentissa säädetään, valvova viranomainen voisi kuitenkin toimialallaan tukea myös muita tiedonvaihtoyhteisöjä tai toimijat voisivat sopia muiden tiedonvaihtoyhteisön perustamisesta.

Kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn osallistuvien kesken voitaisiin jakaa erityisesti pykälän 2 momentissa tarkoitettuja tietoja. Kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn osallistuvien kesken voitaisiin jakaa myös muita kyberuhkien ja poikkeamien torjumiseksi tarpeellisia tietoja, kuten suosituksia, jotka koskevat kyberhyökkäysten havaitsemiseen käytettävien kyberturvallisuustyökalujen konfigurointia. Mahdollisuudesta luovuttaa välitystietoja tai haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä säädetään jäljempänä 24 §:n 1 momentissa. Jakamisjärjestelyn osapuolilla tulisi olla mahdollisuus sopia menettelyistä ja toimintatavoista jaettujen tietojen käsittelemisessä tai tietojen luottamuksellisuuden osalta säännöksen estämättä.

Kun CSIRT-yksikkö tukee jakamisjärjestelyjä jakamalla kyberturvallisuustietoja jakamisjärjestelyyn osallistuville, olisi kyseiseen vapaaehtoiseen jakamisjärjestelyyn osallistuvalla taholla erikseen laissa säädetty tiedonsaantioikeus niihin tietoihin, joita kyberturvallisuustietojen vapaaehtoisessa jakamisjärjestelyssä jaetaan. Näin ollen kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn osallistuvat tahot voisivat saada kyseiset tiedot tiedonhallintalain 22 ja 24 §:ssä tarkoitetulla tavalla.

Ehdotetulla 22 §:llä täytäntöönpantaisiin NIS2-direktiivin 29 artikla.

23 §. *Tietoturvaloukkausten havainnointipalveluun liittyvä tiedonkäsittely.* Pykälässä säädettäisiin tiedonkäsittelystä 19 §:n 5 momentissa tarkoitetussa tietoturvaloukkausten havainnointipalvelussa, mikä olisi tarpeen siltä osin kuin palvelussa olisi käsiteltävänä sähköisiä viestejä tai välitystietoja. Pykälä olisi erityissäännös suhteessa sähköisen viestinnän 17 luvussa sähköisen viestin ja välitystietojen käsittelystä säädettyyn.

Pykälän *1 momentin* nojalla havainnointipalvelua käyttävä taho, palvelukeskus ja CSIRT-yksikkö voisivat luovuttaa toisilleen viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden seurannan kannalta tarpeellisia tietoja kyberuhkien ehkäisemiseksi, havaitsemiseksi, poikkeamien hallitsemiseksi ja niistä palautumiseksi tai niiden vaikutusten lieventämiseksi. CSIRT-yksikkö voisi luovuttaa 1 momentissa tarkoitettuja tietoja katseluyhteyden avulla taikka teknisen rajapinnan avulla siten kuin tiedonhallintalain 24 §:ssä säädetään. Siinä määrin kuin tietoturvaloukkausten havainnointipalvelun toteuttamiseksi on välttämätöntä, luovutettavat tiedot voivat sisältää palvelua käyttävän tahon palvelussa käsiteltäväksi pyytämiä sellaisia sähköisiä viestejä tai niihin liittyviä välitystietoja, joita sillä on oikeus käsitellä sähköisen viestinnän palveluista annetun lain 272 §:n nojalla.

Luovutettavat tiedot voisivat sisältää siten muiden tietojen ohella myös palvelua käyttävän tahon palvelussa käsiteltäväksi pyytämiä sähköisiä viestejä tai niihin liittyviä välitystietoja siinä määrin kuin se on välttämätöntä tietoturvaloukkausten havainnointipalvelun toteuttamiseksi. Palvelussa voitaisiin käsitellä muuta tietoa kuin luottamuksellista sähköistä viestintää tai välitystietoja, mutta näistä tietotyypeistä olisi tarpeen säätää erikseen sähköisen viestinnän palveluista annetussa laissa säädettyjen käsittelyrajoitusten vuoksi. Säännöksen tarkoituksena olisi selkeyttää, että näitä tietotyyppejä saisi ehdotetun 1 momentin nojalla luovuttaa ja käsitellä sähköisen viestinnän palveluista annetun lain 136 §:n 4 momentin estämättä, jos pykälässä säädetyt edellytykset täyttyvät. Säännöksen tarkoituksena olisi myös selkeyttää palvelussa tietojen käsittelyä suhteessa sähköisen viestinnän palvelusta annetun lain 137 §:n edellytyksiin. Tietotyyppejä, joita taholla olisi oikeus käsitellä sähköisen viestinnän palveluista annetun lain 272 §:n nojalla, ovat esimerkiksi palvelussa käsiteltäväksi pyydetty sähköinen viestintä, siihen liittyvät välitystiedot ja muut viestintää kuvaavat loki- tai metatiedot sekä tietoturvaloukkausten ja niiden uhkien tunnistamiseen käytettävät tarpeelliset tunnisteet eli vaarantumisindikaattorit.

Edellytyksenä viestien tai välitystietojen luovuttamiselle olisi välttämättömyyden lisäksi se, että havainnointipalvelua käyttävällä taholla olisi oikeus käsitellä näitä tietoja sähköisen viestinnän palveluista annetun lain 272 §:n nojalla. Sähköisen viestinnän palveluista annetun lain 272 §:ssä säädetään viestinnän välittäjän ja lisäarvopalvelun tarjoajan sekä niiden lukuun toimivan oikeudesta ryhtyä välttämättömiin toimiin tietoturvasta huolehtimiseksi. Sähköisen viestinnän palveluista annetun lain 272 §:n 3 ja 4 momentissa säädetyt edellytykset tietojen käsittelylle soveltuisivat myös tietoturvaloukkausten havainnointipalvelussa. Toimenpiteet olisi toteutettava huolellisesti ja ne olisi mitoitettava suhteessa torjuttavan häiriön vakavuuteen. Toimenpiteitä toteutettaessa ei saisi rajoittaa sananvapautta taikka luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä. Toimenpiteet olisi lopetettava, jos niiden toteuttamiselle ei enää olisi pykälässä säädettyjä edellytyksiä.

Pykälän *2 momentissa* täsmennettäisiin säännökset, joita aina sovellettaisiin palvelun toteuttamisessa riippumatta siitä, onko palvelunkeskus tai CSIRT-yksikkö sähköisen viestinnän palveluista annetussa laissa tarkoitettu lisäarvopalvelun tarjoaja. Edellä 1 momentissa säädetty edellytys oikeudelle käsitellä viestejä tai välitystietoja sähköisen viestinnän palveluista annetun lain 272 §:n nojalla pitää sisällään edellytyksen siitä, että tahon on oltava sähköisen viestinnän palveluista annetussa laissa tarkoitettu viestinnän välittäjä. CSIRT-yksiköllä olisi oikeus käyttää palvelun tuottamisen yhteydessä saamiaan välitystietoja ja muita tietoja kansallisen kyberturvallisuuden tilannekuvan ylläpitämiseksi.

Pykälän *3 momentissa* täsmennettäisiin, että CSIRT-yksiköllе tietoturvaloukkausten havainnointipalvelun toteuttamiseksi luovutettuja viestejä ja välitystietoja koskisi myös, mitä sähköisen viestinnän palveluista annetun lain 316 §:n 4 momentissa säädetään merkittävien tietoturvaloukkausten tai -uhkien selvittämistä koskevien tietojen hävittämisestä sekä 319 §:n 1 momentissa salassapitovelvollisuudesta.

24 §. *Kyberuhkiin ja poikkeamiin liittyvien eräiden tietojen luovuttaminen.* Pykälässä olisi eräitä lain soveltamiseksi tarpeellisia säännöksiä kyberuhkiin ja poikkeamiin liittyvien tietojen luovuttamisesta. Pykälä olisi erityissäännös suhteessa sähköisen viestinnän palveluista annettuun lakiin.

Pykälän *1 momentissa* säädettäisiin toimijan tai muun kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn osallistuvan tahon mahdollisuudesta luovuttaa sähköisen viestinnän palveluista annetun lain 136 §:n 4 momentin estämättä oma-aloitteisesti tietoa kyberuhkaan tai poikkeamaan liittyvästä välitystiedosta tai haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä CSIRT-yksikölle, valvovalle viranomaiselle tai toiselle samaan kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn osallistuvalle taholle. Kyberuhkien ja poikkeamien hallitsemiseksi ja haitallisten vaikutusten ehkäisemiseksi olisi välttämätöntä, että toimijalla olisi mahdollisuus antaa oma-aloitteisesti tietoa haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä ja sen välitystiedoista erityisesti siltä osin kuin se liittyy haitalliseen tietokoneohjelmaan tai käskyn teknisiin ominaisuuksiin ja teknisiin jälkiin. Säännös kattaisi esimerkiksi tiedon antamisen haitalliseen tietokoneohjelmaan liittyvistä lokitiedoista. Toimija voisi luovuttaa 1 momentin nojalla tietoja valvovalle viranomaiselle osana pakollista tai vapaaehtoista raportointia ja CSIRT-yksikölle esimerkiksi merkittävän poikkeaman haitallisten vaikutuksien poistamisen aikana. Kyberturvallisuustietojen vapaaehtoisen jakamisjärjestelyn toteuttamiseksi olisi tarpeen, että vapaaehtoiseen jakamisjärjestelyyn osallistuvat voisivat vastaavasti jakaa tietoja haitallisista tietokoneohjelmista ja käskyistä jakamisjärjestelyyn osallistuvien kesken. Jos pykälän nojalla tapahtuvassa luovuttamisessa olisi kyse henkilötiedoista, olisi erikseen noudatettava myös, mitä yleisessä tietosuoja-asetuksessa ja tietosuojalaissa henkilötiedoista säädetään.

Pykälän *2 momentissa* säädettäisiin CSIRT-yksikön oikeudesta luovuttaa ehdotetun lain nojalla saamiaan ja hankkimiaan tietoja siten kuin sähköisen viestinnän palveluista annetun lain 319 § :n 2 ja 3 momentissa säädetään. Säännös olisi tarpeen CSIRT-yksikön tehtävien toteuttamiseksi. Muun ohella sähköisen viestinnän palveluista annetun lain 319 §:n 3 momentin nojalla oikeus luovuttaa tietoja on ainoastaan siinä laajuudessa kuin se on tarpeen tietoturvaloukkausten ehkäisemiseksi ja selvittämiseksi, ja tietojen luovuttamisella ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.

Pykälän *3 momentissa* säädettäisiin CSIRT-yksikölle tietojen vapaaehtoisen luovuttajan suojaksi tiedon käyttörajoituksesta, joka rajaisi CSIRT-yksikölle vapaaehtoisesti luovutettujen tietojen käyttämistä tiedon luovuttanutta koskevassa rikostutkinnassa, hallintomenettelyssä tai muussa tiedon luovuttanutta koskevassa päätöksenteossa. Jos CSIRT-yksikkö saisi ehdotetussa laissa säädetyn tehtävien hoitamisen yhteydessä muun kuin laissa säädetyn raportointivelvoitteen alaisen tiedon, tällaista tietoa ei saisi käyttää tiedon vapaaehtoisesti luovuttaneeseen kohdistuvassa rikosprosessissa tai hallinnollisessa prosessissa. Säännös olisi välttämätön toimijoiden ja CSIRT-yksikön välisen luottamuksellisen yhteistyön mahdollistamiseksi kyberuhkien ja poikkeamien haitallisten vaikutusten torjumisessa etenkin, kun CSIRT-yksikkö olisi sijoitettu Liikenne- ja viestintävirastoon, joka hoitaisi myös eräisiin toimijoihin kohdistuvia valvovan viranomaisen tehtäviä. Rajoitus koskee kuitenkin vain tiedon ilmoittaneeseen tahoon kohdistuvaa rikostutkintaa tai päätöksentekoa. Se ei myöskään estäisi tiedon luovuttanutta tahoa itse tekemästä asiassa esimerkiksi rikosilmoitusta. Kuitenkin jos kysymys olisi epäillystä tahallisesta ja vakavasta lain vastaisesta toiminnasta ja ilmoittaminen olisi tarpeen merkittävän kyberuhkan

torjumiseksi, CSIRT-yksiköllä olisi oikeus riskiarvionsa perusteella tehdä tietoihin perustuva ilmoitus tämän lain rikkomista valvovalle viranomaiselle.

Säännös vastaisi NIS2-direktiivin johdantokappaletta 41 siitä, että toimijoiden ja CSIRT-yksiköiden välisen luottamuksen lujittamiseksi tapauksissa, joissa CSIRT on osa toimivaltaista viranomaista, jäsenvaltioiden olisi voitava harkita CSIRT-yksiköiden operatiivisten tehtävien, erityisesti tietojen jakamisen ja toimijoille annettavan tuen, erottamista toiminnallisesti toimivaltaisten viranomaisten valvontatoimista. Tietojen vapaaehtoisen luovuttajan suojaksi säädettävällä rajoituksella erotettaisiin valvontatoiminnassa ja CSIRT-yksikön operatiivisessa toiminnassa käytettäviä tietoja ja edistettäisiin toimijan oikeussuojan toteutumista.

25 §. *Valvovat viranomaiset*. Pykälässä säädettäisiin lain noudattamista valvovista viranomaisista. Laissa tarkoitettaisiin valvovalla viranomaisella NIS2-direktiivin mukaista toimivaltaista viranomaista.

Pykälän *1 momentissa* osoitettaisiin sektorikohtaiset valvovat viranomaiset, jotka valvoisivat lain, sen nojalla annettujen määräysten sekä NIS2-direktiivin nojalla annettujen säädösten, eli komission täytäntöönpanosäädösten noudattamista kunkin sektorin toimijoiden osalta.

Liikenne- ja viestintävirasto olisi tässä laissa tarkoitettu valvova viranomainen liikenne- ja avaruussektorilla, digitaalisen infrastruktuurin palvelujen, TVT-palvelujen, posti- ja kuriiripalvelujen ja digitaalisten palvelujen tarjoamisen osalta, moottoriajoneuvojen, perävaunujen, puoliperävaunujen ja muiden kulkuneuvojen valmistuksen osalta sekä tutkimusorganisaatioiden osalta.

Energiavirasto olisi tässä laissa tarkoitettu valvova viranomainen sähkön, kaukolämmityksen ja –jäähdytyksen sekä maakaasun jakelu- tai siirtoverkonhaltijoiden osalta.

Turvallisuus- ja kemikaalivirasto olisi tässä laissa tarkoitettu valvova viranomainen muiden kaasualan toimijoiden, öljy- ja vetyalan toimijoiden, kemikaalien valmistuksen, tuotannon ja jakelun osalta sekä tietokoneiden, elektronisten ja optisten tuotteiden, sähkölaitteiden ja muiden koneiden ja laitteiden valmistuksen osalta.

Sosiaali- ja terveysalan lupa- ja valvontavirasto olisi tässä laissa tarkoitettu valvova viranomainen terveyssektorin palveluiden tarjoamisen osalta.

Etelä-Savon elinkeino-, liikenne- ja ympäristökeskus olisi tässä laissa tarkoitettu valvova viranomainen talous- ja jäteveden käsittelyn osalta sekä jätehuollon palveluiden osalta.

Ruokavirasto olisi tässä laissa tarkoitettu valvova viranomainen elintarvikesektorin palveluiden tarjoamisen osalta.

Lääkealan turvallisuus- ja kehittämiskeskus olisi tässä laissa tarkoitettu valvova viranomainen muiden lääkinnällisten laitteiden valmistajien paitsi kansanterveysuhan aikana kriittisten lääkinnällisten laitteiden valmistajien osalta.

Pykälän *2 momentissa* säädettäisiin valvovan viranomaisen tehtävästä. Valvovan viranomaisen tehtävänä olisi valvoa toimialallaan tämän lain, sen nojalla annettujen määräysten sekä NIS2-direktiivin nojalla annettujen säädösten noudattamista.

Pykälän *3 momentissa* säädettäisiin valvonnasta tilanteessa, jossa yksi toimija harjoittaisi toimintaa laaja-alaisesti usealla toimialalla siten, että toimijaan kohdistuisi 1 momentin nojalla

useamman kuin yhden viranomaisen valvontatoimivalta. Tässä tilanteessa kukin valvova viranomainen valvoisi toimijaa vain sen toiminnan osalta, joka kuuluu kyseisen viranomaisen valvottavana olevaan toimialaan. Jos sama toimija toimisi usealla eri toimialalla, kohdistuisi sen eri toimintoihin siten eri valvovien viranomaisten valvontaa. Valvovilta viranomaisilta edellytettäisiin tällöin yhteistyötä valvonnan toteuttamiseksi tavalla, joka säästää valvonnan kohteen ja valvovien viranomaisten resursseja. Valvovien viranomaisten tulisi esimerkiksi koordinoida kyseiseen toimijaan kohdistettavia valvontatoimenpiteitä ja hyödyntää toistensa tekemiä riskiarviointeja soveltuvin osin. Toimijaan ei tulisi kohdistaa saman asian vuoksi päällekkäisiä valvontatoimenpiteitä.

26 §. *Valvonnan kohdistaminen*. NIS2-direktiivin vähimmäisvaatimuksen mukaisesti tämän lain, sen nojalla annettujen määräysten sekä NIS2-direktiivin nojalla annettujen säädösten ennakkovalvonta kohdistettaisiin keskeisiin toimijoihin. Keskeinen toimija määriteltäisiin NIS2-direktiivin keskeisen toimijan kriteereitä vastaavasti. Muulla kuin keskeisellä toimijalla viitattaisiin NIS2-direktiivin mukaisiin tärkeisiin toimijoihin, eli soveltamisalaan kuuluviin muihin kuin keskeisiin toimijoihin.

NIS2-direktiivin 32 artiklan 1 kohdasta, 33 artiklan 1 kohdasta ja johdantokappaleesta 122 ilmenee lähtökohta valvonnan jakaminen keskeisten ja tärkeiden toimijoiden välillä ennakko- ja jälkivalvontaan. Keskeisiin toimijoihin olisi sovellettava ennakoivaa valvontaa ja tärkeisiin toimijoihin, eli muihin kuin keskeisiin toimijoihin, olisi sovellettava lähtökohtaisesti vain jälkikäteistä valvontaa silloin, jos on näyttöä, viitteitä tai tietoja, joiden mukaan tärkeä toimija ei noudata NIS2-direktiivin ja sitä täytäntöönpanevan sääntelyn velvoitteita.

Keskeisiä toimijoita olisivat liitteessä I tarkoitetut toimijat, jotka ylittävät keskisuuren toimijan määritelmässä tarkoitetut kynnysarvot. Keskeisiä toimijoita olisivat siten kokoperusteisesti suuret yritykset, joiden palveluksessa on vähintään 250 työntekijää taikka joiden vuotuinen liikevaihto on yli 50 miljoonaa euroa ja tase on yli 43 miljoonaa euroa. Jos toimijan palveluksessa on alle 250 työntekijää mutta sekä vuotuinen liikevaihto että tase ylittävät kyseiset raja-arvot, toimija ylittäisi keskisuuren toimijan määritelmän. Keskisuuren toimijan määritelmän ylittymisessä olisi huomioitava toimijan toiminnan laajuus kokonaisuudessaan, ei ainoastaan liitteessä I tarkoitetun toiminnan osalta.

Lisäksi keskeisiä toimijoita olisivat koosta riippumatta hyväksytyt luottamuspalvelun tarjoajat, aluetunnusrekisterit, DNS-palveluntarjoajat, CER-direktiivin nojalla kriittisiksi määritellyt toimijat sekä toimijat, jotka on määritelty tämän lain 3 §:n 2 momentin nojalla annetussa valtioneuvoston asetuksessa keskeisiksi.

Keskeisiä toimijoita olisivat yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat, jotka täyttävät tai ylittävät keskisuuren toimijan määritelmän.

Keskeisten toimijoiden lisäksi valvova viranomainen voisi kohdistaa valvontaa ja 29-30 §:ssä tarkoitettuja toimia muuhun toimijaan kuin keskeiseen toimijaan silloin, kun on perusteltu syy epäillä, että kyseinen toimija ei ole noudattanut tätä lakia, sen nojalla annettuja määräyksiä tai NIS2-direktiivin nojalla annettuja säädöksiä. Perustellulla syyllä tarkoitettaisiin valvovan viranomaisen tietoon tulevaa näyttöä, viitteitä tai tietoja, joiden mukaan toimija ei väitetysti noudattaisi sille laissa säädettyjä velvoitteita erityisesti riskienhallinnan tai raportoinnin osalta. Muihin kuin keskeisiin toimijoihin voitaisiin kohdistaa valvontaa lähtökohtaisesti vain silloin, jos valvovan viranomaisten tietoon tulee perusteltu syy eli näyttöä, viitteitä tai tietoja, joiden perusteella viranomainen epäilee, että kyseinen toimija ei ole noudattanut tätä lakia, sen nojalla annettuja määräyksiä tai NIS2-direktiivin nojalla annettuja säädöksiä. Tällaista näyttöä, viitteitä

tai tietoja voivat olla esimerkiksi muiden viranomaisten, toimijoiden, kansalaisten, tiedotusvälineiden tai muiden lähteiden toimittamat tai julkisesti saatavilla olevat tiedot tai valvovalle viranomaiselle tehty ilmianto, joka ei ole ilmeisen perusteeton.

Valvottavien toimijoiden määrä vaihtelee sektoreittain ja toimijoiden merkitys yhteiskunnan kriittisille toiminnoille sekä niihin kohdistuvien kyberturvallisuusriskien määrä vaihtelee. Näistä syistä olisi tarpeen, että valvova viranomainen voisi tarvittaessa asettaa tämän lain mukaiset valvontatehtävänsä tärkeysjärjestykseen riskiperusteisesti. Valvonnan, eli toimijoihin kohdistettavien valvontatoimenpiteiden laadun ja määrän tulisi olla suhteellista ja perustua kyberturvallisuusriskien arviointiin. Kyberturvallisuusriskien arvioinnissa olisi otettava huomioon toimijoihin kohdistuvien kyberturvallisuusriskien laatu ja määrä, mahdollisesta poikkeamasta aiheutuvat vaikutukset yhteiskunnalle, toimijoiden yleisen kyberturvallisuusmaturiteetin laatu, valvontaviranomaisten käytettävissä olevat resurssit sekä yhteistyö muiden viranomaisten kanssa. Viranomainen voisi toteuttaa riskiperusteisuutta esimerkiksi laatimalla valvontasuunnitelman, jossa se luokittelisi valvonnan kohteet erilaisiin riskiluokkiin ja määrittelisi niiden perusteella toimijoihin kohdistettavat valvontatoimenpiteet ja niiden tiheyden tai toimijoilta säännöllisesti pyydettävät tiedot ja niiden yksityiskohtaisuudelle asetettavat vaatimukset. Valvovilla viranomaisilla ei kuitenkaan olisi velvollisuutta laatia valvontasuunnitelmaa ja tehtävien asettamista tärkeysjärjestykseen voisi tehdä myös muilla tavoin. Valvonta ja tehtävien asettaminen tärkeysjärjestykseen toteutettaisiin NIS2-direktiivin 31 artiklan 1 ja 2 kohdan mukaisesti.

Valvovan viranomaisen tulisi ottaa valvonnan kohdistamisessa ja täytäntöönpanotoimenpiteiden käyttämisestä päätettäessä huomioon ainakin liitteessä I tai II tarkoitetun toiminnan laatu ja laajuus, eli esimerkiksi se, kuinka merkittävä toimija on kyseisellä toimialalla ja millaisia vaikutuksia sen toiminnan häiriintymisellä olisi yhteiskunnassa. Lisäksi valvovan viranomaisen olisi yksittäisiä tietojärjestelmiä tai viestintäverkkoja koskevissa asioissa huomioitava kyseisen tietojärjestelmän tai viestintäverkon merkitys liitteessä I tai II tarkoitetulle toiminnalle. Lain tavoitteiden kannalta sellaisilla tietojärjestelmillä ja viestintäverkoilla, jotka ovat tämän lain liitteissä tarkoitetun toiminnan kannalta keskeisiä, olisi suurempi merkitys kuin sellaisilla tietojärjestelmillä ja viestintäverkoilla, joihin kohdistuva häiriö ei vaikuttaisi liitteissä tarkoitettuun toimintaan. Jos lain soveltamisalaan kuuluvan toimijan toiminnassa on esimerkiksi havaittu puutteita ja toimijan todetaan rikkoneen sille säädettyjä velvoitteita, olisi toimijaan kohdistettavia toimenpiteitä määritettäessä otettava huomioon NIS2-direktiivin 32 artiklan 7 kohdassa säädetyt seikat, muun muassa rikkomisen vakavuus ja kesto, kyseisen toimijan aiemmat rikkomukset, rikkomuksen vaikutukset muihin palveluihin sekä aiheutunut vahinko ja toimenpiteet, joita toimija on toteuttanut vahingon ehkäisemiseksi tai lieventämiseksi.

Pykälän *4 momentissa* säädettäisiin lisäksi valvovan viranomaisen oikeudesta jättää asia tutkimatta, jos kyse on ilmeisen perusteettomasta pyynnöstä. Päätös tutkimatta jättämisestä olisi tehtävä viivytyksettä. Momentti olisi tarpeen esimerkiksi tilanteessa, jossa valvovan viranomaisen toimintaa pyrittäisiin haittaamaan tekemällä sille resursseja kuormittavia perusteettomia ilmoituksia käsiteltäväksi. Momentti olisi kansallinen lisäys täytäntöönpanolle.

Pykälällä täytäntöönpantaisiin NIS2-direktiivin 3 artiklan 1-2 kohdat, 31 artiklan 1-2 kohdat, 32 artiklan 1 kohta ja 33 artiklan 1 kohta.

27 §. *Valvovan viranomaisen tiedonsaantioikeus*. Pykälässä säädettäisiin valvovan viranomaisen tarpeellisista tiedonsaantioikeuksista valvontatehtävän toteuttamiseksi.

Pykälän *1 momentissa* säädettäisiin valvovan viranomaisen oikeudesta saada salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä tässä laissa säädettyjen

tehtäviensä suorittamiseksi välttämättömät tiedot. Tiedonsaantioikeuden käyttäminen olisi ensisijainen ja pääasiallinen toimijoihin kohdistuva toimenpide, jolla valvova viranomainen toteuttaisi valvontaa. Viranomaisella olisi oikeus päästä toimijan hallussa oleviin asiakirjoihin ja tietoihin kuten riskienhallinnan toimintamalliin, sekä saada näyttöä kyberturvallisuusperiaatteiden täytäntöönpanosta, kuten mahdolliset turvallisuusauditointien tulokset ja niiden perustana oleva näyttö, toimijan itse tekemät riskiarvioinnit tai lokitiedot kyberuhkatapahtumista. Tiedonsaantioikeuden avulla viranomainen voisi kartoittaa tiedot tehdystä riskienhallinnan toimintamallista ja sen hyväksymisestä, tiedot johdolle järjestetyistä koulutuksista, tiedot havaituista poikkeamista, kyberuhista ja läheltä piti -tilanteista, tietoja tietoturvan toteutukseen liittyen, tiedot poikkeamien hallinnan toteutuksesta sekä tiedot toiminnan ja palveluiden jatkuvuuden varmistamisesta. Edellytyksenä tiedon pyytämiselle salassapitosäännösten estämättä olisi, että tiedot olisivat välttämättömiä valvontatehtävän suorittamiseksi. Pyytäessään toimijalta säännöksen nojalla tietoja, valvovan viranomaisen olisi ilmoitettava pyynnön tarkoitus sekä täsmennettävä pyydetyt tiedot. Toimijan olisi luovutettava pyydetyt tiedot viipymättä, viranomaisen pyytämässä muodossa ja maksutta.

Jos valvonnan kohteena oleva toimija olisi ulkoistanut osan tai kaikki kyberturvallisuusprosesseistaan ja valvova viranomainen esittäisi toimijalle tietopyynnön, toimija olisi velvollinen toimittamaan tiedon riippumatta siitä, onko tieto toimijan vai ulkoistetun tahon hallussa. Toimija olisi tarvittaessa velvollinen hankkimaan pyydetyt tiedot toimittajaltaan ja toimittamaan ne valvovalle viranomaiselle.

Pykälän *2 momentin* mukaan valvovalla viranomaisella olisi myös salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa tehtäviensä yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto toiselle valvovalle viranomaiselle ja CSIRT-yksikölle, jos se on niille säädettyjen tehtävien hoitamiseksi välttämätöntä. Salassa pidettävän tiedon, kuten tietojärjestelmien turvaamiseen liittyvät tiedon luovuttaminen toiselle valvovalle viranomaiselle voisi olla välttämätöntä esimerkiksi tilanteessa, jossa yhtä toimijaa valvoo useampi kuin yksi viranomainen, ja valvonnan tehokkaaksi tai tarkoituksenmukaiseksi järjestämiseksi olisi voitava vaihtaa toimijaa koskevia tietoja viranomaisten kesken. Salassa pidettävän tiedon luovuttaminen CSIRT-yksikölle voisi olla välttämätöntä esimerkiksi poikkeamatilanteiden selvittämiseksi tai valvottavan toimijan avustamiseksi poikkeaman käsittelyssä. Salassapitovelvoite koskisi myös tiedon vastaanottavaa viranomaista. Edellytyksenä on lisäksi, että tiedon saaminen on laissa säädetyn tehtävän hoitamiseksi välttämätöntä.

Pykälällä täytäntöönpantaisiin NIS2-direktiivin artiklan 32 kohdan 2 ensimmäisen alakohdan e-g alakohdat ja osin d alakohta, artiklan 32 kohta 3 sekä artiklan 33 kohdan 2 ensimmäisen alakohdan c-f alakohdat ja kohta 3.

28 §. *Valvovan viranomaisen tiedonsaantioikeus välitystiedosta, sijaintitiedosta ja haitallisen tietokoneohjelman tai käskyn sisältävästä sähköisestä viestistä.*

Pykälän *1 momentissa* säädettäisiin valvovan viranomaisen tiedonsaantioikeudesta välitystietojen, sijaintitietojen sekä sähköisten viestien osalta. Valvovalla viranomaisella olisi salassapitosäännösten tai muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada tieto välitystiedosta, sijaintitiedosta tai haitallisen tietokoneohjelman tai käskyn sisältävästä sähköisestä viestistä, jos se olisi välttämätöntä kyberturvallisuuden riskienhallintavelvoitteiden noudattamisen valvomista varten tai merkittävän poikkeaman selvittämiseksi. Kyberturvallisuuden riskienhallintavelvoitteesta säädettäisiin 7–9 §:ssä sekä eräiden toimijoiden osalta niistä voitaisiin säätää myös NIS2-direktiivin nojalla annetuissa komission täytäntöönpanoasetuksissa. Li-

säksi kyberturvallisuuden riskienhallintavelvoitteiden sisältöä voitaisiin tarkentaa valvovien viranomaisten määräyksillä. Tiedonsaantioikeus koskisi lisäksi merkittävien poikkeamien selvittämistä. Merkittävällä poikkeamalla tarkoitettaisiin 11 §:n 1 momentissa tarkoitettua merkittävää poikkeamaa. Merkittävän poikkeaman selvittämisellä tarkoitettaisiin merkittävän poikkeaman syiden selvittämistä sekä siitä aiheutuvien haitallisten vaikutusten rajoittamista tai ennalta ehkäisemistä. Laissa säädetty erillinen ja täsmällinen tiedonsaantioikeus näitä tietoja koskien olisi tarpeen viestinnän luottamuksellisuuden suojan edellyttämistä syistä.

Pykälän *2 momentissa* säädettäisiin 1 momentissa tarkoitettujen tietojen salassapidosta, edelleen luovuttamisesta ja hävittämisestä. Sähköisen viestinnän palveluista annetun lain 316 §:n 4 momentissa ja 319 §:ssä säädettyä sovellettaisiin valvovan viranomaisen tämän pykälän nojalla saamiin ja hankkimiin tietoihin. Tiedot olisivat viranomaisessa salassa pidettäviä, eikä niitä saisi luovuttaa kuin laissa säädetyin edellytyksin. Merkittäviin poikkeamiin liittyvien tietojen osalta tietoja olisi välttämättömässä laajuudessa mahdollista luovuttaa sähköisen viestinnän palveluista annetun lain 319 §:n 2 momentin mukaisissa tilanteissa esimerkiksi tahoille, joihin voi kohdistua vastaava tietoturvaloukkaus, jotta uhkaan voidaan ennalta varautua. Viittauksesta seuraisi myös, että valvovan viranomaisen olisi hävitettävä tämän pykälän nojalla saamansa tiedot viesteistä, välitystiedoista ja sijaintitiedoista, kun ne eivät enää ole tarpeen tässä pykälässä tarkoitettujen tehtävien hoitamiseksi.

Pykälällä täytäntöönpantaisiin osin NIS2-direktiivin 32 artiklan 2 kohdan ensimmäisen alakohdan f alakohta sekä 33 artiklan 2 kohdan ensimmäisen alakohdan e alakohta.

29 §. *Tarkastusoikeus*. Pykälässä säädettäisiin valvovan viranomaisen tarkastusoikeudesta. Pykälällä pantaisiin täytäntöön NIS2-direktiivin 32 artiklan 2 kohdan a ja osin d alakohta ja 33 artiklan 2 kohdan a ja osin c alakohta sekä 32 artiklan 4 kohdan g alakohdat.

Pykälän *1 momentin* nojalla valvovalla viranomaisella olisi oikeus tehdä toimijaa koskeva tarkastus laissa tai sen nojalla annetussa määräyksessä taikka NIS2-direktiivin nojalla annetussa säädöksessä asetettujen velvoitteiden noudattamisen valvomiseksi siinä laajuudessa kuin se on tarpeen. Tarkastus voitaisiin tehdä toimijan tiloissa tai tietojärjestelmässä. Tietojärjestelmässä tehtävä tarkastus voisi olla esimerkiksi teknisten riskienhallintakeinojen havainnointia taikka tietokantojen, laitteistojen, palomuurien, salauksen ja verkkojen heikkouksien tunnistamista. Toimijan tiloissa tapahtuva tarkastus voisi kohdistua esimerkiksi pääsynhallintaan ja tilaturvallisuutta koskeviin seikkoihin. Muuta toimijan tiloissa toteutettavaa tarkastusta voisi olla myös kirjallisen aineiston perusteella tapahtuva tarkastaminen, kuten toimijan laatimien toimintakäsikirjojen, ohjeiden, prosessikuvausten, koulutuskirjanpidon, ulkopuolisen tarkastuksen tulosten tai muun relevantin aineiston tarkastaminen ja vaatimustenmukaisuuden arviointi.

Valvovalla viranomaisella olisi riskiarviointinsa perusteella ja valvonnan kohdentamisessa huomioon otettavat seikat huomioiden oikeus määritellä, kuinka tarkastuksia toimijoihin kohdistettaisiin. Tarkastuksessa voisi olla kyse satunnaistarkastuksesta, tarkastuksesta merkittävän poikkeaman jälkeen tai riskiarviointiin perustuvista säännöllisistä tarkastuksista yhteiskunnan toiminnan kannalta kriittisimmille toimijoille. Tarkastustoimivaltuudella katettaisiin myös NIS2-direktiivin 32 artiklan 4 kohdan g alakohdassa tarkoitettu valvonta siitä, että toimija noudattaa riskienhallinta- ja raportointivelvoitteita. Tarkastus voisi kohdistua joko toimijaan kokonaisvaltaisesti tai kohdennetusti riskienhallinnan tai toimijan osa-alueeseen. Tarkastuksen suorittajalla olisi oltava sellainen koulutus ja kokemus kuin tarkastuksen suorittamiseksi on tarpeen.

Pykälän *2 momentissa* säädettäisiin valvovan viranomaisen mahdollisuudesta päätöksellä käyttää apunaan tarkastuksessa taikka pyytää tarkastuksen suorittajaksi toinen valvova viranomai-

nen, tietoturvallisuuden arviointilaitos tai ulkopuolinen tietotekniikan asiantuntija, jos se tarkastuksen laadun tai laajuuden vuoksi olisi tarpeellista. Viranomainen voisi tietoturvallisuuden arviointilaitokselle tai ulkopuoliselle asiantuntijalle osoitetussa toimeksiannossa määritellä, millaista pätevyyttä arviointilaitokselta tai asiantuntijalta edellytetään ja mitä kriteeristöä arviointilaitoksen tai asiantuntijan tulee käyttää. Mahdollisuus siirtää tarkastustehtävä toiselle viranomaiselle tai ulkopuoliselle asiantuntijalle olisi tarpeen tilanteessa, jossa tarkastus edellyttäisi sellaista teknistä erityisosaamista, jota valvovalla viranomaisella ei olisi. Toisella valvovalla viranomaisella ei kuitenkaan olisi velvollisuutta antaa virka-apua tähän tarkoitukseen, vaan kyse olisi hallintolain 10 §:ssä tarkoitetusta viranomaisten yhteistyöstä. Ulkopuolisen asiantuntijan käyttämisessä olisi kyse tältä osin julkisen hallintotehtävän siirtämisestä yksityiselle ja asiantuntijaan tulisi soveltaa, rikoslain virkavastuuta koskevia säännöksiä. Edellä 1 momentissa säädetty vaatimus koulutuksesta ja kokemuksesta soveltuisi myös siirrettäessä tarkastustehtävä toiselle viranomaiselle tai ulkopuoliselle asiantuntijalle. Tarkastuksesta aiheutuvasta kustannuksesta vastaisi tarkastuksen suorittamisesta päättänyt valvova viranomainen.

Pykälän *3 momentissa* säädettäisiin tarkastusta suorittavan tiedonsaantioikeudesta ja oikeudesta päästä tarkastuksen edellyttämässä laajuudessa tarkastuksen kohteena olevaan viestintäverkkoon tai tietojärjestelmään ja tiloihin. Toimijan olisi päästettävä tarkastaja tarkastusta varten tarpeellisiin tiloihin. Tarkastuksen kannalta tarpeelliset tilat riippuvat toiminnan laadusta, ja ne voisivat olla esimerkiksi toimijan toimitiloja, tuotantolaitosten tiloja ja infrastruktuuria, taikka etenkin liikennesektorilla kulkuvälineitä. Tarkastusta ei saisi suorittaa pysyväisluonteiseen asumiseen tarkoitetuissa tiloissa. Tarkastaja voisi tarkastaa yrityksen toimitilojen, tietojärjestelmien ja tietoliikennejärjestelyjen suojaamiseksi toteutetut sekä muut turvallisuusjärjestelyt. Tarkastusta suorittavalla olisi oikeus saada tutkittavakseen valvontatehtävän kannalta välttämättömät tiedot, asiakirjat, laitteet ja ohjelmistot, suorittaa tarvittavia testejä ja mittauksia sekä tarkastaa toimijan toteuttamat turvallisuusjärjestelyt. Tarkastajan olisi voitava suorittaa tarvittavia testejä ja mittauksia, kuten tunkeutumis- tai kuormitustestauksia osana tarkastusta.

Pykälän *4 momentti* olisi aineellinen viittaus hallintolakiin sen tarkastusta koskevan säännöksen soveltumisesta myös pykälässä tarkoitetussa.

30 §. *Turvallisuusauditointi.* Pykälän *1 momentissa* säädettäisiin valvovan viranomaisen oikeudesta päätöksellä velvoittaa toimija teettämään kyberturvallisuuden riskienhallintaan kohdistuva turvallisuusauditointi. Teettämisvelvoite tarkoittaisi toimijalle velvoitetta omalla kustannuksellaan teettää velvoitteen mukainen turvallisuusauditointi. Edellytyksenä olisi, että toimijaan olisi kohdistunut merkittävä poikkeama, joka on aiheuttanut palvelujen vakavan toimintahäiriön tai huomattavaa aineellista tai aineetonta vahinkoa, tai että toimijan olisi havaittu olennaisesti ja vakavasti laiminlyöneen toteuttaa kyberturvallisuuden riskienhallintaa taikka muutoin toimineen olennaisesti ja vakavasti laissa tai sen nojalla taikka NIS 2 –direktiivin nojalla säädetyn velvoitteen vastaisesti. Turvallisuusauditointivelvoitteen asettaminen voisi tulla kyseeseen vain, mikäli sen tavoitetta ei olisi lievemmällä keinoin saavutettavissa.

Pykälän *2 momentissa* säädettäisiin valvovan viranomaisen oikeudesta saada tieto teetetyn turvallisuusauditoinnin tuloksesta. Momentissa säädettäisiin myös valvovan viranomaisen oikeudesta päätöksellä velvoittaa toimija toteuttamaan turvallisuusauditoinnin suosittelemat kohtuulliset ja oikeasuhtaiset toimenpiteet kyberturvallisuuden riskienhallinnan kehittämiseksi.

Pykälällä täytäntöönpantaisiin NIS2-direktiivin 32 artiklan 2 kohdan ensimmäisen alakohdan b alakohta osin, c alakohta, toinen alakohta osin ja kolmas alakohta sekä neljännen alakohdan f alakohta. Pykälällä täytäntöönpantaisiin myös NIS2-direktiivin 33 artiklan 2 kohdan ensimmäisen alakohdan b alakohta, 2 kohdan toinen ja kolmas alakohta ja 4 kohdan f alakohta.

31 §. *Valvontapäätös, huomautus ja varoitus*. Pykälän *1 momentissa* säädettäisiin valvovan viranomaisen toimivallasta antaa toimijalle velvoittava päätös lain, sen nojalla annetun määräyksen tai NIS2-direktiivin nojalla annetun säädöksen vastaisen toiminnan korjaamiseksi. Valvova viranomainen voisi päätöksellä velvoittaa toimijan määräajassa korjaamaan puutteet velvoitteiden noudattamisessa, jos valvonnassa havaittaisiin virheitä, laiminlyöntejä tai muita puutteita tässä laissa, sen nojalla annetuissa määräyksissä tai NIS2-direktiivin nojalla annetuissa säädöksissä säädettyjen velvoitteiden noudattamisessa. Valvova viranomainen voisi esimerkiksi velvoittaa toimijan korjaamaan havaitut puutteet tai laiminlyönnit, lopettamaan sääntelyn vastainen toiminta ja pidättäytymään tästä toiminnasta vastaisuudessa sekä määrätä toimija täyttämään raportointivelvoitteensa määrätyllä tavalla ja määrätyn ajan kuluessa. Valvova viranomainen voisi myös velvoittaa keskeisen toimijan julkistamaan kyseiset puutteet tai muut seikat, jotka liittyvät tämän lain, sen nojalla annettujen määräysten tai NIS2-direktiivin nojalla annettujen säädösten rikkomiseen.

Pykälän *2 momentissa* säädettäisiin varoituksen tai huomautuksen antamisesta. Valvova viranomainen voisi antaa keskeiselle toimijalle myös huomautuksen tai varoituksen. Huomautus tai varoitus olisi seuraamus, joka voisi liittyä korjausvelvoitepäätökseen, mutta myös sellaiseen päätökseen, jolla päätetään valvontaprosessi ilman korjausvelvoitteita.

Pykälällä täytäntöönpantaisiin NIS2-direktiivin 32 artiklan 4 kohdan a-e ja h alakohdat ja 33 artiklan 4 kohdan a-g alakohdat sekä 21 artiklan 4 kohta.

32 §. *Luvanvaraisen tai sertifioidun toiminnan rajoittaminen ja luvan tai sertifioinnin peruuttaminen.* Pykälässä tarkoitettu toiminnan rajoittaminen ja luvan tai sertifioinnin peruuttaminen koskisi vain sellaisia keskeisiä toimijoita, joiden toiminta edellyttää viranomaisen myöntämää lupaa tai sertifiointia. Toimivaltuus ei siten mahdollistaisi esimerkiksi ilmoituksenvaraisen toiminnan rajoittamista tai kieltämistä. Valvova viranomainen voisi rajoittaa tai peruuttaa sellaisen luvan tai sertifioinnin, jonka se on itse myöntänyt. Muiden luvanvaraista tai sertifiointia edellyttävää toimintaa harjoittavien toimijoiden osalta luvan tai sertifioinnin rajoittamisesta säädettäisiin edelleen asianomaista toimintaa koskevassa erityislainsäädännössä. Valvova viranomainen voisi kuitenkin esittää muulle toimivaltaiselle viranomaiselle toiminnan rajoittamista tai luvan taikka sertifioinnin peruuttamista. Toimivalta koskisi vain keskeistä toimijaa.

Valvovan viranomaisen olisi annettava toimijalle huomautus tai varoitus sekä varattava kohtuullinen määräaika puutteen tai laiminlyönnin korjaamiseksi ennen pykälässä tarkoitetun päätöksen tai päätösesityksen tekemistä. Luvanvaraisen tai sertifioidun toiminnan rajoittaminen taikka luvan tai sertifioinnin peruuttaminen olisikin viimesijainen valvontatoimenpide, mitä ennen valvovan viranomaisen olisi käytettävä lievempiä keinoja toimijan toiminnan korjaamiseksi. Luvan peruuttaminen olisi sidottava vakaviin tai olennaisiin rikkomuksiin tai laiminlyönteihin sekä siihen, että luvanhaltijalle mahdollisesti annetut huomautukset tai varoitukset eivät ole johtaneet toiminnassa esiintyneiden puutteiden korjaamiseen. Ehdotuksen luvan peruuttamista koskevat edellytykset on sidottu NIS2-direktiivin soveltamisalaan kuuluvia keskeisiä toimijoita koskeviin keskeisimpiin velvoitteisiin.

Luvanvaraisen tai sertifioidun toiminnan rajoittamisen sekä luvan tai sertifioinnin peruuttamisen edellytyksenä olisi, että toimija on jättänyt olennaisesti ja vakavasti noudattamatta sille asetettuja velvoitteita. Esimerkkinä olennaisesta laiminlyönnistä olisi esimerkiksi se, ettei toimija ole luonut lainkaan 8 §:ssä tarkoitettua kyberturvallisuuden riskienhallinnan toimintamallia tai toteuttanut sen edellyttämiä hallintatoimenpiteitä ollenkaan ja laiminlyönyt viranomaisen kehotuksen tai velvoittavan päätöksen korjaavien toimenpiteiden toteuttamisesta. Olennainen ja vakava velvoitteiden laiminlyönti edellyttäisi myös niin yksilöityä ja yksiselitteistä laiminlyöntiä toimijaan selvästi soveltuvaan velvoitteeseen, ettei sen laadusta olisi tulkinnanvaraisuutta.

Valvovan viranomaisen tulisi harkita, onko lupa tai sertifiointi syytä peruuttaa väliaikaisesti, vai olisiko toiminnan osittainen rajoittaminen riittävä toimenpide. Toiminnan rajoittaminen tulisi olla ensisijainen keino puuttua lainvastaiseen toimintaan, ja etenkin jos kyseessä on sellainen toimija, joka tarjoaa kyseistä palvelua tai infrastruktuuria ainoana Suomessa. Toiminnan rajoittaminen sekä luvan tai sertifioinnin peruuttaminen voitaisiin kuitenkin joka tapauksessa määrätä olemaan voimassa vain toiminnassa esiintyneiden puutteiden tai laiminlyöntien vakavuuteen suhteutetun määräajan. Määräaika voisi olla esimerkiksi muutama kuukausi. Toiminnan rajoittaminen sekä luvan tai sertifioinnin peruuttaminen voisi kuitenkin olla voimassa korkeintaan siihen asti, että tarvittavat toimet puutteen tai laiminlyönnin korjaamiseksi on toteutettu. Jos puutteita ei olisi korjattu määräajan kuluessa, valvova viranomainen voisi päättää tai esittää päätettäväksi myös luvan ehtojen muuttamista toiminnan rajoittamiseksi tai luvan taikka sertifioinnin peruuttamista pysyvästi.

Pykälällä täytäntöönpantaisiin NIS2-direktiivin 32 artiklan 5 kohdan ensimmäisen alakohdan a-alakohta. Toimivaltaa voisi soveltaa vain keskeiseen toimijaan, sillä NIS2-direktiivi ei edellytä vastaavaa valvontatoimivaltaa muuhun kuin keskeiseen toimijaan kohdistuen.

33 §. *Johdon toiminnan rajoittaminen.* Pykälässä säädettäisiin valvovan viranomaisen toimivaltuudesta rajoittaa keskeisen toimijan johdossa toimivien henkilöiden toimintaa, jos nämä toistuvasti ja vakavasti rikkovat ehdotetussa 10 §:ssä säädettyjä velvollisuuksiaan. Kyse olisi yksittäiselle henkilölle määrättävästä määräaikaisesta kiellosta toimia kyseisen yhtiön ylimmissä johtotehtävissä, joihin kuuluisi esimerkiksi hallituksen jäsenet ja varajäsenet, hallintoneuvoston jäsenet ja varajäsenet, toimitusjohtaja tai muu siihen rinnastettava tehtävä sekä toimitusjohtajan välittömään alaisuuteen kuuluvat tehtävät, joissa toimivilla henkilöillä on tosiasiallinen päätösvalta tämän lain noudattamista koskevista kysymyksistä. Tällaiset tehtävät voisivat organisaation rakenteesta riippuen kuulua esimerkiksi talousjohtajalle, operatiiviselle johtajalle, hallintojohtajalle tai muulle vastaavalle ylimmälle johdolle. Pykälä ei kuitenkaan koskisi yksityisiä elinkeinonharjoittajia tai henkilöyhtiöitä, eli avoimia yhtiöitä tai kommandiittiyhtiöitä.

Johdon toiminnan rajoittaminen on ankara seuraamus, ja kiellon määräämisen tulisi olla poikkeuksellista. Valvovan viranomaisen olisi annettava toimijalle huomautus tai varoitus sekä kohtuullinen määräaika lain vastaisen toiminnan korjaamiseksi ennen johdon toiminnan rajoittamista. Toimintakiellon edellytyksenä oleva rikkomusten toistuvuus ja vakavuus, mikä edellyttäisi sitä, että toimijalle olisi jo aiemmin määrätty rikkomuksesta tai laiminlyönnistä hallinnollinen seuraamus tai valvova viranomainen olisi muuten puuttunut toimijan lainvastaiseen tai puutteelliseen toimintaan. Kyse olisi näin ollen viimesijaisesta keinosta estää lainvastaisen menettelyn toistuminen. Valvovan viranomaisen olisi kussakin yksittäistapauksessa arvioitava, onko toimintakielto tarkoituksenmukaisin valvontatoimenpide.

Johdon toiminnan rajoittaminen ehdotetun pykälän nojalla ei kuitenkaan olisi mahdollista, jos keskeinen toimija on julkishallinnon toimija.

Pykälällä täytäntöönpantaisiin NIS2-direktiivin 32 artiklan 5 kohdan b alakohta. Toimivaltaa voisi soveltaa vain keskeiseen toimijaan, sillä NIS2-direktiivi ei edellytä vastaavaa valvontatoimivaltaa muuhun kuin keskeiseen toimijaan kohdistuen.

34 §. *Ilmoitus tietosuojavaltuutetulle.* NIS2-direktiivi ei rajoita yleisen tietosuoja-asetuksen soveltamista. Valvovan viranomaisen olisikin ilmoitettava tietosuojavaltuutetulle, jos se valvonnan tai täytäntöönpanon yhteydessä havaitsee sellaisen laiminlyönnin, joka voisi johtaa tai on jo johtanut sellaiseen henkilötietojen tietoturvaloukkaukseen, josta on ilmoitettava tietosuojavaltuutetulle yleisen tietosuoja-asetuksen nojalla.

Yleisen tietosuoja-asetuksen 33 artiklan mukaista ilmoitusvelvollisuutta ei sovelleta yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoamisen yhteydessä tapahtuneisiin henkilötietojen tietoturvaloukkauksiin, koska sen sijasta sovelletaan erityislainsäädäntöä (Tietosuojaneuvoston lausunto 5/2019 sähköisen viestinnän tietosuojadirektiivin ja yleisen tietosuojaasetuksen vuorovaikutuksesta erityisesti tietosuojaviranomaisten toimivallan, tehtävien ja valtuuksien osalta, k. 44). Yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat ilmoittavat palveluun kohdistuvista tietoturvaloukkauksista Liikenne- ja viestintävirastolle sähköisen viestinnän palveluista annetun lain 275 §:n ja henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annetun Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY mukaisten henkilötietojen tietoturvaloukkausten ilmoittamiseen sovellettavista toimenpiteistä annetun komission asetuksen 611/2013 mukaisesti. Näin ollen pykälässä säädetty velvollisuus ei kuitenkaan koskisi Liikenne- ja viestintäviraston tietoon tulleita teletoimintaa koskevia henkilötietojen tietoturvaloukkauksia, jotka se käsittelisi sähköisen viestinnän tietosuojadirektiivin mukaisena toimivaltaisena viranomaisena.

Pykälällä täytäntöönpantaisiin NIS2-direktiivin 35 artiklan 1 ja 3 kohdat.

35 §. *Uhkasakko, teettämisuhka ja keskeyttämisuhka.* Pykälässä säädettäisiin valvovan viranomaisen mahdollisuudesta asettaa antamansa päätöksen tehosteeksi uhkasakko, teettämisuhka tai keskeyttämisuhka. Hallinnollisen tehosteen asettamisesta ja täytäntöönpanosta säädetään uhkasakkolaissa, jota sovellettaisiin tehosteeseen.

36 §. *Oikaisuvaatimus*. Pykälässä säädettäisiin siitä, miten valvovan viranomaisen päätöksiin vaadittaisiin oikaisua. Oikaisua saisi vaatia vain valvovan viranomaisen tämän lain 30-33 §:n nojalla tehtyihin päätöksiin. Oikaisusta säädetään hallintolaissa. Valvovan viranomaisen oikaisuvaatimuksen johdosta antamiin päätöksiin voisi hakea muutosta siten kuin oikeudenkäynnistä hallintoasioissa annetussa laissa on säädetty. Pykälän 2 momentin nojalla viranomainen voisi kuitenkin määrätä, että viranomaisen päätöstä olisi noudatettava lainvoimaa vailla, ellei muutoksenhakuviranomainen toisin määrää.

37 §. *Hallinnollinen seuraamusmaksu*. Pykälässä säädettäisiin hallinnollisesta seuraamusmaksusta. Seuraamusmaksu olisi lain rikkomisesta määrättävä hallinnollinen sanktio, jonka määräämisessä noudatettaisiin hallintolain säännöksiä hallintoasian käsittelystä. Seuraamusmaksun määräisi sektorikohtaisista valvovista viranomaisista koostuva seuraamusmaksulautakunta. Pykälällä pantaisiin täytäntöön NIS2-direktiivin 34 artikla muiden 5 luvun säännösten kanssa.

Pykälän *1 momentissa* määriteltäisiin teot, joista hallinnollinen seuraamusmaksu voitaisiin määrätä toimijalle. Seuraamusmaksu voitaisiin määrätä riskienhallintavelvoitteen laiminlyönnistä, riskienhallintatoimenpiteiden toteuttamisen laiminlyönnistä, velvoittavien poikkeamailmoitusten ja -raporttien tekemisen laiminlyönnistä tai toimijaluetteloon ilmoittautumisen laiminlyönnistä.

Pykälän *2 momentissa* säädettäisiin, ettei hallinnollista seuraamusmaksua voitaisi määrätä valtion viranomaisille, valtion liikelaitoksille, kunnallisille viranomaisille, itsenäisille julkisoikeudellisille laitoksille, eduskunnan virastoille, tasavallan presidentin kanslialle eikä Suomen evankelisluterilaiselle kirkolle ja Suomen ortodoksiselle kirkolle eikä niiden seurakunnille, seurakuntayhtymille ja muille elimille. Momentilla käytettäisiin NIS2-direktiivin 34 artiklan 7 kohdan mukaista kansallista liikkumavaraa siitä, ettei julkishallinnon toimijoille määrätä direktiivin edellyttämiä hallinnollisia sanktioita.

38 §. *Seuraamusmaksulautakunta*. Pykälässä säädettäisiin seuraamusmaksulautakunnasta, joka määräisi hallinnollisen seuraamusmaksun. Seuraamusmaksulautakunta olisi uusi elin, joka

koostuisi valvovien viranomaisten nimeämistä jäsenistä. Seuraamusmaksulautakunta ei olisi päätoiminen, vaan se kokoontuisi tarvittaessa seuraamusmaksun määräämistä koskevan asian käsittelemiseksi. Seuraamusmaksu määrättäisiin sektorikohtaisen valvovan viranomaisen esityksestä.

Pykälän *1 momentissa* säädettäisiin siitä, että hallinnollisen seuraamusmaksun määräisi seuraamusmaksulautakunta valvovan viranomaisen esityksestä. Valvova viranomainen voisi esittää seuraamusmaksulautakunnalle hallinnollisen seuraamusmaksun määräämistä, jos se havaitsisi valvontatoiminnassa lain vastaista menettelyä. Valvovan viranomaisen tehtävänä olisi huolehtia asian riittävästä selvittämisestä valvontatoiminnassa siten, että esitys seuraamusmaksun määräämisestä voidaan tehdä siten, että esityksessä on selvitys sen perusteena olevasta rikkomuksesta tai laiminlyönnistä. Hallinnollinen seuraamusmaksu määrättäisiin maksettavaksi valtiolle.

Pykälän *2 momentissa* säädettäisiin seuraamusmaksulautakunnan kokoonpanosta. Lautakunta koostuisi kunkin valvovan viranomaisen nimeämästä jäsenestä ja varajäsenestä. Liikenne- ja viestintävirasto nimeäisi lautakunnan puheenjohtajan ja varapuheenjohtajan. Seuraamusmaksulautakunnan jäsenen ja varajäsenen yleisenä kelpoisuusehtona olisi perehtyneisyys kyberturvallisuuden riskienhallintaan sekä NIS2-direktiivin ja sitä täytäntöönpanevan lainsäädännön asettamiin velvoitteisiin kyseisen valvovan viranomaisen valvontatoimialalla. Lautakunnan puheenjohtajalta ja varapuheenjohtajalta edellytettäisiin tehtävän edellyttämää riittävää oikeudellista asiantuntemusta. Lautakunta nimettäisiin kolmen vuoden määräajaksi. Lautakunnan jäsen toimisi tehtävässään riippumattomasti ja puolueettomasti. Lautakunnan tehtävä olisi jäsenelle tai varajäsenelle sivutoiminen.

Pykälän *3 momentissa* säädettäisiin seuraamusmaksulautakunnan päätöksenteosta. Päätös tehtäisiin esittelystä. Käsiteltävänä olevasta asiasta riippuen esittelijä tulisi valvovasta viranomaisesta. Esittelijänä toimisi virkamies siitä valvovasta viranomaisesta, jonka valvottavana olevaan toimijatyyppiin kohdistuva asia olisi ratkaistavana. Päätökseksi tulisi se kanta, jota enemmistö on kannattanut. Äänten mennessä tasan päätökseksi tulisi se kanta, joka on lievempi sille, johon seuraamus kohdistuu.

Pykälän *4 momentissa* säädettäisiin seuraamusmaksulautakunnan tietojensaantioikeudesta. Lautakunnalla olisi oikeus saada salassapitosäännösten estämättä maksutta tehtäviensä hoidon kannalta välttämättömät tiedot. Lautakunnalla olisi voitava hankkia tieto asiaan vaikuttavista seikoista seuraamusmaksun määräämiseksi tai määräämättä jättämiseksi.

39 §. *Seuraamusmaksun määrääminen*. Pykälässä säädettäisiin seikoista, jotka olisi otettava huomioon hallinnollisen seuraamusmaksun määräämisessä. Hallinnollisen seuraamusmaksun määrä perustuisi kokonaisarviointiin, jossa olisi huomioitava tapauksen olosuhteet sekä säännöksessä kuvatut seikat. Huomioitavat seikat vastaisivat NIS2-direktiivin 32 artiklan 7 kohdassa säädettyjä seikkoja, jotka on otettava huomioon myös toimijaan kohdistuvia valvontatoimenpiteitä arvioitaessa.

Harkitessa seuraamusmaksun suuruutta tulisi varmistaa, että sanktio ja sen määrä ovat oikeassa suhteessa tekoon tai laiminlyöntiin ja siitä aiheutuvan riskin vakavuuteen ja toteutumisen todennäköisyyteen nähden. Kokonaisarvioinnissa olisi otettava huomioon siten rikkomuksen tai laiminlyönnin laatu ja laajuus, moitittavuuden aste, kesto ja toimijan pyrkimykset toimia omaaloitteisesti sille säädetyn velvollisuuden mukaisesti. Rikkomuksen tai laiminlyönnin moitittavuutta olisi arvioitava erityisesti niiden oikeushyvien näkökulmasta, joita tällä lailla ja NIS2-direktiivillä pyritään suojaamaan.

Säännöksellä pantaisiin täytäntöön NIS2-direktiivin 34 artiklan 3 kohta, joka edellyttää NIS2-direktiivin 32 artiklan 7 kohdassa tarkoitettujen seikkojen huomioimista hallinnollisen seuraamusmaksun määräämisessä.

40 §. *Seuraamusmaksun enimmäismäärä*. Pykälässä säädettäisiin hallinnollisen seuraamusmaksun enimmäismääristä. Hallinnollisen seuraamusmaksun enimmäismäärä olisi matalin sallittu enimmäismäärä NIS2-direktiivin 34 artiklan 4 ja 5 kohtien edellyttämällä tasolla. Enimmäismäärä olisi joko euromääräinen tai %-osuus liikevaihdosta sen mukaan, kumpi määristä on suurempi. Enimmäismäärä keskeiselle toimijalle olisi suurempi kuin muille toimijoille. Keskeisellä toimijalla tarkoitettaisiin keskeistä toimijaa 26 §:n 2 momentin mukaisesti.

41 §. *Seuraamusmaksun määräämättä jättäminen ja täytäntöönpano*. Pykälässä säädettäisiin seuraamusmaksun määräämättä jättämisestä ja täytäntöönpanosta.

Pykälän *1 momentin* mukaan seuraamusmaksu jätettäisiin määräämättä, jos:

1) toimija on oma-aloitteisesti ryhtynyt riittäviin toimenpiteisiin rikkomuksen tai laiminlyönnin korjaamiseksi välittömästi sen havaitsemisen jälkeen ja ilmoittanut siitä viivytyksettä valvovalle viranomaiselle sekä toiminut yhteistyössä valvovan viranomaisen kanssa eikä rikkomus tai laiminlyönti ole vakava tai toistuva;

2) rikkomusta tai laiminlyöntiä on pidettävä vähäisenä; tai

3) seuraamusmaksun määräämistä on pidettävä ilmeisen kohtuuttomana muutoin kuin 1 tai 2 kohdassa tarkoitetulla perusteella.

Perustuslakivaliokunta on käytännössään edellyttänyt, että viranomaisen harkinnan sanktion määräämättä jättämisestä tulee olla sidottua harkintaa siten, että seuraamusmaksu on jätettävä määräämättä laissa säädettyjen edellytysten täyttyessä (ks. PeVL 49/2017 vp ja PeVL 39/2017 vp.)

Säännöksen tarkoituksena olisi varmistaa, että seuraamusmaksua ei siis määrättäisi niissä tilanteissa, joissa se olisi kohtuutonta joko 1 momentin 1 tai 2 kohdassa tarkoitettujen seikkojen perusteella tai muutoin jonkin vastaavan seikan tai seikkojen perusteella ilmeisen kohtuutonta.

Pykälän *2 momentissa* säädettäisiin seuraamusmaksun määräämisoikeuden vanhentumisesta. Seuraamusmaksua ei saisi määrätä, jos on kulunut yli viisi vuotta siitä, kun rikkomus tai laiminlyönti on tapahtunut. Jos rikkomus tai laiminlyönti on ollut luonteeltaan jatkuvaa, määräaika lasketaan siitä, kun rikkomus tai laiminlyönti on päättynyt.

Pykälän *3 momentissa* säädettäisiin, että seuraamusmaksua ei voida määrätä sille, jota epäillään samasta teosta esitutkinnassa, syyteharkinnassa tai tuomioistuimessa vireillä olevassa rikosasiassa. Seuraamusmaksua ei voitaisi määrätä myöskään sille, jolle on samasta teosta annettu lainvoimainen tuomio. Säännös vastaisi niin sanottua ne bis in idem –periaatetta eli kaksoisrangaistavuuden kieltoa.

Pykälän *4 momentissa* säädettäisiin, että seuraamusmaksua ei voida määrätä, jos rikkomuksessa tai laiminlyönnissä on kyse samasta teosta, josta on määrätty yleisen tietosuoja-asetuksen 83 artiklassa tarkoitettu seuraamusmaksu. Momentilla pantaisiin täytäntöön NIS2-direktiivin 35 artiklan 2 kohta. Kyse voisi olla esimerkiksi puutteista tarpeellisten riskienhallintatoimenpiteiden tunnistamisessa tai niiden toteuttamisessa taikka henkilötietojen käsittelemisestä ja säilyt-

tämisestä muutoin yleisen tietosuoja-asetuksen 5 artiklan vastaisesti, minkä johdosta aiheutuneesta henkilötietojen loukkauksesta yleisen tietosuoja-asetuksen nojalla toimivaltainen viranomainen määräisi yleisen tietosuoja-asetuksen 83 artiklassa tarkoitetun seuraamusmaksun.

Pykälän *5 momentissa* säädettäisiin seuraamusmaksun täytäntöönpanosta. Seuraamusmaksun täytäntöönpanosta huolehtisi Oikeusrekisterikeskus. Lain nojalla maksettavaksi määrätty seuraamusmaksu pannaan täytäntöön siinä järjestyksessä kuin sakon täytäntöönpanosta annetussa laissa (672/2002) säädetään. Seuraamusmaksu vanhenisi viiden vuoden kuluttua siitä, kun sen määräämistä koskeva päätös on saanut lainvoiman.

42 §. *Muutoksenhaku*. Hallinnollista seuraamusmaksua koskevaan päätökseen olisi oikeus hakea muutosta oikeudenkäynnistä hallintoasioissa annetussa laissa säädetyssä järjestyksessä.

43 §. *Toimijaluettelo.* Ehdotuksella pantaisiin täytäntöön NIS2-direktiivin 3 artiklan 3–6 kohdat, jotka edellyttävät jäsenvaltiota ylläpitämään luetteloa keskeisistä ja tärkeistä toimijoista. Verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden vastaavasta velvoitteesta säädettäisiin sähköisen viestinnän palveluista annetun lain 165 §:ssä. Lisäksi ehdotuksella pantaisiin täytäntöön NIS2-direktiivin 27 artikla, joka edellyttää eräiden toimijoiden osalta tarkempien tietojen keräämistä ja ilmoittamista ENISA:lle sen perustamaa rekisteriä varten, sekä NIS2-direktiivin 29 artiklan 4 kohta, joka edellyttää ilmoitusta valvovalle viranomaiselle osallistumisesta 22 §:ssä tarkoitettuun kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn.

Ehdotetussa *1 momentissa* säädettäisiin toimijoiden velvollisuudesta ilmoittaa toimijaluetteloa varten valvovalle viranomaiselle NIS2-direktiivin 3 artiklan 4 kohdassa tarkoitetut tiedot. Lisäksi valvonnan kohdistamista varten edellytettäisiin ilmoittamaan siitä, onko toimija 26 §:ssä tarkoitettu keskeinen toimija. Valvovalle viranomaiselle olisi ilmoitettava myös NIS2-direktiivin 29 artiklan 4 kohdan johdosta osallistumisesta 22 §:ssä tarkoitettuun kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn. Tietojen ilmoittamisessa ja toimijaluettelon pitämisessä voitaisiin ottaa huomioon Euroopan komission tai Euroopan unionin kyberturvallisuusvirasto ENISA:n antamat ohjeet ja mallit.

Ehdotetussa *2 momentissa* säädettäisiin DNS-palveluntarjoajien, aluetunnusrekisterien, pilvipalvelujen tarjoajien, datakeskuspalvelujen tarjoajien, sisällönjakeluverkkojen tarjoajien, hallintapalvelun tarjoajien, tietoturvapalveluntarjoajien sekä verkossa toimivien markkinapaikkojen tarjoajien, verkossa toimivien hakukoneiden tarjoajien ja verkkoyhteisöalustojen tarjoajien osalta 1 momenttia täydentävästä ilmoitusvelvollisuudesta. Näitä toimijoita edellytettäisiin ilmoittamaan lisäksi NIS2-direktiivin 27 artiklan 2 kohdassa tarkoitetut tiedot.

Ehdotetun *3 momentin nojalla* valvova viranomainen voisi antaa tarkempia teknisiä määräyksiä tietojen ilmoittamisesta toimijaluetteloon. Toimijaluettelon laatimisen ja ylläpitämisen helpottamiseksi valvovan viranomaisen olisi tarjottava, jos mahdollista, toimijalle mahdollisuus itse sekä rekisteröityä että päivittää tietoja luettelossa. Lisäksi momentissa säädettäisiin NIS2-direktiivin 3 ja 27 artikloissa säädettyjä enimmäisaikoja vastaavasti, että muutoksista 1 momentissa tarkoitettuihin tietoihin olisi ilmoitettava enintään kahden viikon kuluessa ja 2 momentissa tarkoitettuihin tietoihin enintään kolmen kuukauden kuluessa muutoksesta.

Ehdotetussa *4 momentissa* säädettäisiin NIS2-direktiivin 3 artiklan edellyttämän toimijaluettelon ylläpitämisestä, 3 artiklan 5 kohdassa tarkoitettujen ilmoituksien tekemisestä Euroopan komissiolle ja NIS-yhteistyöryhmälle sekä 27 artiklan 4 kohdassa tarkoitetusta tietojen toimittamisesta ENISA:lle.

NIS2-direktiivin 3 artiklan 5 kohdan nojalla valvovien viranomaisten olisi ilmoitettava viimeistään 17.4.2025 ja sen jälkeen kahden vuoden välein keskeisten toimijoiden lukumäärä kullakin toimialalla ja toimialan osalla komissiolle ja NIS-yhteistyöryhmälle. Lisäksi komissiolle olisi ilmoitettava tiedot NIS2-direktiivin 2 artiklan 2 kohdan b–e alakohdan nojalla lain soveltamisalaan kuuluvista toimijoista tieto toimijoiden lukumäärästä, liitteessä I tai II tarkoitetusta toimialasta ja toimialan osasta, tarjotun palvelun tyypistä sekä siitä, minkä alakohdan nojalla ne kuuluvat soveltamisalaan.

NIS2-direktiivin 27 artiklan 4 kohdan nojalla keskitetyn yhteyspisteen olisi toimitettava 27 artiklan 2 ja 3 kohdassa tarkoitetut tiedot – poislukien 2 kohdan f alakohdassa tarkoitetut tiedot eli toimijan IP-osoitealueet – ilman aiheetonta viivytystä ENISA:lle. Tämän ilmoituksen tekemistä varten valvovalla viranomaisella olisi oikeus toimittaa kansalliselle yhteyspisteelle ilmoituksen tekemiseksi tarpeelliset tiedot, eli 27 artiklan 2 ja 3 kohdassa tarkoitetut tiedot IP-osoitealueet poislukien.

44 §. *Kansallinen kyberturvallisuusstrategia*. Pykälässä säädettäisiin kansallisen kyberturvallisuusstrategian laatimisesta, päivittämisestä, vähimmäissisällöstä ja Euroopan komissiolle tehtävästä tiedoksiannosta. Ehdotuksella pantaisiin täytäntöön NIS2-direktiivin 7 artikla.

Kansallisella kyberturvallisuusstrategialla tarkoitetaan NIS2-direktiivin 6 artiklan 4 kohdan nojalla yhtenäistä kehystä, jossa määritellään kyberturvallisuusalan strategiset tavoitteet ja painopisteet sekä hallintotapa niiden saavuttamiseksi kansallisesti. NIS2-direktiivin 7 artiklan 1 kohdan mukaisesti kansallisessa kyberturvallisuusstrategiassa olisi määritettävä strategiset tavoitteet, tavoitteiden saavuttamiseksi tarvittavat resurssit sekä asianmukaiset politiikka- ja sääntelytoimenpiteet kyberturvallisuuden korkean tason saavuttamiseksi ja ylläpitämiseksi.

Kansallisen kyberturvallisuusstrategiaan olisi sisällytettävä vähintään NIS2-direktiivin 7 artiklan 1 ja 2 kohdissa tarkoitetut seikat. Kansallista kyberturvallisuusstrategiaa olisi arvioitava säännöllisesti ja vähintään viiden vuoden välein. Tarvittaessa strategia olisi ajantasaistettava keskeisten suorituskykyindikaattorien perusteella NIS2-direktiivin 7 artiklan 4 kohdan mukaisesti. Kansallisen kyberturvallisuusstrategian ja sen arvioinnissa käytettävien keskeisten suorituskykyindikaattorien kehittämisessä tai ajantasaistamisessa voisi pyynnöstä saada tukea Euroopan unionin kyberturvallisuusvirasto ENISA:lta.

Kansallinen kyberturvallisuusstrategia voisi olla itsenäinen strategia tai osa toista asiakirjaa, strategiaa tai valtioneuvoston periaatepäätöstä. Ehdotuksessa ei siten säädettäisi tai rajattaisi strategian muotoa. Kansallisen kyberturvallisuusstrategian hyväksymisestä, päivittämisestä ja tiedoksiannosta Euroopan komissiolle vastaisi valtioneuvosto.

Kansallinen kyberturvallisuusstrategia olisi annettava NIS2-direktiivin 7 artiklan 3 kohdan mukaisesti tiedoksi Euroopan komissiolle kolmen kuukauden kuluessa sen hyväksymisestä. Tiedoksiannon ulkopuolelle voitaisiin jättää tiedot, joiden luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta tai olisi vastoin siihen liittyvää tärkeää etua. Kansallisen kyberturvallisuusstrategian julkisuus muilta osin määräytyisi julkisuuslain mukaan.

45§. *Laajamittaisten kyberturvallisuuspoikkeamien ja –kriisien hallintasuunnitelma.* Pykälässä säädettäisiin kansallisen laajamittaisten kyberturvallisuuspoikkeamien ja –kriisien hallintasuunnitelman laatimisesta sekä kyberkriisinhallintaviranomaisesta. Ehdotuksella pantaisiin täytäntöön NIS2-direktiivin 9 artikla.

Pykälän *1 momentissa* säädettäisiin NIS2-direktiivin 9 artiklassa tarkoitetun kansallisen laajamittaisten kyberturvallisuuspoikkeamien ja –kriisien hallintasuunnitelman laatimisesta, josta

vastaisi Liikenne- ja viestintävirasto. Suunnitelma olisi laadittava yhteistoiminnassa 25 §:ssä tarkoitettujen valvovien viranomaisten, poliisihallituksen, suojelupoliisin, Puolustusvoimien ja huoltovarmuuskeskuksen kanssa. Suunnitelman laatimiseen voisi osallistua tarpeen mukaan myös muita viranomaistahoja. Laajamittaisella kyberturvallisuuspoikkeamalla tarkoitettaisiin poikkeamaa, joka aiheuttaa niin laajan häiriön, ettei Suomella yksin ole valmiuksia hallita sitä, tai jolla on merkittävä vaikutus myös toiseen EU-jäsenvaltioon.

Pykälän *2 momentissa* säädettäisiin suunnitelmaan sisällytettävistä tiedoista. Suunnitelmaan olisi sisällytettävä NIS2-direktiivin 9 artiklassa säädetyt tiedot. Säännöksen tarkoituksena ei olisi rajata, mitä tietoja suunnitelmaan voidaan sisällyttää. Lisäksi 2 momentissa säädettäisiin NIS2-direktiivin 9 artiklassa tarkoitetusta kyberkriisinhallintaviranomaisesta. Suomessa NIS2-direktiivin 9 artiklan 1 kohdan tarkoittamana kyberkriisinhallintaviranomaisena toimisi kukin viranomainen sille erikseen laissa säädettyjen tehtävien mukaisesti. Näitä viranomaisia olisivat tässä laissa tarkoitetut valvovat viranomaiset, poliisi, suojelupoliisi, Puolustusvoimat ja Liikenne- ja viestintävirasto. Kyberkriisinhallintaviranomaisten välisenä koordinaattorina toimisi Liikenne- ja viestintäviraston Kyberturvallisuuskeskus. Kyberkriisinhallintaviranomaisten tehtäviä, vastuita ja yhteistoimintaa täsmennettäisiin suunnitelmassa.

Pykälän *3 momentissa* säädettäisiin kansallinen laajamittainen kyberkriisinhallintasuunnitelmaa koskevasta tiedonantovelvollisuudesta. Tieto suunnitelmasta olisi annettava NIS2-direktiivin 9 artiklan 5 kohdan mukaisesti asiaankuuluvia tietoja Euroopan komissiolle ja Euroopan kyberkriisien yhteysorganisaatioiden verkostolle (EU-CyCLONe) kolmen kuukauden kuluessa sen hyväksymisestä. Tiedoksiannon ulkopuolelle voitaisiin jättää suunnitelman osat tai tiedot, joista tiedon antaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta tai olisi vastoin siihen liittyvää tärkeää etua. Kansallisen kyberkriisinhallintasuunnitelman julkisuus muilta osin määräytyisi julkisuuslain mukaan.

46 §. *Viranomaisten yhteistyö.* Pykälässä olisi erityissäännöksiä viranomaisten välisestä yhteistyöstä. Tiedonvaihto ei itsessään perustaisi oikeutta poiketa salassapitosäännöksistä sitä toteutettaessa. Tarpeellisen yhteistyön laajuuden määrittämisessä painoarvo olisi annettava NIS2-direktiivin 13 artiklan ja sen tavoitteiden tulkinnalle. Pykälällä pantaisiin täytäntöön NIS2-direktiivin 13 artiklan 1, 4 ja 5 kohdat, 32 artiklan 9 ja 10 kohdat ja 33 artiklan 6 kohta.

Pykälän *1 momentissa* säädettäisiin valvovan viranomaisen ja CSIRT-yksikön velvollisuudesta tehdä yhteistyötä tämän lain ja NIS2-direktiivin mukaisten tehtävien toteuttamisessa. Momentilla pantaisiin täytäntöön NIS2-direktiivin 13 artiklan 1 kohta yhdessä voimassa olevan hallintolain 10 §:n kanssa.

Pykälän *2 momentissa* säädettäisiin valvova viranomaisten, CSIRT-yksikön ja keskitetyn yhteyspisteen velvollisuudesta tehdä tarvittaessa yhteistyötä poliisin tai muun esitutkintaviranomaisen, tietosuojavaltuutetun, siviili-ilmailun turvallisuudesta vastaavan viranomaisen, eIDAS-asetuksen mukaisten valvontaelinten, DORA-asetuksen mukaisen toimivaltaisen viranomaisen, teledirektiivin mukaisen kansallisen sääntelyviranomaisen ja CER-direktiivin mukaisen toimivaltaisen viranomaisen kanssa. Momentilla pantaisiin täytäntöön NIS2-direktiivin 13 artiklan 4 kohta yhdessä voimassa olevan hallintolain 10 §:n kanssa. Valvovien viranomaisten, CSIRT-yksikön ja keskitetyn yhteyspisteen olisi tarvittaessa tehtävä yhteistyötä myös muiden viranomaisten, kuten Puolustusvoimien ja suojelupoliisin kanssa siten, kuin hallintolain 10 §:ssä on säädetty.

Pykälän *3 momentissa* olisi erityissäännös valvovan viranomaisen ja CER-direktiivin mukaisen toimivaltaisen viranomaisen yhteistyöstä.

Valvovan viranomaisen ja CER-direktiivin mukaisen toimivaltaisen viranomaisen tulisi vaihtaa säännöllisesti tietoja kriittisten toimijoiden määrittämisestä sekä riskeistä, kyberuhkista ja poikkeamista ja muista kuin kyberturvallisuuteen liittyvistä riskeistä, uhkista ja poikkeamista, jotka vaikuttavat CER-direktiivin nojalla kriittisiksi toimijoiksi määriteltyihin toimijoihin, sekä näiden riskien, uhkien ja poikkeamien hallintatoimenpiteistä.

Valvovien viranomaisten olisi ilmoitettava CER-direktiivin mukaiselle toimivaltaiselle viranomaiselle, kun se käyttää 4 luvussa säädettyjä toimivaltuuksia CER-direktiivin nojalla kriittiseksi tunnistettuun toimijaan. Lisäksi valvova viranomainen voisi CER-direktiivin mukaisen toimivaltaisen viranomaisen perustellusta pyynnöstä kohdistaa 4 luvussa säädettyjä toimivaltuuksia CER-direktiivin nojalla kriittiseksi tunnistettuun toimijaan.

Momentilla täytäntöönpantaisiin NIS2-direktiivin 13 artiklan 5 kohta osin ja 32 artiklan 9 kohta.

Pykälän *4 momentissa* säädettäisiin valvovan viranomaisen velvollisuudesta ilmoittaa DORA-asetuksen 32 artiklan 1 kohdan nojalla perustetulle valvontafoorumille, kun se käyttää valvonta- ja täytäntöönpanovaltuuksia toimijaan, joka on nimetty kriittiseksi TVT-palveluntarjoajana olevaksi kolmanneksi osapuoleksi DORA-asetuksen 31 artiklan nojalla. Momentilla pantaisiin täytäntöön NIS2-direktiivin 32 artiklan 10 kohta ja 33 artiklan 6 kohta.

Pykälän *5 momentissa* säädettäisiin valvovien viranomaisten, eIDAS-asetuksen mukaisten valvontaelinten, DORA-asetuksen toimivaltaisen viranomaisen ja teledirektiivin mukaisen kansallisen sääntelyviranomaisen velvollisuudesta vaihtaa keskenään säännöllisesti tietoja merkittävistä poikkeamista ja kyberuhkista. Momentilla täytäntöönpantaisiin NIS2-direktiivin 13 artiklan 5 kohta osin.

47 §. *Voimaantulo.* Lain voimaantulo esitetään NIS2-direktiivin 41 artiklassa säädetyn kansallisen täytäntöönpanon määräaikaa vastaavasti 18. päiväksi lokakuuta 2024.

Lain 43 § koskien toimijoiden velvoitetta ilmoittaa tietoja valvovalle viranomaiselle ehdotetaan kuitenkin tulevaksi voimaan vasta 1.1.2025 alkaen, mikä antaisi toimijoille ja valvoville viranomaisille siirtymäaikaa toimijaluettelon muodostamisen ja siihen tietojen ilmoittamisen osalta. NIS2-direktiivi ei edellytä ilmoitettavien tietojen perusteella Euroopan komissiolle tehtävien ilmoituksien tekemistä ennen vuotta 2025.

7.2 Laki julkisen hallinnon tiedonhallinnasta annetun lain muuttamisesta

1 §. *Lain tarkoitus.* Pykälään ehdotetaan lisättäväksi uusi *2 momentti*, jossa todettaisiin, että lailla pannaan julkishallinnon toimialalla täytäntöön NIS2-direktiivi. Momentissa myös määriteltäisiin NIS2-direktiivi. Direktiivissä säädetyistä kyberturvallisuuteen liittyvistä velvoitteista ja niiden noudattamisen valvonnasta julkishallinnon toimialalla säädettäisiin uudessa 4 a luvussa. Lisäksi ehdotettuun 2 momenttiin sisältyisi informatiivinen viittaus ehdotettuun lakiin kyberturvallisuuden riskienhallinnasta eli NIS2-direktiivin täytäntöönpanon yleislakiin. Aineellinen viittaus mainittuun lakiin sisältyisi ehdotettuun 18 h §:ään, jossa säädettäisiin Liikenne- ja viestintäviraston tehtävistä.

2 §. *Määritelmät*. Pykälään lisättäisiin NIS2-direktiivin täytäntöönpanon edellyttämät, ehdotetussa uudessa 4 a luvussa käytetyt määritelmät eli uudet kohdat 17 - 26, joista muut kuin merkittävän poikkeaman määritelmä sisältyvät direktiivin 6 artiklaan. Merkittävä poikkeama on määritelty direktiivin 23 artiklan 3 kohdassa.

Tiedonhallintalakiin ehdotetut uudet määritelmät vastaavat sisällöltään ehdotetun kyberturvallisuuden riskienhallintaa koskevan lain 2 §:n vastaavia määritelmiä, joiden säännöskohtaisissa perusteluissa on perusteltu myös muutaman määritelmän muotoilun muutokset suhteessa direktiiviin. Tiedonhallintalain määritelmissä käytetään toimijan sijaan viranomaisen käsitettä, koska tiedonhallintalaissa säädetyt julkishallinnon toimialan toimijat ovat viranomaisia.

Ehdotetussa *21 kohdassa* määriteltyä merkittävää kyberuhkaa ei ole määritelty ehdotetussa kyberturvallisuuden riskienhallintaa koskevassa laissa. Merkittävällä kyberuhkalla tarkoitettaisiin kyberuhkaa, jonka voidaan sen teknisten ominaisuuksien perusteella olettaa vaikuttavan mahdollisesti vakavasti viranomaisen verkko- ja tietojärjestelmiin tai sen palvelujen käyttäjiin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa.

Ehdotetussa *25 kohdassa* määritelty merkittävä poikkeama on määritelty ehdotetun kyberturvallisuuden riskienhallintaa koskevan lain 11 §:n 1 momentissa.

Koska pykälään ehdotetaan lisättäväksi uusia kohtia, niiden edellä olevaa 16 kohtaa olisi muutettava niin, että kohtien väliin ei jää pistettä.

3 §. *Lain soveltamisala ja sen rajoitukset.* Pykälää ehdotetaan muutettavan siten, että siihen lisättäisiin uusi *2 momentti*, jossa säädettäisiin ehdotetun uuden 4 a luvun soveltamisalasta. Voimassa olevan 3 §:n 2 – 5 momentti siirtyisivät 3 – 6 momentiksi. Myös Ahvenanmaata koskevaa pykälän 5 momenttia (2 momentin lisäämisen jälkeen 6 momenttia) ehdotetaan muutettavaksi.

Direktiivin 2 artiklassa säädetään sen vähimmäissoveltamisalasta julkishallinnon toimijoihin. Direktiivin 2 artiklan 2 kohdan f) alakohdan mukaan direktiiviä sovelletaan, kun toimija on julkishallinnon toimija, i) jonka jäsenvaltio on kansallisen lainsäädäntönsä mukaisesti määritellyt keskustason julkishallinnon toimijaksi; ii) jonka jäsenvaltio on kansallisen lainsäädäntönsä mukaisesti määritellyt aluetason julkishallinnon toimijaksi ja joka riskiperusteisen arvioinnin perusteella tarjoaa palveluja, joiden häiriintymisellä voisi olla merkittävä vaikutus yhteiskunnan tai talouden kriittisiin toimintoihin.

Ehdotetun uuden 2 momentin mukaan 4 a lukua sovellettaisiin tiedonhallintalain 4 §:n 1 momentin 1 kohdassa tarkoitettuihin valtion virastoihin ja laitoksiin, valtion liikelaitoksiin, 4 §:n 1 momentin 9 kohdassa tarkoitettuihin itsenäisiin julkisoikeudellisiin laitoksiin sekä hyvinvointialueisiin, hyvinvointiyhtymiin ja Helsingin kaupunkiin niiden hoitaessa laissa hyvinvointialueiden järjestämisvastuulle säädettyjä tehtäviä. Lisäksi 4 a lukua sovellettaisiin [CER-lain] nojalla julkishallinnon toimialan kriittisiksi toimijoiksi määriteltyihin toimijoihin.

Pykälän 2 momentissa ehdotettu sääntely kattaisi direktiivissä säädetyn vähimmäissoveltamisalan julkishallinnon toimijoiden osalta. Valtion virastoja ja laitoksia, myös valtion aluehallintoviranomaisia kuten aluehallintovirastoja ja elinkeino-, liikenne- ja ympäristökeskuksia voidaan pitää kansallisen lainsäädäntömme mukaisesti direktiivissä tarkoitettuina keskustason julkishallinnon toimijoina. Momentissa tarkoitettuihin valtion virastoihin ja laitoksiin lukeutuisivat tiedonhallintalain 4 §:n 1 momentin 1 kohdan mukaisina tiedonhallintoyksikköinä toimivat valtion virastot ja laitokset mukaan lukien niissä toimivat viranomaiset.

Sääntelyä sovellettaisiin myös valtion liikelaitoksiin sekä itsenäisiin julkisoikeudellisiin yhteisöihin tietyin poikkeuksin. Liikelaitoksista soveltamisalaan kuuluisivat esimerkiksi Senaattikiinteistöt ja Metsähallitus. Puolustuskiinteistöihin ei sovellettaisi sääntelyä, koska sen toiminta liittyy pääosin maanpuolustukseen ja kansalliseen turvallisuuteen, kuten Puolustusvoimien, johon sääntelyä ei myöskään sovellettaisi.

Tiedonhallintalain 4 §:n 1 momentin 9 kohdassa tarkoitettuja itsenäisiä julkisoikeudellisia laitoksia ovat muun muassa Kansaneläkelaitos, Suomen Pankki, Työterveyslaitos, Suomen riistakeskus, Suomen metsäkeskus, Eläketurvakeskus, Keva ja Kuntien takauskeskus. Niistä muihin kuin Suomen Pankkiin sovellettaisiin 4 a lukua. Yliopistolain (558/2009) mukaisiin julkisoikeudellisiin yliopistoihin sääntely ei soveltuisi, koska yliopistot on mainittu tiedonhallintalain 4 §:n 1 momentissa omassa kohdassaan (kohta 10) – eli ne eivät ole lain 4 §:n 1 momentin 9 kohdassa tarkoitettuja itsenäisiä julkisoikeudellisia laitoksia. Julkisoikeudellinen laitos on itsenäinen julkisoikeudellinen oikeushenkilö, joka on yleensä perustettu erityisellä säädöksellä julkisoikeudellisen laitoksen asemaan. Itsenäisillä julkisoikeudellisilla laitoksilla on tavallisesti myös oma talous ja hallinto. Itsenäiset julkisoikeudelliset laitokset ovat oikeustoimikelpoisia. Julkisoikeudellinen laitos ei kuulu varsinaiseen hallintokoneistoon, mutta se hoitaa erikseen määriteltyä julkista tehtävää ja käyttää julkista valtaa. Ne päättävät ihmisiin kohdistuvista oikeuksista ja velvollisuuksista ja niiden toiminnasta on säädetty laissa. Laitoksen itsenäisyys merkitsee lähinnä sen korostettua riippumattomuutta hallintokoneiston ohjauksesta. Niiden toimintaa valvoo kuitenkin valtio. Valinta eri organisaatiomuotojen välillä (esimerkiksi valtion virasto vai julkisoikeudellinen laitos) on ollut epäsystemaattista ja osin satunnaista. Edellä todettu huomioon ottaen itsenäiset julkisoikeudelliset laitokset olisi luettava NIS2-direktiivin liitteen I kohdassa 10 tarkoitettuihin keskustason julkishallinnon toimijoihin, joihin pääsääntöisesti on sovellettava direktiiviä.

Lisäksi 4 a luvun soveltamisalaan kuuluisivat hyvinvointialueet ja hyvinvointiyhtymät ja Helsingin kaupunki, jotka olisi katsottava kansallisen lainsäädännön mukaisesti direktiivissä tarkoitetuiksi aluetason julkishallinnon toimijoiksi niiden toteuttaessa hyvinvointialueiden järjestämisvastuulle säädettyjä tehtäviä. Hyvinvointialueiden, hyvinvointiyhtymien ja Helsingin kaupungin järjestämisvastuulle kuuluvat lakisääteisesti sosiaali- ja terveydenhuolto sekä pelastustoimi. Julkisen ja yksityisen terveydenhuollon tarjoajat kuuluvat NIS2-direktiivin liitteen I kohdan 5 Terveys-toimialaan, jonka osalta direktiivissä säädetyistä velvoitteista ja valvonnasta säädettäisiin ehdotetussa kyberturvallisuuden riskienhallintaa koskevassa laissa. Tällöin ehdotettu tiedonhallintalain sääntely ulottaisi direktiivin velvoitteet koskemaan myös hyvinvointialueiden ja hyvinvointiyhtymien hallintoa sekä Helsingin kaupungin hallintoa sosiaali- ja terveydenhuollon ja pelastustoimen osalta. Lisäksi sääntely koskisi sosiaalihuollon ja pelastustoimen viranomaisia hyvinvointialueilla, hyvinvointiyhtymissä ja Helsingin kaupungissa. Hallinnon toimivuus on edellytys sille, että hyvinvointialueet ja –yhtymät sekä Helsingin kaupunki voivat toteuttaa niille säädetyt yhteiskunnan kriittisisiksi toiminnoiksi lukeutuvat tehtävät.

Direktiivin 2 artiklan 7 kohdan mukaan direktiiviä ei sovelleta julkishallinnon toimijoihin, jotka harjoittavat toimintaa kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla, mukaan lukien rikosten ennalta estäminen, tutkiminen, paljastaminen ja rikoksiin liittyvät syytetoimet. Direktiivin johdanto-osan kappaleen 8 mukaan: ”julkishallinnon toimijoista olisi jätettävä direktiivin soveltamisalan ulkopuolelle ne, jotka harjoittavat toimintaa pääasiassa kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla, mukaan lukien rikosten ennalta estäminen, tutkiminen, paljastaminen ja rikoksiin liittyvät syytetoimet. Niitä julkishallinnon toimijoita, joiden toiminta liittyy vain marginaalisesti mainittuihin aloihin, ei kuitenkaan olisi jätettävä tämän direktiivin soveltamisalan ulkopuolelle. Tätä direktiiviä sovellettaessa sääntelyvaltaa käyttävien toimijoiden ei katsota harjoittavan toimintaa lainvalvonnan alalla, joten niitä ei kyseisellä perusteella jätetä tämän direktiivin soveltamisalan

ulkopuolelle”. Tämän perusteella lain 4 a luvun soveltamisalasta rajattaisiin pois sellaiset valtion viranomaiset ja laitokset, jotka harjoittavat toimintaa mainituilla aloilla. Näin ollen 4 a lukua ei sovellettaisi Puolustusvoimiin, Puolustuskiinteistöihin, poliisin hallinnosta annetussa laissa (110/1992) tarkoitettuihin poliisiyksikköihin (poliisiyksikköjä ovat mainitun lain 1 §:n mukaan Poliisihallitus ja sen alaiset yksiköt sekä suojelupoliisi), Rajavartiolaitokseen, Tullin rikostorjuntaan, Syyttäjälaitokseen, eikä turvallisuusverkkolaissa tarkoitettuun turvallisuusverkon palvelutuotantoon ja palvelujen käyttöön. Turvallisuusverkon palvelutuotantoon ja käyttöön kohdistuva rajaus tarkoittaisi sitä, että 4 a lukua ei sovellettaisi Valtion tieto- ja viestintätekniikkakeskus Valtorin turvallisuusverkkolain mukaiseen toimintaan. Suomen Erillisverkot Oy:öön 4 a lukua ei sovellettaisi ilman turvallisuusverkkorajaustakaan, sillä Suomen Erillisverkot Oy ei kuulu mihinkään viranomaisryhmään, joihin 4 a lukua 3 §:n alun pääsäännön mukaan sovellettaisiin. Turvallisuusverkon palvelujen käytön osalta rajaus tarkoittaisi sitä, että ne turvallisuusverkon palvelujen käyttäjät (esimerkiksi tasavallan presidentin kanslia, ministeriöt ja Maahanmuuttovirasto), jotka kuuluisivat 4 a luvun soveltamisalaan, eivät olisi velvollisia ilmoittamaan turvallisuusverkon IP-osoitteita taikka ilmoittamaan turvallisuusverkon poikkeamista. Liikenne- ja viestintäviraston valvontatoimivalta taikka tiedonsaanti- tai tarkastusoikeus ei myöskään kohdistuisi turvallisuusverkon palveluihin eikä niiden käyttöön. Tiedonsaantioikeuden ja tarkastusoikeuden rajoituksista ehdotetaan säädettäväksi myös niitä koskevissa pykälissä.

Direktiivin 6 artiklan 35 kohdan mukaan julkishallinnon toimijan käsitteen ulkopuolelle jäävät kansalliset oikeuslaitokset, parlamentit ja keskuspankit. Tämän perusteella 4 a luvun soveltamisalan ulkopuolelle rajautuisivat tuomioistuimet, valitusasioita käsittelemään perustetut lautakunnat, Suomen pankki sekä eduskunnan valtiopäivätoiminta ja eduskunnan virastot. Näistä Suomen Pankki mainittaisiin 3 §:n 2 momentissa erikseen 4 a luvun soveltamisalan ulkopuolelle rajautuvana tahona. Tuomioistuimet, valitusasioita käsittelemään perustetut lautakunnat ja eduskunnan virastot on erotettu tiedonhallintalain 4 §:n 1 momentin mukaisessa tiedonhallintayksiköitä koskevassa luettelossa valtion virastoista ja laitoksista omiksi toimijoikseen omissa 4 §:n 1 momentin kohdissaan (kohdat 2 ja 3). Niitä ei siten olisi pidettävä myöskään ehdotetussa 3 §:n 2 momentin mukaisina lain 4 §:n 1 momentin 1 kohdassa tarkoitettuina valtion virastoina ja laitoksina, eivätkä ne kuuluisi 4 a luvun soveltamisalaan.

Pykälän 2 momentin viimeisen virkkeen mukaan valvovan viranomaisen valvontatoimivaltuuksia ja tiedonsaanti- sekä tarkastusoikeutta ei sovellettaisi tasavallan presidentin kansliaan, valtioneuvoston oikeuskanslerin toimintaan eikä Kansaneläkelaitokseen. Rajoitukset johtuvat pääosin näiden julkiseen sektoriin kuuluvien organisaatioiden perustuslaissa säädetystä asemasta, jonka perusteella valtion keskushallintoon kuuluvien viranomaisten ohjaustoimivaltaa ei voida ulottaa näiden organisaatioiden sisäisen hallinnon ohjaukseen (esim. PeVL 46/2010).

Vaikka osa julkishallinnon toimijoista sekä turvallisuusverkon palvelutuotanto ja palvelujen käyttö ehdotetaan direktiivin sallimalla tavalla jätettäväksi pois NIS 2-sääntelyn soveltamisalasta, ei se sulkisi pois kyseisten julkishallinnon toimijoiden oikeutta hyödyntää esimerkiksi Liikenne- ja viestintäviraston valvontatehtävästä erillisiä CSIRT- palveluja, joista - ja joihin liittyvästä tietojen käsittelystä - säädettäisiin laissa kyberturvallisuuden riskienhallinnasta. Lisäksi nämä 4 a luvun sääntelyn ulkopuolella olevat toimijat voisivat tehdä 18 f §:ssä tarkoitettuja vapaaehtoisia ilmoituksia Liikenne- ja viestintävirastolle. Tietojen luovuttamisesta vapaaehtoisten ilmoitusten yhteydessä säädettäisiin 18 f §:ssä.

Pykälän voimassa olevan 5 momentin sääntely siirtyisi 6 momentiksi, jonka loppuun lisättäisiin virke, jonka mukaan lain 4 a lukua sovelletaan Ahvenanmaan maakunnassa toimiviin valtion viranomaisiin, jollei 2 momentista muuta johdu. NIS2 -direktiivin sääntelyä on julkishallinnon

toimialalla arvioitava viranomaisten toimintaa koskevana sääntelynä, jolloin maakunnan ja valtakunnan välisen lainsäädäntövallan tarkastelu perustuisi Ahvenanmaan itsehallintolain (1144/1991, jäljempänä itsehallintolaki) sääntelyyn maakunnan ja valtakunnan viranomaisista. Itsehallintolaissa säädetään maakunnan itsehallinnosta ja lainsäädäntövallan jakautumisesta maakunnan ja valtakunnan välillä. Mainitun lain 4 luvussa säädetään maakunnan toimivallasta ja 5 luvussa valtakunnan toimivallasta. Itsehallintolain 18 §:n 1 kohdan mukaan maakunnalla on lainsäädäntövalta asioissa, jotka koskevat maakuntapäivien järjestysmuotoa ja tehtäviä sekä maakuntapäivien jäsenten vaalia, maakunnan hallitusta sekä sen alaisia viranomaisia ja laitoksia. Itsehallintolain 27 §:n 3 kohdan mukaan valtakunnalla on lainsäädäntövalta asioissa, jotka koskevat valtion viranomaisten järjestysmuotoa ja toimintaa. Ahvenanmaalla toimivaa valtakunnan viranomaista on pidettävä direktiivissä tarkoitettuna keskustason julkishallinnon toimijana, johon direktiiviä on sovellettava. Tämän vuoksi 4 a luvussa säädettyä olisi sovellettava myös Ahvenanmaalla toimivaan valtion viranomaiseen. Myös Ahvenanmaalla toimiviin valtion viranomaisiin sovellettaisiin 2 momentissa säädettyjä rajauksia – eli esimerkiksi Rajavartiolaitoksen toimintaan Ahvenanmaallakaan ei sovellettaisi 4 a lukua.

10 §. *Julkisen hallinnon tiedonhallintalautakunta.* Pykälän *1 momentin 2 kohtaa* muutettaisiin siten, että mainitussa kohdassa tiedonhallintalautakunnalle säädetty edistämistehtävä ei koskisi 4 a luvussa säädettyä. Lain 4 a luvun sääntelyn noudattamista valvoisi esityksessä ehdotetun mukaisesti Liikenne- ja viestintävirasto. Vaikka tiedonhallintalautakunta ei voi antaa mainitun kohdan nojalla viranomaisille sitovia ohjeita tai määräyksiä, eivätkä sen edistämistehtävän nojalla antamat kannanotot ja suositukset ole sitovia, voisi tiedonhallintalautakunnan 4 a lukuun kohdistuva edistämistehtävä aiheuttaa ristiriitaa 4 a luvun noudattamista valvovan viranomaisen toiminnan kanssa ja vaarantaa valvovan viranomaisen toiminnan riippumattomuuden. Tämän vuoksi olisi perusteltua, ettei tiedonhallintalautakunnan edistämistehtävä kohdistuisi 4 a luvun sääntelyyn. Tiedonhallintalautakunnan ja Liikenne- ja viestintäviraston tulisi tehdä yhteistyötä tietoturvallisuuteen ja kyberturvallisuuteen liittyvien ohjeiden ja suositusten laatimisessa niin, että niiden antama ohjeistus olisi tarvittavilta osin yhdenmukaista.

18 §. *Turvallisuusluokiteltavat asiakirjat valtionhallinnossa.* Pykälän *1 momenttia* muutettaisiin siten, että turvallisuusluokitteluvelvollisuus koskisi myös Suomen Erillisverkot Oy:tä ja sen kokonaan omistamaa tytäryhtiötä niiden hoitaessa turvallisuusverkkolaissa tarkoitettuja tehtäviä.

Tiedonhallintalakia sovelletaan tietyiltä osin myös julkista hallintotehtävää hoitaviin valtion erityistehtäväyhtiöihin. Esimerkiksi lain 4 lukua sovelletaan näihin. Lain 18 §:n 1 momentin sisällöstä johtuen mainitut toimijat eivät tällä hetkellä kuitenkaan saa käyttää tiedonhallintalaissa tarkoitettua asiakirjojen turvallisuusluokittelua oman toimintansa asiakirjoihin.

Muutos tarkoittaisi, että Suomen Erillisverkot Oy sekä sen kokonaan omistama tytäryhtiö olisivat velvollisia turvallisuusverkkolain mukaisessa toiminnassaan luokittelemaan toimintaansa liittyviä asiakirjoja valtion virastojen ja laitosten tapaan. Turvallisuusluokittelulle on tiedonhallinnan näkökulmasta ilmennyt tarvetta Suomen erillisverkot Oy:ssä, joka harjoittaa turvallisuuden tai varautumisen kannalta kriittistä toimintaa. Suomen Erillisverkot Oy:öön ja sen turvallisuusverkkolain mukaisia tehtäviä hoitavaan tytäryhtiöön sovelletaan turvallisuusverkkolain 19 §:n 1 momentin mukaan julkisuuslakia silloin, kun ne hoitavat mainitussa laissa niille säädettyjä tehtäviä. Ne laativat siis julkisuuslaissa tarkoitettuja asiakirjoja ja niiden toiminta ja osa asiakirjoista on salassa pidettäviä ja merkityksellisiä turvallisuusluokittelun perusteena mainitun Suomen turvallisuuden kannalta. Tiedonvaihdossa ja yhteistyössä asiakirjoja turvallisuusluokittelevien viranomaisten kanssa on tärkeää, että on olemassa yhtenäiset vaatimukset asiakirjojen luokittelusta, merkitsemisestä ja niiden käsittelyssä noudatettavista menettelyistä.

4 a luku Kyberturvallisuusvelvoitteet ja niiden noudattamisen valvonta

Tiedonhallintalakiin ehdotetaan lisättäväksi uusi 4 a luku, jossa säädettäisiin yksinomaan NIS2-direktiivin täytäntöönpanon edellyttämistä seikoista. Ehdotettujen säännösten sijoittaminen omaan lukuunsa on perusteltua siksi, että luvun säännökset koskisivat ainoastaan rajattua määrää tiedonhallintayksiköistä ja viranomaisista. Myös 4 a luvussa Liikenne- ja viestintävirastolle ehdotetut NIS2 –direktiivissä tarkoitetun toimivaltaisen viranomaisen eli valvovan viranomaisen tehtävät rajautuisivat ehdotetussa 4 a luvussa säädettyjen velvoitteiden noudattamisen valvontaan.

18 a §. *Toimijajaottelu ja toimintaa koskeva ilmoitus.* Pykälässä säädettäisiin NIS2-direktiivin 3 artiklan 4 kohtaan ja 29 artiklan 4 kohtaan perustuvasta ilmoitusvelvollisuudesta toimivaltaiselle viranomaiselle. Vastaavat säännökset ehdotetussa kyberturvallisuuden riskienhallintaa koskevassa laissa sisältyisivät lain 43 §:ään.

Direktiivin 3 artiklan 3 kohdan mukaan jäsenvaltioiden on viimeistään 17 päivänä huhtikuuta 2025 laadittava luettelo keskeisistä ja tärkeistä toimijoista sekä verkkotunnusten rekisteröintipalveluja tarjoavista toimijoista. Jäsenvaltioiden on tarkasteltava luetteloa uudelleen säännöllisesti ja vähintään kahden vuoden välein ja saatettava se tarvittaessa ajan tasalle. Direktiivin 3 artiklan 5 kohdan a alakohdan mukaan toimivaltaisten viranomaisten on viimeistään 17 päivänä huhtikuuta 2025 ja sen jälkeen kahden vuoden välein ilmoitettava komissiolle ja direktiivin 14 artiklassa tarkoitetulle yhteistyöryhmälle luetteloon kirjattujen keskeisten ja tärkeiden toimijoiden lukumäärä kullakin liitteessä I tai II tarkoitetulla toimialalla ja toimialan osalla. Direktiivin 29 artiklan 4 kohdan mukaan jäsenvaltioiden on varmistettava, että keskeiset ja tärkeät toimijat ilmoittavat toimivaltaisille viranomaisille osallistumisestaan 29 artiklan 2 kohdassa tarkoitettuihin kyberturvallisuustietojen jakamisjärjestelyihin, kun ne liittyvät tällaisiin järjestelyihin, tai tapauksen mukaan vetäytymisestään tällaisista järjestelyistä, kun vetäytyminen tulee voimaan.

Pykälän *1 momentin* mukaan 4 a luvun soveltamisalaan kuuluvat tiedonhallintayksiköt olisivat NIS2-direktiivin liitteen I 10 kohdassa tarkoitetun julkishallinnon toimialan keskeisiä toimijoita, lukuun ottamatta hyvinvointialueita ja hyvinvointiyhtymiä sekä Helsingin kaupunkia, jotka olisivat tärkeitä toimijoita. Direktiivin 3 artiklan 1 kohdan d alakohdan mukaan keskustason julkishallinnon toimijaa on pidettävä direktiivissä tarkoitettuna keskeisenä toimijana. CER-direktiivin nojalla kriittiseksi toimijaksi määriteltyä toimijaa on NIS 2 -direktiivin 3 artiklan 1 kohdan f alakohdan mukaan pidettävä keskeisenä toimijana. Muita julkishallinnon toimijoita on pidettävä tärkeinä toimijoina.

Se, onko toimija keskeinen vai tärkeä, vaikuttaa komissiolle ja yhteistyöryhmälle direktiivin 3 artiklan 5 kohdan a alakohdan perusteella ilmoitettaviin toimijalukumääriin sekä siihen, tuleeko toimijaan kohdistaa 32 artiklassa tarkoitettuja keskeisiin toimijoihin liittyviä valvonta- ja täytäntöönpanotoimenpiteitä (etukäteisvalvontaa) vai 33 artiklassa tarkoitettuja tärkeisiin toimijoihin liittyviä valvonta- ja täytäntöönpanotoimenpiteitä (jälkikäteisvalvontaa).

Pykälän *2 momentissa* säädettäisiin julkishallinnon toimijoiden velvollisuudesta ilmoittaa tietyt tiedot itsestään toimivaltaiselle viranomaiselle. Liikenne- ja viestintävirasto voisi esimerkiksi perustaa verkkosivuilleen digitaalisen palvelun tietojen ilmoittamiseksi.

Tiedonhallintayksikön olisi ilmoitettava tiedonhallintayksikön nimi, osoite ja ajantasaiset yhteystiedot, mukaan lukien sähköpostiosoitteet ja puhelinnumerot. Lisäksi toimijan tulisi ilmoittaa sen käyttämät IP-osoitealueet. Tiedonhallintayksikön pitäisi myös ilmoittaa, toimiiko se julkishallinnon toimialalla keskeisenä vai tärkeänä toimijana, luettelo muista Euroopan unionin jäsenvaltioista, joissa se tarjoaa palvelujaan sekä osallistumisesta kyberturvallisuuden riskienhallintaa koskevan lain 22 §:ssä tarkoitettuun kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn.

Pykälän *3 momentin* mukaan tiedonhallintayksikön olisi viipymättä, viimeistään kahden viikon kuluessa muutoksesta, ilmoitettava kaikista muutoksista 1 momentin nojalla annettuihin tietoihin.

Tiedonhallintayksikön tulisi huolehtia, että se saa ilmoituksia varten tarvitsemansa tiedot IP-osoitealueista siltä, joka tarjoaa sille tieto- ja viestintäteknisiä palveluja. Valtion tieto- ja viestintätekniikkakeskus Valtori kuuluisi myös ilmoitusvelvollisuuden alaan muun toimintansa paitsi turvallisuusverkon palvelutuotannon ja palvelujen käytön osalta. Valtorin tulisi myös huolehtia osaltaan siitä, että sen palveluja käyttävillä tiedonhallintayksiköillä on tieto niiden palveluissa käytettävistä IP-osoitealueista ja niiden muutoksista, niin että ne voivat osaltaan täyttää ilmoitusvelvollisuuden ja pitää tietonsa ajan tasalla. Luonnollisesti tiedonhallintayksiköllä voi olla myös omia IP-osoitteita, joita koskevista tiedoista ne vastaisivat itsenäisesti. IP-osoitealueet ovat melko stabiileja, joten niitä koskevien tietojen ajan tasalla pitämisen ei pitäisi muodostaa suurempaa rasitetta.

Direktiivin 3 artikla 4 kohdan 3 alakohdan mukaan komissio antaa Euroopan unionin kyberturvallisuusviraston (ENISA) avustuksella ilman aiheetonta viivytystä ohjeita ja malleja ilmoitusvelvoitteiden täyttämiseksi. Valvovan viranomaisen tulisi ottaa komission ohjeet huomioon tarkoituksenmukaisella tavalla tiedonhallintayksiköiden ohjeistamisessa ja neuvonnassa.

18 b §. *Kyberturvallisuuden riskienhallintavelvoite ja riskienhallinnan toimintamalli.* Pykälässä säädettäisiin direktiivin 20 – 22 artiklaan perustuvista kyberturvallisuuden riskienhallinnasta ja riskienhallinnan toimintamallista sekä johdon vastuusta. Direktiivin 21 artiklaan sisältyvä kyberturvallisuuden riskienhallintatoimenpiteitä koskeva luettelo sisältyisi 18 c §:ään. Ehdotetussa kyberturvallisuuden riskienhallintaa koskevassa laissa tiedonhallintalakiin ehdotettuja 18 b ja c §:ää vastaavista NIS 2 –direktiivin riskienhallintavelvoitteista säädettäisiin lain 7-10 §:ssä, joiden säännöskohtaisissa perusteluissa on esitetty muun muassa direktiivin johdantolauseissa riskienhallinnasta todettua sekä muita soveltuvia esimerkkejä riskienhallinnan toteuttamiseen.

Pykälän *1 momentin* mukaan tiedonhallintayksikön olisi tunnistettava, arvioitava ja hallittava riskejä, joita kohdistuu sen toiminnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Momentissa kuvataan myös riskienhallinnan tarkoitus eli viestintäverkkojen ja tietojärjestelmien, niiden käyttäjien ja muiden henkilöiden suojaaminen kyberuhilta. Tiedonhallintayksikön tulisi riskien tunnistamisen, arvioinnin ja hallinnan keinoin varmistua siitä, että toiminnassa käytettävien verkko- ja tietojärjestelmien turvallisuustaso ja riskienhallintatoimenpiteiden taso on riittävä ja oikeasuhtainen riskeihin nähden. Säännös vastaa pitkälti tiedonhallintalain 13 §:n sääntelyä riskiarviointiin perustuvasta tietoturvallisuustoimenpiteiden mitoittamisesta. Kyberturvallisuus ei käsitteenä täysin vastaa tietoturvallisuuden käsitettä, koska tietoturvallisuus suojaa tietoa kaikissa muodoissaan – ei pelkästään tietojärjestelmissä. Lisäksi kyberturvallisuuteen määritelmätasolla sisältyy henkilöiden suojaamisen ulottuvuus, joka toki seuraa myös tietoturvallisuuden toteuttamisesta.

Ehdotetun *2 momentin* mukaan tiedonhallintayksikön olisi laadittava kyberturvallisuuden riskienhallinnan toimintamalli ja ylläpidettävä sitä. Toimintamallissa tulisi tunnistaan tiedonhallintayksikön viestintäverkkoihin ja tietojärjestelmiin sekä niiden fyysiseen ympäristöön kohdistuvat riskit kaikki vaaratekijät huomioivan lähestymistavan mukaisesti. Kyberturvallisuuden riskienhallinnan toimintamallissa olisi lisäksi kuvattava kyberturvallisuuden riskienhallinnan tavoitteet, menettelyt ja vastuut sekä 18 c §:ssä tarkoitetut tekniset, operatiiviset ja organisatoriset kyberturvallisuuden riskienhallintatoimenpiteet. Riskienhallinnan tavoitteet, menettelyt ja vastuut yleensä kuvataan ehdotetun 18 c §:n 2 momentin 1 kohdassa riskienhallinnan toimintaperiaatteissa, mutta näiden kuvaamista korostettaisiin myös ehdotetussa 18 b §:n 2 momentissa,

jotta kuvaaminen olisi selkeä vaatimus riippumatta siitä, kuinka riskienhallinnan toimintaperiaatteiden sisältö ymmärretään. Riskienhallinta on luonteeltaan jatkuvaa ja laadittua riskienhallinnan toimintamallia olisi myös ylläpidettävä, sillä verkko- ja tietojärjestelmien turvallisuuteen kohdistuvat riskit muuttuvat ja kehittyvät ajan myötä niin kuin suojaustoimetkin.

Kyberturvallisuuden riskienhallintatoimenpiteiden olisi perustuttava kaikki vaaratekijät huomioivaan toimintamalliin, jolla pyritään suojaamaan verkko- ja tietojärjestelmät ja näiden järjestelmien fyysinen ympäristö sellaisilta tapahtumilta kuin varkaus, tulipalo, tulva, televiestintä- tai sähkökatko. Riskienhallinnalla suojattaisiin verkko- ja tietojärjestelmiä myös luvattomalta fyysiseltä pääsyltä tietoihin sekä tietojenkäsittely-ympäristöä vahingolta ja häirinnältä, jotka saattaisivat vaarantaa viestintäverkoissa- ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden.

Tiedonhallintalain 5 §:n 1 momentin mukaan tiedonhallintayksikön on ylläpidettävä sen toimintaympäristön tiedonhallintaa määrittelevää ja kuvaavaa tiedonhallintamallia. Pykälän 2 momentin 5 kohdan mukaisesti tiedonhallintamallin on sisällettävä tiedot tietoturvallisuustoimenpiteistä. Lisäksi pykälän 3 momentin mukaan suunniteltaessa tiedonhallintamallin sisältöön vaikuttavia olennaisia hallinnollisia uudistuksia ja tietojärjestelmien käyttöönottoa tiedonhallintayksikön on arvioitava näihin kohdistuvat muutokset ja niiden vaikutukset suhteessa pykälässä yksilöityyn tiedonhallintalain sääntelyyn.

Esityksessä ei ehdoteta säädettävän, että tiedonhallintamalliin tulisi sisällyttää kyberturvallisuuteen liittyviä toimenpiteitä tai että tiedonhallintamallin muutosvaikutusten arvioinnissa olisi otettava huomioon 4 a luvun säännökset. Ehdotetun sääntelyn mukaan tiedonhallintayksiköllä olisi kuitenkin oltava dokumentoituna 18 b ja c §:ssä tarkoitetut kyberturvallisuuden riskienhallintaan liittyvät asiat. Lisäksi kyseiset toimenpiteet olisivat käytännössä osin vastaavia, jotka viranomaisen on otettava huomioon osana 4 luvun mukaisia tietoturvatoimenpiteitä. Tämän vuoksi olisi tarkoituksenmukaista, että 4 a luvun soveltamisalaan kuuluvat tiedonhallintayksiköt sisällyttäisivät harkintansa mukaan 18 b ja c §:ssä ehdotettavat toimet osaksi tiedonhallintamalliaan, vaikka siihen kohdistuvasta velvoitteesta ei erikseen säädettäisi. Tämä hyödyttäisi myös viranomaista, kun sen tiedonhallintaa määrittelevä ja kuvaava aineisto olisi koottuna samaan dokumentaatioon.

Pykälän *3 momentin* mukaan tiedonhallintayksikön johto vastaisi kyberturvallisuuden riskienhallinnan toteuttamisen ja valvonnan järjestämisestä sekä hyväksyisi kyberturvallisuuden riskienhallinnan toimintamallin ja valvoisi sen toteuttamista. Tiedonhallintayksikön johdolla tulisi myös olla riittävä perehtyneisyys kyberturvallisuuden riskienhallintaan.

Tiedonhallintayksikön johdolla (direktiivissä hallintoelin, englanniksi management body) tarkoitettaisiin virastojen ja laitosten työjärjestyksissä sekä eri toimijoiden hallintosäännöissä määriteltyä virastopäällikköä tai johtavaa toimielintä. Johdolla tarkoitettaisiin valtion viraston tai laitoksen päällikköä, joka on tyypillisesti virkanimikkeeltään pääjohtaja tai ylijohtaja. Kuntalain (410/2015) 38 §:n 2 momentin mukaan kunnanhallitus johtaa kunnan toimintaa, hallintoa ja taloutta. Siten Helsingin kaupunginhallitus toimisi lähtökohtaisesti momentissa tarkoitettuna tiedonhallintayksikön johtona, ellei vastuuta ole delegoitu hallintosäännössä jollekin muulle toimielimelle tai viranhaltijalle, kuten kaupunginjohtajalle. Itsenäisissä julkisoikeudellisissa laitoksissa johdolla tarkoitettaisiin kutakin laitosta koskevien säännösten perusteella määriteltyä johtoa, joka voi delegoida vastuitaan muulle johdolle.

Käytännössä johto vastaisi siitä, että tiedonhallintayksikössä toteutetaan kyberturvallisuuden riskienhallintaa ja että sitä kehitetään. Johdon tulisi myös huolehtia siitä, että kyberturvallisuuden riskienhallinnan toimintamalli mukaan lukien kyberturvallisuuden riskienhallintatoimenpiteet pidetään ajan tasalla. Lisäksi johdon tulisi järjestää kyberturvallisuuden riskienhallinnan valvonta.

Toimijan johdolla tulisi niin ikään olla riittävä ja ajantasainen perehtyneisyys kyberturvallisuuden riskienhallintaan, mikä edellyttäisi perehtyneisyyden hankkimista joko kouluttautumalla tai muulla vastaavalla tavalla säännöllisin väliajoin. Osana 18 c §:ssä tarkoitettuja kyberturvallisuuden riskienhallintatoimenpiteitä johdon tulisi huolehtia myös henkilöstön kyberturvallisuuskoulutuksen järjestämisestä. Kyberturvallisuuden riskienhallinnan koulutuksen tarkoituksena olisi antaa riittävät tiedot ja taidot henkilölle, jotta tämä kykenisi tunnistamaan riskejä ja arvioimaan kyberturvallisuusriskien hallintakäytäntöjä ja niiden vaikutusta tiedonhallintayksikön toimintaan mukaan lukien sen tarjoamiin palveluihin.

Tiedonhallintalain 4 §:n 2 momentissa on säädetty tiedonhallintayksikön johdolle velvollisuus huolehtia muun muassa, että tiedonhallintayksikössä on määritelty tiedonhallinnan toteuttamiseen liittyvien tehtävien vastuut sekä ajantasaiset ohjeet sekä tarjolla koulutusta, jolla varmistetaan, että henkilöstöllä ja tiedonhallintayksikön lukuun toimivilla on riittävä tuntemus voimassa olevista tiedonhallintaa, tietojenkäsittelyä sekä asiakirjojen julkisuutta ja salassapitoa koskevista säädöksistä, määräyksistä ja tiedonhallintayksikön ohjeista; sekä järjestetty riittävä valvonta tiedonhallintaan liittyvien säädösten, määräysten ja ohjeiden noudattamisesta. Voimassa olevan sääntelyn lisäksi ehdotetulla säännöksellä korostettaisiin kyberturvallisuuden riskienhallinnan merkitystä henkilöstön koulutuksessa sekä velvoitettaisiin johto huolehtimaan myös omasta koulutuksestaan, jotta johdolla olisi edellytykset vastata kyberturvallisuuden riskienhallinnasta ja sen valvonnasta.

NIS2-direktiivin 20 artiklan 1 kohdan mukaan jäsenvaltioiden on varmistettava, että keskeisten ja tärkeiden toimijoiden hallintoelimet voidaan saattaa vastuuseen, jos toimijat rikkovat kyseistä artiklaa. Lisäksi todetaan, että kohdan soveltaminen ei rajoita kansallisen lainsäädännön soveltamista, kun on kyse julkisiin laitoksiin sovellettavista vastuusäännöistä taikka virkamiesten tai vaalilla valittujen tai nimettyjen toimenhaltijoiden vastuusta. Vastuuseen saattaminen olisi mahdollista esimerkiksi rikoslain (39/1889) 41 luvun 9 tai 10 §:n perusteella virkavelvollisuuden rikkomisena tai tuottamuksellisena virkavelvollisuuden rikkomisena.

18 c §. *Kyberturvallisuuden riskienhallintatoimenpiteet.* Pykälässä säädettäisiin direktiivin 21 artiklassa tarkoitetuista riskienhallintatoimenpiteistä. Pykälän *1 momentissa* säädettäisiin tiedonhallintayksikön velvollisuudeksi toteuttaa kyberturvallisuuden riskienhallintatoimenpiteet sekä määriteltäisiin yleisellä tasolla, mitä on otettava huomioon riskienhallintatoimenpiteitä valittaessa ja kuvattaessa kyberturvallisuuden riskienhallinnan toimintamalliin. Säännöksen mukaan toimenpiteiden tulisi olla asianmukaiset ja oikeasuhtaiset suhteessa käytetyille viestintäverkoille ja tietojärjestelmille aiheutuviin riskeihin, viestintäverkon tai tietojärjestelmän merkitykseen tiedonhallintayksikön toiminnalle sekä niissä ilmenevän poikkeaman yhteiskunnallisiin ja taloudellisiin vaikutuksiin. Lisäksi toimenpiteiden mitoittamisessa olisi otettava huomioon tiedonhallintayksikön koko, sen toiminnan laatu, poikkeaman todennäköisyys ja vakavuus, toimenpiteistä aiheutuvat kustannukset sekä ajantasainen kehitys huomioiden käytettävissä olevat tekniset mahdollisuudet torjua kyberuhka.

Direktiivin johdanto-osan 83 kappaleen mukaan kyberturvallisuusriskien hallintatoimenpiteitä ja raportointivelvoitteita olisi sovellettava asiaankuuluviin keskeisiin ja tärkeisiin toimijoihin riippumatta siitä, hoitavatko kyseiset toimijat verkko- ja tietojärjestelmiensä ylläpidon sisäisesti

vai ovatko ne ulkoistaneet sen. Tiedonhallintayksikkö vastaisi kyberturvallisuuden riskienhallinnasta ja oikeasuhtaisten riskienhallintatoimenpiteiden toteuttamisesta silloinkin, kun se hankkii tieto- ja viestintäteknisiä palveluja ulkopuoliselta toimittajalta. Valtion tieto- ja viestintätekniikkakeskus Valtorin toiminta valtion yhteisten perustietotekniikka- ja tietojärjestelmäpalvelujen tuottajana ja kehittäjänä perustuu valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä annettuun lakiin (1226/2013) ja sen nojalla annettuun asetukseen (132/2014). Valtion tieto- ja viestintätekniikkakeskus Valtori sopii tuottamistaan palveluista tiedonhallintayksiköiden kanssa tehtävissä palvelusopimuksissa. Ehdotettu pykälä velvoittaa Valtion tieto- ja viestintätekniikkakeskus Valtoria toteuttamaan kyberturvallisuuden riskienhallintatoimenpiteet, jotka ovat asianmukaiset ja oikeasuhteiset suhteessa sen tuottamiin valtion yhteisiin perustietotekniikka- ja tietojärjestelmäpalveluihin. Valtion tieto- ja viestintätekniikkakeskus Valtorin tulisi myös kuvata nämä toimenpiteet palvelukuvauksissaan ja asettaa ne palvelua käyttävän tiedonhallintayksikön saataville esimerkiksi asiakastyötilaan, jossa pidetään saatavilla muitakin palvelujen kuvauksia kuten yleisen tietosuoja-asetuksen mukaisia vaikutusarviointeja.

Pykälän *2 momentissa* säädettäisiin kyberturvallisuuden riskienhallintatoimenpiteiden tarkoituksesta sekä lueteltaisiin toimenpidekokonaisuudet, joiden tulisi ainakin sisältyä kyberturvallisuuden riskienhallintatoimenpiteisiin.

Ehdotetun 2 momentin johdantolauseen mukaan kyberturvallisuuden riskienhallintatoimenpiteillä tunnistetaan poikkeamariskit, ehkäistään, havaitaan ja hallitaan poikkeamia, palaudutaan niistä ja lievennetään niiden vaikutuksia. Lisäksi säännöksessä täsmennettäisiin, että kyberturvallisuuden riskienhallintatoimenpiteillä suojataan viestintäverkkoja ja tietojärjestelmiä ja niiden fyysistä ympäristöä kyberuhkilta ja poikkeamilta sekä minimoidaan poikkeamien vaikutus tiedonhallintayksikön toimintaan, sen palvelujen vastaanottajiin ja muihin palveluihin.

Pykälän 2 momenttiin sisältyvä 12-kohtainen luettelo kyberturvallisuuden riskienhallintatoimenpiteiden toimenpidekokonaisuuksista vastaa ehdotetun kyberturvallisuuden riskienhallintaa koskevan lain 9 §:n 2 momenttiin sisältyvää luetteloa, jonka säännöskohtaisissa perusteluissa on kuvattu tarkemmin momenttiin sisältyvien kohtien 1 – 12 sisältöä. Tässä kuvataan ainoastaan erityisesti julkishallinnon toimialaa koskevia seikkoja liittyen toimenpidekokonaisuuksiin.

Momentin *1 kohdassa* edellytettäisiin, että tiedonhallintayksikön on riskienhallintatoimenpiteenä toteutettava kyberturvallisuuden riskienhallinnan toimintaperiaatteet ja kyberturvallisuuden riskienhallintatoimenpiteiden vaikuttavuuden arviointi. Momentin *2 kohdassa* edellytettäisiin, että tiedonhallintayksiköllä on myös viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet. Säännökset vastaavat osin tiedonhallintalain 13 §:1 momentissa riskiarvioon perustuvasta tietoturvallisuudesta huolehtimisesta säädettyä, joskaan 13 §:ssä ei nimenomaisesti edellytetä tietoturvallisuuden toimintaperiaatteiden laatimista.

Momentin *3 kohdassa* edellytettäisiin, että tiedonhallintayksikkö huolehtii riskienhallintatoimenpiteenä ja kuvaa kyberturvallisuuden riskienhallinnan toimintamalliin viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuuden sekä tarvittavat menettelyt haavoittuvuuksien käsittelyyn ja julkistamiseen. Osin vastaavasti tiedonhallintalain 13 §:n 4 momentin mukaan viranomaisen on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet.

Momentin *4 kohdassa* edellytettäisiin toimitusketjujen turvallisuudesta huolehtimista yhtenä riskienhallinnan toimenpidekokonaisuutena. Direktiivin 22 artiklan mukaan direktiivin 14 artiklassa tarkoitettu yhteistyöryhmä voi yhteistyössä komission ja ENISAn kanssa tehdä koordinoituja turvallisuusriskinarviointeja tietyistä kriittisistä TVT-palvelujen, TVT-järjestelmien tai TVT-tuotteiden toimitusketjuista ottaen huomioon tekniset ja tarvittaessa muut kuin tekniset

riskitekijät. Nämä turvallisuusriskiarvioinnit voisivat koskea myös julkishallinnon toimialaa. Siltä osin kun tällaisia riskiarviointeja on laadittu, tiedonhallintayksikön tulisi hyödyntää riskiarvioita soveltuvin osin.

Momentin *5 kohdan* mukaan riskienhallintatoimenpiteisiin kuuluisi omaisuudenhallinta ja turvallisuuden kannalta tärkeiden toimintojen tunnistaminen.

Momentin *6 kohdan* mukaan tulisi huolehtia henkilöstöturvallisuudesta ja kyberturvallisuuskoulutuksesta. Henkilöstöturvallisuuteen liittyvistä asioista ja henkilöstön koulutuksesta säädetään myös muun muassa tiedonhallintalain 4 §:n 2 momentissa ja 12 §:ssä.

Kohdassa 7 edellytetään tiedonhallintayksikön huolehtivan pääsynhallinnan ja todentamisen menettelyistä. Tiedonhallintayksikön tulisi tarvittaessa käyttää vahvan tunnistamisen ja todennuksen, monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisuja. Pääsynhallintaan ja todentamisen menettelyihin liittyvät myös tiedonhallintalain 14, 16 ja 17 §.

Kohdassa 8 edellytettäisiin salausmenetelmien käyttämistä koskevien toimintaperiaatteita ja menettelyjä sekä tarvittaessa toimenpiteitä suojatun sähköisen viestinnän käyttöön. Tiedonhallintalaissa salausmenetelmiin liittyy erityisesti lain 14 §.

Kohdassa 9 edellytettäisiin poikkeamien havainnointia ja käsittelyä turvallisuuden ja toimintavarmuuden ylläpitämiseksi ja palauttamiseksi.

Kohdassa 10 edellytettäisiin varmuuskopiointia, palautumissuunnittelua, kriisinhallintaa ja muuta toiminnan jatkuvuuden hallintaa. Tiedonhallintalain 13 a §:llä tavoitellaan pitkälti samaa – eli tietoaineistojen käsittelyn, tietojärjestelmien hyödyntämisen sekä niihin perustuvan toiminnan jatkuvuuden hallintaa. Lain 13 a §:n mukaan tiedonhallintayksikön on selvitettävä sen tietoaineistojen käsittelyn, tietojärjestelmien hyödyntämisen sekä niihin perustuvan toiminnan jatkuvuuteen kohdistuvat olennaiset riskit. Riskiarvioinnin perusteella tiedonhallintayksikön on valmiussuunnitelmin ja häiriötilanteissa tapahtuvan toiminnan etukäteisvalmisteluin sekä muilla toimenpiteillä huolehdittava, että sen tietoaineistojen käsittely, tietojärjestelmien hyödyntäminen ja niihin perustuva toiminta jatkuvat mahdollisimman häiriöttömästi normaaliolojen häiriötilanteissa sekä valmiuslaissa tarkoitetuissa poikkeusoloissa. Lisäksi ehdotetussa 10 kohdassa mainittaisiin NIS 2 – direktiiviä vastaavalla tavalla erityisesti, että tiedonhallintayksikön tulisi jatkuvuuden hallinnan osana tarvittaessa huolehtia suojattujen varaviestintäjärjestelmien käyttömahdollisuudesta.

Ehdotetussa *11 kohdassa* edellytettäisiin perustason kyberhygieniakäytäntöjä toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi. Kyberhygieniakäytäntöjä ei erityisesti mainita tiedonhallintalaissa, mutta ne sisältyvät ainakin osittain lain 13 §:n säädettyyn velvollisuuteen varmistaa tietoaineistojen tietoturvallisuus riskienhallintaan perustuvilla tietoturvallisuustoimenpiteillä.

Ehdotetun *12 kohdan* mukaan tiedonhallintayksikön tulisi toteuttaa ja 18 b §:n nojalla kuvata toimenpiteet viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön suojaamiseksi ja tilaturvallisuuden varmistamiseksi sekä välttämättömien resurssien varmistamiseksi. Tiedonhallintalain 15 §:n mukaan tietoaineistoja on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia.

Lisäksi asiakirjojen turvallisuusluokittelusta valtionhallinnossa annettu valtioneuvoston asetus (1101/2019) sisältää edellä kohtien 1-12 yhteydessä tiedonhallintalain osalta kuvattuja vaatimuksia tarkempia vaatimuksia turvallisuusluokiteltujen asiakirjojen käsittelylle.

18 d §. *Ilmoitusvelvollisuus merkittävästä poikkeamasta.* Pykälässä säädettäisiin viranomaisen kolmiportaisesta velvollisuudesta raportoida merkittävät poikkeamat julkishallinnon toimialan valvovalle viranomaiselle, Liikenne- ja viestintävirastolle. Pykälä perustuu direktiivin 23 artiklaan. Ilmoitusvelvollisuudesta direktiivin liitteiden muiden toimialojen osalta säädettäisiin kyberturvallisuuden riskienhallintaa koskevan lain 11-13 §:ssä. Mainittujen pykälien perustelut sisältävät täydentäviä esimerkkejä poikkeamailmoituksiin liittyen.

Pykälän *1 momentissa* säädettäisiin raportoinnin ensimmäisestä vaiheesta eli ensi-ilmoituksesta, joka viranomaisen olisi toimitettava ilman aiheetonta viivytystä, viimeistään 24 tunnin kuluessa siitä, kun se on tullut tietoiseksi merkittävästä poikkeamasta. Ensi-ilmoituksessa olisi ilmoitettava poikkeamasta, epäilläänkö merkittävän poikkeaman johtuvan lainvastaisesta tai vihamielisestä teosta ja voiko sillä olla rajat ylittäviä vaikutuksia sekä näiden vaikutusten todennäköisyys. Kyse olisi eräänlaisesta ennakkovaroituksesta, jonka olisi sisällettävä vain ne tiedot, jotka ovat välttämättömiä, jotta Liikenne- ja viestintävirasto tulee tietoiseksi merkittävästä poikkeamasta ja jotta asianomainen toimija voi tarvittaessa pyytää apua. Tässä pykälässä säädetyt ilmoitusvelvollisuudet – varsinkin ensi-ilmoitus ja 2 momentissa tarkoitettu jatkoilmoitus - tulisi toteuttaa vain siinä laajuudessa, että poikkeaman käsittelyn toimet voidaan suorittaa tehokkaasti. Pykälän 3 momentissa tarkoitetun loppuraportin tarkoituksena on tarjota valvovalle viranomaiselle ja toimijalle itselleen arvokasta kokemusta poikkeamasta ja parantaa ajan mittaan sekä toimijan että julkishallinnon ja muidenkin toimialojen kyberresilienssiä.

Säännöksessä mainitun 24 tunnin aikarajan laskeminen alkaa siitä, kun viranomainen on tullut tietoiseksi merkittävästä poikkeamasta. Tietoiseksi tuleminen voi riippua siitä, tapahtuuko poikkeama virka-aikaan vai yöllä tai viikonloppuna. Säännöksellä ei velvoiteta viranomaista järjestämään ympärivuorokautista päivystystä ensiraportin toimittamista varten. Päivystyksen tarve, kohde ja laajuus arvioidaan viranomaisen 18 b ja c §:n mukaisesti toteutetussa riskienhallinnassa.

Viranomaisen tulisi huolehtia siitä, että sen alihankkija toimittaa sille tarpeelliset tiedot poikkeamailmoituksen tekemiseksi ja tekee yhteistyötä viranomaisen kanssa niin, että viranomainen pystyy täyttämään poikkeamailmoituksia koskevat velvoitteensa. Yksityinen alihankkija voi kuulua yleislaissa tarkoitetun ilmoitusvelvollisuuden piiriin, jos se tarjoaa direktiivin liitteissä kuvattuja TVT-palveluja tai digitaalisen infrastruktuurin palveluja. Tämä ei kuitenkaan poista viranomaisen ilmoitusvelvollisuutta julkishallinnon toimialan valvovalle viranomaiselle.

Valtion tieto- ja viestintätekniikkakeskus Valtorilla on itsenäinen ilmoitusvelvollisuus valtion yhteisiin tieto- ja viestintäteknisiin palveluihin kohdistuvista merkittävistä poikkeamista. Sillä olisi velvollisuus ilmoittaa poikkeamista niille käyttäjäviranomaisille, joita poikkeama koskee, jotta nämä viranomaiset voisivat omalta osaltaan tehdä ilmoituksen Liikenne- ja viestintävirastolle. Valtorin ilmoitus ei yksinomaan olisi riittävä sen palvelua käyttävän viranomaisen osalta, koska Valtori ei välttämättä pysty arvioimaan ilmoituksessa edellytettyjä seikkoja, kuten poikkeaman lopullisia vaikutuksia mukaan lukien mahdollisia rajat ylittäviä vaikutuksia. Valtorin ilmoitusvelvollisuus koskisi vain sen omaa toimintaa ja se ei koskisi sen palveluja käyttävän viranomaisen toimialasidonnaisissa tietojärjestelmissä ilmeneviä merkittäviä poikkeamia, ellei poikkeama ilmene myös Valtorin palvelussa.

Pykälän *2 momentissa* säädettäisiin raportoinnin toisesta vaiheesta eli jatkoilmoituksesta, joka olisi toimitettava ilman aiheetonta viivytystä, viimeistään 72 tunnin kuluessa siitä, kun viranomainen on tullut tietoiseksi merkittävästä poikkeamasta. Jatkoilmoituksessa olisi ajantasaistettava ensi-ilmoituksessa annetut tiedot ja esitettävä ensimmäinen arvio merkittävästä poikkeamasta, sen vakavuudesta ja vaikutuksista sekä vaarantumisindikaattorit (Indicator of Compromise) eli IoC-tieto, jos sellaisia on saatavilla. Viranomainen voisi tehdä ensi- ja jatkoilmoitukset myös kerralla, mikäli sillä olisi ensi-ilmoituksen määräajassa, eli viipymättä ja viimeistään 24 tunnin kuluessa poikkeaman havaitsemista saatavilla molempien ilmoitusten edellyttämät tiedot.

Pykälän *3 momentissa* säädettäisiin merkittävää poikkeamaa koskevasta loppuraportista, joka olisi toimitettava viimeistään kuukauden kuluttua jatkoilmoituksen tekemisestä. Loppuraportin tulisi sisältää yksityiskohtainen kuvaus poikkeamasta, sen vakavuus ja vaikutukset mukaan lukien. Loppuraportissa tulisi myös kuvata poikkeaman todennäköisesti aiheuttaneen uhkan tai juurisyyn tyyppi sekä toteutetut ja meneillään olevat toimenpiteet vaikutusten lieventämiseksi. Jos poikkeamalla on rajat ylittäviä vaikutuksia, myös ne tulisi kuvata.

Ehdotetun *4 momentin* mukaan, jos poikkeama on edelleen meneillään, kun 3 momentissa tarkoitettu loppuraportti pitäisi toimittaa, olisi loppuraportin sijaan toimitettava väliraportti. Tämän jälkeen olisi toimitettava loppuraportti kuukauden kuluessa siitä, kun viranomainen on lopulta käsitellyt poikkeaman. Väliraportin tarkoituksena olisi kuvata poikkeaman käsittelyn etenemistä, poikkeaman vaikutuksia ja muita asian vaikutukseen liittyviä olennaisia tekijöitä sekä muutoksia ensi- ja jatkoilmoituksen tietoihin. Liikenne- ja viestintävirasto voisi poikkeaman kestäessä pyytää viranomaiselta lisätietoja tai väliraportin asiaan liittyvistä tilannepäivityksistä ja käsittelyn etenemisestä.

18 e §. *Poikkeamailmoituksen vastaanottaminen.* Pykälässä säädettäisiin Liikenne- ja viestintäviraston vastauksesta poikkeamailmoitukseen. Pykälä perustuu direktiivin 23 artiklan 5 kohtaan.

Liikenne- ja viestintäviraston olisi pykälän mukaan ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 24 tunnin kuluessa 18 d §:n 1 momentissa tarkoitetun ensi-ilmoituksen vastaanottamisesta annettava viranomaiselle vastaus. Tämä ei kuitenkaan edellyttäisi valmiutta päivystää viikonloppuisin, öisin tai arkipyhinä. Vastauksessa olisi oltava alustava palaute merkittävästä poikkeamasta, viranomaisen pyynnöstä ohjeita tai operatiivisia neuvoja koskien poikkeaman käsittelyä sekä ohjeet merkittävän poikkeaman ilmoittamisesta esitutkintaviranomaiselle, jos asiassa epäillään rikosta. NIS2-direktiivin 23 artiklan 5 kohdan mukaan, jos CSIRT-yksikkö ei ole ilmoituksen vastaanottaja, toimivaltaisen viranomaisen on annettava ohjeet yhteistyössä CSIRT:n kanssa. Liikenne- ja viestintävirastossa toimiva NIS2 – direktiivissä tarkoitettu CSIRT-yksikkö osallistuisi tarvittavalla tavalla poikkeamailmoituksen käsittelyyn.

18 f §. *Vapaaehtoinen ilmoittaminen.* Pykälässä säädettäisiin viranomaisten ja muiden julkishallinnon toimijoiden mahdollisuudesta ilmoittaa Liikenne- ja viestintävirastolle myös vapaaehtoisesti poikkeamista, kyberuhkista ja läheltä piti-tilanteista. Pykälä perustuu direktiivin 30 artiklaan. Ehdotetussa kyberturvallisuuden riskienhallintaa koskevassa laissa vapaaehtoisesta ilmoittamisesta säädettäisiin lain 15 §:ssä.

Direktiivin johdanto-osan kappaleen 105 mukaisesti ennakoiva lähestymistapa kyberuhkiin on ratkaiseva osa kyberturvallisuusriskien hallintaa, jonka avulla toimivaltaisten viranomaisten olisi pystyttävä estämään tehokkaasti kyberuhkien toteutuminen poikkeamina, jotka voivat aiheuttaa huomattavaa aineellista ja aineetonta vahinkoa. Tätä varten kyberuhkista ilmoittaminen on erittäin tärkeää. Siksi toimijoita kannustetaan raportoimaan vapaaehtoisesti kyberuhkista.

Pykälän *1 momentin* mukaan viranomainen voisi ilmoittaa Liikenne- ja viestintävirastolle myös muista kuin merkittävistä poikkeamista sekä kyberuhkista ja läheltä piti –tilanteista. Myös muut tiedonhallintalain 3 §:ssä mainitut, joita ilmoitusvelvollisuus ei koskisi, voisivat ilmoittaa merkittävistä poikkeamista, poikkeamista, kyberuhkista ja läheltä piti –tilanteista Liikenne- ja viestintävirastolle.

Sähköisen viestinnän palveluista annetun lain 304 §:n 7 kohdan mukaan Liikenne- ja viestintäviraston tehtäviin kuuluu kerätä tietoa verkkopalveluihin, viestintäpalveluihin, lisäarvopalveluihin sekä tietojärjestelmiin kohdistuvista tietoturvaloukkauksista ja niiden uhkista sekä viestintäverkkojen ja viestintäpalvelujen vika- ja häiriötilanteista. Liikenne- ja viestintävirasto ottaa jo nykyisin vastaan tietoturvallisuusloukkauksia ja –uhkia koskevia ilmoituksia ja käsittelee niitä resurssiensa mukaan. Säännöksellä ei ole tarkoitus rajoittaa kuvattua mahdollisuutta vapaaehtoisesti ilmoittaa Liikenne- ja viestintävirastolle. Direktiivissä kuitenkin edellytetään, että näitä vapaaehtoisia ilmoituksia käsitellään lähtökohtaisesti vastaavalla tavalla kuin niitä ilmoituksia, joita koskee 18 d §:ssä tarkoitettu raportointivelvollisuus.

Mikäli poikkeamalla on rajat ylittäviä vaikutuksia, on CSIRT-yksikön, toimivaltaisen viranomaisen tai keskitetyn yhteyspisteen tarvittaessa ja erityisesti silloin, kun merkittävä poikkeama koskee vähintään kahta jäsenvaltiota, tiedotettava merkittävästä poikkeamasta ilman aiheetonta viivytystä niille muille jäsenvaltioille, joihin poikkeama vaikuttaa, ja ENISAlle (23 artikla 6 kohta). Lisäksi keskitetyn yhteyspisteen on toimitettava ENISAlle kolmen kuukauden välein yhteenvetoraportti, joka sisältää anonymisoidut koontitiedot merkittävistä poikkeamista, poikkeamista, kyberuhkista ja läheltä piti -tilanteista, joista on ilmoitettu joko ilmoitusvelvoitteen johdosta tai vapaaehtoisesti (23 artikla 9 kohta). Näistä yhteistyövelvoitteista säädettäisiin kyberturvallisuuden riskienhallintaa koskevan lain 17 ja 18 §:ssä ja näihin velvoitteisiin viitattaisiin ehdotetussa tiedonhallintalain 18 h §:n 3 momentissa.

Pykälän *2 momentin* mukaan Liikenne- ja viestintäviraston olisi käsiteltävä vapaaehtoiset ilmoitukset 18 e §:ssä säädettyä menettelyä noudattaen, mutta Liikenne- ja viestintävirasto voisi asettaa etusijalle 18 d §:ssä tarkoitettujen ilmoitusten käsittelyn vapaaehtoisten ilmoitusten käsittelyyn nähden.

Pykälän *3 momentissa* säädettäisiin tietojen luovuttamisesta vapaaehtoisen ilmoituksen yhteydessä. Viranomaiset ja muut lain 3 §:ssä mainitut voisivat vapaaehtoisen ilmoituksen yhteydessä luovuttaa Liikenne- ja viestintävirastolle tietoja, jotka Liikenne- ja viestintävirastolla on oikeus saada 18 i §:n 1 ja 2 momentin nojalla. Tietojen luovuttamiseen sovellettaisiin myös, mitä 18 i §:n 3 momentissa säädetään eräiden salassa pidettävien tietojen luovuttamisesta.

18 g §. *Tiedotusvelvollisuus merkittävästä kyberuhkasta ja poikkeamasta.* Pykälässä säädettäisiin tiedonhallintayksikön velvollisuudesta tiedottaa sen palveluihin kohdistuvista merkittävistä kyberuhkista ja poikkeamista. Pykälä perustuu NIS2 – direktiivin 23 artiklan 1, 2 ja 7 kohtaan sekä 32 artiklan 4 kohdan e)-alakohtaan. Kyberturvallisuuden riskienhallintaa koskevassa laissa vastaava sääntely sisältyisi lain 14 §:ään.

Pykälän *1 momentin* mukaan viranomaisen olisi ilmoitettava viipymättä merkittävästä poikkeamasta sen palvelujen vastaanottajille, jos merkittävä poikkeama todennäköisesti haittaa sen palvelujen tarjoamista.

Pykälän *2 momentin* mukaan viranomaisen olisi ilmoitettava viipymättä merkittävästä kyberuhkasta sekä kyberuhkan hallitsemiseksi käytettävissä olevista toimenpiteistä niille palvelujensa vastaanottajille, joihin merkittävä kyberuhka saattaa vaikuttaa.

Pykälän *3 momentissa* säädettäisiin tilanteesta, jossa merkittävän poikkeaman julkistaminen on yleisen edun mukaista. Yleisen edun mukaisesta tilanteesta olisi kyse esimerkiksi silloin, kun yleinen tietoisuus olisi tarpeen merkittävän poikkeaman estämiseksi tai meneillään olevan merkittävän poikkeaman käsittelemiseksi. Jos poikkeamasta ilmoittaminen yleisölle on yleisen edun mukaista, Liikenne- ja viestintävirasto voisi velvoittaa viranomaisen tiedottamaan merkittävästä poikkeamasta tai kuultuaan viranomaista tiedottaa asiasta itse. NIS2 – direktiivin 23 artiklan 7 kohdan mukaan jäsenvaltion CSIRT-yksikkö tai tapauksen mukaan sen toimivaltainen viranomainen sekä tarvittaessa muiden asianomaisten jäsenvaltioiden CSIRT-yksiköt tai toimivaltaiset viranomaiset voivat asianomaista toimijaa kuultuaan tiedottaa merkittävästä poikkeamasta yleisölle tai vaatia toimijaa tekemään niin.

18 h §. *Toimivaltainen viranomainen.* Pykälässä säädettäisiin NIS 2 – direktiivin julkishallinnon toimialan toimivaltaisen viranomaisen tehtävästä sekä siihen kuuluvasta valvontatehtävästä. Pykälä perustuu NIS 2 – direktiivin 8 artiklan 1 ja 2 kohtaan, 31 artiklaan ja 32 artiklan 4 kohdan g alakohtaan ja 7 kohtaan sekä 33 artiklan 1 kohtaan.

Pykälän *1 momentin* mukaan Liikenne- ja viestintäviraston tehtävänä olisi toimia NIS 2 – direktiivin 8 artiklan 1 kohdassa tarkoitettuna toimivaltaisena viranomaisena julkishallinnon toimialalla. Julkishallinnon toimiala määriteltäisiin 18 a §:ssä. Momentin toisen virkkeen mukaan Liikenne- ja viestintäviraston tehtävänä olisi sen lisäksi mitä edellä tässä luvussa säädetään poikkeamailmoitusten käsittelystä, valvoa tässä luvussa ja tämän luvun tai NIS 2 – direktiivin nojalla annetuissa säädöksissä säädettyjen velvoitteiden noudattamista julkishallinnon toimialalla sekä ylläpitää julkishallinnon toimialan toimijaluetteloa 18 a §:n nojalla toimitetuista tiedoista.

Liikenne- ja viestintävirastolla ei, toisin kuin ehdotetun kyberturvallisuuden riskienhallintaa koskevan lain mukaisella valvovalla viranomaisella, olisi määräyksenantovaltuutta. Sen sijaan Liikenne- ja viestintävirasto voi luonnollisesti laatia ohjeita ja suosituksia kyberturvallisuusriskien hallintatoimista ja hyvistä käytännöistä. Liikenne- ja viestintäviraston ja tiedonhallintalautakunnan tulisi tehdä yhteistyötä tietoturvallisuuteen ja kyberturvallisuuteen liittyvien ohjeiden ja suositusten laatimisessa niin, että niiden antama ohjeistus olisi tarvittavilta osin yhdenmukaista.

Pykälän *2 momentin* mukaan Liikenne- ja viestintäviraston olisi valvontatoimiaan suorittaessaan ja 18 l §:ssä tarkoitettua valvontapäätöstä tehdessään otettava huomioon NIS2 – direktiivin 32 artiklan 7 kohdassa säädetyt seikat, kuten mainitussa direktiivin kohdassa edellytetään. Lisäksi 2 momentissa mahdollistettaisiin direktiivin sallimalla tavalla, että Liikenne- ja viestintävirasto voisi asettaa tässä laissa säädetyt valvontatehtävänsä tärkeysjärjestykseen soveltaen riskiperusteista lähestymistapaa. Viranomaisen valvonnan, eli toimijoihin kohdistettavien toimenpiteiden ja niiden määrän tulisi olla tällöin suhteellista ja perustua kyberturvallisuusriskien arviointiin. Direktiivin johdanto-osan kappaleen 124 mukaan toimivaltainen viranomainen voisi luokitella keskeiset toimijat riskiluokkiin ja määritellä kullekin riskiluokalle suositeltavat valvontatoimenpiteet ja -keinot, kuten paikalla tehtävien tarkastusten, kohdennettujen turvallisuusauditointien tai turvallisuusskannausten käyttö, aikaväli ja tyypit sekä pyydettävien tietojen tyyppi ja yksityiskohtaisuus. Tällaisten valvontamenetelmien ohella voitaisiin käyttää työohjelmia, ja niitä voitaisiin arvioida ja tarkastella uudelleen säännöllisesti, myös esimerkiksi resurssien jakamisen ja tarpeiden osalta. Julkishallinnon toimijoiden suhteen valvontavaltuuksia olisi käytettävä kansallisten lainsäädäntö- ja toimielinkehysten mukaisesti.

Lisäksi 2 momentissa säädettäisiin, että Liikenne- ja viestintävirasto voisi kohdistaa valvontaa hyvinvointialueeseen, hyvinvointiyhtymään tai Helsingin kaupunkiin vain, jos on perusteltu syy epäillä, että mainittu ei ole noudattanut tässä luvussa taikka tämän luvun tai NIS 2 – direktiivin

nojalla annetuissa säädöksissä säädettyä. Direktiivin mukaan toimijaan tulee kohdistaa etukäteisvalvontaa vain, jos se on keskeinen toimija. Muihin (tärkeisiin) toimijoihin kohdistetaan vain jälkikäteisvalvontaa. Hyvinvointialueet, hyvinvointiyhtymät ja Helsingin kaupunki olisivat NIS 2 –direktiivin mukaisia tärkeitä toimijoita. Perustellulla syyllä tarkoitettaisiin valvovan viranomaisen tietoon tulevaa näyttöä, viitteitä tai tietoja, joiden mukaan toimija ei väitetysti noudattaisi sille laissa säädettyjä velvoitteita erityisesti riskienhallinnan tai raportoinnin osalta. Tällaista näyttöä, viitteitä tai tietoja voivat olla esimerkiksi muiden viranomaisten, toimijoiden, kansalaisten, tiedotusvälineiden tai muiden lähteiden toimittamat tai julkisesti saatavilla olevat tiedot tai valvovalle viranomaiselle tehty ilmianto, joka ei ole ilmeisen perusteeton.

Direktiivin 32 artiklan 4 kohdan g alakohdassa edellytetään, että toimivaltaisen viranomaisen pitää voida nimetä valvova virkamies, joka valvoo tarkoin määriteltyjen tehtävien puitteissa määräkauden ajan, että asianomaiset toimijat noudattavat 21 ja 23 artiklaa. Liikenne- ja viestintävirasto voisi ilman erityistä lain säännöstäkin antaa palveluksessaan olevalle virkamiehelle valvontaan liittyviä erityisiä tehtäviä ja kohdentaa erityistä valvontaa toimijaan tai toimijoihin.

Pykälän *3 momentti* sisältäisi aineellisen viittaussäännöksen ehdotettuun lakiin kyberturvallisuuden riskienhallinnasta. Tiedonhallintalaissa säädettäisiin ainoastaan toimijoiden velvoitteista ja niiden noudattamisen valvonnasta ja valvontatoimista NIS2 – direktiivin liitteen I 10 kohdassa tarkoitetulla julkishallinnon toimialalla. Muilta osin direktiivin sääntely pantaisiin täytäntöön ehdotetulla lailla kyberturvallisuuden riskienhallinnasta.

Liikenne- ja viestintäviraston olisi 18 a §:ssä tarkoitettujen toimintaa koskevien ilmoitusten, 18 d ja f §:ssä tarkoitettujen poikkeamailmoitusten ja muiden valvontatehtävässä saatujen tietojen käsittelyssä sekä yhteistyössä NIS 2 – direktiivissä tarkoitettujen muiden viranomaisten, Euroopan unionin toimielinten, erillisvirastojen ja yhteistyöelinten kanssa sekä tietojen luovuttamisessa niille noudatettava mitä kyberturvallisuuden riskienhallinnasta annetun lain 6 §:n 4 momentissa, 15 §:n 3 momentissa, 17 §:ssä, 25 §:n 3 momentissa, 27 §:n 2 momentissa, 34 §:ssä, 43 §:n 4 momentissa ja 46 §:ssä säädetään tietojen käsittelystä valvovassa viranomaisessa sekä valvovan viranomaisen yhteistyöstä NIS 2 – direktiivissä tarkoitettujen muiden viranomaisten, Euroopan unionin toimielinten, erillisvirastojen ja yhteistyöelinten kanssa sekä tietojen luovuttamisesta niille.

Lisäksi momentissa todettaisiin informatiivisesti, että NIS 2 – direktiivissä tarkoitetusta keskistetystä yhteyspisteestä ja CSIRT-yksiköstä ja niiden tehtävistä, tietojen käsittelystä sekä yhteistyöstä NIS 2 – direktiivissä tarkoitettujen muiden viranomaisten, Euroopan unionin toimielinten, erillisvirastojen ja yhteistyöelinten kanssa säädetään kyberturvallisuuden riskienhallinnasta annetussa laissa.

18 i §. *Toimivaltaisen viranomaisen tiedonsaantioikeus.* Pykälässä säädettäisiin Liikenne- ja viestintäviraston tiedonsaantioikeuksista. Pykälä perustuu NIS2 – direktiivin 32 artiklan 2 kohdan ensimmäisen alakohdan e-g kohtiin, 32 artiklan 2 kohdan 3 alakohtaan sekä 32 artiklan 3 kohtaan. Ehdotetun 2 momentin osalta kyse on kansallisesta sääntelystä, jolla selvennetään viestintään liittyvien tietojen käsittelyä toimivaltaisessa viranomaisessa.

Pykälän *1 momentin* mukaan Liikenne- ja viestintävirastolla olisi 4 a luvun mukaisia tehtäviä suorittaessaan oikeus saada salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä tehtäviensä suorittamiseksi välttämättömät tiedot viranomaisilta, joihin sovelletaan 4 a lukua. Viranomaisen olisi luovutettava tiedot viipymättä, pyydetyssä muodossa ja maksutta.

Liikenne- ja viestintävirastolla olisi oikeus päästä dataan, asiakirjoihin ja tietoihin sekä saada näyttöä kyberturvallisuusperiaatteiden täytäntöönpanosta, kuten mahdolliset 18 k §:n perusteella tai muutoin tehtyjen arviointien tulokset ja niiden perustana oleva näyttö. Tiedonsaantioikeus koskisi myös tilannetta, jossa viranomainen on ulkoistanut osan tai kaikki kyberturvallisuusprosesseistaan. Viranomainen olisi silloin velvollinen hankkimaan pyydetyt tiedot toimittajaltaan. Liikenne- ja viestintävirastolla olisi lisäksi oikeus saada esimerkiksi ulkoistamiseen liittyvät tiedot, kuten siihen liittyvät sopimukset. Pyytäessään viranomaiselta tietoja, valvovan viranomaisen olisi ilmoitettava pyynnön tarkoitus ja täsmennettävä pyydetyt tiedot.

Pykälän *2 momentin* mukaan Liikenne- ja viestintävirastolla olisi salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada viranomaiselta välitystieto, sijaintitieto tai haitallisen tietokoneohjelman tai käskyn sisältävä viesti, jos se on välttämätöntä 18 b ja c §:ssä säädettyjen kyberturvallisuuden riskienhallintavelvoitteiden noudattamisen valvomiseksi tai merkittävän poikkeaman selvittämiseksi.

Lisäksi 2 momentissa säädettäisiin, että mainittujen tietojen käsittelyyn Liikenne- ja viestintävirastossa sovelletaan mitä sähköisen viestinnän palveluista annetun lain 316 §:n 4 momentissa ja 319 §:ssä säädetään Liikenne- ja viestintäviraston viestistä, välitystiedosta, sijaintitiedosta sekä luottamuksellisen radiolähetyksen sisällöstä ja olemassaolosta saamien ja hankkimien tietojen salassapidosta, luovuttamisesta ja hävittämisestä. Liikenne- ja viestintävirastolla on sähköisen viestinnän palveluista annetun lain 319 §:n 2 momentin nojalla oikeus luovuttaa tietoturvaloukkauksia koskevan tiedonkeruun ja selvittämisen yhteydessä saamiaan välitystietoja ja muita tietoja viestinnän välittäjälle, lisäarvopalvelun tarjoajalle, yhteisölle, tilaajalle ja käyttäjälle jos sitä on käytetty hyväksi tietoturvaloukkauksessa, se on joutunut tietoturvaloukkauksen kohteeksi tai siihen todennäköisesti voi kohdistua tietoturvaloukkaus ja jos Liikenne- ja viestintäviraston arvion mukaan on syytä epäillä, että on tehty jokin lain 316 §:n 2 momentin 1–12 kohdassa mainittu rikos. Mainittu säännös mahdollistaa sen, että Liikenne- ja viestintävirastolle toimitettuja tai sen valvontatoimen yhteydessä saamia tietoja voidaan hyödyntää kyberturvallisuusuhkien torjunnassa sekä poikkeamien käsittelyssä myös muissa tahoissa kuin siinä viranomaisessa, jolta tiedot ovat peräisin. Sähköisen viestinnän palveluista annetun lain 319 §:n 3 momentin mukaan Liikenne- ja viestintävirastolla on oikeus luovuttaa tietoja siten kuin 2 momentissa säädetään ainoastaan siinä laajuudessa kuin se on tarpeen tietoturvaloukkausten ehkäisemiseksi ja selvittämiseksi eikä tietojen luovuttamisella saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.

Pykälän *3 momentissa* säädettäisiin Liikenne- ja viestintäviraston tiedonsaantioikeuden rajoituksista. Säännöksen ensimmäisen virkkeen mukaan pykälässä säädetty tiedonsaantioikeus ei velvoittaisi luovuttamaan Liikenne- ja viestintävirastolle tietoja turvallisuusverkkolaissa tarkoitetusta turvallisuusverkon palvelutuotannosta tai palvelujen käytöstä eikä tietoja, joiden luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin niihin liittyvää tärkeää etua.

Säännöksen toisen virkkeen mukaan viranomainen voisi kuitenkin (vapaaehtoisesti ja harkintansa mukaan) luovuttaa julkisuuslain julkisuus- tai salassapito-olettaman sisältävän salassapitosäännöksen osoittamissa rajoissa Liikenne- ja viestintävirastolle tietoja myös turvallisuusverkon palvelutuotannosta ja palvelujen käytöstä sekä maanpuolustukseen ja kansalliseen turvallisuuteen liittyviä tietoja, jotka ovat yleisöltä salassa pidettäviä. Säännöksen toisella virkkeellä on tarkoitus selventää sitä, että vaikka mainitut tiedot on lähtökohtaisesti rajattu Liikenne- ja viestintäviraston tiedonsaantioikeuden ulkopuolelle, niin niitä voitaisiin viranomaisen harkinnan mukaan, kuten tähänkin asti, luovuttaa Liikenne- ja viestintävirastolle julkisuuslaissa sallitulla tavalla. Mahdollisuus voisi tulla sovellettavaksi esimerkiksi silloin kun viranomainen, jo-

hon 4 a lukua ei sovellettaisi toiminnan ollessa maanpuolustukseen tai kansalliseen turvallisuuteen liittyvää, haluaisi vapaaehtoisesti ilmoittaa Liikenne- ja viestintävirastolle kyberuhkasta tai poikkeamasta. Julkisuuslaki mahdollistaa yleisöltä salassa pidettävän asiakirjan luovuttamisen (yleensä toiselle viranomaiselle), jos salassapitosäännös sisältää vahinkoedellytyslausekkeen eikä salassapitosäännöksen suojaama intressi vaarannu tietoa luovutettaessa. Tällöin asiakirjaan merkitään salassa pitoa ja mahdollista turvallisuusluokkaa koskeva tieto sen osoittamiseksi, minkälaisia tietoturvallisuustoimenpiteitä asiakirjaa käsiteltäessä noudatetaan. Samalla merkinnällä osoitetaan merkitsijän käsitys siitä, että asiakirja on salassa pidettävä. Julkisuuslakiin sisältyvä edellä kuvattu mahdollisuus luovuttaa yleisöltä salassa pidettäviä asiakirjoja ja tietoja toiselle viranomaiselle koskee myös Liikenne- ja viestintävirastoa. Näin ollen Liikenne- ja viestintävirasto voi julkisuuslain sallimissa rajoissa luovuttaa saamiaan salassa pidettäviä tietoja toisille viranomaisille, esimerkiksi kyberturvallisuusuhkan torjumiseksi tai poikkeaman käsittelemiseksi. Tietojen luovuttamisella ei saa vaarantaa niitä etuja, joita salassapitosäännöksellä tai -säännöksillä suojataan. Tietojen luovuttamisessa on otettava huomioon myös turvallisuusluokiteltua tietoa koskeva lähtökohta, jonka mukaan sen antamisesta päättää asiakirjan laatinut viranomainen.

Momentin kolmannessa virkkeessä säädettäisiin turvallisuusluokiteltuun tietoon liittyen, että jos viranomainen olisi luovuttamassa Liikenne- ja viestintävirastolle sen 1 ja 2 momentissa säädetyn tiedonsaantioikeuden ulkopuolelle jäävää asiakirjaa, jonka toinen viranomainen on turvallisuusluokitellut tai jonka käsiteltäväksi asiakirjan sisältämän tiedon luonteen arviointi kokonaisuudessaan kuuluu, asiakirjan tai tiedon antamisesta päättäisi luokittelun tehnyt viranomainen tai se viranomainen, jonka arvioitavaksi asia kokonaisuudessaan kuuluu.

Erityisesti pykälän 3 momentin mukaisia tietoja luovutettaessa on syytä harkita tietojen edelleen luovuttamisen rajoittamista, mikäli tiedon luovuttaminen vaarantaisi Suomen keskeisiä turvallisuusetuja. Tässä yhteydessä olisi arvioitava myös, onko mahdollista luovuttaa jotain uhkaan tai poikkeamaan yleisellä tasolla liittyvää tietoa siten, että Suomen keskeiset turvallisuusedut eivät vaarannu. NIS 2 –direktiivissä ei edellytetä ehdotetussa 3 momentissa tarkoitettujen tietojen luovuttamista esimerkiksi EU:n toimielimille, erillisvirastoille, yhteistyöelimille taikka muille viranomaisille. Erityisesti turvallisuusluokitellun salassa pidettävän tiedon kohdalla korostuu sen viranomaisen arvio, jolla on edellytykset arvioida tiedon luonnetta suhteessa salassapitosäännöksellä suojattuun etuun. Julkisuuslain 15 §:n 3 momentin mukaan, jos viranomaiselta pyydetään asiakirjaa, johon julkisen hallinnon tiedonhallinnasta annetun lain mukaisesti on ollut velvollisuus tehdä asiakirjaa käsiteltäessä noudettavia tietoturvallisuusvaatimuksia koskeva turvallisuusluokkamerkintä ja jonka muu viranomainen on laatinut, viranomaisen on siirrettävä asia asiakirjan laatineen viranomaisen ratkaistavaksi.

Momentin neljännen virkkeessä todettaisiin selvyyden vuoksi, että kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitetun erityissuojattavan tietoaineiston käsittelyssä on noudatettava mitä mainitussa laissa säädetään. Erityissuojattavan tietoaineiston luovuttamisen edellytyksiä olisi siis arvioitava mainitun lain ja tietoaineistoon soveltuvan kansainvälisen tietotuvallisuusvelvoitteen perusteella.

18 j §. *Tarkastusoikeus.* Pykälässä säädettäisiin Liikenne- ja viestintäviraston tarkastusoikeudesta. Pykälä perustuu NIS2 – direktiivin 32 artiklan 2 kohdan ensimmäisen alakohdan a-d kohtiin sekä 32 artiklan 2 kohdan toiseen ja kolmanteen alakohtaan.

Pykälän *1 momentin* mukaan Liikenne- ja viestintävirastolla olisi siinä laajuudessa kuin se on tarpeen, oikeus tehdä 4 a luvussa taikka 4 a luvun tai NIS 2 – direktiivin nojalla annetuissa säädöksissä säädettyjen velvoitteiden noudattamisen valvomiseksi viranomaiseen kohdistuva

tarkastus. Tarkastus voitaisiin tehdä joko paikan päällä tai muualla kuin paikan päällä. Tarkastukseen voisi sisältyä teknisiä toimenpiteitä, kuten tietokantojen, laitteistojen, palomuurien, salauksen ja verkkojen heikkouksien tunnistamista turvallisuusskannauksella. Laissa kyberturvallisuuden riskienhallinnasta säädetään erikseen CSIRT-yksikön haavoittuvuuskartoituksista ja niissä saatujen tietojen sallituista käyttötarkoituksista. Liikenne- ja viestintäviraston tarkastukset voisivat olla säännöllisiä, satunnaistarkastuksia tai tapauskohtaisia (esimerkiksi merkittävän poikkeaman jälkeen). Tarkastukset voisivat olla suppeampia, tiettyyn aihealueeseen keskittyviä tai laajempia, toiminnan kokonaisvaltaisia tarkastuksia.

Pykälän *2 momentin* mukaan tarkastuksen suorittajalla olisi oltava tarkastuksen laatuun ja laajuuteen nähden riittävä koulutus ja kokemus. Liikenne- ja viestintäviraston olisi varmistettava, että tarkastuksen suorittajalla on kyseisten tehtävien suorittamiseen vaadittavat taidot ja että tarkastus toteutetaan objektiivisesti.

Pykälän *3 momentin* mukaan tarkastusta suorittavalla olisi tarkastuksen suorittamiseksi oikeus päästä muihin kuin pysyväisluonteiseen asumiseen tarkoitettuihin tiloihin ja tarkastuksen kohteena olevaan viestintäverkkoon tai tietojärjestelmään sekä oikeus salassapitosäännösten estämättä saada tutkittavakseen tarkastustehtävän kannalta tarpeelliset tiedot, asiakirjat, laitteet ja ohjelmistot, suorittaa tarvittavia testejä ja mittauksia sekä tarkastaa viranomaisen toteuttamat turvallisuusjärjestelyt. Liikenne- ja viestintävirastolla olisi tiedonsaantioikeutensa perusteella oikeus myös tarkastusta ennen sekä tarkastuksen kestäessä saada tutkittavakseen viranomaisen kirjallista aineistoa, kuten toimijan laatimia toimintakäsikirjoja, ohjeita, prosessikuvauksia, koulutuskirjanpitoa ja tietoturvallisuusarvioinnin tuloksia.

Lisäksi momentti sisältäisi aineellisen viittaussäännöksen hallintolain 39 § soveltumisesta tarkastuksessa noudatettavaan menettelyyn. Mainittu säännös ei muutoin sovellu valvontatyyppiseen tarkastukseen. Hallintolain 39 §:n 1 momentissa säädetään muun muassa viranomaisen velvollisuudesta ilmoittaa tarkastuksen aloittamisajankohdasta asianosaiselle, jollei ilmoittaminen vaaranna tarkastuksen tarkoituksen toteutumista. Lisäksi säädetään asianosaisen oikeudesta olla läsnä tarkastuksessa sekä siitä, että tarkastus on suoritettava aiheuttamatta tarkastuksen kohteelle tai sen haltijalle kohtuutonta haittaa. NIS2 – direktiivin johdanto-osan 123 kappaleen mukaan ”toimivaltaisten viranomaisten valvontatehtävien suorittaminen ei saisi tarpeettomasti haitata asianomaisen toimijan liiketoimintaa. Kun toimivaltaiset viranomaiset suorittavat keskeisiin toimijoihin liittyviä valvontatehtäviään, kuten paikalla tehtäviä tarkastuksia ja muuta kuin paikalla toteutettavaa valvontaa, tämän direktiivin rikkomisten tutkintaa, turvallisuusauditointia tai turvallisuusskannausta, niiden olisi minimoitava vaikutus asianomaisen toimijan liiketoimintaan”. Hallintolain 39 §:n 2 momentissa säädetään kirjallisesta tarkastuskertomuksesta.

Pykälän *4 momentti* sisältäisi viittauksen 18 i §:n 3 momenttiin ehdotettuihin tiedonsaantioikeuden rajoituksiin, jotka soveltuisivat myös tarkastukseen.

18 k §. *Avustavan tehtävän antaminen hyväksytylle arviointilaitokselle ja arvioinnin teettäminen.* Pykälässä säädettäisiin tietoturvallisuuden arviointilaitoslaissa (1405/2011, jäljempänä *arviointilaitoslaki*) tarkoitetun hyväksytyn tietoturvallisuuden arviointilaitoksen hyödyntämisestä tarkastustoiminnassa sekä tilanteessa, jossa Liikenne- ja viestintävirasto valvovana viranomaisena velvoittaisi viranomaisen itse teettämään kyberturvallisuuden riskienhallintaan kohdistuvan arvioinnin. Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain 3 §:n mukaan valtionhallinnon viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnissa vain Liikenne- ja viestintäviraston palveluja taikka sellaista arviointilaitosta, joka on saanut Viestintäviraston hyväksynnän arviointilaitoslain mukaan. Säännöksen perusteluissa (HE 45/2011 vp, s. 11) todetaan, että

tarkoitus on varmistaa, että valtionhallinnon viranomaiset käyttävät vain luotettavia ulkopuolisia tietoturvallisuuden arviointipalveluja ja että säännös on tarpeen valtionhallinnon tietoturvallisuuden kehittämiseksi yhtenäisellä tavalla ja ilman perustaltaan epäasiallisia kustannuksia. Samoilla perusteilla ehdotetussa säännöksessä rajattaisiin tarkastustehtävän antaminen ja arvioinnin suorittaminen hyväksyttyihin arviointilaitoksiin.

Pykälän *1 momentin* mukaan Liikenne- ja viestintävirasto voisi antaa 18 j §:ssä tarkoitettuun tarkastustehtävään liittyvän avustavan tehtävän tietoturvallisuuden arviointilaitoksista annetussa laissa tarkoitetulle hyväksytylle tietoturvallisuuden arviointilaitokselle. Säännökseen sisältyisi myös hyväksytyn arviointilaitoksen määritelmä. Liikenne- ja viestintävirasto voisi antaa avustavan tehtävän arviointilaitokselle, jonka pätevyysalue olisi soveltuva avustavan tehtävän suorittamiseen.

Pykälän *2 momentin* mukaan Liikenne- ja viestintävirasto voisi velvoittaa viranomaisen teettämään hyväksytyn arviointilaitoksen suorittaman kyberturvallisuuden riskienhallintaan kohdistuvan arvioinnin, jos viranomaiseen on kohdistunut merkittävä poikkeama, joka on aiheuttanut palvelujen vakavan toimintahäiriön tai huomattavaa aineellista tai aineetonta vahinkoa; tai viranomainen on olennaisesti ja vakavasti laiminlyönyt 18 b tai c §:ssä tarkoitettujen kyberturvallisuuden riskienhallintavelvoitteiden noudattamisen. Arvioinnin tilaisi arvioinnin kohteena oleva viranomainen, joka myös vastaisi arvioinnin kustannuksista. Mikäli arviointilaitosten palvelujen saannissa olisi viivettä, Liikenne- ja viestintäviraston tulisi ottaa huomioon tämä velvoittaessaan, esimerkiksi mikäli se asettaa arvioinnin teettämiselle jonkin määräajan.

Pykälän *3 momentin* mukaan hyväksytyn arviointilaitoksen palveluksessa olevaan tarkastuksen tai arvioinnin suorittajaan sovellettaisiin, mitä 18 j §:n 2–4 momentissa säädetään tarkastuksen suorittajan kokemuksesta ja koulutuksesta sekä tarkastuksen suorittajan oikeuksista. Hyväksytyn arviointilaitoksen henkilöstön pätevyys varmistetaan lähtökohtaisesti silloin kun arviointilaitos hyväksytään arviointilaitoslain mukaisessa menettelyssä. Hyväksytyn arviointilaitoksen palveluksessa olevalla tarkastuksen tai arvioinnin suorittajalla olisivat samat tarkastustoimivaltuudet ja tiedonsaantioikeudet kuin Liikenne- ja viestintäviraston palveluksessa olevalla tarkastuksen suorittajalla. Liikenne- ja viestintävirastolla olisi luonnollisesti ehdotetun 18 i §:n nojalla oikeus saada tieto teetetyn tarkastuksen tai arvioinnin tuloksista sekä oikeus 18 l §:n nojalla velvoittaa viranomainen korjaaviin toimenpiteisiin, mikäli tarkastuksessa tai arvioinnissa käy esille, että viranomainen ei ole noudattanut 4 a luvussa taikka 4 a luvun tai NIS 2 – direktiivin nojalla annetuissa säädöksissä säädettyjä velvoitteita.

Lisäksi 3 momentissa säädettäisiin hyväksytyn arviointilaitoksen palveluksessa olevan henkilön rikosoikeudellisesta virkavastuusta ja siihen sisältyisi myös informatiivinen viittaus vahingonkorvauslakiin.

18 l §. *Seuraamukset.* Pykälässä säädettäisiin Liikenne- ja viestintäviraston valvontapäätöksestä eli oikeudesta velvoittaa tiedonhallintayksikkö toteuttamaan 4 a luvussa tai sen nojalla taikka NIS 2 –direktiivin nojalla säädetyt velvoitteet. Pykälä perustuu NIS2 – direktiivin 32 artiklan 1, 4 ja 7 kohtaan.

Pykälän *1 momentin* mukaan Liikenne- ja viestintävirasto voisi päätöksellään velvoittaa viranomaisen määräajassa korjaamaan puutteet tässä luvussa taikka tämän luvun tai NIS2-direktiivin nojalla annetuissa säädöksissä säädettyjen velvoitteiden noudattamisessa. Liikenne- ja viestintävirasto voisi myös velvoittaa viranomaisen julkistamaan kyseiset puutteet tai muut seikat, jotka liittyvät mainittujen säännösten rikkomiseen. Liikenne- ja viestintävirasto voisi päätöksessään yksilöidä ne toimenpiteet, jotka on suoritettava poikkeaman ehkäisemiseksi tai korjaa-

miseksi tai muun puutteen korjaamiseksi. Momentin mukainen valvontapäätös olisi hallintopäätös, jonka tekemiseen sovellettaisiin hallintolakia. Asiaa selvitettäessä ja ratkaistaessa tulisi siten ottaa huomioon, sen lisäksi mitä tässä pykälässä säädetään, muun muassa hallintolaissa asian selvittämisestä, asianosaisen kuulemisesta sekä päätöksen perustelemisesta säädetty.

Pykälän *2 momentin* mukaan Liikenne- ja viestintävirasto voisi antaa viranomaiselle huomautuksen tai varoituksen. Varoituksen voisi antaa, jos huomautusta ei asiasta ilmenevät seikat kokonaisuudessaan huomioiden voitaisi pitää riittävänä.

Pykälän *3 momentissa* säädettäisiin Liikenne- ja viestintäviraston mahdollisuudesta asettaa uhkasakko valvontapäätöksen toteuttamisen tehosteeksi. Pykälä perustuu NIS2 – direktiivin 32 artiklan 1 kohtaan, jonka mukaan jäsenvaltioiden on varmistettava, että keskeisiä toimijoita koskevat tässä direktiivissä säädettyjen velvoitteiden noudattamisen valvonta- tai täytäntöönpanotoimenpiteet ovat vaikuttavia, oikeasuhteisia ja varoittavia ja että niissä otetaan huomioon kunkin yksittäisen tapauksen olosuhteet sekä 34 artiklan 6 kohtaan, jonka mukaan jäsenvaltiot voivat säätää valtuudesta määrätä uhkasakkoja, jotta keskeinen tai tärkeä toimija saadaan lopettamaan tämän direktiivin rikkominen toimivaltaisen viranomaisen aiemman päätöksen mukaisesti. Julkishallinnon toimialalla ei direktiivin 32 artiklan 5 kohdan mukaan edellytetä sovellettavan toiminnan keskeyttämisen mahdollistavia velvoitteita eikä julkishallinnon toimialalla ole direktiivin 34 artiklan 7 kohdan mukaan välttämätöntä soveltaa hallinnollista sakkoa täytäntöönpanokeinona. Mainittuja päätöksen täytäntöönpanon tehosteita ei ole tarkoitus soveltaa julkishallinnon toimialalla, joten täytäntöönpanon tehosteeksi jää virkavastuun lisäksi uhkasakko. Momenttiin sisältyisi myös informatiivinen viittaus uhkasakkolakiin.

18 m §. *Muutoksenhaku.* Pykälään sisältyisi säännös mahdollisuudesta hakea oikaisua Liikenne- ja viestintäviraston valvontapäätökseen sekä informatiiviset viittaukset oikaisuvaatimusmenettelyä ja muutoksenhakua koskeviin yleislakeihin.

7.3 Laki sähköisen viestinnän palveluista annetun lain muuttamisesta

2 §. *Eräiden säännösten soveltaminen*. Säännöksen 2 momentti ehdotetaan kumottavaksi. Momentissa säädetään kumottavaksi ehdotettavassa 247 a §:ssä tarkoitetun verkossa toimivan markkinapaikan, hakukonepalvelun ja pilvipalvelun tarjoajan toimintaan sovellettavasta lainsäädännöstä EU-jäsenvaltioiden kesken NIS1-direktiivin mukaisesti. Momentti kumottaisiin 247 a §:n kumoamisen johdosta tarpeettomana, koska näitä toimijoita koskeva NIS2-direktiivin mukainen sääntely pantaisiin täytäntöön ensimmäisellä lakiehdotuksella. Vastaava säännös sisältyisi ensimmäisen lakiehdotuksen 2 §:n 3 momenttiin.

165 §. *Verkkotunnusvälittäjän ilmoitusvelvollisuudet.* Säännöksen *1 momenttia* ehdotetaan muutettavan siten, että verkkotunnusvälittäjän ilmoitusvelvollisuutta laajennettaisiin kattamaan NIS2-direktiivin 27 artiklan 2 kohdassa tarkoitetut tiedot. Verkkotunnusvälittäjien tulisi siten ilmoittaa verkkotunnusrekisteriä hallinnoivalle viranomaiselle eli Liikenne- ja viestintävirastolle myös eräitä osoitetietoja ja muita ajantasaisia yhteystietoja, IP-osoitealueet sekä luettelo jäsenvaltioista joissa se tarjoaa palvelujaan. Ehdotuksella täytäntöönpantaisiin NIS2-direktiivin 27 artiklan 2 kohta verkkotunnusvälittäjien osalta.

Lisäksi säännökseen lisättäisiin *uusi 4 momentti*, jonka mukaan Liikenne- ja viestintäviraston olisi toimitettava eräitä tietoja verkkotunnusvälittäjien ilmoituksista myös kyberturvallisuuden riskienhallinnasta annetun lain 19 §:ssä tarkoitetulle keskitetylle yhteyspisteelle NIS2-direktiivin 27 artiklan 4 kohdassa tarkoitetun ilmoituksen tekemiseksi.

167 §. *Tietojen merkitseminen verkkotunnusrekisteriin ja tietojen julkaiseminen*. Säännöksen *1 momenttia* ehdotetaan muutettavaksi NIS2-direktiivin 28 artiklan 1 ja 2 kohdan edellyttämällä tavalla. Verkkotunnuksen käyttäjä olisi velvollinen ilmoittamaan verkkotunnusvälittäjälle oikeat, ajantasaiset ja yksilöivät käyttäjä- ja yhteystiedot sekä niissä tapahtuvat muutokset. Verkkotunnusvälittäjän tai sen puolesta toimivan tahon, kuten yksityisyys- tai välityspalvelujen tarjoajan tai jälleenmyyjän, olisi merkittävä verkkotunnusrekisteriin verkkotunnuksen käyttäjää koskevien tietojen lisäksi myös rekisteröityä verkkotunnusta koskevat tiedot, kuten tieto rekisteröidystä verkkotunnuksesta sekä rekisteröintipäivä.

Säännökseen ehdotetaan lisättävän *uusi 2 momentti*, jonka mukaan Liikenne- ja viestintävirasto voisi estää verkkotunnuksen rekisteröinnin verkkotunnusrekisteriin, jos se epäilee 1 momentissa tarkoitettujen tietojen olevan puutteellisia tai virheellisiä. Liikenne- ja viestintäviraston olisi kuitenkin ensin kehotettava verkkotunnusvälittäjää todentamaan tiedot oikeiksi kohtuullisessa määräajassa. Liikenne- ja viestintäviraston olisi julkaistava käytössään olevat, käyttäjätietojen oikeellisuuden varmistamista koskevat toimintaperiaatteet ja menettelyt.

Säännöksen aikaisemmat 2-4 momentit siirtyisivät uuden 2 momentin lisäämisen johdosta 3-5 momenteiksi. Säännöksen *3 momenttia* ehdotetaan muutettavaksi siten, että Liikenne- ja viestintävirasto olisi velvollinen julkaisemaan verkkotunnusrekisterin tiedot. Tiedot olisi julkaistava ilman aiheetonta viivytystä ja joko Liikenne- ja viestintäviraston internet-sivuilla tai muussa sähköisessä palvelussa. Velvoite ei kuitenkaan koskisi rekisterin sisältämiä henkilötietoja, vaan henkilötietojen luovuttamiseen viranomaisen ylläpitämästä rekisteristä säädetään erikseen viranomaisen toiminnan julkisuudesta annetun lain (1999/621, jäljempänä *julkisuuslaki*) 16 §:n 3 momentissa. Julkisuuslaista poiketen Liikenne- ja viestintäviraston olisi kuitenkin vastattava verkkotunnusten rekisteritietoihin pääsyä koskevaan pyyntöön ilman aiheetonta viivytystä ja viimeistään 72 tunnin kuluessa pyynnön vastaanottamisesta. Vastaamiselle asetettava määräaika ei tarkoittaisi sitä, että tietopyyntö olisi käsiteltävä kokonaisuudessaan annetussa 72 tunnin määräajassa. Mikäli esimerkiksi Liikenne- ja viestintävirastolle toimitettu tietopyyntö on sillä tavalla puutteellinen tai epäselvä, että sen perusteella ei voida arvioida, onko tietojen luovuttaminen tietosuojalainsäädännön mukaista, Liikenne- ja viestintäviraston olisi vastattava tietopyynnön esittäjälle esimerkiksi lisätietopyynnöllä laissa asetetun määräajan kuluessa. Liikenne- ja viestintäviraston olisi lisäksi julkaistava käytössään olevat toimintaperiaatteet ja menettelyt verkkotunnusten rekisteröintitietojen luovuttamisesta.

Säännöksen *5 momentissa* on säädetty Liikenne- ja viestintävirastolle annettavasta määräyksenantovaltuudesta. Liikenne- ja viestintäviraston määräyksenantovaltuutta ehdotetaan laajennettavan siten, että Liikenne- ja viestintävirasto voisi antaa tarkempia määräyksiä myös verkkotunnuksen käyttäjää koskevien tietojen varmistamisesta. Tällä tarkoitettaisiin esimerkiksi toimintaperiaatteita ja menettelyjä, joita verkkotunnusvälittäjien olisi otettava käyttöön, jotta ne voivat varmistua siitä että 1 momentissa tarkoitetut, verkkotunnuksen käyttäjän ilmoittamat tiedot ovat oikeita ja ajantasaisia.

Ehdotetuilla muutoksilla pantaisiin täytäntöön NIS2-direktiivin 28 artiklan 1-2 kohdat sekä 3-5 kohdat aluetunnusrekisterin osalta.

170 §. *Verkkotunnusvälittäjän muut velvollisuudet.* Säännöksen 1 momenttiin lisättäisiin *uusi 8 kohta,* jonka mukaan verkkotunnusvälittäjän olisi julkaistava sen käytössä olevat toimintaperiaatteet ja menettelyt, joilla varmistetaan, että verkkotunnusrekisterin tiedot ovat 167 §:n 1 momentin mukaiset. Mainitun 167 §:n mukaan verkkotunnusvälittäjän tai sen puolesta toimivan tahon, kuten yksityisyys- tai välityspalvelujen tarjoajan tai jälleenmyyjän, on merkittävä verkkotunnusrekisteriin verkkotunnuksen käyttäjää sekä rekisteröityä verkkotunnusta koskevat oi-

keat, ajantasaiset ja yksilöivät tiedot sekä kuulemisiin ja tiedoksiantoihin käytettävä sähköpostiosoite. Lisäksi 1 momenttiin ehdotetaan lisättävän *uusi 9 kohta*, jonka mukaan verkkotunnusvälittäjän on ilman aiheetonta viivytystä asetettava julkisesti saataville muut verkkotunnuksen rekisteröintitiedot kuin henkilötiedot. Verkkotunnusvälittäjän olisi lisäksi ehdotetun *10 kohdan* mukaisesti annettava pääsy verkkotunnusten rekisteröintitietoihin tietosuojalainsäädännön mukaisesti ja maksuttomasti. Verkkotunnusvälittäjän olisi lisäksi vastattava rekisteritietoihin pääsyä pyytävälle ilman aiheetonta viivytystä ja viimeistään 72 tunnin kuluessa siitä, kun verkkotunnusvälittäjä on vastaanottanut lainmukaisen ja asianmukaisesti perustellun pyynnön. Mikäli pyyntö on esimerkiksi sillä tavalla puutteellinen tai epäselvä, että sen perusteella ei voida arvioida, onko tietojen luovuttaminen tietosuojalainsäädännön mukaista, verkkotunnusvälittäjän olisi vastattava pyynnön esittäjälle esimerkiksi lisätietopyynnöllä laissa asetetun määräajan kuluessa. Lisäksi 1 momenttiin ehdotettaisiin lisättävän *uusi 11 kohta*, jonka mukaan verkkotunnusvälittäjän olisi julkaistava sen käyttämät toimintaperiaatteet ja menettelyt verkkotunnusten rekisteröintitietojen luovuttamisesta.

Säännöksen *2 momentissa* on säädetty Liikenne- ja viestintävirastolle annettavasta määräyksenantovaltuudesta. Liikenne- ja viestintäviraston määräyksenantovaltuutta ehdotetaan laajennettavan 1 momenttiin lisättävien 8-11 kohtien johdosta siten, että Liikenne- ja viestintävirasto voisi antaa tarkempia määräyksiä myös tarkoitetuista julkisesti saataville asetettavista tiedoista, pääsyn antamisesta tietoihin sekä toimintaperiaatteista ja menettelyistä.

Säännökseen ehdotetaan lisättävän *uusi 3 momentti*, joka selkeyttäisi 1 momentin 6-7 kohtien suhdetta ehdotettuun kyberturvallisuuden riskienhallinnasta annettuun lakiin. NIS2-direktiivin soveltamisalaan kuuluvien DNS-palveluntarjoajien osalta velvollisuudesta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja poikkeamien ilmoittamisesta säädettäisiin jatkossa kyberturvallisuuden riskienhallinnasta annetussa laissa. Sen sijaan sellaisten verkkotunnusvälittäjien, jotka eivät toimi DNS-palveluntarjoajina, vastaavat velvoitteet olisivat jatkossakin 1 momentin 6-7 kohdissa.

Ehdotetuilla muutoksilla pantaisiin täytäntöön NIS2-direktiivin 28 artiklan 3-5 kohdat verkkotunnusvälittäjien osalta.

247 §. *Viestinnän välittäjän ja lisäarvopalvelun tarjoajan velvollisuus huolehtia tietoturvasta.* Säännökseen ehdotetaan lisättävän selkeyttävä momentti siitä, että NIS2-direktiivin soveltamisalaan kuuluvien viestinnän välittäjien ja lisäarvopalvelun tarjoajien osalta velvollisuuteen huolehtia tietoturvasta ja siihen kohdistuvista riskeistä sovellettaisiin myös kyberturvallisuuden riskienhallinnasta annettua lakia.

247 a §. *Verkossa toimivan markkinapaikan, hakukonepalvelun ja pilvipalvelun tarjoajan velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.* Säännös ehdotetaan kumottavaksi vastaavan velvoitteen siirtyessä kyberturvallisuudesta annettavaan lakiin. Säännöksen tarkoituksena on ollut siinä tarkoitettujen toimijoiden osalta NIS1-direktiivin täytäntöönpano. Jatkossa 247 a §:ssä tarkoitettujen toimijoiden vastaavasta riskienhallintavelvoitteesta säädettäisiin kyberturvallisuuden riskienhallinnasta annetussa laissa. Näin ollen säännös ehdotetaan kumottavaksi tarpeettomana.

275 §. *Häiriöilmoitukset Liikenne- ja viestintävirastolle*. Säännöksen 1 momentista ehdotetaan poistettavaksi Liikenne- ja viestintäviraston velvollisuus toimittaa komissiolle ja Euroopan unionin kyberturvallisuusvirastolle vuosittainen tiivistelmäraportti momentin nojalla annetuista ilmoituksista. Kyseinen velvoite on lisätty lakiin teledirektiivin 40 artiklan täytäntöönpanemiseksi. NIS2-direktiivillä kumotaan teledirektiivin 40 artikla, joten sitä täytäntöönpaneva kansallinen säännös ehdotetaan kumottavaksi tarpeettomana.

Säännöksestä ehdotetaan kumottavaksi sen 2 momentti, jossa säädetään kumottavaksi ehdotettavassa 247 a §:ssä tarkoitettujen toimijoiden velvollisuudesta ilmoittaa merkittävistä tietoturvallisuuteen liittyvistä häiriöistä. Momentti on lisätty lakiin NIS1-direktiivin täytäntöönpanemiseksi 247 a §:ssä tarkoitettujen toimijoiden osalta. Jatkossa 247 a §:ssä tarkoitettujen toimijoiden vastaavasta NIS2-direktiivin nojalla tapahtuvasta ilmoitusvelvollisuudesta säädettäisiin kyberturvallisuuden riskienhallinnasta annetussa laissa. Näin ollen säännös ehdotetaan kumottavaksi tarpeettomana.

Samalla nykyiset 3–5 momentit siirtyisivät uusiksi 2–4 momentiksi ja niistä poistettaisiin viittaukset kumottavaan 2 momenttiin. Kumottavassa 247 a §:ssä tarkoitettujen toimijoiden osalta 275 §:n vanhaa 3 momenttia vastaava säännös sisältyisi ensimmäisen lakiehdotuksen 11 §:ään, vanhaa 4 momenttia vastaava määräyksenantovaltuus sisältyisi ensimmäisen lakiehdotuksen 11 §:ään ja vanhaa 5 momenttia vastaava säännös sisältyisi ensimmäisen lakiehdotuksen 17 §:ään. Voimassa olevan 275 §:n 4 momentin nojalla annettuja määräyksiä koskisi siirtymäsäännös.

308 §. *Yhteistyö eri viranomaisten kanssa.* Pykälän 3 momenttia ehdotetaan muutettavaksi siten, että viittaus verkko- ja tietoturvadirektiivin 11 artiklassa tarkoitettuun yhteistyöryhmään muutetaan viittaukseksi NIS2-direktiivin 14 artiklassa tarkoitettuun yhteistyöryhmään. Momenttiin lisättäisiin viittaus myös NIS2-direktiivin 15 artiklassa tarkoitettuun CSIRT-verkostoon ja 16 artiklassa tarkoitettuun Euroopan kyberkriisien yhteysorganisaatioiden verkostoon (EU-CyCLONe). Momentista poistettaisiin viittaus verkko- ja tietoturvadirektiivin 10 artiklan 3 kohdan mukaisen tiivistelmäraportin toimittamiseen mainitun direktiivin kumoamisen johdosta. NIS2-direktiivin osalta vastaavasta raportointivelvollisuudesta Liikenne- ja viestintävirastolle säädettäisiin ehdotetussa kyberturvallisuuden riskienhallinnasta annetun lain 19 §:ssä.

313 §. *Valvonta-asioiden käsittely Liikenne- ja viestintävirastossa.* Pykälän 2 momentin 2 kohtaa ehdotetaan muutettavaksi siten, että kohdasta poistettaisiin viittaus kumottavaksi ehdotettavaan 247 a §:än. Jatkossa oikeudesta jättää asia tutkimatta säädettäisiin kyberturvallisuuden riskienhallinnasta annetun lain 26 §:ssä.

318 §. *Tietojen luovuttaminen viranomaisesta.* Pykälän 4 momenttia ehdotetaan muutettavaksi osin lainsäädäntöteknisistä syistä. Momentista poistettaisiin viittaus 275 §:n nykyiseen 2 momenttiin, joka ehdotetaan kumottavaksi. Lisäksi viittaus verkko- ja tietoturvadirektiivin 11 artiklassa tarkoitettuun yhteistyöryhmään muutettaisiin viittaukseksi NIS2-direktiivin 14 artiklassa tarkoitettuun yhteistyöryhmään ja 15 artiklassa tarkoitettuun CSIRT-verkostoon.

7.4 Laki ilmailulain 128 a §:n ja 128 b §:n kumoamisesta

Ehdotuksella kumottaisiin ilmailulain 128 a § ja 128 b §, jotka koskevat lennonvarmistuspalvelun tarjoajan sekä yhteiskunnan toiminnan kannalta merkittävän lentoaseman pitäjän velvollisuutta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä ilmoittaa siihen liittyvistä häiriöistä viranomaiselle. Säännökset on lisätty ilmailulakiin NIS1-direktiivin toimeenpanemiseksi. Säännökset kumottaisiin, sillä ehdotettuun kyberturvallisuuden riskienhallinnasta annettavaan lakiin sisältyisi lennonvarmistuspalvelun tarjoajia ja lentoaseman pitäjiä koskevat vastaavat velvollisuudet.

Ehdotuksen myötä kumoutuisi myös yhteiskunnan toiminnan kannalta merkittävistä lentoasemista ja satamista annettu valtioneuvoston asetus (361/2018) yhdessä turvatoimilain 7 e ja 7 f §:n kumoamista koskevan ehdotuksen kanssa. Kumoutuva asetus on annettu kumottavaksi ehdotettavien ilmailulain 128 a §:n ja turvatoimilain 7 e §:n nojalla. Koska molemmat asetuksenantovaltuuden sisältävät säännökset ehdotetaan kumottavaksi, niiden nojalla annettu valtioneuvoston asetus ei jäisi voimaan. Velvoitteita sovellettaisiin jatkossa NIS2-direktiivin ja ehdotetun

yleislain soveltamisalaan kuuluviin lentoasemiin ja satamiin, eikä siten olisi tarpeellista määritellä erikseen yhteiskunnan toiminnan kannalta merkittäviä lentoasemia ja satamia laissa tai sen nojalla.

7.5 Laki raideliikennelain 169 §:n kumoamisesta

Ehdotuksella kumottaisiin raideliikennelain 169 §, joka koskee valtion rataverkon haltijan sekä liikenteenohjauspalvelun tarjoajan velvollisuutta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä ilmoittaa viestintäverkkoihin ja tietojärjestelmiin liittyvistä häiriöistä viranomaiselle. Säännös kumottaisiin, sillä ehdotettuun kyberturvallisuuden riskienhallinnasta annettuun lakiin sisältyisi jatkossa vastaava velvollisuus rataverkon haltijalle ja liikenteenohjauspalvelun tarjoajalle.

7.6 Laki liikenteen palveluista annetun lain muuttamisesta

140 §. *Tietoturva tieliikenteen ohjaus- ja hallintapalvelussa.* Pykälää ehdotetaan muutettavaksi siten, että nykyiset 1 – 4 momentti kumottaisiin. Ehdotettuun kyberturvallisuuden riskienhallinnasta annettuun lakiin sisältyisi jatkossa vastaava velvollisuus tieliikenteen ohjaus- ja hallintapalvelun tarjoajalle. Uutena *1 momenttina* säädettäisiin informatiivinen viittaussäännös mainittuun lakiin. Pykälän nykyinen 5 momentti siirtyisi uudeksi *2 momentiksi* muuttamattomana.

161 §. *Älykkään liikennejärjestelmän ylläpitäjän velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen.* Pykälä ehdotetaan kumottavaksi. Pykälä koskee älykkään liikennejärjestelmän ylläpitäjän velvollisuutta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä ilmoittaa siihen liittyvistä häiriöistä viranomaiselle. Säännös kumottaisiin, sillä ehdotettuun kyberturvallisuuden riskienhallinnasta annettuun lakiin sisältyisi jatkossa vastaava velvollisuus älykkään liikennejärjestelmän ylläpitäjälle.

7.7 Laki alusliikennepalvelulain 18 a §:n kumoamisesta.

Ehdotuksella kumottaisiin alusliikennepalvelulain 18 a §, joka koskee VTS-palveluntarjoajan velvollisuutta ilmoittaa viestintäverkkoihin ja tietojärjestelmiin kohdistuvista merkittävistä tietoturvallisuuteen liittyvistä häiriöistä Liikenne- ja viestintävirastolle. Säännös kumottaisiin, sillä ehdotettuun kyberturvallisuuden riskienhallinnasta annettuun lakiin sisältyisi jatkossa vastaava velvollisuus VTS-palveluntarjoajalle.

7.8 Laki eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain 7 e ja 7 f §:n kumoamisesta

Ehdotuksella kumottaisiin turvatoimilain 7 e ja 7 f §:t, jotka koskevat yhteiskunnan toiminnan kannalta merkittävän satamanpitäjän velvollisuutta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä ilmoittaa siihen liittyvistä häiriöistä viranomaiselle. Säännökset kumottaisiin, sillä ehdotettuun kyberturvallisuuden riskienhallinnasta annettuun lakiin sisältyisi jatkossa satamanpitäjiä koskevat vastaavat velvollisuudet.

Ehdotuksella kumoutuisi myös yhteiskunnan toiminnan kannalta merkittävistä lentoasemista ja satamista annettu valtioneuvoston asetus (361/2018) yhdessä ilmailulain 128 a ja 128 b §:n kumoamista koskevan ehdotuksen kanssa. Velvoitteita sovellettaisiin jatkossa NIS2-direktiivin ja ehdotetun yleislain soveltamisalan mukaisesti.

7.9 Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain muuttamisesta

2 §. *Soveltamisala ja suhde muuhun lainsäädäntöön.* Lain 2 §:n *3 momenttia* ehdotetaan muutettavaksi niin, että sen mukaan sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetulla lailla annettaisiin toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annetulla Euroopan parlamentin ja neuvoston direktiiviä (EU) 202/2555 ja sen täytäntöönpanemiseksi ehdotettua kyberturvallisuuden riskienhallinnasta annettua lakia täydentävät ja täsmentävät säännökset käsiteltäessä sosiaali- ja terveydenhuollon asiakastietoja ja asiakkaan itsensä tuottamia hyvinvointitietoja sosiaali- ja terveyspalveluiden järjestämisen ja toteuttamisen käyttötarkoituksissa. Samalla muutettaisiin viittaus vastaamaan uutta 14.12.2022 voimaan tullutta NIS2-direktiiviä.

NIS2-direktiiviä ja kyberturvallisuuden riskienhallinnasta annettua lakia täydentävää ja täsmentävää sääntelyä on lain 10 luvussa Tietoturvallisuuden ja tietosuojan omavalvonnasta. Lain 77 §:ssä säädetään palvelunantajien velvoitteesta laatia tietoturvasuunnitelma ja selvittää siinä, miten pykälässä tarkemmin eriteltyjä asiakas- ja potilastietojen käsittelyyn liittyviä vaatimuksia varmistetaan. Vaatimukset liittyvät esimerkiksi tietojärjestelmän käyttöympäristön soveltuvuuteen tietojärjestelmien asianmukaisen sekä tietoturvan ja tietosuojaan varmistavaan käyttöön, ja käyttöympäristöön sekä tietojärjestelmiin kohdistuvien riskien hallinnasta huolehtimiseen. Vaatimus koskee sekä julkisia että yksityisiä sosiaali- ja terveydenhuollon palvelunantajia. Terveyden ja hyvinvoinnin laitos voi antaa tarkempia määräyksiä tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista sekä tietoturvallisuuden todentamisesta. Täydentävää ja täsmentävää sääntelyä on myös lain 78 §:ssä, jossa säädetään tietoturvallisuuden omavalvonnan toteuttamisesta ja vastuista, mm. palvelunantajan vastaavan johtajan vastuusta huolehtia siitä, että tietoturvasuunnitelma laaditaan ja sitä noudatetaan.

90 §. *Ilmoittaminen tietojärjestelmän ja hyvinvointisovelluksen olennaisten vaatimusten poikkeamista sekä tietoverkkoihin kohdistuvista tietoturvallisuuden häiriöistä.* Pykälän *2 momentissa* viitattaisiin terveydenhuollon palvelunantajan velvoitteiden osalta kyberturvallisuuden riskienhallinnasta annetun lain 12-15 §:ään. Terveydenhuollossa kyberturvallisuuden riskienhallinnasta annettua lakia sovelletaan muissakin kuin asiakastietojen käsittelyn tilanteissa, joten soveltamisen kannalta on selkeää noudattaa samaa sääntelyä kaikissa tilanteissa. Selkeyden vuoksi asiakastietolaissa olisi kuitenkin viittaus kyberturvallisuuden riskienhallinnasta annettuun lakiin. Momentissa säädettäisiin edelleen vastaavista velvoitteista sosiaalihuollon palvelunantajille, apteekeille, Kansaneläkelaitokselle ja tietojärjestelmäpalveluntuottajille, tietojärjestelmän valmistajille ja välittäjille, joiden toimintaan ei kyberturvallisuuden riskienhallinnasta annettua lakia sovelleta.

Pykälän *3 momenttia* ehdotetaan muutettavaksi siten, että palvelunantajan sijaan sääntely koskisi vain sosiaalihuollon palvelunantajia, koska terveydenhuollon palvelunantajien velvoitteista säädetään jatkossa kyberturvallisuuden riskienhallinnasta annetussa laissa.

Pykälän *4 momentti* kumottaisiin, koska se on koskenut ainoastaan julkista terveydenhuoltoa ja vastaava sääntely on jatkossa kyberturvallisuuden riskienhallinnasta annetussa laissa.

7.10 Laki sähkömarkkinalain muuttamisesta

29 a §. *Verkonhaltijan velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen*. Pykälä ehdo-

tetaan kumottavaksi, sillä verkonhaltijan velvollisuudesta huolehtia käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta säädettäisiin jatkossa ehdotetussa kyberturvallisuuden riskienhallinnasta annetussa laissa.

62 §. *Suljettua jakeluverkkoa koskevat erityissäännökset.* Pykälän *1 momenttia* muutettaisiin poistamalla siitä viittaus kumottavaan 29 a §:ään. Muutos olisi lainsäädäntötekninen.

7.11 Laki maakaasumarkkinalain 34 a §:n kumoamisesta

Ehdotuksella kumottaisiin maakaasumarkkinalain 34 a §, joka koskee siirtoverkonhaltijan velvollisuutta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä ilmoitusvelvollisuutta merkittävistä tietoturvallisuuteen liittyvistä häiriöistä. Säännös kumottaisiin, sillä ehdotettuun kyberturvallisuuden riskienhallinnasta annettuun lakiin sisältyisi jatkossa vastaava velvollisuus siirtoverkonhaltijalle.

7.12 Laki energiavirastosta annetun lain 1 §:n muuttamisesta

1 §. *Tehtävät.* Lain 1 §:ssä säädetään Energiaviraston tehtävistä. Pykälän *2 momenttiin* ehdotetaan lisättäväksi uusi 21 kohta, jonka mukaan Energiavirasto hoitaisi tehtävät, jotka sille on säädetty kyberturvallisuuden riskienhallinnasta annetussa laissa. Energiavirasto olisi yksi kyberturvallisuuden riskienhallinnasta annetun lain 24 §:ssä tarkoitetuista valvovista viranomaisista.

7.13 Laki sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain 28 §:n muuttamisesta

28 §. *Energiaviraston oikeus luovuttaa tietoja toiselle viranomaiselle*. Pykälän 1 momentin 1 kohtaa ehdotetaan muutettavan siten, että siitä poistettaisiin maininta salassa pidettävän tiedon luovuttamisesta Liikenne- ja viestintävirastolle. Kyseinen kohta poistettaisiin, sillä ehdotettuun kyberturvallisuuden riskienhallinnasta annetun lain 27 §:än sisältyisi jatkossa vastaava mahdollisuus luovuttaa salassa pidettävää tietoa toiselle viranomaiselle.

7.14 Laki vesihuoltolain 35 §:n muuttamisesta

Ehdotuksella kumottaisiin vesihuoltolain 35 §:n 2 momentin 3 kohta, joka koskee tietoturvallisuuteen liittyvien tehtävien hoitamiseksi välttämättömien tietojen luovuttamista Liikenne- ja viestintävirastolle salassapitovelvollisuuden estämättä. Kyseinen kohta kumottaisiin, sillä ehdotettuun kyberturvallisuuden riskienhallinnasta annetun lain 27 §:än sisältyisi jatkossa vastaava mahdollisuus luovuttaa salassa pidettävää tietoa toiselle viranomaiselle.

8 Lakia alemman asteinen sääntely

8.1 Esityksellä ehdotettavat uudet valtuudet lakia alemman asteisen sääntelyn antamiseksi

Hallituksen esitykseen sisältyy ehdotuksia lain tasoisen sääntelyn täydentämisestä lakia alemman asteisin säännöksin. Ehdotettuja uusia säännöksiä täsmentävät alemman asteiset säännökset annettaisiin valtioneuvoston aseuksella, ministeriön asetuksella ja muun viranomaisen oikeussäännöin. Lisäksi esitykseen sisältyy ehdotuksia lakia alemman asteisen sääntelyn ja sen antamisvaltuuden kumoamisesta.

Eräiden toimijoiden saattaminen kyberturvallisuuden riskienhallinnasta annetun lain soveltamisalaan valtioneuvoston asetuksella.

Esitykseen sisältyy ehdotus valtuudesta säätää valtioneuvoston asetuksella poikkeus kyberturvallisuuden riskienhallinnasta annetun lain soveltamisalaan sen kokokriteerin osalta. Tämä toteutettaisiin kyberturvallisuuden riskienhallinnasta annettavaan lakiin ehdotetun 3 § 2 momentin valtuussäännöksen nojalla, jonka mukaan valtioneuvoston asetuksella säädetään lain soveltamisesta sellaiseen liitteessä I tai II tarkoitettua toimintaa harjoittavaan tai toimijatyyppiä olevaan toimijaan sen koosta riippumatta laissa lueteltujen toimijaa koskevien edellytysten täyttyessä.

Valtioneuvoston asetuksella voitaisiin siten säätää lain soveltamisesta sellaiseen toimijaan, johon lakia ei muuten sovellettaisi, koska toimija ei täytä keskisuuren yrityksen määritelmää. Edellytyksenä olisi, että toimija olisi lain liitteessä tarkoitettua toimijatyyppiä tai harjoittaisi liitteessä tarkoitettua toimintaa ja toimijaa koskisi laissa säädetty kriteeri, joka vastaisi NIS2-direktitvin 2 artiklan 2 kohdan b-e alakohtaa.

NIS2-direktiivin 2 artiklan 2 kohdan b – e alakohdan nojalla edellytetään, että NIS2-direktiivin mukaisia riskienhallinta- ja raportointivelvoitteita olisi sovellettava alakohdissa tarkoitettuihin toimijoihin niiden koosta riippumatta toimialoilla, jotka kuuluvat direktiivin alaan. Kriteerit tällaisille toimijoille toimijoita ovat:

b) toimija tarjoaa ainoana jäsenvaltiossa palvelua, joka on yhteiskunnan tai talouden kriittisten toimintojen ylläpitämisen kannalta keskeinen;
c) häiriö toimijan tarjoamassa palvelussa voisi vaikuttaa merkittävästi yleiseen järjestykseen, yleiseen turvallisuuteen tai kansanterveyteen;
d) häiriö toimijan tarjoamassa palvelussa voisi aiheuttaa merkittävän systeemisen riskin erityisesti aloilla, joilla tällaisella häiriöllä voisi olla rajatylittäviä vaikutuksia;
e) toimija on kriittinen, koska sillä on erityisen suuri merkitys kansallisella tai alueellisella tasolla kyseisen toimialan tai palvelutyypin tai jäsenvaltion muiden keskinäisriippuvaisten toimialojen kannalta;

Esityksessä ehdotetaan, että tällaiset toimijat voitaisiin saattaa kyberturvallisuuden riskienhallinnasta ehdotettavan lain soveltamisalaan koosta riippumatta valtioneuvoston asetuksella.

Kyberturvallisuuden riskienhallinnasta annetussa laissa säädettäisiin NIS2-direktiivin velvoitteista sen vähimmäissoveltamisalaan kuuluville toimijoille, joita näissä kohdissa tarkoitetut toimijat myös ovat. Lain soveltamisalan ulottamisessa tällaisiin toimijoihin on kysymys hyvin yksityiskohtaisesta toimijoiden tai toimijatyypin määrittämisestä. Nämä toimijat kuuluisivat poikkeuksellisesti toiminnan erityisen laadun vuoksi lain ja NIS2-direktiivin velvoitteiden soveltamisalaan koosta riippumatta. Ottaen huomioon kriteerien laatu, soveltamisala näitä toimijoita koskien olisi altis muutoksille, jos toimijoiden toiminnassa tai toimintaympäristössä tapahtuu muutoksia. Näiden syiden johdosta lainsäädäntövallan siirto olisi lakiteknisesti tarpeellista. Ennakoitavissa on, että soveltamisalan ulottaminen kuvattuihin toimijoihin olisi poikkeuksellista ja soveltamisalaan kuuluvien toimijoiden ja toimijatyyppien joukko muuttuva yhteiskunnan kehityksen myötä.

Ehdotettu asetuksenantovaltuus täyttäisi perustuslain 80 §:ssä säädetyt vaatimukset. Asetuksella ei voitaisi poiketa lain säännöksistä tai säätää muusta kuin lain soveltamisalan ulottamisesta laissa säädetyin kriteerein tarkoitettuihin toimijoihin. Asetuksella ei voitaisi säätää muutoksista

niihin oikeuksiin ja velvollisuuksiin, joita toimijoille kyberturvallisuuden riskienhallinnasta annetussa laissa asetetaan. Asetuksenantovaltuutta koskeva säännös on arvioitu asianmukaiseksi ja tarkkarajaiseksi.

Liikenne- ja viestintäministeriön asetuksenantovaltuus maksuista

Kyberturvallisuuden riskienhallinnasta esitetyn lain 19 § 6 momentissa säädettäisiin liikenne- ja viestintäministeriölle asetuksenantovaltuus maksuista tai niiden perusteista, joita CSIRT-yksikkö voisi periä säännöksen 2 momentin 1 ja 2 kohdassa tarkoitetusta palvelusta, joka on tarjottu toimijan tai muun tahon pyynnöstä. Asetuksenantovaltuus olisi tarpeen, sillä kyseessä olisi uudenlaisen palvelun tarjoamisesta perittävien maksujen perusteiden asettamiseksi CSIRT-yksikkö olisi sijoitettuna Liikenne- ja viestintäviraston Kyberturvallisuuskeskukseen. Asetuksenantovaltuus osoitettaisiin valtioneuvoston sijasta liikenne- ja viestintäministeriölle, koska asian sisällön kannalta ministeriön asetus olisi riittävä säädöstaso ja liikenne- ja viestintäministeriön asetuksella on vakiintuneesti säädetty Liikenne- ja viestintäviraston suoritteiden maksuperusteista.

Viranomaisen määräyksenantovaltuudet

Esitykseen sisältyy useita ehdotuksia määräyksenantovaltuudesta valvovalle viranomaiselle tai Liikenne- ja viestintävirastolle. Määräyksenantovaltuudet ovat tarkkarajaisia ja määräyksiä voitaisiin antaa vain laissa säädettyjen seikkojen tarkentamisesta rajatulle kohderyhmälle. Määräyksenantovaltuudet ovat tarpeellisia teknisten seikkojen täsmentämiseksi sekä sektorikohtaisten erityispiirteiden huomioimiseksi. Määräyksenantovaltuuksien katsotaan olevan asiallisia siten, että ne ovat täsmällisesti rajattuja ja koskevat määrättyjä asioita, joihin on sääntelyn kohteeseen liittyviä erityisiä syitä, eikä sääntelyn asiallinen merkitys edellytä, että asiasta säädetään lailla tai asetuksella.

Kyberturvallisuuden riskienhallinnasta esitetyn lain 9 § 4 momentissa säädettäisiin toimialallaan valvovalle viranomaiselle valtuus antaa valvontatoimialallaan tarkempia teknisiä määräyksiä momentissa tarkoitetuista seikoista riskienhallinnan osalta. Viranomaisen määräyksenantovaltuus koskisi momentin mukaisten kyberturvallisuuden riskienhallintavelvoitteeseen liittyvien seikkojen sisällön tarkentamista ja täsmentämistä. Tarkemmat määräykset voisivat kuitenkin koskea vain teknisiä seikkoja, eli niillä ei saisi laajentaa 9 §:ssä säädettyjä velvoitteita tai asiallisesti muuttaa velvoitteiden sisältöä. Määräysten olisi oltava teknologianeutraaleja. Määräyksenantovaltuus olisi tarpeen, sillä mainituista riskienhallinnan seikoista voisi olla soveltamisen kannalta tarpeellista täsmentää erityisesti sektorikohtaisten toimintaan liittyvien erityispiirteiden huomioimiseksi. Lisäksi teknologisen kehityksen johdosta olisi tarpeellista, että valvova viranomainen voisi määräyksellä pitää riskienhallintaan liittyviä seikkoja ajantasaisina. Määräyksillä voitaisiin siten pitää riskienhallintavelvoite ajan tasalla ja huomioida paremmin sektorikohtaisia erityispiirteitä riskienhallinnan toteuttamisen osalta. Tällä toteutetaan osaltaan NIS 2 –direktiivin tavoitetta toteuttaa riskienhallintatoimenpiteitä siten, että turvallisuuden taso on oikeassa suhteessa riskeihin.

Kyberturvallisuuden riskienhallinnasta esitetyn lain 11 § 5 momentissa säädettäisiin valvovalle viranomaiselle valtuus antaa omalla toimialallaan tarvittaessa tarkentavia teknisiä määräyksiä siitä, milloin 1 momentissa tarkoitettu poikkeama on merkittävä, loppuraportissa ilmoitettavista tiedoista sekä merkittävien poikkeamien ja 12-13 §:ssä tarkoitettujen tietojen ilmoittamismenettelystä. Määräyksenantovaltuus on tarpeen, sillä määräyksillä voitaisiin säätää sektorikohtaisesti merkityksellisistä seikoista yksityiskohtaisemmin ja sektoreiden erityispiirteet huomioiden.

Sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain muutettava 90 §:n 2 momentti sisältää määräyksenantovaltuudet Terveyden ja hyvinvoinnin laitokselle antaa tarkempia määräyksiä siitä, milloin häiriö on merkittävä sekä häiriöilmoituksen sisällöstä, muodosta ja toimittamisesta. Esityksellä ei muutettaisi mainittua määräyksenantovaltuutta, mutta määräyksenantovaltuus kohdistuisi myös tietojärjestelmistä ja viestintäverkoista aiheutuviin häiriöihin.

Sähköisen viestinnän palveluista annetun lain muuttamisesta annettavan lain 165 §:n 3 momentti sisältää määräyksenantovaltuuden Liikenne- ja viestintävirastolle verkkotunnusvälittäjän ennen toimintansa aloittamista tehtävän ilmoituksen tekemisestä ja sen sisällöstä. Esityksellä ei muutettaisi mainittua määräyksenantovaltuuslauseketta nykyisestä, mutta määräyksenantovaltuuden alaan olisivat merkityksellisiä pykälän 1, 2 ja 4 momenttiin ehdotettavat muutokset.

Sähköisen viestinnän palveluista annetun lain muuttamisesta annettavan lain 167 § 5 momentissa on säädetty Liikenne- ja viestintävirastolle annettavasta määräyksenantovaltuudesta, jossa Liikenne- ja viestintäviraston määräyksenantovaltuutta ehdotetaan laajennettavan siten, että Liikenne- ja viestintävirasto voisi antaa tarkempia määräyksiä myös verkkotunnuksen käyttäjää koskevien tietojen varmentamisesta. Tällä tarkoitettaisiin esimerkiksi toimintaperiaatteita ja menettelyjä, joita verkkotunnusvälittäjien olisi otettava käyttöön, jotta ne voivat varmistua siitä että 1 momentissa tarkoitetut, verkkotunnuksen käyttäjän ilmoittamat tiedot ovat oikeita ja ajantasaisia.

Sähköisen viestinnän palveluista annetun lain muuttamisesta annettavan lain 170 § 2 momentissa on säädetty Liikenne- ja viestintävirastolle annettavasta määräyksenantovaltuudesta. Liikenne- ja viestintäviraston määräyksenantovaltuutta ehdotetaan laajennettavan 1 momenttiin lisättävien 8-11 kohtien johdosta siten, että Liikenne- ja viestintävirasto voisi antaa tarkempia määräyksiä myös tarkoitetuista julkisesti saataville asetettavista tiedoista, pääsyn antamisesta tietoihin sekä toimintaperiaatteista ja menettelyistä.

Sähköisen viestinnän palveluista annetun lain muuttamisesta annettavan lain 275 § 3 momentissa on säädetty Liikenne- ja viestintävirastolle annettavasta määräyksenantovaltuudesta, jonka nojalla Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä 1 momentissa tarkoitettujen ilmoitusten sisällöstä, muodosta ja toimittamisesta.

8.2 Esityksellä kumottavat valtuudet antaa lakia alemman asteisia säännöksiä.

Valtioneuvoston asetus yhteiskunnan toiminnan kannalta merkittävistä lentoasemista ja satamista

Ehdotuksella kumottaisiin ilmailulain 128 a § jonka 3 momentti sisältää asetuksenantovaltuuden valtioneuvostolle säätää, milloin lentoasemaa on pidettävä yhteiskunnan toiminnan kannalta merkittävänä. Ehdotuksella kumottaisiin eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain 7 e § jonka 3 momentin mukaan valtioneuvoston asetuksella säädetään, milloin 1 momentissa tarkoitettua satamaa on pidettävä yhteiskunnan toiminnan kannalta merkittävänä.

Ehdotuksen myötä kumoutuisi yhteiskunnan toiminnan kannalta merkittävistä lentoasemista ja satamista annettu valtioneuvoston asetus (361/2018) yhdessä eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain 7 e ja 7 f §:n kumoamista koskevan ehdotuksen kanssa. Kumoutuva asetus on annettu kumottavaksi ehdotettavien ilmailulain

128 a §:n ja eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain 7 e §:n nojalla. Koska molemmat asetuksenantovaltuuden sisältävät säännökset ehdotetaan kumottavaksi, niiden nojalla annettu valtioneuvoston asetus ei jäisi voimaan. Asetuksenantovaltuus yhteiskunnan toiminnan kannalta merkittävistä satamista tai lentoasemista ei olisi jatkossa tarpeen, sillä NIS2-velvoitteita sovellettaisiin jatkossa NIS2-direktiivin ja ehdotetun yleislain soveltamisalan kokokriteerin mukaisesti soveltamisalaan kuuluviin lentoasemiin ja satamiin. Jatkossa ei siten olisi tarpeellista säätää erikseen yhteiskunnan toiminnan kannalta merkittävistä lentoasemista ja satamista lailla tai sen nojalla annetulla valtioneuvoston asetuksella.

Viranomaisen määräyksenantovaltuudet

Esityksellä kumottaisiin NIS1-direktiivin sektorikohtaisia täytäntöönpanosäännöksiä, koska päällekkäiset säännökset sisältyisivät jatkossa kyberturvallisuuden riskienhallinnasta annettuun lakiin. NIS 1 –direktiivin sääntelyn johdosta viranomaisille annetut määräyksenantovaltuudet edellä luetelluissa laeissa kumottaisiin, koska poikkeaman merkittävyydestä ja ilmoituksen sisällöstä, muodosta ja toimittamisesta säänneltäisiin jatkossa kyberturvallisuuden riskienhallinnasta ehdotetussa laissa. Valvovan viranomaien määräyksenantovaltuus poikkeaman merkittävyydestä, poikkeaman loppuraportin sisällöstä sekä merkittävien poikkeamien ja poikkeaman väliraportin ja loppuraportin mukaisten tietojen ilmoitusmenettelystä sisältyisi jatkossa kyberturvallisuuden riskienhallinnasta ehdotetun lain 11 §:n 4 momenttiin.

Ehdotuksella kumottaisiin ilmailulain 128 b § jonka 4 momentin mukaan Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu poikkeama on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta. Säännös ei olisi tarpeen, sillä vastaava määräyksenantovaltuus sisältyisi jatkossa kyberturvallisuuden riskienhallinnasta annettuun lakiin.

Ehdotuksella kumottaisiin raideliikennelain 169 § jonka 5 momentin mukaan Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä siitä, milloin 2 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta. Säännös ei olisi tarpeen, sillä vastaava määräyksenantovaltuus sisältyisi jatkossa kyberturvallisuuden riskienhallinnasta annettuun lakiin.

Ehdotuksella kumottaisiin maakaasumarkkinalain 34 a § jonka 5 momentin mukaan Energiavirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta. Säännös ei olisi tarpeen, sillä vastaava määräyksenantovaltuus sisältyisi jatkossa kyberturvallisuuden riskienhallinnasta annettuun lakiin.

Ehdotuksella kumottaisiin sähkömarkkinalain 29 a § jonka 5 momentin mukaan Energiavirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta sekä lain 49 a § 5 momentti, joka sisältää määräyksenantovaltuuden Energiavirastolle antaa tarkempia määräyksiä ilmoituksen sisällöstä, muodosta ja toimittamisesta. Säännös ei olisi tarpeen, sillä vastaavat säännökset ja niitä koskeva määräyksenantovaltuus sisältyisi jatkossa kyberturvallisuuden riskienhallinnasta annettuun lakiin.

Ehdotuksella kumottaisiin eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain 7 f § jonka 4 momentin mukaan Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta. Säännös ei olisi tarpeen, sillä vastaava

määräyksenantovaltuus sisältyisi jatkossa kyberturvallisuuden riskienhallinnasta annettuun lakiin.

Ehdotuksella kumottaisiin alusliikennepalvelulain 18 a § jonka 4 momentin mukaan Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta. Säännös ei olisi tarpeen, sillä vastaava määräyksenantovaltuus sisältyisi jatkossa kyberturvallisuuden riskienhallinnasta annettuun lakiin.

Ehdotuksella kumottaisiin liikenteen palveluista annetun lain 18 luvun 161 § jonka 5 momentin mukaan Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä siitä, milloin 2 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta. Säännös ei olisi tarpeen, sillä vastaava määräyksenantovaltuus sisältyisi jatkossa kyberturvallisuuden riskienhallinnasta annettuun lakiin.

9 Voimaantulo

Ehdotetaan, että lait tulevat voimaan pääosin 18.10.2024. Ensimmäiseen lakiehdotukseen sisältyvä toimijoiden rekisteröitymistä ja tietojen toimittamista valvovalle viranomaiselle koskeva 43 § ehdotetaan tulevaksi voimaan 1.1.2025.

NIS2-direktiivi edellyttää, että jäsenvaltiot antavat ja julkaisevat direktiivin noudattamisen edellyttämät säännökset viimeistään 17.10.2024 ja soveltavat niitä 18.10.2024 alkaen. Lain voimaantulo esitetään NIS2-direktiivin 41 artiklassa säädetyn kansallisen täytäntöönpanon määräaikaa vastaavasti 18. päiväksi lokakuuta 2024.

Lain 43 §:ssä tarkoitettu toimijaluetteloon ilmoittautuminen ehdotetaan kuitenkin tulevaksi voimaan 1.1.2025 alkaen, mikä antaisi valvoville viranomaisille ja toimijoille lisää siirtymäaikaa toimijaluetteloon ilmoittautumista varten. NIS2-direktiivi ei edellytä viranomaisilta toimijaluettelon tietoihin perustuvien ilmoituksien tekemistä ennen vuotta 2025.

10 Toimeenpano ja seuranta

NIS2-direktiivi sisältää komissiolle direktiivin toimivuutta koskevan uudelleentarkasteluvelvoitteen, josta säädetään direktiivin 40 artiklassa.

Komission on viimeistään 17.10.2027 ja sen jälkeen 36 kuukauden välein tarkasteltava direktiivin toimivuutta ja annettava siitä kertomus Euroopan parlamentille ja neuvostolle. Kertomuksessa arvioidaan erityisesti asianomaisten toimijoiden koon sekä NIS2-direktiivin liitteissä I ja II tarkoitettujen toimialojen, toimialan osien ja toimijatyyppien merkitystä talouden ja yhteiskunnan toiminnalle kyberturvallisuuden näkökulmasta. Tätä tarkoitusta varten ja strategisen ja operatiivisen yhteistyön edistämiseksi edelleen komissio ottaa huomioon NIS2-direktiivin 14 artiklassa tarkoitetun yhteistyöryhmän ja CSIRT-verkoston kertomukset strategisella ja operatiivisella tasolla saaduista kokemuksista. Komission uudelleentarkastelukertomukseen liitetään tarvittaessa lainsäädäntöehdotus.

Kansallisella tasolla ehdotettujen lakien toimeenpanoa seuraa liikenne- ja viestintäministeriö. Seurannassa arvioidaan erityisesti soveltamisalaan kuuluviin toimijoihin kohdistuvia vaikutuksia, kyberturvallisuuden hallintatoimenpiteitä ja merkittävien poikkeamien ilmoitusmääriä sekä viranomaisyhteistyön ja sektorikohtaisesti hajautetun valvontamallin toteutumista suhteessa

lain tavoitteisiin ja arvioituihin vaikutuksiin. Kyberturvallisuuden riskienhallinnasta annettavasta laista toteutetaan jälkiarviointi vuosien 2026–2027 aikana.

Liikenne- ja viestintävirasto jatkaa NIS1-direktiivin täytäntöönpanon yhteydessä perustetun valvovien viranomaisten kansallisen yhteistyöryhmän toimintaa sääntelyn täytäntöönpanon tukemiseksi valvovissa viranomaisissa. Valvovien viranomaisten on tarvittaessa tuettava toimijoita sääntelyn toimeenpanossa ohjeiden, suositusten, tiedottamisen ja neuvonnan keinoin.

11 Suhde muihin esityksiin

11.1 Esityksen riippuvuus muista esityksistä

Esityksellä on yhteys kriittisten toimijoiden häiriönsietokyvystä annetun Euroopan parlamentin ja neuvoston direktiivin (CER-direktiivi, (EU) 2022/2557) kansallista täytäntöönpanoa koskevaan säädöshankkeeseen (SM047:00/2022) ja hankkeessa valmisteltavaan hallituksen esitykseen. Hankkeen tiedot löytyvät Valtioneuvoston hankeikkunasta: https://valtioneuvosto.fi/hanke?tunnus=SM047:00/2022 ja täytäntöönpanoon liittyvä hallituksen esitys on suunniteltu annettavaksi eduskunnalle / on annettu [ ]. CER-direktiivin nojalla yhteiskunnan kriittisiksi toimijoiksi tunnistettaviin toimijoihin on sovellettava NIS2-direktiivin velvoitteita. Näin ollen kyberturvallisuuden riskienhallinnasta annettavan lain soveltamisala ehdotetaan kattamaan myös tämän hankkeen yhteydessä CER-direktiivin nojalla yhteiskunnan kriittisiksi toimijoiksi tunnistettavat toimijat. Esitykseen sisältyy myös ehdotuksia CER-direktiivin ja NIS2-direktiivin nojalla annettua sääntelyä valvovien viranomaisten välisestä yhteistyöstä.

Esityksellä on yhteys finanssialan digitaalisen häiriönsietokykyasetuksen (DORA-asetus, (EU) 2022/2554) kansallista täytäntöönpanoa koskevaan säädöshankkeeseen (VM067:00/2023) ja hankkeessa valmisteltavaan hallituksen esitykseen. Hankkeen tiedot löytyvät Valtioneuvoston hankeikkunasta: https://vm.fi/hanke?tunnus=VM067:00/2023 ja asetusta täydentävä hallituksen esitys on suunniteltu annettavaksi eduskunnalle / on annettu [ ] . DORA-asetuksessa säännellään sen soveltamisalaan kuuluville toimijoille NIS2-direktiivin velvoitteita yksityiskohtaisempia vaatimuksia kyberturvallisuuden riskienhallinnasta, joita olisi sovellettava näihin toimijoihin NIS2-direktiivin sijasta DORA-asetuksen 1 artiklan 2 kohdan ja NIS2-direktiivin 4 artiklan mukaisesti. DORA-asetukseen ja NIS2-direktiiviin sisältyy lisäksi säännöksiä valvovien viranomaisten välisestä yhteistyöstä.

11.2 Suhde talousarvioesitykseen

[Täydennetään myöhemmin]

12 Suhde perustuslakiin ja säätämisjärjestys

Esitys sisältää perustuslain kannalta merkityksellisiä ehdotuksia suhteessa perustuslain 2 §:n 3 momentissa säädettyyn julkisen vallan käytön lakisidonnaisuuteen, perustuslain 10 §:ssä turvattuun yksityiselämän, henkilötietojen ja luottamuksellisen viestinnän suojaan, perustuslain 18 §:ssä turvattuun elinkeinovapauteen, perustuslain 21 §:ssä turvattuun oikeusturvaan, perustuslain 80 §:ssä asetuksen antamisesta ja lainsäädäntövallan siirtämisestä säädettyyn, perustuslain 81 §:ssä valtion toiminnan maksullisuudesta säädettyyn sekä perustuslain 124 §:ssä hallintotehtävän antamisesta muulle kuin viranomaiselle säädettyyn.

12.1 Luottamuksellisen viestinnän suoja

Ehdotukseen sisältyy useita säännöksiä, jotka ovat merkityksellisiä perustuslain 10 §:ssä turvatun viestinnän luottamuksellisuuden kannalta. Näitä sisältyy erityisesti ehdotuksen 20 §:ään, jossa on kyse verkkopohjaisesta haavoittuvuuskartoituksesta ja lisäksi ehdotuksen 22, 24 ja 28 §:iin, joissa on kyse välitystietojen ja haitallisen tietokoneohjelman tai käskyn sisältävään viestiin liittyvästä tietojen luovuttamisesta.

Perustuslain 10 §:n mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Lisäksi kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. Pykälän 4 momentin mukaan lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Perustuslakivaliokunta on todennut, että perustuslain 10 §:ssä turvatun yksityiselämän suojan lähtökohtana on yksilön oikeus elää omaa elämäänsä ilman viranomaisten ja ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista siihen. (PeVL 53/2005 vp, s. 2, PeVL 36/2002 vp, s. 5/II, PeVL 9/2004 vp, s. 5/II).

Euroopan unionin perusoikeuskirjan 7 artiklassa on säädetty jokaisen oikeudesta siihen, että hänen viestejään kunnioitetaan. Luottamuksellisen viestin suoja on turvattu myös Euroopan ihmisoikeussopimuksen (SopS 63/1999) 8 artiklassa, jonka mukaan jokaisella on oikeus nauttia kirjeenvaihtoonsa kohdistuvaa kunnioitusta. Viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen paitsi, kun laki sen sallii ja se on välttämätöntä demokraattisessa yhteiskunnassa kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen tai rikollisuuden estämiseksi, terveyden tai moraaliin suojaamiseksi tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi.

Lisäksi ehdotuksien arvioinnissa on merkityksellistä huomioida sähköisen viestinnän tietosuojadirektiivin eli Euroopan parlamentin ja neuvoston henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla antaman direktiivin (2002/58/EY, ns. ePrivacy-direktiivi) 5 artikla, jonka nojalla jäsenvaltioiden on varmistettava sähköisen viestinnän luottamuksellisuus. Sähköisen viestinnän tietosuojadirektiivin 15 artiklan nojalla jäsenvaltio voi toteuttaa lainsäädännöllisiä toimenpiteitä, joilla sähköisen viestinnän luottamuksellisuutta rajoitetaan, jos tällaiset rajoitukset ovat välttämättömiä, asianmukaisia ja oikeasuhteisia muun ohella sähköisen viestintäjärjestelmän luvattoman käytön torjunnan, tutkinnan ja selvittämisen vuoksi.

Haavoittuvuuskartoitus

Viestinnän luottamuksellisuutta on tarkasteltava ensinnäkin ehdotuksen 20 §:ssä tarkoitetun haavoittuvuuskartoituksen näkökulmasta. Ehdotuksen mukaan CSIRT-yksiköllä olisi oikeus oma-aloitteisesti, ennakoivalla ja ei-intrusiivisella tavalla havainnoida ja kartoittaa yleisesti saatavilla olevista viestintäverkoista ja tietojärjestelmistä haavoittuvuuksia tai turvattomia viestintäverkkoja, laitteita tai järjestelmiä. Havainnoinnin tarkoituksena on saada tieto haavoittuvasta kohteesta ennen haavoittuvuuden hyväksikäyttöä ja saada tieto haavoittuvuuden olemassaolosta välitettyä haavoittuvaa kohdetta hallinnoivalle taholle, jotta korjaaviin toimenpiteisiin voidaan ryhtyä ja mahdollisilta haavoittuviin laitteisiin tai järjestelmiin liittyviltä tietoturvaloukkauksilta voidaan välttyä korjaavien toimenpiteiden avulla. Kartoituksen taustalla on arvioitu siten olevan painava peruste kyberuhkiin varautumiseksi ja kyberhyökkäyksistä aiheutuvien haitallisten vaikutuksien torjumiseksi yhteiskunnassa.

Haavoittuvuuskartoituksen teknistä toteuttamistapaa on käsitelty tarkemmin pykälää koskevissa säännöskohtaisissa perusteluissa, mutta niiden perusteella voidaan todeta, että toiminnan ei arvioida olevan perusoikeuksien kautta merkittävä muutoin, kuin sen yhteydessä käsiteltävien tietojen näkökulmasta. Ehdotus ei mahdollista tunkeutumista viestintäverkkoihin tai järjestelmiin vaan kyse on yleiseen viestintäverkkoon avoinna olevien suojattomien laitteiden ja järjestelmien havainnoinnista. Haavoittuvuuskartoituksessa ei käsitellä viestintäverkossa tai tietojärjestelmässä olevaa tietoa tai viestintää. Haavoittuvuuskartoituksessa kuitenkin käsitellään viestinnän luottamuksellisuuden kannalta merkityksellisiä välitystietoja. Välitystiedot toimivat teknisinä tunnistetietoina haitalliselle toiminnalle, minkä vuoksi niiden käsittely on välttämätöntä haavoittuvien kohteiden tai haavoittuvuuksien havaitsemiseksi tietyissä teknisissä tilanteissa, kuten esimerkiksi haittaohjelmaliikenteen havaitsemiseksi. Ehdotus rajaa viestin sisältöä koskevan tietojen käsittelyn pois havainnointitoiminnan piiristä, joten ehdotusta ei tältä osin ole tarpeen arvioida viestin sisältöä koskevien perusoikeuskysymysten valossa.

Luottamuksellisen viestin suojaan liittyen perustuslakivaliokunta on todennut viestien tunnistamistietojen, joista sittemmin on alettu käyttää termiä välitystieto, jäävän luottamuksellisen viestin salaisuuden ydinalueen ulkopuolelle, minkä vuoksi valiokunta on esimerkiksi pitänyt mahdollisena, että tunnistamistietojen saamisoikeus jätetään sitomatta tiettyihin rikostyyppeihin, jos sääntely muutoin täyttää perusoikeuksien yleiset rajoitusedellytykset (PeVL 7/1997 vp, s. 2/I, PeVL 26/2001 vp, s. 3/II). Perustuslakivaliokunta on kuitenkin todennut, että sähköisen viestinnän käyttöön liittyvät tunnistamistiedot sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen voivat kuitenkin olla yksityiselämän suojan näkökulmasta siinä määrin ongelmallisia, että kategorinen erottelu suojan reuna- ja ydinalueeseen ei aina ole perusteltua, vaan huomiota on yleisemmin kiinnitettävä myös rajoitusten merkittävyyteen (PeVL 18/2014 vp, s. 6/II). Ehdotuksen tarkoittamassa käsittelytarkoituksessa voidaan todeta, että kyse ei ole sellaisesta tietojen kokoamisesta tai yhdistämisestä, jolla olisi merkittävää vaikutusta yksityiselämän suojan kannalta, koska kyse on enemmänkin välitystiedon käyttämisestä teknisenä tunnisteena haavoittuvan laitteen havaitsemiseksi.

Ehdotuksen on arvioitu täyttävän myös täsmällisyyden ja tarkkarajaisuuden vaatimuksen. Ehdotus sisältää useita toimintaa rajaavia tekijöitä. Ensinnäkin toiminta on rajattu yleisesti saatavilla oleviin viestintäverkkoihin ja tietojärjestelmiin eli ehdotus rajaa ulkopuolelle muun muassa yksityiset verkot. Toiminnan tarkoitus on rajattu haavoittuvien tai turvattomasti konfiguroitujen viestintäverkkojen ja tietojärjestelmien havaitsemiseksi ja havainnoista asianomaisille tahoille ilmoittamiseksi sekä kyberturvallisuuden tilannekuvan ylläpitämiseksi. Toimintaa ei siten voisi harjoittaa muuta tarkoitusta varten. Tietoja voitaisiin hankkia teknisin kyselyin telepäätelaitteiden ja tietojärjestelmien sekä niiden tietoliikennejärjestelyjen yksilöintitiedoista, käytetyistä ohjelmistoista ja niiden toiminnasta, teknisestä toteutuksesta ja niiden avulla tarjotuista palveluista. Kyseisten tietojen on arvioitu olevan välttämättömiä muun muassa kriittisiä haavoittuvuuksia sisältävien laitteiden havainnoimiseksi sekä haavoittuvuudesta aiheutuvan kyberuhkan vakavuuden arvioimiseksi. Tiedot on lueteltu ehdotuksessa tyhjentävästi. Ehdotusta on rajattu lisäksi siten, että toiminta ei saa aiheuttaa haittaa kartoituksen kohteena olevan laitteen tai järjestelmän toiminnalle, eikä toiminnalla saa lisäksi hankkia tietoa yleisessä viestintäverkossa tai yleisesti saatavilla olevassa viestintäpalvelussa välitettävänä olevasta viestinnästä, mikä on merkityksellistä myös suhteellisuusperiaatteen toteutumisen näkökulmasta.

Haavoittuvuuskartoituksen aikana käsiteltävien tietojen perusoikeuksiin kohdistuvien rajoitusten on arvioitu olevan oikeasuhtaisia saatavaan hyötyyn nähden. Kartoituksella saavutetaan merkittäviä hyötyjä tietoturvaloukkausten ennalta ehkäisemisen kautta, joilla voi olla yksilöiden ja yhteiskunnan kannalta merkittäviäkin vaikutuksia esimerkiksi tietomurtojen tai toiminnan häiritsemisen muodossa. Ehdotus on myös rajattu edellä kuvatulla tavalla siten, että se täyttää kokonaisuudessaan oikeasuhtaisuuden vaatimuksen.

Ehdotuksen ei arvioida olevan oikeusturvan toteutumisen kannalta ongelmallinen, sillä ehdotuksen nimenomaisena tavoitteena on saada tieto haavoittuvista laitteista ja järjestelmistä niitä hallinnoivien tahojen tietoon. Lisäksi ehdotuksessa on tehty erityisesti oikeusturvan kannalta merkittäviä rajauksia sen suhteen, mihin tietoa voidaan käyttää. Tietoja voitaisiin käyttää vain kartoituksen kohteelle viestintäverkkoon tai tietojärjestelmään kohdistuvista haavoittuvuuksista ja riskeistä ilmoittamiseksi sekä kyberuhkien tunnistamiseksi, kyberturvallisuuden tilannekuvan ylläpitämiseksi ja haavoittuvuuksista tiedottamiseksi. Ehdotus sisältää myös velvoitteen tarpeettomien tietojen poistamisesta.

Ehdotuksen ei ole arvioitu olevan ongelmallinen myöskään ihmisoikeusvelvoitteiden kannalta. Euroopan unionin tuomioistuin (EUT) ja Euroopan ihmisoikeustuomioistuin (EIT) ovat useissa ratkaisuissaan käsitelleet lähinnä valtiollisten toimijoiden kohdentamatonta tiedonhankintaa-, käsittelyä ja -säilytystä, jolla tyypillisesti on liittymäkohtia siviili- tai sotilastiedusteluun. Euroopan ihmisoikeussopimuksen (EIS) 8 ja 10 artikloja koskevissa tapauksissa on yleisesti huomioitu artikloissa muotoillut oikeuksien rajoitusperusteet, joiden keskeisenä sisältönä on lailla säätämisen vaatimus sekä välttämättömyys demokraattisessa yhteiskunnassa, esimerkiksi kansallisen ja yleisen turvallisuuden varmistamiseksi. Täten kohdentamattoman tiedonhankinnan (”bulk interception”) EIS:n kontekstissa tulisi tapahtua esimerkiksi kansallisen turvallisuuden turvaamiseksi siten, että tiedonhankinnasta säädetään kansallisella lailla, ja että puuttuminen yksityisen oikeuteen on välttämätöntä demokraattisessa yhteiskunnassa (esim. Kennedy v. the United Kingdom, kohta 155 ; Roman Zakharov v. Russia, kohta 236). EIT on ratkaisuissaan *Big Brother Watch and Others v. the United Kingdom* sekä *Centrum för Rättvisa v. Sweden* luonut kehyksen, jonka nojalla voidaan arvioida lainsäädäntötoimenpiteiden reunaehtoja ja riittävyyttä. Huomionarvoista on, että perustuslakivaliokunta ei ole lausuntokäytännössään myöskään pitänyt mahdollisena yleistä, kohdentamatonta ja kaiken kattavaa tietoliikenteen seurantaa tiedustelutoiminnan yhteydessä (PeVM 4/2018 vp, s. 8). Nyt käsillä olevassa ehdotuksessa ei olisi kysymys tämänkaltaisesta tiedonhankinnasta tai tietoliikenteen seurannasta.

Ehdotettu haavoittuvuuskartoitustoiminta poikkeaa EIT:n ja EUT:n käsittelemien tapausten kohdentamattomasta tiedonhankinnasta kahdella merkittävällä tavalla. Kuvatuissa ratkaisuissa tarkoitettu toiminta käytännössä tarkoittaisi tiedon keräämistä tietoliikenteestä kaappaamalla itse liikennettä viestinnän osapuolten välissä. Haavoittuvuuskartoitustoiminnassa ei kaapattaisi tai analysoitaisi osapuolten välistä viestintää. Haavoittuvuuskartoitusta toteuttava taho toimisi sen sijaan itse viestinnän osapuolen roolissa lähettämällä yleisessä viestintäverkossa palvelimelle pyyntöjä ja analysoimalla palvelimen lähettämiä teknisiä vastauksia pyyntöihin, mikä mahdollistaa haavoittuvuuden havainnointia. Tässä tilanteessa toimitaan tietoliikenteen eri tasolla, joka ei ole vastaavalla tavalla ongelmallinen ihmisoikeusvelvoitteiden toteutumisen tai luottamuksellisen viestinnän näkökulmasta, koska kysymys ei olisi viestinnän seuraamisesta. Lisäksi toisena merkittävänä erona on toiminnan tarkoitus. Tuomioistuinten ratkaisut ovat keskittyneet usein tiedusteluviranomaisten harjoittamaan toimintaan eli tiedon hankintaan turvallisuutta uhkaavasta toiminnasta. Ehdotuksen tarkoituksena sen sijaan on kartoituksen kohteena olevien toimijoiden tietoturvan parantaminen havainnoimalla viestintäverkkojen ja tietojärjestelmien julkisesti saatavilla olevia teknisiä ominaisuuksia ja sitä kautta muun muassa viestinnän luottamuksellisuuden edistäminen sekä viestintäverkossa ja tietojärjestelmässä välitettävänä olevan viestinnän tai tietojen suojaaminen ja turvallisuuden parantaminen.

Ehdotukseen sisältyy myös edellä mainittua havainnointikartoitusta kohdennetumpi havainnointikartoitus, joka tapahtuisi kohteen pyynnöstä. Pyynnöstä tapahtuvan haavoittuvuuskartoituksen ei ole arvioitu olevan perusoikeusnäkökulmasta erityisen ongelmallinen erityisesti, koska kysymys on kohteen pyynnöstä toteutettavasta toimenpiteestä, jonka laajuuden kartoituksen pyytäjä voisi määritellä. Kohdennettu haavoittuvuuskartoitus ei sisällä mahdollisuutta käsitellä viestinnän sisältöä ilman viestinnän osapuolen suostumusta. Haavoittuvuuskartoituksella

ei saisi hankkia tietoa viestintäverkossa tai yleisesti saatavilla olevassa viestintäpalvelussa välitettävänä olevasta viestinnästä.

Edellä esitetyin perustein haavoittuvuuskartoitusta koskevan ehdotuksen arvioidaan olevan perustuslain 10 §:n edellytysten mukainen.

Välitystietoja ja haitallista sisältöä koskeva tiedonvaihto

Ehdotuksen 22, 24 ja 28 § sisältävät säännöksiä välitystietoja ja haitallisen tietokoneohjelman tai käskyn sisältävään viestiin liittyvästä tietojen luovuttamisesta. Ehdotuksen 22 §:ssä on kyse vapaaehtoisessa jakamisjärjestelyssä mukana olevien toimijoiden tiedonvaihdosta ja CSIRT-yksikkö voisi luovuttaa haitallista tietokoneohjelmaa tai käskyä sisältävän viestin jakamisjärjestelyyn osallistuvalle taholle, mikäli se on tarpeen kyberuhkien ehkäisemiseksi, havaitsemiseksi, poikkeamien hallitsemiseksi ja niistä palautumiseksi sekä vaikutusten lieventämiseksi.

Lisäksi ehdotuksen 24 § sisältää toimijan tai 22 §:ssä tarkoitettuun vapaaehtoiseen jakamisjärjestelyyn osallistuvan tahon mahdollisuudesta luovuttaa välitystietoa tai haitallisen tietokoneohjelman tai käskyn sisältävän viestin oma-aloitteisesti CSIRT-yksikölle, valvovalle viranomaiselle tai toiselle ehdotuksen mukaiseen jakamisjärjestelyyn osallistuvalle taholle silloin, kun kyse on kyberuhkaan tai poikkeamaan liittyvästä välitystiedosta.

Ehdotuksen 28 §:n mukaan valvovalla viranomaisella on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada toimijalta välitystieto, sijaintitieto tai haitallisen tietokoneohjelman tai käskyn sisältävä viesti, jos se on välttämätöntä kyberturvallisuuden riskienhallintavelvoitteiden valvomista varten tai merkittävien poikkeamien selvittämiseksi.

Viestinnän luottamuksellisuuden kannalta edellä on jo tuotu esiin välitystietoja koskeva käytäntö, jonka mukaan perustuslakivaliokunta on pitänyt mahdollisena, että tunnistamistietojen saamisoikeus jätetään sitomatta tiettyihin rikostyyppeihin, jos sääntely muutoin täyttää perusoikeuksien yleiset rajoitusedellytykset, sillä välitystietojen ei ole katsottu kuuluvan perustuslain 10 §:n ydinalueeseen. Myöhemmässä käytännössään valiokunta on kuitenkin todennut, että sähköisen viestinnän käyttöön liittyvät tunnistamistiedot sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen voivat kuitenkin olla yksityiselämän suojan näkökulmasta siinä määrin ongelmallisia, että kategorinen erottelu suojan reuna- ja ydinalueeseen ei aina ole perusteltua, vaan huomiota on yleisemmin kiinnitettävä myös rajoitusten merkittävyyteen (PeVL 18/2014 vp, s. 6/II). Ehdotuksen mukaisissa tiedonvaihtotilanteissa ei arvioida olevan yksityiselämän suojan kyse kannalta merkittävästä rajoituksesta. Tiedoilla voidaan tunnistaa ja estää haitallista liikennettä ja tietoa käytetään teknisenä tunnisteena edellä kuvattuihin tarkoituksiin eikä niinkään yksityiselämää koskevana tietona.

Haitallisen tietokoneohjelman ja käskyn sisältävän viestin voidaan ajatella koskevan kuitenkin viestin sisältöä. Viestin sisältö on sellaisenaan nauttinut perinteisesti vahvasti perusoikeussuojaa ja yksityisen viestin sisällön on tulkittu olevan viestinnän luottamuksellisuuden suojan ydinalueella. Toisaalta haitallisen tietokoneohjelman tai käskyn sisältävässä viestissä kysymys on usein automatisoidusti luodusta kalasteluviestistä, jonka tarkoituksena on saada kohde erehdytettyä suorittamaan haitallinen tietokoneohjelma tai luovuttamaan hyökkääjälle hyödyllistä tietoa. Haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelyn tarkoituksena ei ole saada selkoa viestin sisällöstä eikä tämänkaltaisen viestin sisällössä pääasiallisesti ole luottamuksellisen viestinnän suojan ydinalueeseen kuuluvaa henkilökohtaista, vain toisen osapuolen vastaanotettavaksi tarkoitettua viestintää. Haitallisen tietokoneohjelman tai käskyn sisältävä

viesti on pääasiallisesti haitallisen tietokoneohjelman automaattisesti luoma tai kyberhyökkäystä suorittavan tahon ennalta tuntemattomalle vastaanottajajoukolle lähettämä kalasteluviesti. Perustellusti voidaan päätyä myös tulkintaan, jossa tämänkaltainen kyberhyökkäyksen toteuttamiseksi luotu haitallisen tietokoneohjelman tai käskyn sisältävä viesti ei kuuluisi viestinnän luottamuksellisuuden suojan ydinalueelle. Viestin käsittelyn tarkoituksena olisi tutkia tai selvittää haittaohjelman teknisiä ominaisuuksia sekä varoittaa yleisöä vastaavasta viestistä. Perustuslakivaliokunnan arvion varaan jää, missä määrin kuvatun kaltainen haittaohjelmaviestintä nauttii viestinnän luottamuksellisuuden suojaa tai sijoittuu viestinnän luottamuksellisuuden suojan ydinalueelle esimerkiksi viestin teknisten haittaohjelmaominaisuuksien tai välitystietojen osalta.

Ehdotusten tarkoituksena on tietoturvan parantaminen haitallisista teknologioista tiedon jakamisen kautta, jolloin haitallisen tietokoneohjelman tai käskyn tietoja taikka välitystietoja voitaisiin käyttää tietoturvan vaarantumista aiheuttavan toiminnan tunnistamiseen sekä vastaavalta haitallisen tietokoneohjelman tai käskyn sisältävältä viestiltä suojautumiseen ja sen teknisten ominaisuuksien selvittämiseen. Haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsitteleminen tässä tarkoituksessa on usein välttämätöntä. Haitallisen tietokoneohjelman ja käskyn sisältävässä viestissä on usein kyse haitallisen tietokoneohjelman automaattisesti luomasta viestistä, jossa viestin lähettäjänä ei ole luonnollista henkilöä, vaan haittaohjelma tai sen ohjelmoinut taho. Haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsitteleminen mahdollistaa sen teknisten ominaisuuksien selvittämisen sekä yleisön varoittamisen vastaavasta viestistä. Lisäksi oikeusjärjestelmässä omaksutun shikaanikiellon näkökulmasta voidaan argumentoida, että luottamuksellisen viestinnän suojaa ei tulisi tulkita tavalla, joka estäisi haittaohjelmaviestistä sen teknisten tietojen käsittelemistä haittaohjelman ehkäisemiseksi, milloin luottamuksellisen viestinnän suojalla suojattaisiin toimintaa, jonka tarkoituksena vakavasti vaarantaa juuri luottamuksellisen viestinnän suojaa sähköisessä viestinnässä. Erityisesti yhteiskunnan kriittisten toimijoiden kybervarautumisen kannalta olisi tärkeää, että hyökkäyksissä käytettäviä haittaohjelmia koskevia tietoja voitaisiin jakaa hyökkäysten potentiaalisten kohteiden kesken.

Sotilastiedustelulaissa (590/2019) on tietoliikennetiedustelun yhteydessä säädetty mahdolliseksi luovuttaa haitallisen tietokoneohjelman tai käskyn sisältävä tieto yrityksille ja yhteisöille sekä viranomaisille. Ehdotusta on perusteltu siten, että yhteiskunnan kokonaissuojautumisen kannalta tärkeää, että hyökkäyksissä käytettäviä haittaohjelmia koskevia tietoja voitaisiin mahdollisimman laajasti luovuttaa hyökkäysten potentiaalisille kohteille. Tällaisten tietojen luovuttamisoikeudesta säätämällä voitaisiin osaltaan turvata yritysten ja yhteisöjen mahdollisuuksia ryhtyä sellaisiin toimenpiteisiin tietoturvastaan huolehtimiseksi, joista säädetään sähköisen viestinnän palveluista annetun lain 272 §:ssä. Kyseisen säännöksen mukaiset toimenpiteet voivat pitää sisällään muun muassa viestin sisällön automaattisen selvittämisen, viestinen välittämisen ja vastaanottamisen automaattisen estämisen tai rajoittamisen sekä tietoturvaa vaarantavien haitallisten tietokoneohjelmien automaattisen poistamisen viesteistä (HE 203/2017 vp). Asiaa koskevassa hallituksen esityksessä perustuslakivaliokunta ei nostanut ehdotettua säännöstä esiin perusoikeuksien kannalta ongelmallisena.

Yleisesti arvioituna ehdotuksilla on ensisijaisesti luottamuksellisen viestin suojaa rajoittava vaikutus tiedonvaihtotilanteissa. Toisaalta tiedonvaihdon perusteena on muun muassa luottamuksellisen viestinnän suojaaminen kyberuhkiin varautumisen ja niiltä suojautumisen kautta, jolloin luottamuksellisen viestinnän suojaamista välillisesti edistettäisiin sitä yksittäisessä tilanteessa rajoittamalla. Luottamuksellisen viestin suojaamista koskeva perusoikeusvaikutus olisi siten välillinen seuraus niistä toimenpiteistä, joita viranomaiset tietoturvaloukkauksen selvittämisen, ennaltaehkäisemisen ja vaikutusten poistamisen yhteydessä tekevät.

Perustuslakivaliokunta on todennut viestien tunnistamistietojen, joista sittemmin on alettu käyttää termiä välitystieto, jäävän luottamuksellisen viestin salaisuuden ydinalueen ulkopuolelle, minkä vuoksi valiokunta on esimerkiksi pitänyt mahdollisena, että tunnistamistietojen saamisoikeus jätetään sitomatta tiettyihin rikostyyppeihin, jos sääntely muutoin täyttää perusoikeuksien yleiset rajoitusedellytykset (PeVL 7/1997 vp, s. 2/I, PeVL 26/2001 vp, s. 3/II). Ehdotuksessa olisi kyse kuvatusta tilanteesta, sillä ehdotuksien arvioidaan täyttävän yleiset rajoitusedellytykset muun ohella lailla säätämisestä, täsmällisyydestä ja tarkkarajaisuudesta, rajoituksen hyväksyttävyydestä, suhteellisuudesta ja ydinalueen koskemattomuudesta.

Kuvatun kaltaisen haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelyn arvioidaan jäävän viestinnän luottamuksellisuuden suojan ydinalueen ulkopuolelle, kun otetaan huomioon käsittelyn tarkoitus ja tavoite suhteessa rajoituksen laatuun ja merkittävyyteen. Lisäksi velvoittava direktiivin täytäntöönpano edellyttää näiden tietojen käsittelemisen mahdollisuutta, jotta ehdotuksen tavoitteet voidaan saavuttaa. Ehdotus täyttäisi myös muilta osin yleiset rajoitusedellytykset. Näin ollen tietojen vaihtoa koskevien ehdotusten arvioidaan olevan siten perustuslain mukaisia, että ehdotus voidaan käsitellä tavanomaisessa lainsäädäntöjärjestyksessä. Haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelyä koskevan ehdotuksen johdosta esityksestä olisi kuitenkin tarpeen pyytää perustuslakivaliokunnan lausunto.

12.2 Julkisen hallintotehtävän antaminen muulle kuin viranomaiselle ja viranomaisen suoritteen maksullisuus

Ulkopuolisen asiantuntijan käyttäminen apuna tarkastuksessa.

Kyberturvallisuuden riskienhallinnasta ehdotetun lain 29 §:n nojalla valvova viranomainen voisi tehdä toimijaa koskevan tarkastuksen käyttäen apunaan tai valtuuttamalla tarkastuksen suorittajaksi tietoturvallisuuden arviointilaitoksen tai ulkopuolisen tietotekniikan asiantuntijan, jos se on tarkastuksen laadun tai laajuuden vuoksi tarpeellista. Ehdotetun tiedonhallintalain 18 k §:n nojalla Liikenne- ja viestintävirasto voisi antaa tarkastustehtävään liittyvän avustavan tehtävän tietoturvallisuuden arviointilaitoksista annetussa laissa (1405/2011) tarkoitetulle hyväksytylle tietoturvallisuuden arviointilaitokselle. Ehdotukset ovat merkityksellisiä perustuslain 124 §:n kannalta, jonka mukaan julkinen hallintotehtävä voidaan antaa muulle kuin viranomaiselle vain lailla tai lain nojalla, jos se on tarpeen tehtävän tarkoituksenmukaiseksi hoitamiseksi eikä vaaranna perusoikeuksia, oikeusturvaa tai muita hyvän hallinnon vaatimuksia. Merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan kuitenkin antaa vain viranomaiselle.

Perustuslakivaliokunnan lausuntokäytännössä on painotettu, että perustuslain 124 §:n tarkoituksenmukaisuusvaatimus on oikeudellinen edellytys, joka vaatii tapauskohtaista arviointia jokaisen viranomaisorganisaation ulkopuolelle annettavaksi esitetyn julkisen hallintotehtävän kohdalla. Tällöin on huomioitava muun muassa hallintotehtävän luonne (PeVL 44/2016 vp s.5, PeVL 26/2017 vp, s.49, PeVL 5/2014 vp, s.3/I, PeVL 8/2014 vp, s.3/II, PeVL 23/2013 vp, s.3/I, PeVL 65/2010 vp, s.2/II). Tarkoituksenmukaisuusarvioinnissa tulee perustuslain esitöiden mukaan huomioida hallinnon sisäiset tarpeet sekä yksityisten henkilöiden ja yhteisöjen tarpeet (PeVL 44/2016 vp, s.5, HE 1/1998 vp, s.179/II).

Tarkastuksen suorittamisessa lähtökohtana olisi se, että valvova viranomainen suorittaa itse tarkastuksen. Perustuslakivaliokunnan lausuntokäytännön nojalla tarkastus voi valvonnan kohteina oleviin seikkoihin liittyvien ammatillisten ja teknisten erityispiirteiden vuoksi olla joissain tilanteissa tarkoituksenmukaista suorittaa viranomaisen siihen valtuuttaman asiantuntijan toimesta (PeVL 40/2002 vp, s.3, PeVL 44/2016 vp, s.5). Tarpeellisuusvaatimus voi täyttyä esimerkiksi silloin, kun tarkastuksen tekeminen edellyttää osaamista tai resursseja, joita viranomaisella ei ole (PeVL 29/2013 vp, s.2/I). Ehdotetun 29 §:n 2 momentin mukaan ulkopuolisen

asiantuntijan käyttäminen olisi mahdollista vain, jos tarkastuksen laatu ja laajuus sitä edellyttää. Käytännössä ehdotus koskisi siis tilannetta, jossa tarkastuksen tarkastus kohdistuisi sellaisiin seikkoihin, joiden tarkastaminen vaatisi sellaista teknistä erityisosaamista tai poikkeuksellista osaamista, jota viranomaisella itsellään ole hallussa.

Perustusvaliokunta on katsonut, että annettaessa hallintotehtäviä muulle kuin viranomaiselle on oikeusturvan ja hyvän hallinnon vaatimusten noudattaminen turvattava säännösperusteisesti (PeVL 26/2001 vp, s.5/II, PeVL 2/2001 vp, s.2). Lisäksi perustusvaliokunta on viimeaikaisessa lausuntokäytännössään katsonut, että yrityksiin kohdistuvissa valvontatyyppisten tarkastuksen sääntelyssä on syytä viitata hallintolain tarkastuksia koskeviin 39 §:n yleissäännöksiin (PeVL 44/2016 vp s.6, PeVL 35/2014 vp, s.4/I ja PeVL 29/2013 vp, s.2). Tämä perustuslakivaliokunnan lausuntokäytäntö on esityksessä huomioitu ehdotetuissa kyberturvallisuuden riskienhallintaa koskevan lain 29 §:n 4 momentissa ja tiedonhallintalain 18 j §:n 3 momentissa, joiden mukaan tarkastuksessa noudatettavaan menettelyyn sovelletaan hallintolain 39 §:ä.

Perustuslakivaliokunta on katsonut, että perusoikeuksien, oikeusturvan ja hyvän hallinnon vaatimusten turvaamisesta voidaan huolehtia asianomaisten henkilöiden pätevyyden ja sopivuuden avulla (PeVL 5/2006 vp, s.8/9, PeVL 67/2002 vp, s.5/7 ja PeVL 2/2002 vp, s.2). Lisäksi tehtäviä hoitavien henkilöiden julkisen valvonnan tulee olla asianmukaista (PeVL 2/2002 vp, s. 2, PeVL 5/2006 vp, s.8 ja HE 1/1998 vp, s.179/II). Ehdotetussa kyberturvallisuuden riskienhallintaa koskevan lain 29 §:n 2 momentissa ja tiedonhallintalain 18 j §:n 2 momentissa säädetään, että tarkastajalla tulee olla tarkastustehtävän laatuun ja laajuuteen nähden sellainen koulutus ja kokemus, joka on tarpeen tehtävän hoitamiseksi. Tämä pätevyysvaatimus koskee myös sellaista ulkopuolista asiantuntijaa, joka voidaan määrätä tekemään tarkastus 27 §:n 2 momentin nojalla. Perusoikeuksien, oikeusturvan ja hyvän hallinnon osalta perustuslakivaliokunta on lisäksi katsonut, että tarkastuksessa noudatetaan hallinnon yleislakeja ja että asioita käsitellään virkavastuulla (PeVL 20/2006 vp, s. 2, PeVL 46/2002 vp, s. 10, PeVL 33/2004 vp, s. 7/II, PeVL 11/2006 vp, s. 3). Esitettyjen kyberturvallisuuden riskienhallintaa koskevan lain 29 §:n 2 momentin ja tiedonhallintalain 18 k §:n 3 momentin mukaan ulkopuoliseen asiantuntijaan ja hyväksytyn arviointilaitoksen palveluksessa olevaan henkilöön sovellettaisiin rikosoikeudellista virkavastuuta koskevia säännöksiä hänen hoitaessaan kyseisen pykälän mukaisesti annettuja julkisoikeudellisia hallintotehtäviä. Lakiin ei enää nykyisin ole välttämätöntä sisällyttää perustuslain 124 §:ään perustuvaa viittausta hallinnon yleislakeihin, mikäli ehdotuksesta käy selvästi ilmi, että hallinnon yleislakeja sovelletaan PL 124 §:ssä tarkoitettuun toimintaan (PeVL 20/2006 vp, s.2) Hallinnon yleislakeja sovelletaan silloin, kun kyse on viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 4 §:n 2 momentin mukaisesta toimijasta.

Perustuslain 124 §:n mukaan merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan antaa vain viranomaiselle. Ehdotetuissa kyberturvallisuuden riskienhallintaa kokevan lain 29 §:ssä ja tiedonhallintalain 18 k §:ssä ei olisi kysymys merkittävän julkisen vallan käyttämisestä. Perustuslakivaliokunta on lausunnoissaan katsonut, että merkittävänä julkisen vallan käyttämisenä pidetään esimerkiksi perusoikeuksiin puuttumista ((HE 1/1998 vp, s. 179/II, PeVL 28/2001 vp, s.5), itsenäiseen harkintaan perustuvaa voimakeinojen käyttöä (HE 1/1998 vp, s. 179/II, PeVL 28/2001 vp, s.5) ja kotirauhan piiriin kohdistuvia tarkastusvaltuuksia (PeVL 40/2002 vp, s.3/II, PeVL 46/2001 vp, s.3/II). Ulkopuolista tarkastajaa ei voida määrätä ainakaan yksin suorittamaan tarkastusta tiloissa, jotka kuuluvat kotirauhan piiriin (PeVL 29/2013 vp, s.2). Perustuslakivaliokunnan lausuntokäytäntö on huomioitu ehdotuksen 29 §:n 3 momentissa ja tiedonhallintalain 18 j §:n 3 momentissa, joiden mukaan tarkastaja on päästettävä muihin, kuin pysyväisluonteiseen asumiseen tarkoitettuihin tiloihin.

Edellä esitetyin perustein ehdotus ulkopuolisen asiantuntijan käyttämisestä tarkastuksessa ei arvioida olevan ristiriidassa perustuslain 124 §:n kanssa.

Viranomaisen suoritteen maksullisuus

Hallituksen esityksen 19 §:n 6 momentin ehdotuksen nojalla CSIRT-yksikkö voisi periä maksun eräistä suoritteistaan ja maksun määrästä ja perusteista säädettäisiin liikenne- ja viestintäministeriön asetuksella. Ehdotus on merkityksellinen perustuslain 81 §:n 2 momentin näkökulmasta, jonka mukaan valtion viranomaisten, palvelujen ja muun toiminnan maksullisuuden sekä maksujen suuruuden yleisistä perusteista säädetään lailla. Perustuslain esitöiden mukaan lailla on säädettävä maksujen suuruuden määrittämisessä noudatettavista periaatteista, kuten omakustannusarvon tai liiketaloudellisten perusteiden noudattamisesta (HE 1/1998 vp, s. 135/I).

Perustuslakivaliokunnan vakiintuneen käytännön mukaan valtiosääntöoikeudellisille maksuille on ominaista, että ne ovat korvausta tai vastiketta julkisen vallan palveluista. Maksujen vastikesuhdetta arvioitaessa tulee kiinnittää huomiota muun muassa suoritteiden yksilöitävyyteen, kustannusvastaavuuteen sekä siihen, onko maksu pakollinen vai vapaaehtoinen (PeVL 49/2006 vp, s. 2 ja siinä viitatut perustuslakivaliokunnan lausunnot).

Ehdotetussa 19 § 6:ssä olisi kysymys yksilöidystä ja yksittäiseen toimijaan kohdistuvasta viranomaisen suoritteesta, jonka tuottamisesta aiheutuu olennaisia ja palvelun käytön määrään sidonnaisia kustannuksia viranomaiselle. Toimijalle viranomaisen tarjoaman palvelun hankkiminen ja vastaanottaminen olisi vapaaehtoista ja maksuvelvollisuus perustuisi viimesijassa toimijan omaan harkintaan palvelun tarpeesta. Laissa säädettäisiin CSIRT-yksikön palveluista, joiden tarjoaminen voisi olla perittävän maksun perusteena. Lisäksi maksun edellytyksenä olisi palvelun tarjoaminen toimijan pyynnöstä ja viranomaisaloitteiset suoritteet eivät voisi olla maksun perusteena. Ehdotuksen arvioidaan vastaavan niitä edellytyksiä, jotka perustuslain 81 §:n 2 momentin perusteella kohdistuu valtion maksujen sääntelyyn.

12.3 Elinkeinonvapaus

Toimijoiden ilmoittautumisvelvollisuus valvovalle viranomaiselle

Esitykseen sisältyy ehdotus soveltamisalaan kuuluvien toimijoiden velvollisuudesta ilmoittaa valvovalle viranomaiselle kyberturvallisuuden riskienhallinnasta annetun lain 43 §:ssä tarkoitetut tiedot toimijaluettelon ylläpitämiseksi. Lisäksi sähköisen viestinnän palveluista annetun lain 165 §:ssä säädettäisiin nykyistä yksityiskohtaisemmin verkkotunnusvälittäjän tiedoista, jotka on ilmoitettava ennen toiminnan aloittamista. Ehdotukset tarkoittaisivat käytännössä soveltamisalaan kuuluvan toimijan ilmoitusvelvollisuutta toiminnasta valvovalle viranomaiselle ja ne olisivat siten merkityksellisiä perustuslain 18 §:ssä turvatun elinkeinovapauden kannalta.

NIS2-direktiivin täytäntöönpano edellyttää ilmoitusvelvollisuuden mukaisten tietojen keräämistä näiltä toimijoilta. Lisäksi ilmoittautumisvelvollisuus toisi valvovan viranomaisen tietoon kyberturvallisuuden riskienhallinnasta annetun lain soveltamisalaan kuuluvat toimijat ja mahdollistaisi valvonnan kohdentamisen näihin toimijoihin.

Kyberturvallisuuden riskienhallinnasta annetun lain 43 §:n mukaan toimijoiden olisi ilmoitettava valvovalle viranomaiselle 43 §:n 1 momentin a-f kohdissa listatut tiedot toimijaluettelon ylläpitämiseksi. Näiden tietojen lisäksi DNS-palveluntarjoajien, aluetunnusrekisterien, pilvipalvelujen tarjoajien, datakeskuspalvelujen tarjoajien, sisällönjakeluverkkojen tarjoajien, hallintapalvelun tarjoajien, tietoturvapalveluntarjoajien sekä verkossa toimivien markkinapaikkojen tarjoajien, verkossa toimivien hakukoneiden tarjoajien ja verkkoyhteisöalustojen tarjoajien on ilmoitettava valvovalle viranomaiselle 3 §:n 2 momentin a-c kohdan tiedot. Pykälän 3 momen-

tissa säädetään lisäksi toimijan velvollisuudesta ilmoittaa muutoksista sekä valvovan viranomaisen oikeudesta antaa tarkempia määräyksiä tietojen ilmoittamisesta. Valvova viranomainen ylläpitäisi toimijaluetteloa ilmoituksiin perustuen.

Perustuslakivaliokunta on lausunnossa PeVL 52/2002 vp katsonut, ettei pelkästä ilmoitusvelvollisuudesta säätäminen ole itsessään elinkeinovapauden kannalta ongelmallista etenkään, kun viranomaisen ei edellytetä tekevän ilmoituksen johdosta päätöstä. Ehdotetussa ilmoitusvelvollisuudessa olisi kyse kuvatun kaltaisesta tilanteesta. Toisaalta perustuslakivaliokunta on lausuntokäytännössään katsonut, että velvollisuus tehdä toiminnasta ilmoitus valvovalle viranomaiselle ja luovuttaa tälle tietoja tilanteessa, jossa ilmoituksen tekemättä jättäminen johtaa kielteisiin seurauksiin, rinnastuu usein luvanvaraisuuteen ja merkitsee näin ollen puuttumista elinkeinovapauteen (PeVL 45/2001 vp). Ilmoitusvelvollisuudessa on kuitenkin kyse luvanvaraisuutta lievemmin elinkeinonvapauteen puuttuvasta velvoitteesta. Perustuslakivaliokunta ei ole katsonut ilmoitusvelvollisuutta elinkeinovapauden kannalta ongelmallisena, kun ilmoituksen tekemättä jättämiselle ei ole asetettu kieltoa harjoittaa elinkeinotoimintaa (PeVL 16/2009 vp) tai viranomaisen ei edellytetä tekevän ilmoituksen johdosta päätöstä (PeVL 52/2002 vp ja 54/2002 vp). Esityksessä asetettaisiin toimijalle velvoite ilmoittaa vaaditut tiedot viranomaiselle silloin, kun se kuuluisi NIS2-direktiivin edellyttämän ilmoitusvelvollisuuden soveltamisalaan. Ilmoituksen tekeminen ei ole toiminnan harjoittamisen edellytys eikä valvovan viranomaisen edellytetä tekevän päätöstä ilmoituksen johdosta. Ilmoitusvelvollisuuden laiminlyönti olisi kuitenkin sanktioitu hallinnollisella seuraamuksella ja valvovalla viranomaisella olisi toimivalta määrätä laiminlyönti oikaistavaksi uhkasakon tai keskeyttämisuhkan nojalla. Lisäksi valvovalla viranomaisella olisi viimesijassa oikeus käyttää muita laissa säädettyjä toimivaltuuksia lain vastaisen menettelyn oikaisemiseksi ja valvova viranomainen ylläpitäisi toimijaluetteloa ilmoituksiin perustuen.

Ehdotetussa ilmoitusvelvollisuudessa olisi kyse elinkeinovapauden rajoittamisesta ja ehdotuksen olisi täytettävä perusoikeutta rajoittavalta lailta vaadittavat yleiset edellytykset, kuten hyväksyttävyyden sekä täsmällisyyden ja tarkkarajaisuuden vaatimukset (PeVL 58/2014 vp, s.5, PeVL 19/2009 vp, s.2). Elinkeinovapauden rajoittamiselle tulee perustuslakivaliokunnan mukaan olla hyväksyttävä ja painava peruste (PeVL 15/2008 vp, s.2). Esityksen tavoitteena on parantaa kyberturvallisuutta vahvistamalla soveltamisalaan kuuluvien toimijoiden kykyä hallita kyberuhkia ja ehkäistä merkittäviä poikkeamia, millä pyritään kyberturvallisuusriskien hallitsemiseen yhteiskunnan toiminnan kannalta kriittisissä toiminnoissa niiden tarjoamien palveluiden jatkuvuuden turvaamiseksi. Ehdotuksella arvioidaan olevan luvanvaraisen toiminnan rajoittamiseksi painava ja hyväksyttävä syy.

Toimijoiden velvollisuus ilmoittautua valvovalle viranomaiselle ja toimijaluettelon ylläpitäminen mahdollistaa toimijoille esityksen nojalle asetettujen velvoitteiden valvonnan sekä laajassa kyberhäiriötilanteessa sen vaikuttavuuden ennakoinnin arvioinnin sekä Suomessa että EU:n tasolla. NIS2-direktiivin toimeenpano edellyttää ilmoitusvelvollisuudesta säätämistä. Säännökseltä edellytettäisiin *täsmällisyyttä ja tarkkarajaisuutta* (PeVL 15/2008 vp, s.2, PeVL 33/2005 vp, s.2) ja elinkeinovapauden rajoitusten olennaisen sisällön, kuten rajoitusten laajuuden ja edellytysten tulisi ilmetä laista (PeVL 19/2009 vp, s.2). Laissa olisi määritelty ne toimijat, joihin ilmoitusvelvollisuus kohdistuu ja ilmoitettavat tiedot olisi määritelty tyhjentävästi lain tasolla. Lisäksi perustuslakivaliokunta on lausuntokäytännössään katsonut, että viranomaistoiminnan tulisi olla *ennustettavaa* ja viranomaisen toimivaltuuksien määräytyä *sidotussa harkinnassa* (PeVL 10/2012 vp, s.4, PeVL 24/2000 vp, s.2). Viranomaistoiminnan ennustettavuutta tukee se, että rekisteröinnin edellytyksistä ja pysyvyydestä säännellään (PeVL 19/2009 vp, s.2, PeVL 15/2008 vp, s.2). Valvova viranomainen pitäisi ilmoituksien perusteella toimijarekisteriä valvottavan toimialan soveltamisalaan kuuluvista toimijoista. Perustuslakivaliokunta on lausuntokäytännössään edellyttänyt sitä, että laista ilmenisi, että rekisteriin merkittäisiin jokainen, joka

harjoittaa lain sääntelemää toimintaa (PeVL 45/2001 vp). Ehdotetusta 43 §:stä ilmenisi, että valvova viranomainen ylläpitää valvontatoimialansa osalta toimijaluetteloa ilmoitettujen tietojen perusteella.

Kyberturvallisuuden riskienhallinnasta esitetyn lain 43 § ja sähköisen viestinnän palveluista annetun lain 165 §:ään ehdotettavat muutokset vastaisivat perustuslakivaliokunnan käytännöstä ilmeneviä reunaehtoja elinkeinovapautta rajoittavalle säännökselle eikä niiden arvioida siten olevan ristiriidassa perustuslain 18 §:n 1 momentissa turvatun elinkeinovapauden kannalta tavalla, joka estäisi lakiesityksen käsittelemisen tavallisen lain säätämisjärjestyksessä. .

Luvanvaraisen tai sertifioidun toiminnan rajoittaminen

Ehdotuksen 32 §:än sisältyy ehdotus luvanvaraisen tai sertifioidun toiminnan rajoittamisesta ja luvan tai sertifioinnin peruuttamisesta. Ehdotuksella pantaisiin täytäntöön NIS2-direktiivin 32 artiklan 5 kohdan valvovalta viranomaiselta edellyttämä toimivalta. Ehdotus erityisesti luvanvaraisen toiminnan rajoittamisesta tai luvan peruuttamisesta on merkityksellinen perustuslain 18 §:ssä turvattun elinkeinovapauden kannalta. Viranomaiselle voidaan myöntää toimivalta rajoittaa yritysten toimiluvan mukaista toimintaa. Perustuslakivaliokunta on kuitenkin edellyttänyt tällaisissa tilanteissa, että rajoitussääntelyä puoltavat perusoikeusjärjestelmän kannalta hyväksyttävät ja painavat syyt. Perustuslakivaliokunta on lausunnossaan tuonut muun muassa esille, että esimerkiksi rahoitusmarkkinoiden vakauden ja turvaamisen sekä sitä kautta asiakkaan suojaamiseen liittyvät perusteet puoltavat sääntelyä, jolla voidaan puuttua voimakkaasti perustuslaissa suojattuun omaisuuden suojaan ja elinkeinovapauteen (esim. PeVL 43/2004 vp, s.2/I tai PeVL 35/2014 vp, s. 3). Nyt käsillä oleva ehdotus kohdistuu kyberturvallisuusriskien hallitsemiseen yhteiskunnan toiminnan kannalta kriittisissä toiminnoissa niiden tarjoamien palveluiden jatkuvuuden turvaamiseksi, joten ehdotuksella arvioidaan olevan luvanvaraisen toiminnan rajoittamiseksi painava ja hyväksyttävä syy.

Luvan peruuttamista on elinkeinotoiminnan sääntelyn yhteydessä pidetty yksilön oikeusasemaan puuttuvana toimenpiteenä jyrkempänä kuin esimerkiksi luvan epäämistä. Tämän vuoksi luvan peruuttaminen olisi välttämätöntä sitoa vakaviin tai olennaisiin rikkomuksiin tai laiminlyönteihin sekä siihen, että luvanhaltijalle mahdollisesti annetut huomautukset tai varoitukset sekä puutteen tai laiminlyönnin korjaamiseksi annettu kohtuullinen määräaika eivät ole johtaneet toiminnassa esiintyneiden puutteiden korjaamiseen (esim. PeVL 13/2014 vp, s. 3 tai PeVL 34/2012 vp, s. 2). Ehdotuksen luvan peruuttamista koskevat edellytykset on sidottu direktiivin toimijoita keskeisimmin koskevaan velvoitteeseen eli ehdotuksessa tarkoitettuun riskienhallinnan toimintamalliin ja siihen liittyvien tarkoitettujen riskinhallintatoimenpiteiden toteuttamatta jättämiseen. Lisäksi lupa voitaisiin peruuttaa, jos keskeinen toimija olisi jättänyt olennaisesti noudattamatta muita ehdotetun lain tai NIS2-direktiivin nojalla annettujen velvoitteiden noudattamista. Ehdotuksen 32 §:n mukaiset toimet olisivat viimesijaisia keinoja suhteessa muihin valvontatoimivaltuuksiin.

Luvan peruuttaminen voisi kohdistua vain 26 §:ssä tarkoitettuihin keskeisiin toimijoihin. Luvan peruuttaminen olisi viimesijainen toimenpide suhteessa muihin valvontatoimivaltuuksiin. Luvan peruuttaminen edellyttäisi olennaista ja vakavaa lain rikkomusta tai laiminlyöntiä sekä sitä, että luvanhaltijalle annetut huomautukset tai varoitukset sekä puutteen tai laiminlyönnin korjaamiseksi annettu kohtuullinen määräaika ei ole johtanut puutteiden korjaamiseen. Viimesijainen harkinta luvanvaraisen toiminnan peruuttamisesta tai keskeyttämisestä olisi luvan myöntäneellä viranomaisella.

Luvanvaraisen toiminnan rajoittamista koskevan ehdotuksen ei edellä esitetyin katsota olevan ristiriidassa suhteessa perustuslakiin.

Johdon toiminnan rajoittaminen

Hallituksen esityksen 33 §:n mukaan valvova viranomainen voisi määräajaksi, enintään viideksi vuodeksi, kieltää henkilöä toimimasta henkilöä toimimasta keskeisen toimijan hallituksen jäsenenä ja varajäsenenä, hallintoneuvoston jäsenenä ja varajäsenenä, toimitusjohtajana tai muussa siihen rinnastettavassa asemassa, sekä toimitusjohtajan välittömään alaisuuteen kuuluvissa tehtävissä, jotka ovat keskeisen toimijan ylimpiä johtotehtäviä tai joissa tosiasiallisesti johdetaan sen toimintaa, jos tämä on toistuvasti ja vakavasti rikkonut 11 §:ssä säädettyjä velvoitteita. Ehdotuksella pantaisiin täytäntöön NIS2-direktiivin 32 artiklan 5 kohdan valvovalta viranomaiselta edellyttämä toimivalta. Ehdotus on merkityksellinen perustuslain 18 §:ssä turvatun elinkeinovapauden kannalta, jonka mukaan jokaisella on oikeus lain mukaan hankkia toimeentulonsa valitsemallaan työllä, ammatilla tai elinkeinolla.

Johdon toiminnan rajoittamista koskevia säännöksiä on säädetty perustuslakivaliokunnan myötävaikutuksella (PeVL 67/2002 vp, s.3, PeVL 28/2008 vp, s.2). Perustuslakivaliokunnan lausuntokäytännön nojalla toimintakiellon tulee olla laissa määritelty, sille tulee olla hyväksyttävä peruste ja sitä koskevan sääntelyn on oltava täsmällistä. (PeVL 16/2003 vp, s.3, PeVL 67/2002 vp, s.3, PeVL 52/2001 vp, s.3-4).

Johdon toiminnan rajoittamisesta säädettäisiin perustuslakivaliokunnan lausuntokäytännön mukaisesti lain tasolla, ehdotuksen 32 §:ssä. Perustuslakivaliokunta on edellyttänyt hyväksyttävää perustetta sellaiselta säännökseltä, joka rajoittaa johdon toimintaa. Perusteena on velvoittavan EU-säännöksen täytäntöönpano, millä tavoitellaan yhteiskunnan toiminnan kannalta keskeisten toimijoiden kyberturvallisuuden häiriönsietokyvyn parantumista. NIS2-direktiivi edellyttää toimijan johdon henkilökohtaista vastuuta kyberturvallisuuden riskienhallinta- ja raportointivelvoitteiden toteuttamisesta toimijassa sekä mahdollisuutta kieltää henkilön toiminta keskeisen toimijan johdossa, jos toimija ei huomautuksesta tai varoituksesta huolimatta kohtuullisessa määräajassa korjaa puutetta tai laiminlyöntiä sääntelyn noudattamisessa. Ehdotuksen mukaan, mikäli toimijan johto toimisi toistuvasti ja vakavasti laissa säädetyn velvollisuuden vastaisesti, voitaisiin johdon toimintaa rajoittaa. Rajoitus kohdistuisi luonnollisen henkilön toimintaan yksittäisen toimijan johdossa. Säännöksen tavoitteena olisi vahvistaa laissa asetettujen toimenpiteiden vaikuttavuutta ja varoittavuutta.

Perustuslakivaliokunta on lausunnoissaan korostanut perustuslainmukaisuutta vahvistavana seikkana sitä, että kieltomahdollisuuden piiriin on sisällytetty vain pieni määrä tehtäviä ja sitä, että sääntelyn kohderyhmä on pidetty suppeana (PeVL 52/2001 vp, s.4, PeVL 16/2003 vp, s.3). Säädösehdotuksessa johdon toiminnan rajoittamisen mahdollisuutta on rajattu siten, että se voi kohdistua vain toimijan ylimpään johtoon, eli esityksen 33 §:ssä määriteltyihin henkilöihin. Lisäksi kielto ei olisi yleinen kielto, vaan kohdistuisi vain luonnollisen henkilön toimintaan tietyn toimijan ylimmässä johdossa. Kielto ei rajoittaisi luonnollisen henkilön muuta elinkeinoharjoittamista tai mahdollisuutta toimia valitsemassaan ammatissa. Edellytyksenä olisi lisäksi keinon viimesijaisuus. Valvovan viranomaisen olisi ennen päätöksen tekemistä annettava keskeiselle toimijalle huomautus tai varoitus sekä varattava kohtuullinen määräika puutteen tai laiminlyönnin korjaamiseksi. Nämä edellytykset varmistavat tilanteen, jossa johdon toimintaa voitaisiin rajoittaa vain viimesijaisesti ja poikkeuksellisesti.

Kiellon vaikutuksia elinkeinovapauden rajoittamisen näkökulmasta lieventää myös se, että kiellon kohteena olevalla henkilöllä on mahdollisuus hakeutua muihin tehtäviin sekä samassa organisaatiossa, että muissa organisaatioissa. Kielto ei lisäksi tulisi koskemaan yksityisiä elinkeinonharjoittajia tai henkilöyhtiöitä, eli avoimia yhtiöitä tai kommandiittiyhtiöitä, joissa yksityinen elinkeinonharjoittaja tai henkilöyhtiön yhtiömiehet vastaavat yhtiön veloista henkilökohtaisesti Johdon toiminnan rajoittamisen mahdollisuuden rajaaminen vain tiettyihin säännöksessä

esitettyihin henkilöihin silloin kun kysymyksessä on vakava ja toistuva, 10 §:ssä säädetyn velvoitteen rikkominen tukee perustuslakivaliokunnan vaatimusta sääntelyn täsmällisyydestä, ja vahvistaa sääntelyn perustuslainmukaisuutta. Toimenpide voisi kohdistua vain keskeiseen toimijaan.

12.4 Hallinnollinen seuraamusmaksu

Kyberturvallisuuden riskienhallinnasta annettavan lain 5 luvussa säädettäisiin NIS2-direktiivin edellyttämällä tavalla hallinnollisen seuraamusmaksun määräämisestä toimijalle, joka tahallaan tai törkeästä huolimattomuudesta laiminlöisi laissa säädettyä riskienhallintavelvoitetta, ilmoitusvelvollisuutta merkittävistä poikkeamista tai laissa säädetyn ilmoituksen tekemisestä toimijaluetteloa varten. Kysymys olisi lainvastaisesta teosta määrättävästä sanktioluonteisesta hallinnollisesta seuraamuksesta, joka voisi olla määrällisesti huomattava.

Perustuslakivaliokunnan lausuntokäytännön mukaan hallinnollisen seuraamuksen yleisistä perusteista on säädettävä perustuslain 2 §:n 3 momentin edellyttämällä tavalla lailla Lisäksi kysymys on merkittävästä julkisen vallan käytöstä, jota voidaan osoittaa vain viranomaiselle. Laissa on täsmällisesti ja selkeästi säädettävä maksuvelvollisuuden ja maksun suuruuden perusteista sekä maksuvelvollisen oikeusturvasta samoin kuin lain täytäntöönpanon perusteista. Lisäksi valiokunta on katsonut, että vaikka perustuslain 8 §:n rikosoikeudellisen laillisuusperiaatteen täsmällisyysvaatimus ei sellaisenaan kohdistu hallinnollisten seuraamusten sääntelyyn, ei tarkkuuden yleistä vaatimusta kuitenkaan voida tällaisen sääntelyn yhteydessä sivuuttaa (PeVL 43/2013 vp, PeVL 14/2013 vp, PeVL 32/2012 vp ja siinä viitatut lausunnot).

Perustuslakivaliokunta on vakiintuneesti katsonut hallinnollisten seuraamusmaksujen olevan lainvastaisesta teosta määrättäviä sanktioluonteisia hallinnollisia seuraamuksia. Valiokunta on lausunnoissaan rinnastanut asiallisesti rangaistusluonteisen taloudellisen seuraamuksen rikosoikeudelliseen seuraamukseen (PeVL 17/2021 vp, s.6, PeVL 9/2012 vp, s.2). Hallinnollinen seuraamusmaksu on perustuslakivaliokunnan mukaan merkittävää julkisen vallan käyttöä (PeVL 34/2012 vp, s.3, PeVL 17/2012 vp, s.6, PeVL 9/2012 vp, s.2). Perustuslain 2.3 §:n mukaan julkisen vallan käytön tulee perustua lakiin. Perustuslain 124 §:n viimeisen virkkeen mukaan merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan antaa vain viranomaiselle. Seuraamusmaksun määräämistä koskevassa ehdotuksessa on otettu huomioon kuvattu perustuslakivaliokunnan lausuntokäytäntö. Laissa säädettäisiin täsmällisesti, tarkkarajaisesti ja tyhjentävästi teosta tai laiminlyönnistä, joka voisi olla toimijaan kohdistuvan seuraamusmaksun määräämisen perusteena.

Perustuslakivaliokunta on lausunut tietosuoja-asetusta koskevassa arvioinnissaan, että oikeusturvaintressi hallinnollisissa seuraamusmaksuissa on voimakkaasti korostunut, kun otetaan huomioon seuraamusmaksun sanktioluonne ja ankaruus. Perustuslakivaliokunta on edellyttänyt, että menettelyn asianmukaisuuden, riippumattomuuden ja puolueettomuuden varmistamiseksi perustuslain 21 §:n edellyttämällä tavalla, seuraamismaksun päättämisen tulee kuulua monijäsenisen elimen toimivaltaan, jotta ehdotus voidaan käsitellä tavallisen lain säätämisjärjestyksessä. Seuraamusmaksun määräämistä edeltävä asian selvittäminen ja muu valmistelu sekä esittely voitiin osoittaa tietosuojavaltuutetun tehtäväksi (PeVL 14/2018 vp).

Seuraamusmaksun määräämistä ehdotetaan monijäsenisen elimen tehtäväksi oikeusturvaan liittyvistä syistä. Seuraamusmaksun määräisi seuraamusmaksulautakunta, joka koostuisi valvovien viranomaisten nimeämistä jäsenistä. Liikenne- ja viestintävirasto nimeäisi lautakunnan puheenjohtajan ja varapuheenjohtajan. Lautakunta muodostuisi kunkin valvovan viranomaisen siihen määräämästä jäsenestä ja tämän henkilökohtaisesta varajäsenestä. Seuraamusmaksun määräämistä koskevan asian selvittämisestä vastaisi se valvova viranomainen, jonka valvontatoimialaa

koskevasta asiasta olisi kyse ja asian esittelisi tämän valvovan viranomaisen nimeämä jäsen. Laissa olisi lisäksi säännöksiä lautakunnan perehtyneisyyttä, asiantuntemusta, riippumattomuutta ja puolueettomuutta koskien.

Perustuslakivaliokunnan mukaan hallintoviranomaisen toiminnassa on asian käsittelyssä noudatettava perustuslain 21 §:n 2 momentin mukaisia hyvän hallinnon takeita, joita momentin mukaan ovat muun muassa käsittelyn julkisuus, oikeus tulla kuulluksi ja saada perusteltu päätös sekä oikeus hakea muutosta. Perustuslain mukaiset hyvän hallinnon takeet turvataan lailla. Vaikka perustuslain 8 §:n rikosoikeudellisen laillisuusperiaatteen täsmällisyysvaatimus ei sellaisenaan kohdistu hallinnollisten seuraamusten sääntelyyn, ei tarkkuuden yleistä vaatimusta kuitenkaan voida tällaisen sääntelyn yhteydessä sivuuttaa (PeVL 34/2012 vp, s.3-4, PeVL 17/2012 vp, s.6, PeVL 9/2012 vp, s.2).

Perustuslakivaliokunta on lausuntokäytännössään pitänyt ongelmallisena sitä, että asia voitaisiin yksittäistapauksessa ratkaista ilman esittelyä (PeVL 14/2018 vp, s.19). Seuraamuslautakunta tekisi aina päätöksensä esittelystä. Perustuslakivaliokunnan mukaan laissa on täsmällisesti ja selkeästi säädettävä maksuvelvollisuuden ja maksun suuruuden perusteista sekä maksuvelvollisen oikeusturvasta samoin kuin lain täytäntöönpanon perusteista (PeVL 14/2013 vp, s.2, PeVL 34/2012 vp, s.3, PeVL 17/2012 vp, s.6). Ehdotuksessa arvioidaan näistä seikoista säädettäväksi riittävällä tasolla.

Koska seuraamusmaksut ovat määrältään huomattavia, on erityistä huomiota perustuslakivaliokunnan mukaan kiinnitettävä oikeusturvalle asetettaviin vaatimuksiin (PeVL 14/2018 vp, s.18). Seuraamusmaksun määrä perustuisi 34 §:n mukaan kokonaisarviointiin, jossa olisi huomioitava pykälässä säädetyt seikat. Maksun enimmäismäärä on määritelty esityksen 35 §:ssä. Seuraamusmaksua koskevaan päätökseen haettaisiin muutosta valittamalla oikeudenkäynnistä hallintoasioissa säädetyssä järjestyksessä. Seuraamusmaksua koskeva päätös olisi täytäntöönpanokelpoinen vasta lainvoimaisena, minkä on arvioitu turvaavan oikeusturvajärjestelyiden asianmukaisuutta (PeVL 4/2004 vp, s.7-8). Perustuslakivaliokunta on lisäksi käytännössään edellyttänyt, että viranomaisen harkinnan sanktion määräämättä jättämisestä tulee olla sidottua harkintaa siten, että seuraamusmaksu on jätettävä määräämättä laissa säädettyjen edellytysten täyttyessä (PeVL 49/2017 vp, s.5-6, PeVL 39/2017 vp, s.4). Tämä on huomioitu ehdotuksen 37 §:ssä, jonka tarkoituksena on säädöskohtaisten perustelujen mukaan varmistaa, että seuraamusmaksua ei määrättäisi niissä tilanteissa, joissa se olisi kohtuutonta joko 1 momentin 1 tai 2 kohdassa tarkoitettujen seikkojen perusteella tai muutoin jonkin vastaavan seikan tai seikkojen perusteella ilmeisen kohtuutonta.

Ne bis in dem –periaatteen mukaan ketään ei saa saman valtion tuomiovallan nojalla tutkia uudelleen tai rangaista oikeudenkäynnissä rikoksesta, josta hänet on jo lopullisesti vapautettu tai tuomittu syylliseksi kyseisen valtion lakien ja oikeudenkäyntimenettelyn mukaisesti (PeVL 9/2012 vp, s.3, PeVL 14/2013 vp, s.2). Kiellon soveltamisala ulottuu Euroopan ihmisoikeustuomioistuimen ratkaisukäytännössä myös rangaistusluonteisiin hallinnollisiin seuraamuksiin (PeVL 9/2012 vp, s.3) Ehdotuksessa hallituksen esitykseksi periaate on huomioitu 37 §:n 3 momentissa, jonka mukaan seuraamusmaksua ei saa määrätä sille, jota epäillään samasta teosta esitutkinnassa, syyte-harkinnassa tai tuomioistuimessa vireillä olevassa rikosasiassa. Seuraamusmaksua ei saa määrätä myöskään sille, jolle on samasta teosta annettu lainvoimainen tuomio. Seuraamusmaksua ei saisi myöskään määrätä sille, jolle on samasta teosta määrätty yleisen tietosuoja-asetuksen nojalla seuraamusmaksu.

Hallinnollista seuraamusmaksua koskevan ehdotuksen arvioidaan vastaavan edellä kuvattuja perustuslain reunaehtoja.

12.5 Lainsäädäntövallan siirtäminen

Valtioneuvoston asetus soveltamisalaan kuuluvien toimijoiden määrittämisestä.

Kyberturvallisuuden riskienhallinnasta annetun lain 3 §;n 2 momenttiin sisältyy ehdotus, jonka nojalla valtioneuvoston asetuksella voitaisiin säätää lain soveltamisesta liitteessä I tai II tarkoitettua toimintaa harjoittavaan tai toimijatyyppiä olevaan toimijaan koosta riippumatta, jos toimijaa koskisi 2 momentissa säädetty kriteeri.

Perustuslain 80 §:n 1 momentin nojalla tasavallan presidentti, valtioneuvosto ja ministeriö voivat antaa asetuksia tässä perustuslaissa tai muussa laissa säädetyn valtuuden nojalla. Lailla on kuitenkin säädettävä yksilön oikeuksien ja velvollisuuksien perusteista sekä asioista, jotka perustuslain mukaan muuten kuuluvat lain alaan.

Lainsäädäntövallan siirto olisi lakiteknisesti tarpeen, sillä kysymys olisi yksityiskohtaisesta toimijoiden tai toimijatyypin määrittämisestä, joka toiminnan erityisen laadun vuoksi kuuluisi poikkeuksellisesti lain soveltamisalaan toimijan koosta riippumatta. Lisäksi kriteerien laatu huomioon ottaen olisi todennäköistä, että toimijoissa tapahtuisi muutoksia toiminnan laadun tai laajuuden muuttuessa.

Valtioneuvoston asetuksella voitaisiin säätää vain toimijan kuulumisesta lain soveltamisalaan koosta riippumatta, eikä asetuksella voitaisi säätää lain osittaisesta soveltamisesta tai laissa säädettyjen oikeuksien ja velvollisuuksien sisällöstä. Asetuksella voitaisiin ulottaa soveltaminen koosta riippumatta vain lain liitteessä määritellylle toimijalle tai toimijatyypille. Asetuksella ei voitaisi ulottaa soveltamista uudelle toimialalle tai toimijatyypille, joka ei muutoin kuuluisi lain soveltamisalaan. Lisäksi laissa säädettäisiin NIS2-direktiivin velvoittavaa soveltamisalaa vastaavasti poikkeuskriteereistä, joiden täyttäminen olisi edellytyksenä sille, että toimija voitaisiin saattaa lain soveltamisalaan. Näistä syistä on arvioitu, että ehdotus vastaa perustuslain 80 §:n 1 momentin edellytyksiä asetuksenantovaltuudelle siten, että lailla säädetään yksilön oikeuksien ja velvollisuuksien perusteista, ja yksityiskohtainen ja teknisluontoinen poikkeuksellisesti koosta riippumatta sovellettavien toimijoiden määrittely voitaisiin jättää asetuksen tasolle.

Määräyksenantovaltuudet

Perustuslain 80 §:n 2 momentin mukaan viranomainen voidaan lailla valtuuttaa antamaan oikeussääntöjä määrätyistä asioista, jos siihen on sääntelyn kohteeseen liittyviä erityisiä syitä eikä sääntelyn asiallinen merkitys edellytä, että asiasta säädetään lailla tai asetuksella. Lisäksi valtuutuksen tulee perustuslain mukaan olla soveltamisalaltaan täsmällisesti rajattu. Erityinen syy säätää viranomaisen määräystenantovallasta on muun muassa tekninen ja vähäisiä yksityiskohtia koskeva sääntely (PeVL 52/2001 vp, PeVL 46/2001 vp), joka ei sisällä merkittävää harkintavallan käyttöä (PeVL 43/2000 vp). Määräyksenantovaltuuden kattamat asiat tulee määritellä tarkasti laissa, ja sen soveltamisalan tulee olla täsmällisesti rajattu (HE 1/1998 vp).

Kyberturvallisuuden riskienhallinnasta annettava laki sisältäisi ehdotuksia, joilla valvova viranomainen valtuutettaisiin antamaan tarkempia teknisiä määräyksiä kyberturvallisuuden riskienhallinnasta 9 §:n 4 momentin nojalla. Esityksen 9 §:n 4 momentin 1-6 kohdissa on yksilöity laissa säädettyyn riskienhallintavelvollisuuteen liittyvät seikat, joista määräyksen voisi antaa. Lisäksi määräyksenantovaltuus valvovalle viranomaiselle sisältyisi kyberturvallisuuden riskienhallinnasta ehdotetun lain 11 §:n 3 momentin, jonka mukaan valvovalla viranomaisella on toimialallaan mahdollisuus antaa tarkempia teknisiä määräyksiä momentin 1-3 kohdissa yksilöidyistä asioista laissa säädettyyn poikkeamaraportointiin liittyvistä teknisistä seikoista. Kol-

mas valvovalle viranomaiselle kohdennettu määräyksenantovaltuus sisältyy kyberturvallisuuden riskienhallinnasta ehdotetun lain 39 §:n 3 momenttiin, jonka mukaan valvova viranomainen voisi antaa tarkempia määräyksiä toimijaluettelon tietojen ilmoittamisesta. Ehdotukset ovat merkityksellisiä perustuslain 80 § 2 momentin kannalta, jonka mukaan viranomainen voidaan lailla valtuuttaa antamaan oikeussääntöjä määrätyistä asioista, jos siihen on sääntelyn kohteeseen liittyviä erityisiä syitä eikä sääntelyn asiallinen merkitys edellytä, että asiasta säädetään lailla tai asetuksella. Tällaisen valtuutuksen tulee olla soveltamisalaltaan täsmällisesti rajattu.

Perustuslain 80 §:n 2 momentin mukaan viranomainen voidaan lailla valtuuttaa antamaan oikeussääntöjä *määrätyistä asioista*. Valtuutuksen tulee lisäksi olla *soveltamisalaltaan täsmällisesti rajattu*. Perustuslain esitöiden (HE 1/1998 vp, s.133) mukaan edellytys valtuuttaa viranomainen antamaan määräyksiä määrätyistä asioista on yleistä tarkkarajaisuutta pidemmälle menevä vaatimus (myös PeVL 24/2002 vp, s.3). Ehdotuksessa perustuslain vaatimus on huomioitu 9 §:n 4 momentissa ja 11 §:n 3 momentissa yksilöimällä ja listaamalla ne tekniset määräykset, joista viranomainen voi pykälän nojalla antaa tarkempia määräyksiä. Ehdotuksen 43 §:ssä määräyksenantovaltuus on sidottu valtuuteen tarkentaa tietojen ilmoittamista, joka on luonteeltaan tekninen ja tarkkarajainen seikka. Määräyksenantovaltuudet olisivat luonteeltaan teknistä sääntelyä eikä niillä voitaisi antaa yleisiä oikeussääntöjä asioista, joista on niiden merkityksen vuoksi säädettävä lailla tai asetuksella. Perustuslakivaliokunta on lausunnossaan pitänyt Viestintävirastoa sellaisena viranomaisena, jolle määräyksenantovaltaa on mahdollista antaa (mm. PeVL 9/2004 vp, s. 8).

Perustusvaliokunnan mietinnön (PeVM 10/1998 vp, s.23/II) muulle viranomaiselle voidaan osoittaa oikeussääntöjen antamisvaltaa vain poikkeuksellisesti. Perustuslain esitöissä (HE 1/1998 vp, s.133/II) tunnistetaan tarve mahdollistaa muu viranomainen antamaan oikeussääntöjä joistakin sääntelyn kokonaisuuden kannalta vähäisistä yksityiskohdista. Perustuslain 80 §:n 2 momentti edellyttää määräyksenantovaltuuteen liittyvän *erityisiä syitä*. Erityinen syy olisi hallituksen esityksen (HE 1/1998 vp, s.133/II) mukaan käsillä lähinnä silloin, kun kysymyksessä on tekninen ja vähäisiä yksityiskohtia koskeva sääntely, johon ei liity merkittävää harkintavallan käyttöä. Perustuslakivaliokunta on lisäksi pitänyt säädeltävän toiminnan ammatillisia erityispiirteitä perustuslain 80 §:n 2 momentin mukaisina erityisinä syinä (PeVL 17/2004 vp, s.3, PeVL 16/2003 vp, s.3, PeVL 24/2002, s.3). Perustuslakivaliokunta ei ole pitänyt viranomaiselle kohdistettua valtuutta järjestää teknisluonteiset yksityiskohdat perustuslain kannalta ongelmallisena (PeVL 17/2004 vp, s.4, PeVL 16/2003 vp, s.3). Ehdotuksessa viranomaiselle esitetyt määräyksenantovaltuudet ovat luonteeltaan teknisiä. Tämä käy ilmi ehdotuksen 9 §:n 4 momentin, 11 §:n 3 momentin ja 43 § 3 momentin sanamuodoista, joiden mukaan valvova viranomainen voi toimialallaan antaa tarkempia *teknisiä* määräyksiä. Ehdotuksien katostaan olevan edellä kuvattujen reunaehtojen mukaisia.

Määräyksenantovaltuuksilla on tarkoitus antaa viranomaiselle mahdollisuus tarkentaa lain soveltamista antamalla teknisiä määräyksiä säädetyistä seikoista. Määräyksenantovaltuudet ovat tarkkarajaisia ja ne koskevat sääntelyn kokonaisuuden kannalta vähäisiä yksityiskohtia. Lisäksi määräyksenantovaltuus teknisistä seikoista mahdollistaa sektorikohtaisten erityispiirteiden huomioimista sekä sääntelyn yhteensovittamista komission NIS2-direktiivin 21 tai 24 artiklan nojalla antamiin täytäntöönpanosäädöksiin tai delegoituihin asetuksiin. Käsillä ovat perustuslain 80 §:n 2 momentissa tarkoitetut erityiset syyt. Ehdotettujen määräyksenantovaltuuksien katsotaan olevan perustuslain 80 §:n 2 momentin mukaisia.

Esityksen edellä kuvatut ehdotukset ovat täsmällisiä, tarkkarajaisia, ja perustellussa suhteessa niiden tarkoitukseen ja suojeltavaksi pyrittäviin oikeushyviin nähden. Ehdotuksilla ei puututa

perustuslaissa turvattujen oikeuksien ydinalueelle. Ehdotettu sääntely on rajattu siihen laajuuteen, jota NIS2-direktiivin täytäntöönpanon vähimmäistaso edellyttää ja jonka on katsottava olevan sen taustalla olevien tavoitteiden toteutumisen kannalta välttämätöntä ja oikeasuhtaista.

Edellä mainituilla perusteilla arvioidaan, että lakiehdotukset voidaan käsitellä tavallisessa lainsäätämisjärjestyksessä. Haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelyä koskevan ehdotuksen johdosta esityksestä olisi kuitenkin tarpeen pyytää perustuslakivaliokunnan lausunto

Ponsi

Koska kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 direktiivissä on säännöksiä, jotka ehdotetaan pantaviksi täytäntöön lailla, annetaan eduskunnan hyväksyttäviksi seuraavat lakiehdotukset:

1.

Laki

kyberturvallisuuden riskienhallinnasta

Eduskunnan päätöksen mukaisesti säädetään:

1 luku

Yleiset säännökset

1 §

Soveltamisala

Tässä laissa säädetään eräiden yhteiskunnan toiminnan kannalta kriittisten toimijoiden (*toimijat*) kyberturvallisuuden riskienhallinta- ja raportointivelvoitteista sekä tietoturvaloukkauksiin reagoivasta ja niitä tutkivasta yksiköstä (*CSIRT-yksikkö*) ja viranomaisten yhteistyöstä kyberturvallisuuspoikkeamien ja –riskien hallitsemiseksi.

Tällä lailla pannaan täytäntöön toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 (*NIS 2 -direktiivi*).

2 §

Määritelmät

Tässä laissa tarkoitetaan:

1) *aluetunnusrekisterillä* toimijaa, jolle on myönnetty oikeus hallinnoida tiettyä aluetunnusta ja joka kyseistä aluetunnusta hallinnoidessaan vastaa muun muassa verkkotunnusten rekisteröinnistä kyseisen aluetunnuksen alle sekä kyseisen aluetunnuksen teknisestä toiminnasta, myös siihen liittyvien nimipalvelinten toiminnasta, sen tietokantojen ylläpidosta ja aluetunnuksen vyöhyketiedostojen jakelusta nimipalvelimille, riippumatta siitä, suorittaako toimija kyseiset toiminnot itse vai ulkoistaako se ne, ja lukuun ottamatta tilanteita, joissa rekisteri käyttää aluetunnuksia vain omiin tarkoituksiinsa;
2) *CER-direktiivillä* kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta annettua Euroopan parlamentin ja neuvoston direktiiviä (EU) 2022/2557;
3) *datakeskuspalvelulla* palvelua, joka käsittää rakenteita tai rakenteiden ryhmiä, jotka on tarkoitettu datan tallennus-, käsittely- ja siirtopalveluja tarjoavien tietoteknisten ja verkkolaitteiden keskitettyyn ylläpitoon, yhteenliittämiseen ja ohjaukseen yhdessä kaikkien tarvittavien sähkönjakeluun ja toimintaolosuhteiden säätelyyn tarkoitettujen laitteiden ja infrastruktuurien kanssa;
4) *DNS-palveluntarjoajalla* toimijaa, joka tarjoaa
   a) yleisesti saatavilla olevia rekursiivisia verkkotunnusten selvityspalveluja internetin loppukäyttäjille; tai
   b) auktoritatiivisia verkkotunnusten selvityspalveluja kolmansille osapuolille, lukuun ottamatta juurinimipalvelimia;

5) *DORA-asetuksella* finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU) N:o 600/2014, (EU) N:o 909/2014 ja (EU) 2016/1011 muuttamisesta annettua Euroopan parlamentin ja neuvoston asetusta (EU) 2022/2554;
6) *eIDAS-asetuksella* sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta annettua Euroopan parlamentin ja neuvoston asetusta (EU) N:o 910/2014;
7) *haavoittuvuudella* tieto- ja viestintätekniikan tuotteiden tai -palvelujen heikkoutta, alttiutta tai vikaa, jota kyberuhka voi hyödyntää;
8) *hallintapalvelun tarjoajalla* toimijaa, joka tarjoaa TVT-tuotteiden, verkkojen, infrastruktuurin, sovellusten tai muiden viestintäverkkojen ja tietojärjestelmien asentamiseen, hallintaan, käyttöön tai ylläpitoon liittyviä palveluja joko asiakkaan tiloissa tai etäyhteyden välityksellä toteutettavan tuen tai aktiivisen ylläpidon muodossa;
9) *hyväksytyllä luottamuspalvelun tarjoajalla* eIDAS-asetuksen 3 artiklan 20 alakohdassa määriteltyä hyväksyttyä luottamuspalvelun tarjoajaa;
10) *keskisuurella toimijalla* julkista tai yksityistä toimijaa, joka täyttää komission suosituksen 2003/361/EY liitteessä olevan 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset ja jotka tarjoavat palvelujaan tai harjoittavat toimintaansa unionissa. Suosituksen liitteessä olevan 3 artiklan 4 kohtaa ei sovelleta keskisuuren toimijan määrittelyssä;
11) *kyberturvallisuudella* toimia, joita tarvitaan viestintäverkkojen ja tietojärjestelmien, niiden käyttäjien ja muiden asianosaisten henkilöiden suojaamiseksi kyberuhilta;
12) *kyberuhkalla* potentiaalista tilannetta, tapahtumaa tai toimintaa, joka voi vahingoittaa tai häiritä viestintäverkkoja ja tietojärjestelmiä, tällaisten järjestelmien käyttäjiä ja muita henkilöitä tai muulla tavoin vaikuttaa näihin haitallisesti;
13) *luottamuspalvelun tarjoajalla* eIDAS-asetuksen 3 artiklan 19 alakohdassa määriteltyä luottamuspalvelun tarjoajaa;
14) *läheltä piti -tilanteella* tapahtumaa, joka olisi voinut vaarantaa viestintäverkoissa ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden mutta jonka toteutuminen onnistuttiin estämään tai joka ei toteutunut satunnaisesta syystä;
15) *pilvipalvelulla* digitaalista palvelua, joka tarjoaa laajaan etäkäyttöön skaalattavan ja joustavan joukon jaettavissa olevia ja tarveperusteisesti ohjattavia tietoteknisiä resursseja, myös sijainniltaan hajautettuja resursseja;
16) *poikkeamalla* tapahtumaa, joka vaarantaa viestintäverkoissa ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden;
17) *poikkeaman käsittelyllä* mitä tahansa toimia ja menettelyjä, joilla pyritään ehkäisemään ja havaitsemaan poikkeama, analysoimaan, rajoittamaan tai hallitsemaan sitä ja palautumaan siitä;
18) *riskillä* poikkeaman aiheuttamien menetysten tai häiriön mahdollisuutta, joka ilmaistaan tällaisten menetysten tai häiriön suuruuden ja kyseisen poikkeaman toteutumisen todennäköisyyden yhdistelmänä;
19) *sisällönjakeluverkolla* maantieteellisesti hajautettujen palvelimien verkkoa, jonka tarkoituksena on varmistaa digitaalisen sisällön ja digitaalisten palvelujen hyvä saatavuus, käytettävyys ja nopea jakelu internetin käyttäjille sisällön ja palvelujen tarjoajien puolesta;
20) *teledirektiivillä* eurooppalaisesta sähköisen viestinnän säännöstöstä annettua Euroopan parlamentin ja neuvoston direktiiviä (EU) 2018/1972;
21) *tietoturvapalveluntarjoajalla* hallintapalvelun tarjoajaa, joka toteuttaa kyberturvallisuusriskien hallintatoimia tai antaa tukea niitä varten;

22) *TVT-palvelulla* Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 2 artiklan 13 alakohdassa määriteltyä tieto- ja viestintätekniikan palvelua;
23) *TVT-tuotteella* Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 2 artiklan 12 alakohdassa määriteltyä tieto- ja viestintätekniikan tuotetta;
24) *valvovalla viranomaisella* jäljempänä 26 §:n nojalla toimivaltaista valvovaa viranomaista;
25) *verkkoyhteisöalustalla* alustaa, jonka avulla loppukäyttäjät voivat olla yhteydessä toisiinsa, jakaa sisältöä, hakea tietoa ja viestiä keskenään monenlaisilla päätelaitteilla, erityisesti pikaviestikeskustelujen, julkaisujen, videoiden ja suositusten muodossa;
26) *verkossa toimivalla hakukoneella* oikeudenmukaisuuden ja avoimuuden edistämisestä verkossa toimivien välityspalvelujen yrityskäyttäjiä varten annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/1150 2 artiklan 5 alakohdassa tarkoitettua verkossa toimivaa hakukonetta;
27) *verkossa toimivalla markkinapaikalla* kuluttajansuojalain (38/1978) 6 luvun 8 §:n 4 kohdassa tarkoitettua verkossa toimivaa markkinapaikkaa;
28) *viestintäverkolla ja tietojärjestelmällä*
a) teledirektiivin 2 artiklan 1 alakohdassa määriteltyä sähköistä viestintäverkkoa;
b) laitetta taikka yhteen kytkettyjen tai toisiinsa yhteydessä olevien laitteiden ryhmää, joista yksi tai useampi suorittaa ohjelman avulla digitaalisten tietojen automaattista käsittelyä; tai
c) digitaalisia tietoja, joita a ja b alakohdassa tarkoitetuissa järjestelmissä säilytetään, käsitellään, haetaan tai siirretään näiden järjestelmien toimintaa, käyttöä, suojausta tai yllä pitoa varten;
29) *viestintäverkon ja tietojärjestelmän turvallisuudella* viestintäverkon ja tietojärjestelmien kykyä suojautua tietyllä varmuudella tapahtumilta, jotka saattavat vaarantaa kyseisissä viestintäverkoissa ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden;
30) *yleisellä tietosuoja-asetuksella* luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annetun Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679;
31) *yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajalla* sitä, joka tarjoaa sähköisen viestinnän palveluista annetun lain 3 §:n 1 momentin 37 kohdassa tarkoitettua viestintäpalvelua ennalta rajaamattomalle käyttäjäpiirille;
32) *yleisten sähköisten viestintäverkkojen tarjoajalla* sitä, joka tarjoaa sähköisen viestinnän palveluista annetun lain (917/2014) 3 §:n 1 momentin 34 kohdassa tarkoitettua verkkopalvelua;

3 §

Toimijat

Tämän lain soveltamisalaan kuuluvalla toimijalla tarkoitetaan oikeushenkilöä tai luonnollista henkilöä, joka harjoittaa liitteessä I tai II tarkoitettua toimintaa tai on liitteessä I tai II tarkoitettua toimijatyyppiä ja täyttää tai ylittää keskisuuren toimijan määritelmän.

Lisäksi toimijalla tarkoitetaan koosta riippumatta oikeushenkilöä tai luonnollista henkilöä, joka on:

a. yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoaja;
b. luottamuspalvelun tarjoaja;
c. aluetunnusrekisteri;
d. DNS-palveluntarjoaja; tai
e. CER-direktiivin nojalla määritelty kriittinen toimija.

Valtioneuvoston asetuksella säädetään tämän lain soveltamisesta sellaiseen liitteessä I tai II tarkoitettua toimintaa harjoittavaan tai toimijatyyppiä olevaan toimijaan sen koosta riippumatta, jos

1) toimija tarjoaa ainoana palvelua, joka on yhteiskunnan tai talouden kriittisten toimintojen ylläpitämisen kannalta keskeinen;
2) häiriö toimijan tarjoamassa palvelussa vaikuttaisi merkittävästi yleiseen järjestykseen, yleiseen turvallisuuteen tai kansanterveyteen;
3) häiriö toimijan tarjoamassa palvelussa voisi aiheuttaa merkittävän systeemisen riskin erityisesti aloilla, joilla tällaisella häiriöllä voisi olla rajat ylittäviä vaikutuksia; tai
4) toimija on kriittinen, koska sillä on erityisen suuri merkitys kansallisella tai alueellisella tasolla kyseisen toimialan tai palvelutyypin tai jäsenvaltion muiden keskinäisriippuvaisten toimialojen kannalta.

4 §

Soveltamisalan rajaukset

Tätä lain 2 lukua ei sovelleta toimintaan tai palveluihin, joita tarjotaan maanpuolustuksen, kansallisen turvallisuuden, yleisen järjestyksen ja turvallisuuden taikka rikosten ennalta estämisen, rikostutkinnan ja syytetoimien toteuttamiseksi.

Tätä lakia ei sovelleta toimijaan, joka tarjoaa ainoastaan 1 momentissa tarkoitettua toimintaa tai palvelua.

Edellä 1 ja 2 momenttia ei sovelleta, jos toimija on luottamuspalvelun tarjoaja.

Tätä lakia ei sovelleta toimijaan, johon DORA-asetusta ei sovelleta sen 2 artiklan 4 kohdan nojalla.

Tässä laissa ei velvoiteta sellaisen tiedon antamiseen, jonka luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin siihen liittyvää tärkeää etua.

5 §

Suhde muuhun lainsäädäntöön

Jos muussa laissa on tästä laista poikkeavia säännöksiä, joilla varmistetaan korkeampi kyberturvallisuuden taso, niitä sovelletaan tämän lain lisäksi.

Jos Euroopan unionin asetuksessa tai NIS2-direktiivin nojalla säädetyssä komission asetuksessa edellytetään toimialakohtaisesti, että toimija ottaa käyttöön kyberturvallisuusriskien hallintatoimenpiteitä tai ilmoittaa merkittävistä poikkeamista, ja vaatimukset ovat vaikutuksiltaan vähintään tässä laissa säädettyjä vastaavia velvoitteita vastaavia, toimijaan ei sovelleta näiden velvoitteiden tai niiden valvonnan osalta tämän lain 2, 4 ja 5 lukua eikä 43 §:ää.

Henkilötietojen käsittelyn tietoturvallisuudesta säädetään yleisessä tietosuoja-asetuksessa ja tietosuojalaissa (1050/2018).

6 §

Lainkäyttövalta ja alueellisuus

Tätä lakia sovelletaan toimijaan, joka on sijoittautunut Suomeen, jollei laissa toisin säädetä tai Euroopan unionin asetuksesta tai Suomea sitovasta kansainvälisestä velvoitteesta muuta johdu.

Riippumatta valtiosta, johon toimija on sijoittautunut, yleisen sähköisen viestintäverkon tarjoaja ja yleisesti saatavilla olevan sähköisen viestintäpalvelun tarjoaja kuuluu sen jäsenvaltion lainkäyttövallan piiriin, jossa se tarjoaa palvelujaan.

DNS-palveluntarjoaja, aluetunnusrekisteri, pilvipalvelujen tarjoaja, datakeskuspalvelujen tarjoaja, sisällönjakeluverkkojen tarjoaja, hallintapalvelun tarjoaja, tietoturvapalveluntarjoaja sekä verkossa toimivien markkinapaikkojen tarjoaja, verkossa toimivien hakukoneiden tarjoaja ja verkkoyhteisöalustojen tarjoaja kuuluu tässä laissa tarkoitettujen velvoitteiden osalta sen jäsenvaltion lainkäyttövallan piiriin, jossa sijaitsee sen NIS2-direktiivin 26 artiklan 2 kohdassa tarkoitettu päätoimipaikka tai sen NIS2-direktiivin 26 artiklan 3 kohdassa tarkoitettu Euroopan unioniin nimetty edustaja. Tällaisen toimijan, joka ei ole sijoittautunut Euroopan unioniin, mutta joka tarjoaa palvelujaan Euroopan unionin alueella, on nimettävä NIS2-direktiivin 26 artiklan 3 kohdassa tarkoitettu edustaja Euroopan unionin aluetta varten. Jos toimija ei ole sijoittautunut Euroopan unioniin tai asettanut NIS2-direktiivin 26 artiklan 3 kohdassa tarkoitettua nimettyä edustajaa Euroopan unionissa ja toimija tarjoaa palveluita Suomessa, toimija kuuluu tämän lain soveltamisalaan.

Valvova viranomainen voi suorittaa toiseen Euroopan unionin jäsenvaltioon sijoittautuneeseen toimijaan kohdistuvia valvonta- tai täytäntöönpanotoimia siten kuin tässä laissa säädetään, jos toisen jäsenvaltion toimivaltainen viranomainen sitä pyytää ja toimija tarjoaa palveluja Suomessa tai sillä on viestintäverkko tai tietojärjestelmä Suomen alueella. Edellytyksenä on lisäksi, että valvovalla viranomaisella olisi oikeus suorittaa vastaava valvonta- tai täytäntöönpanotoimi tämän lain nojalla, jos toimija olisi sijoittautunut Suomeen.

2 luku

Kyberturvallisuuden riskienhallintavelvoite ja poikkeamista ilmoittaminen

7 §

Kyberturvallisuuden riskienhallintavelvoite

Toimijan on tunnistettava, arvioitava ja hallittava riskejä, joita kohdistuu sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Kyberturvallisuuden riskienhallinnalla tulee estää tai minimoida poikkeamien vaikutus toimintaan, toiminnan jatkuvuuteen, palvelujen vastaanottajiin ja muihin palveluihin.

Toimijan on toteutettava turvallisuus- ja riskienhallintatoimenpiteet, jotka ovat ajantasaisia, oikeasuhtaisia ja riittäviä suhteessa toiminnassa käytettäville viestintäverkoille ja tietojärjestelmille aiheutuviin riskeihin sekä viestintäverkon tai tietojärjestelmän merkitykseen toimijan toiminnan ja palveluntarjonnan kannalta.

8 §

Kyberturvallisuuden riskienhallinnan toimintamalli

Toimijalla on oltava käytössä ajantasainen kyberturvallisuuden riskienhallinnan toimintamalli viestintäverkkojen ja tietojärjestelmien ja niiden fyysisen ympäristön suojaamiseksi poikkeamilta ja niiden vaikutuksilta.

Kyberturvallisuuden riskienhallinnan toimintamallissa on tunnistettava viestintäverkkoihin ja tietojärjestelmiin ja niiden fyysiseen ympäristöön kohdistuvat riskit kaikki vaaratekijät huomioivan lähestymistavan mukaisesti. Kyberturvallisuuden riskienhallinnan toimintamallissa on määritettävä ja kuvattava toimenpiteet, joilla viestintäverkkoja ja tietojärjestelmiä ja niiden fyysistä ympäristöä suojataan riskeiltä ja poikkeamilta (jäljempänä *hallintatoimenpiteet*).

9 §

Kyberturvallisuuden riskienhallinnan toimenpiteet

Toimijoiden on toteutettava kyberturvallisuuden riskienhallinnan toimintamallin mukaiset oikeasuhtaiset tekniset, operatiiviset tai organisatoriset hallintatoimenpiteet viestintäverkkojen ja tietojärjestelmien turvallisuudelle kohdistuvien riskien hallitsemiseksi ja haitallisten vaikutusten estämiseksi tai minimoimiseksi.

Kyberturvallisuuden riskienhallinnan toimintamallissa ja siihen perustuvissa hallintatoimenpiteissä on huomioitava ja ylläpidettävä ajantasaisena vähintään:

1) kyberturvallisuuden riskienhallinnan toimintaperiaatteet ja riskienhallinnan toimenpiteiden vaikuttavuuden arviointi;
2) viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet;
3) viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus sekä tarvittavat menettelyt haavoittuvuuksien käsittelyyn ja julkistamiseen;
4) toimitusketjun toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt;
5) omaisuudenhallinta ja turvallisuuden kannalta tärkeiden toimintojen tunnistaminen;
6) henkilöstöturvallisuus ja kyberturvallisuuskoulutus;
7) pääsynhallinnan ja todentamisen menettelyt;
8) salausmenetelmien käyttämistä koskevat toimintaperiaatteet ja menettelyt sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttöön;
9) poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi;
10) varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan jatkuvuuden hallinta ja tarvittaessa suojattujen varaviestintäjärjestelmien käyttö toimijan toiminnassa;
11) perustason kyberhygieniakäytännöt toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi; sekä
12) toimenpiteet viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön ja tilaturvallisuuden sekä välttämättömien resurssien varmistamiseksi.

Toimenpiteet on suhteutettava toiminnan laatuun ja laajuuteen, toimijan poikkeamasta kohtuudella ennakoitavissa oleviin välittömiin vaikutuksiin, toimijan viestintäverkkojen ja tietojärjestelmien riskialttiuteen, poikkeamien todennäköisyyteen ja vakavuuteen, toimenpiteistä aiheutuviin kustannuksiin sekä ajantasainen kehitys huomioiden käytettävissä oleviin teknisiin mahdollisuuksiin torjua uhka.

Valvova viranomainen voi toimialallaan antaa tarkempia teknisiä määräyksiä:

1) kyberturvallisuuden riskienhallinnan toimintamallissa huomioitavista osa-alueista ja riskienhallinnan ja viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden hallinnan menettelyistä;
2) kehittämisen ja ylläpidon sekä haavoittuvuuksien käsittelyn menettelyistä;
3) omaisuudenhallinnasta ja toimintojen tärkeysluokittelun perusteista;

4) henkilöstöturvallisuuden, kyberturvallisuuskoulutuksen, poikkeamien havainnoinnin ja hallinnan sekä jatkuvuuden hallinnasta;
5) pääsynhallinnan, todentamisen ja salauksen menetelmistä;
6) perustason kyberhygieniakäytännöistä, joilla varmistetaan viestintäverkko- ja tietojärjestelmäturvallisuuden perusluonteiset hallintatoimenpiteet;
7) viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön, tilaturvallisuuden ja välttämättömien resurssien hallintatoimenpiteistä.

Riskienhallinnan toimintamallissa ja hallintatoimenpiteissä on noudatettava lisäksi NIS 2 -direktiivin 21 artiklan 5 kohdan nojalla annettavia Euroopan komission täytäntöönpanosäädöksiä.

10 §

Johdon vastuu

Toimijan johto vastaa kyberturvallisuuden riskienhallinnan toteuttamisen ja valvonnan järjestämisestä sekä hyväksyy riskienhallinnan toimintamallin ja valvoo sen toteuttamista. Toimijan johdolla tulee olla riittävä perehtyneisyys kyberturvallisuuden riskienhallintaan.

Johdolla tarkoitetaan toimijan hallitusta, hallintoneuvostoa, toimitusjohtajaa, tai muussa niihin rinnastettavassa asemassa olevaa, sekä toimitusjohtajan välittömään alaisuuteen kuuluvissa tehtävissä, jotka ovat toimijan ylimpiä johtotehtäviä tai joissa tosiasiallisesti johdetaan sen toimintaa, toimivaa tahoa.

11 §

Poikkeamailmoitukset viranomaiselle

Toimijan on ilmoitettava viipymättä valvovalle viranomaiselle merkittävästä poikkeamasta. Merkittävällä poikkeamalla tarkoitetaan poikkeamaa, joka on aiheuttanut tai voi aiheuttaa palvelujen vakavan toimintahäiriön tai asianomaiselle toimijalle taloudellisia tappioita taikka poikkeama on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa.

Ensi-ilmoitus on tehtävä 24 tunnin kuluessa poikkeaman havaitsemisesta ja jatkoilmoitus 72 tunnin kuluessa poikkeaman havaitsemisesta.

Ensi-ilmoituksessa on ilmoitettava:
1) merkittävän poikkeaman havaitsemisesta;
2) epäilläänkö merkittävän poikkeaman johtuvan rikoksesta tai muusta lainvastaisesta tai vihamielisestä teosta; ja
3) rajat ylittävien vaikutuksien mahdollisuus ja todennäköisyys sekä rajat ylittävien vaikutuksien ennakointiin liittyvät tiedot.

Jatkoilmoituksessa on ilmoitettava:
1) arvio merkittävän poikkeaman laadusta, vakavuudesta ja vaikutuksista;
2) vaarantumisindikaattorit, jos sellaisia on saatavilla; ja
3) mahdolliset päivitykset ensi-ilmoituksen tietoihin.

Valvova viranomainen voi toimialallaan antaa tarkempia teknisiä määräyksiä:
1) siitä, milloin 1 momentissa tarkoitettu poikkeama on merkittävä;
2) 13 §:ssä tarkoitetussa loppuraportissa ilmoitettavista tiedoista; ja
3) merkittävien poikkeamien ja 12–13 §:n mukaisten tietojen ilmoittamismenettelystä.

Edellä 2 momentista poiketen luottamuspalvelun tarjoajan on tehtävä jatkoilmoitus 24 tunnin kuluessa merkittävän poikkeaman havaitsemisesta, jos merkittävä poikkeama vaikuttaa sen luottamuspalvelujen tarjontaan.

12 §

Poikkeaman väliraportti

Toimijan on annettava valvovan viranomaisen pyynnöstä lisätietoja tai väliraportti poikkeaman tilannepäivityksistä ja käsittelyn edistymisestä.

Jos poikkeama on pitkäkestoinen, toimijan on annettava väliraportti oma-aloitteisesti viimeistään kuukauden kuluttua jatkoilmoituksen antamisesta.

13 §

Poikkeaman loppuraportti

Toimijan on annettava valvovalle viranomaiselle loppuraportti kuukauden kuluessa jatkoilmoituksen toimittamisesta tai pitkäkestoisen poikkeaman kohdalla kuukauden kuluessa sen käsittelyn päättymisestä.

Loppuraportin on sisällettävä:

1) yksityiskohtainen kuvaus poikkeamasta, sen vakavuudesta ja vaikutuksista;
2) poikkeaman todennäköisesti aiheuttaneen uhkan tai juurisyyn tyyppi;
3) toteutetut ja meneillään olevat toimenpiteet vaikutusten lieventämiseksi; ja
4) mahdolliset rajat ylittävät vaikutukset.

14 §

Poikkeamasta ja kyberuhkasta ilmoittaminen muulle kuin viranomaiselle

Toimijan on ilmoitettava viipymättä merkittävästä poikkeamasta palvelujensa vastaanottajille, jos merkittävä poikkeama todennäköisesti haittaa toimijan palvelujen tarjoamista.

Toimijan on ilmoitettava viipymättä merkittävästä kyberuhkasta sekä kyberuhkan hallitsemiseksi käytettävissä olevista toimenpiteistä niille palvelujensa vastaanottajille, joihin merkittävä kyberuhka saattaa vaikuttaa.

Jos merkittävästä poikkeamasta ilmoittaminen on yleisen edun mukaista, valvova viranomainen voi velvoittaa toimijan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.

15 §

Vapaaehtoinen ilmoittaminen

Toimijat voivat tehdä vapaaehtoisesti ilmoituksia muista kuin edellä 11 §:ssä tarkoitetuista poikkeamista, kyberuhkista ja läheltä piti –tilanteista valvovalle viranomaiselle.

Valvovan viranomaisen on otettava vastaan toimialallaan vapaaehtoisia poikkeamailmoituksia merkittävistä poikkeamista, poikkeamista, kyberuhkista ja läheltä piti -tilanteista myös muilta kuin tässä laissa tarkoitetuilta toimijoilta.

Valvovan viranomaisen on toimitettava keskitetylle yhteyspisteelle tieto tämän pykälän nojalla tehdyistä ilmoituksista.

16 §

Poikkeamailmoituksen vastaanottaminen

Valvovan viranomaisen on vastattava poikkeamailmoituksen tehneelle taholle viivytyksettä. Vastauksessa on oltava alustava palaute merkittävästä poikkeamasta sekä ohjeet merkittävän poikkeaman ilmoittamisesta esitutkintaviranomaiselle, jos asiassa epäillään rikosta.

Valvova viranomainen voi asettaa etusijalle 11 §:ssä tarkoitettuihin ilmoituksiin vastaamisen ja niiden 17 §:n mukaisen käsittelyn vapaaehtoisiin ilmoituksiin nähden.

17 §

Poikkeamailmoitusten käsittely

Valvovan viranomaisen on toimitettava edellä 11 – 13 §:ssä ja 15 §:ssä tarkoitetut ilmoitukset ja raportit CSIRT-yksikölle. CSIRT-yksikkö antaa toimijan pyynnöstä ohjeita tai operatiivisia neuvoja vaikutuksia lieventävien toimenpiteiden osalta.

Valvovan viranomaisen on toimitettava [CER-direktiivin mukaiselle toimivaltaiselle viranomaisille] tietoa edellä 11 – 13 §:n sekä 15 §:n nojalla ilmoitetuista merkittävistä poikkeamista, poikkeamista, kyberuhkista ja läheltä piti –tilanteista, joista [CER-direktiivin nojalla määritellyt kriittiset toimijat] ovat ilmoittaneet.

Jos poikkeamasta on aiheutunut yleisen tietosuoja-asetuksen 33 artiklassa tarkoitettu henkilötietojen tietoturvaloukkaus, josta on ilmoitettava, valvovan viranomaisen on tiedotettava poikkeaman havaitsemisesta tietosuojavaltuutettua.

Jos merkittävällä poikkeamalla on vaikutuksia muihin EU-jäsenvaltioihin tai muihin toimialoihin, valvovan viranomaisen on tiedotettava merkittävästä poikkeamasta keskitettyä yhteyspistettä ja toimitettava sitä koskevat ilmoitukset, raportit ja muut tiedot keskitetylle yhteyspisteelle.

Jos poikkeama vaikuttaa toiseen jäsenvaltioon, keskitetyn yhteyspisteen on ilmoitettava siitä ilman aiheetonta viivytystä Euroopan unionin kyberturvallisuusvirasto ENISA:lle ja niille jäsenvaltioille, joihin poikkeama vaikuttaa. Keskitetyn yhteyspisteen on pyynnöstä toimitettava myös edellä 11-13 §:ssä tarkoitetut ilmoitukset ja raportit sen EU-jäsenvaltion keskitetylle yhteyspisteelle, johon poikkeama vaikuttaa. Keskitetty yhteyspiste saa luovuttaa tässä tarkoituksessa Euroopan unionin kyberturvallisuusvirasto ENISA:lle ja muiden jäsenvaltioiden keskitetyille yhteyspisteille tietoja merkittävästä poikkeamasta.

18 §

Keskitetty yhteyspiste

Liikenne- ja viestintäviraston Kyberturvallisuuskeskus toimii NIS2-direktiivin 8 artiklan 3 kohdassa tarkoitettuna keskitettynä yhteyspisteenä.

Keskitetyn yhteyspisteen tehtävänä on myös edistää valvovien viranomaisten välistä yhteistyötä ja koordinaatiota tämän lain mukaisten tehtävien toteuttamisessa.

Keskitetyn yhteyspisteen on toimitettava ENISA:lle kolmen kuukauden välein yhteenvetoraportti, joka sisältää anonymisoidut koontitiedot edellä 11 – 13 §:n sekä 15 §:n nojalla ilmoitetuista merkittävistä poikkeamista, poikkeamista, kyberuhkista ja läheltä piti –tilanteista.

3 luku

CSIRT-yksikkö

211

19 §

CSIRT-yksikkö

Liikenne- ja viestintävirastossa toimii CSIRT-yksikkö. CSIRT-yksikön on täytettävä NIS 2 –direktiivin 11 artiklan 1 kohdassa tarkoitetut vaatimukset ja sen toiminta on järjestettävä erilliseksi 25 §:n nojalla tehtävästä valvontatoiminnosta.

CSIRT-yksikön tehtävänä on:

1) seurata ja analysoida kyberuhkia, haavoittuvuuksia ja poikkeamia kansallisella tasolla sekä kerätä niitä koskevia tietoja ja antaa niitä koskevia ennakkovaroituksia, hälytyksiä, ilmoituksia ja tietoja;
2) avustaa pyynnöstä viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden reaaliaikaisessa tai lähes reaaliaikaisessa seurannassa;
3) reagoida poikkeamailmoituksiin ja tarvittaessa avustaa poikkeamasta ilmoittanutta tahoa poikkeaman käsittelyssä;
4) kerätä ja analysoida uhkatietoja ja tietoturvaloukkausten tutkintaa koskevia tietoja;
5) laatia riski- ja poikkeama-analyysejä ja tukea kyberturvallisuuden tilannekuvan ylläpitämistä;
6) osallistua NIS 2 -direktiivin 15 artiklassa tarkoitettuun CSIRT-verkostoon ja avustaa CSIRT-verkoston jäseniä näiden pyynnöstä;
7) nimetä asiantuntijoita NIS 2 -direktiivin 19 artiklassa tarkoitettuihin vertaisarviointeihin;
8) edistää tietoturvallisten tiedonjakovälineiden käyttöönottoa; ja
9) antaa ohjeita ja suosituksia poikkeamien käsittelemisestä, kyberturvallisuuden kriisinhallinnasta ja koordinoidusta haavoittuvuuksien julkistamisesta.

CSIRT-yksikkö voi asettaa tehtäviään tärkeysjärjestykseen käytettävissään olevien voimavarojen mukaisesti soveltaen riskiperusteista lähestymistapaa.

CSIRT-yksikkö tukee 22 §:ssä tarkoitettuja kyberturvallisuustietojen vapaaehtoisia jakamisjärjestelyjä tämän lain soveltamisalaan kuuluvien toimijoiden, muiden tahojen ja CSIRT-yksikön kesken.

CSIRT-yksikkö voi tuottaa edellä 2 momentin 2 kohdassa tarkoitettua viestintäverkon ja tietojärjestelmien reaaliaikaista tai lähes reaaliaikaista tietoturvallisuuden seurantaa koskevaa palvelua viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden varmistamiseksi sekä poikkeamien havaitsemiseksi, selvittämiseksi ja kyberuhkien ennalta estämiseksi (*tietoturvaloukkausten havainnointipalvelu*). CSIRT-yksikkö voi tarjota tietoturvaloukkausten havainnointipalvelua suoraan sitä pyytäville toimijoille tai muille tahoille sekä sellaisille tietoturvapalveluntarjoajille, jotka tarjoavat tietoturvaloukkausten havainnointipalvelua toimijoille tai muille tahoille käytettäväksi (*palvelukeskus*).

Liikenne- ja viestintäministeriön asetuksella säädetään sellaisesta edellä 2 momentin 1 ja 2 kohdassa sekä 20 §:n 4 momentissa tarkoitetusta palvelusta perittävistä maksuista tai niiden perusteista, joka on tarjottu toimijan tai muun tahon pyynnöstä.

20 §

Yleisten viestintäverkkojen ja tietojärjestelmien verkkopohjainen haavoittuvuuskartoitus

CSIRT-yksiköllä on oikeus ennakoivalla, ei-intrusiivisella tavalla havainnoida ja kartoittaa tietoja yleisesti saatavilla olevista eli yleiseen viestintäverkkoon liitetyistä viestintäverkoista ja tietojärjestelmistä haavoittuvuuksien, kyberuhkien ja turvattomasti konfiguroitujen viestintäverkkojen tai tietojärjestelmien havaitsemiseksi (*haavoittuvuuskartoitus*). Haavoittuvuuskartoi-

tus tehdään haavoittuvien tai turvattomasti konfiguroitujen viestintäverkkojen ja tietojärjestelmien havaitsemiseksi ja havainnoista asianomaisille tahoille ilmoittamiseksi sekä kyberturvallisuuden tilannekuvan ylläpitämiseksi.

Haavoittuvuuskartoituksen toteuttamisessa CSIRT-yksiköllä on oikeus yleisen viestintäverkon välityksellä hankkia tietoja yleiseen viestintäverkkoon kytkettyjen telepäätelaitteiden ja tietojärjestelmien sekä niiden tietoliikennejärjestelyjen yksilöintitiedoista, käytetyistä ohjelmistoista ja niiden toiminnasta, teknisestä toteutuksesta ja niiden avulla tarjotuista palveluista. Haavoittuvuuskartoitus ei saa aiheuttaa haittaa kartoituksen kohteena olevan järjestelmän tai palvelun toiminnalle. Haavoittuvuuskartoituksella ei saa hankkia tietoa yleisessä viestintäverkossa tai yleisesti saatavilla olevassa viestintäpalvelussa välitettävänä olevasta viestinnästä.

CSIRT-yksikkö saa käyttää haavoittuvuuskartoituksessa havaittuja, kartoituksen kohteeseen yhdistettävissä olevia tietoja vain kartoituksen kohteelle viestintäverkkoon tai tietojärjestelmään kohdistuvista haavoittuvuuksista ja riskeistä ilmoittamiseksi sekä kyberuhkien tunnistamiseksi, kyberturvallisuuden tilannekuvan ylläpitämiseksi ja haavoittuvuuksista tiedottamiseksi. Tarpeettomat tiedot on poistettava viipymättä.

CSIRT-yksiköllä on oikeus suorittaa kartoituksen kohteen pyynnöstä haavoittuvuuskartoitus kartoituksen kohteen viestintäverkossa tai tietojärjestelmissä edellä 1–3 momentista poikkeavalla tavalla sellaisen haavoittuvuuden, kyberuhkan tai turvattoman konfiguroinnin havaitsemiseksi, jolla voi olla merkittävä vaikutus viestintäverkkoon tai tietojärjestelmään tai niiden avulla tarjottaviin palveluihin (*kohdennettu haavoittuvuuskartoitus*).

Haavoittuvuuskartoituksessa tai kohdennetussa haavoittuvuuskartoituksessa ei saa käsitellä sähköisten viestien sisältöä ilman viestinnän osapuolen suostumusta. Edellä 4 momentin nojalla suoritettavassa kohdennetussa haavoittuvuuskartoituksessa CSIRT-yksiköllä on oikeus tarkkailla ja käyttää välitystietoja, jos se on tarpeen haavoittuvuuden, kyberuhkan tai turvattoman konfiguroinnin havaitsemiseksi. CSIRT-yksikön on hävitettävä haavoittuvuuskartoituksessa saamansa tiedot, kun ne eivät ole enää tarpeen tässä pykälässä tarkoitettujen tehtävien hoitamiseksi.

21 §

Koordinoitu haavoittuvuuksien julkistaminen

CSIRT-yksikkö toimii NIS 2 -direktiivin 12 artiklassa tarkoitettuna koordinaattorina koordinoitua haavoittuvuuksien julkistamista varten. Tässä tehtävässä CSIRT-yksikkö ottaa vastaan ilmoituksia haavoittuvuuksista ja huolehtii tarpeellisista jatkotoimista ilmoituksien johdosta. Ilmoituksen voi antaa nimettömänä.

Koordinaattorina CSIRT-yksikkö määrittää asianomaiset toimijat ja ottaa niihin yhteyttä, avustaa haavoittuvuudesta ilmoittavia tahoja ja neuvottelee haavoittuvuuden julkistamisen aikataulusta sekä koordinoi useisiin toimijoihin vaikuttavien haavoittuvuuksien hallintaa. CSIRT-yksikkö toimii tarvittaessa välittäjänä haavoittuvuudesta ilmoittavan tahon ja TVT-tuotteen tai -palvelun valmistajan tai tarjoajan välillä sekä ohjaa ja neuvoo tietojen ilmoittamiseksi ja tietojen hakemiseksi Euroopan haavoittuvuustietokannasta.

CSIRT-yksiköllä on oikeus ilmoittaa Euroopan haavoittuvuustietokantaan seuraavia tietoja sen tiedossa olevista haavoittuvuuksista:

1) tiedot, jotka sisältävät kuvauksen haavoittuvuudesta;
2) TVT-tuotteet tai TVT-palvelut, joihin haavoittuvuus vaikuttaa, sekä haavoittuvuuden vakavuus niiden olosuhteiden perusteella, joissa sitä voidaan hyödyntää;
3) ohjelmistokorjausten saatavuus ja, jos niitä ei ole saatavilla, valvovan viranomaisen tai CSIRT-yksiköiden antama ohjeistus haavoittuvien TVT-tuotteiden tai –palveluiden käyttäjille siitä, miten julkistetusta haavoittuvuudesta johtuvia riskejä voidaan vähentää.

Jos CSIRT-yksikkö saa tiedon sellaisesta haavoittuvuudesta, jolla voi olla merkittävä vaikutus muihin EU-jäsenvaltioihin, CSIRT-yksikön on tehtävä yhteistyötä kyseisten valtioiden CSIRT-yksiköiden kanssa CSIRT-verkostossa.

22 §

Kyberturvallisuustietojen vapaaehtoiset jakamisjärjestelyt

Toimijoiden, CSIRT-yksikön ja muiden tahojen välillä voidaan muodostaa kyberturvallisuustietojen vapaaehtoisia jakamisjärjestelyitä kyberuhkien ehkäisemiseksi, havaitsemiseksi, poikkeamien hallitsemiseksi ja niistä palautumiseksi tai niiden vaikutusten lieventämiseksi.

Kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn osallistuvien kesken voidaan luovuttaa erityisesti tietoja:

1) kyberuhkista;
2) poikkeamista ja läheltä piti –tilanteista;
3) haavoittuvuuksista;
4) tekniikoista ja menettelyistä;
5) vaarantumisindikaattoreista;
6) kyberhyökkäystaktiikoista;
7) yksittäisistä uhkatoimijoista ja
8) kyberturvallisuushälytyksistä

Jakamisjärjestelyihin osallistuvat toimijat, CSIRT-yksikkö ja muut tahot voivat käsitellä tämän pykälän nojalla saamiaan tietoja vain edellä 1 momentissa mainittuihin tarkoituksiin. CSIRT-yksikkö voi lisäksi käsitellä tietoja kansallisen kyberturvallisuuden tilannekuvan ylläpitämiseksi.

Sen lisäksi, mitä sähköisen viestinnän palveluista annetun lain 319 §:ssä säädetään tietojen luovuttamisesta, CSIRT -yksikkö voi luovuttaa jakamisjärjestelyyn osallistuvalle taholle tämän lain mukaisia tehtäviä suorittaessaan saamansa tiedon kyberuhkaan tai poikkeamaan liittyvästä välitystiedosta tai haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä. Tiedon luovuttamisen edellytyksenä on, että tieto on tarpeen edellä 1 momentissa mainittua tarkoitusta varten.

23 §

Tietoturvaloukkausten havainnointipalveluun liittyvä tiedonkäsittely

Edellä 19 §:n 5 momentissa tarkoitettua tietoturvaloukkausten havainnointipalvelua käyttävä taho, palvelukeskus ja CSIRT-yksikkö voivat luovuttaa toisilleen viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden seurannan kannalta tarpeellisia tietoja kyberuhkien ehkäisemiseksi, havaitsemiseksi, poikkeamien hallitsemiseksi ja niistä palautumiseksi tai niiden vaikutusten lieventämiseksi. Siinä määrin kuin tietoturvaloukkausten havainnointipalvelun toteuttamiseksi on välttämätöntä, luovutettavat tiedot voivat sisältää palvelua käyttävän tahon palvelussa käsiteltäväksi pyytämiä sellaisia sähköisiä viestejä tai niihin liittyviä välitystietoja, joita sillä on oikeus käsitellä sähköisen viestinnän palveluista annetun lain 272 §:n nojalla.

Mahdollisten välitystietojen ja sähköisten viestien käsittelyyn tietoturvaloukkausten havainnointipalvelussa CSIRT-yksikössä ja palvelukeskuksessa sovelletaan, mitä sähköisen viestinnän palveluista annetun lain 136, 137, 138, 145 ja 272 §:ssä säädetään. CSIRT-yksikkö voi lisäksi käyttää palvelun tuottamisen yhteydessä saamiaan välitystietoja ja muita tietoja kansallisen kyberturvallisuuden tilannekuvan ylläpitämiseksi.

Mitä sähköisen viestinnän palveluista annetun lain 316 §:n 4 momentissa säädetään merkittävien tietoturvaloukkausten tai -uhkien selvittämistä koskevien tietojen hävittämisestä sekä 319 §:n 1 momentissa salassapitovelvollisuudesta, koskee myös CSIRT-yksikölle tietoturvaloukkausten havainnointipalvelun toteuttamiseksi luovutettuja viestejä ja välitystietoja.

24 §

Kyberuhkiin ja poikkeamiin liittyvien eräiden tietojen luovuttaminen

Toimija tai muu kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn osallistuva taho voi sähköisen viestinnän palveluista annetun lain 136 §:n 4 momentin estämättä luovuttaa omaaloitteisesti CSIRT-yksikölle, valvovalle viranomaiselle tai toiselle tämän lain mukaiseen vapaaehtoiseen jakamisjärjestelyyn osallistuvalle taholle tietoa kyberuhkaan tai poikkeamaan liittyvästä välitystiedosta tai haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä.

Sen lisäksi mitä tässä laissa säädetään, CSIRT-yksikkö voi luovuttaa tämän lain nojalla saamiaan ja hankkimiaan tietoja siten kuin sähköisen viestinnän palveluista annetun lain 319 §:n 2 ja 3 momentissa säädetään.

Siitä riippumatta, mitä viranomaisten oikeudesta saada salassa pidettäviä tietoja muualla laissa säädetään, CSIRT-yksikön tämän lain mukaista tehtävää hoitaessaan saamaa, muuta kuin pakollisen ilmoitusvelvollisuuden piiriin kuuluvaa tietoa ei saa käyttää tiedon luovuttanutta koskevassa rikostutkinnassa eikä hallinnollisessa tai muussa tiedon luovuttanutta koskevassa päätöksenteossa. Poikkeuksena on kuitenkin tilanne, jossa CSIRT-yksikön riskiarvion perusteella on tarpeen merkittävän kyberuhkan torjumiseksi ilmoittaa epäillystä vakavasta ja tahallisesta tämän lain rikkomisesta valvovalle viranomaiselle.

4 luku

Valvonta

25 §

Valvovat viranomaiset

Tässä laissa tarkoitettu valvova viranomainen on:

a) Liikenne- ja viestintävirasto liitteen I kohdissa 1-7 ja liitteen II kohdissa 1-5 tarkoitettujen toimijoiden osalta.
b) Energiavirasto liitteen I kohdissa 8-9 sekä kohdan 10 alakohdissa a-b tarkoitettujen toimijoiden osalta.
c) Turvallisuus- ja kemikaalivirasto liitteen I kohdan 10 alakohdissa c-g, kohdissa 11-12 sekä liitteen II kohdissa 6 sekä 11-13 tarkoitettujen toimijoiden osalta.
d) Sosiaali- ja terveysalan lupa- ja valvontavirasto liitteen I kohdassa 13 tarkoitettujen toimijoiden osalta.
e) Etelä-Savon elinkeino-, liikenne- ja ympäristökeskus liitteen I kohdissa 14-15 tarkoitettujen toimijoiden osalta sekä liitteen II kohdassa 8 tarkoitettujen toimijoiden osalta.
f) Ruokavirasto liitteen II kohdassa 7 tarkoitettujen toimijoiden osalta.
g) Lääkealan turvallisuus- ja kehittämiskeskus liitteen II kohdissa 9-10 tarkoitettujen toimijoiden osalta.

Valvovan viranomaisen tehtävänä on valvoa tämän lain, sen nojalla annettujen määräysten ja NIS 2 -direktiivin nojalla annettujen säädösten noudattamista 1 momentissa tarkoitetun toiminnan osalta.

Jos 1 momentin nojalla samaa toimijaa valvoisi useampi kuin yksi viranomainen, kukin valvova viranomainen valvoo toimijaa vain 1 momentissa tarkoitetun toiminnan osalta. Valvovien viranomaisten on tehtävä yhteistyötä valvonnan toteuttamisessa.

26 §

Valvonnan kohdistaminen

Valvonta kohdistetaan keskeisiin toimijoihin.

Keskeisellä toimijalla tarkoitetaan
a) liitteessä I tarkoitettua toimijaa, joka ylittää keskisuuren toimijan määritelmän;
b) hyväksyttyjä luottamuspalvelun tarjoajia, aluetunnusrekistereitä sekä DNS-palveluntarjoajia;
c) yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajia, jotka täyttävät tai ylittävät keskisuuren toimijan määritelmän;
d) toimijaa, joka on CER-direktiivin nojalla määritelty kriittiseksi; sekä
e) 3 §:n 2 momentin nojalla annetussa valtioneuvoston asetuksessa keskeiseksi määriteltyä toimijaa;

Valvova viranomainen voi kohdistaa valvontaa ja 29 – 31 §:ssä tarkoitettuja toimia muuhun toimijaan kuin keskeiseen toimijaan vain, jos on perusteltu syy epäillä, että kyseinen toimija ei ole noudattanut tätä lakia, sen nojalla annettuja määräyksiä tai NIS 2 -direktiivin nojalla annettuja säädöksiä.

Valvova viranomainen voi asettaa tässä laissa säädetyt tehtävät tärkeysjärjestykseen riskiperusteisesti. Valvovan viranomaisen on otettava valvonnan kohdistamisessa ja 29–34 §:ssä tarkoitettujen toimien käyttämisestä päätettäessä huomioon:
a) liitteessä I tai II tarkoitetun toiminnan laatu ja laajuus;
b) tietojärjestelmän tai viestintäverkon merkitys liitteessä I tai II tarkoitetulle toiminnalle; ja
c) NIS 2-direktiivin 32 artiklan 7 kohdassa säädetyt seikat;

Valvova viranomainen voi jättää asian tutkimatta, jos kyse on ilmeisen perusteettomasta pyynnöstä. Päätös tutkimatta jättämisestä on tehtävä viivytyksettä.

27 §

Valvovan viranomaisen tiedonsaantioikeus

Valvovalla viranomaisella on tämän lain mukaisia tehtäviä suorittaessaan oikeus saada salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä tehtäviensä suorittamiseksi välttämättömät tiedot tässä laissa tarkoitetuilta toimijoilta. Valvovan viranomaisen on tietopyynnössä ilmoitettava pyynnön tarkoitus sekä täsmennettävä pyydetyt tiedot. Tiedot on luovutettava viipymättä, viranomaisen pyytämässä muodossa ja maksutta.

Valvovalla viranomaisella on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa laissa säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto toiselle valvovalle viranomaiselle, CER-direktiivin mukaiselle valvovalle viranomaiselle ja CSIRT-yksikölle, jos se on valvovalle viranomaiselle, CER-direktiivin mukaiselle valvovalle viranomaiselle tai CSIRT-yksikölle säädettyjen tehtävien hoitamiseksi välttämätöntä.

28 §

Valvovan viranomaisen tiedonsaantioikeus välitystiedosta, sijaintitiedosta ja haitallisen tietokoneohjelman tai käskyn sisältävästä sähköisestä viestistä

Valvovalla viranomaisella on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada toimijalta välitystieto, sijaintitieto tai haitallisen tietokoneohjelman tai käskyn sisältävä viesti, jos se on välttämätöntä kyberturvallisuuden riskienhallintavelvoitteiden valvomista varten tai merkittävien poikkeamien selvittämiseksi.

Mitä sähköisen viestinnän palveluista annetun lain 316 §:n 4 momentissa ja 319 §:ssä säädetään Liikenne- ja viestintäviraston viestistä, välitystiedosta, sijaintitiedosta sekä luottamuksellisen radiolähetyksen sisällöstä ja olemassaolosta saamien ja hankkimien tietojen salassapidosta,

luovuttamisesta ja hävittämisestä, sovelletaan myös valvovan viranomaisen tämän pykälän nojalla saamiin ja hankkimiin tietoihin.

29 §

Tarkastusoikeus

Valvovalla viranomaisella on oikeus tehdä toimijaa koskeva tarkastus. Tarkastus tehdään tässä laissa tai sen nojalla annetussa määräyksessä taikka NIS 2-direktiivin nojalla annetussa säädöksessä asetettujen velvoitteiden noudattamisen valvomiseksi siinä laajuudessa kuin se on tarpeen. Tarkastuksen suorittajalla on oltava sellainen koulutus ja kokemus kuin tarkastuksen suorittamiseksi on tarpeen. Valvova viranomainen voi päätöksellään käyttää tarkastuksessa apuna tai pyytää tarkastuksen suorittajaksi toisen valvovan viranomaisen, tietoturvallisuuden arviointilaitoksen tai ulkopuolisen tietotekniikan asiantuntijan, jos se on tarkastuksen laadun tai laajuuden vuoksi tarpeellista. Ulkopuoliseen asiantuntijaan sovelletaan rikosoikeudellista virkavastuuta koskevia säännöksiä hänen hoitaessaan tämän pykälän mukaisia tehtäviä. Vahingonkorvausvastuusta säädetään vahingonkorvauslaissa (412/1974).

Toimijoiden on tarkastusta varten päästettävä tarkastusta suorittava tarkastuksen edellyttämässä laajuudessa tarkastuksen kohteena olevaan viestintäverkkoon tai tietojärjestelmään ja muihin kuin pysyväisluonteiseen asumiseen tarkoitettuihin tiloihin. Tarkastuksen suorittamiseksi valvovalla viranomaisella, tarkastusta suorittavalla toisella viranomaisella ja ulkopuolisella asiantuntijalla on salassapitosäännösten tai muiden tiedon luovuttamista koskevien rajoitusten estämättä oikeus saada tutkittavakseen valvontatehtävän kannalta välttämättömät tiedot, asiakirjat, laitteet ja ohjelmistot, suorittaa tarvittavia testejä ja mittauksia sekä tarkastaa toimijan toteuttamat turvallisuusjärjestelyt.

Tarkastuksessa noudatettavaan menettelyyn sovelletaan, mitä hallintolain (434/2003) 39 §:ssä säädetään tarkastuksesta.

30 §

Turvallisuusauditointi

Valvovalla viranomaisella on oikeus velvoittaa päätöksellä toimija teettämään kyberturvallisuuden riskienhallintaan kohdistuva turvallisuusauditointi, jos

1) toimijaan on kohdistunut merkittävä poikkeama, joka on aiheuttanut palvelujen vakavan toimintahäiriön tai huomattavaa aineellista tai aineetonta vahinkoa; tai
2) toimija on olennaisesti ja vakavasti laiminlyönyt toteuttaa 8 §:ssä tarkoitettun kyberturvallisuuden riskienhallinnan toimintamallin tai sen edellyttämiä hallintatoimenpiteitä taikka muutoin olennaisesti ja vakavasti toiminut tässä laissa tai sen nojalla taikka NIS 2 –direktiivin nojalla säädetyn velvoitteen vastaisesti.

Valvovalla viranomaisella on oikeus saada tieto teetetyn turvallisuusauditoinnin tuloksista sekä päätöksellä velvoittaa toimija toteuttamaan turvallisuusauditoinnin suosittelemat kohtuulliset ja oikeasuhtaiset toimenpiteet kyberturvallisuuden riskienhallinnan kehittämiseksi.

31 §

Valvontapäätös, huomautus ja varoitus

Valvova viranomainen voi päätöksellä velvoittaa toimijan määräajassa korjaamaan puutteet tässä laissa tai sen nojalla annetuissa määräyksissä taikka NIS 2-direktiivin nojalla annetuissa säädöksissä säädettyjen velvoitteiden noudattamisessa. Valvova viranomainen voi velvoittaa

toimijan julkistamaan kyseiset puutteet tai muut seikat, jotka liittyvät tämän lain, sen nojalla annettujen määräysten tai NIS 2-direktiivin nojalla annettujen säädösten rikkomiseen.

Valvova viranomainen voi antaa toimijalle huomautuksen tai varoituksen. Varoituksen voi antaa, jos huomautusta ei asiasta ilmenevät seikat kokonaisuudessaan huomioiden voida pitää riittävänä.

32 §

Luvanvaraisen tai sertifioidun toiminnan rajoittaminen ja luvan tai sertifioinnin peruuttaminen

Valvova viranomainen voi väliaikaisesti rajoittaa keskeiselle toimijalle myönnetyn luvan tai sertifioinnin mukaista toimintaa tai peruuttaa luvan tai sertifioinnin taikka kun muu viranomainen on toimivaltainen lupa- tai sertifiointiviranomainen, tehdä sille päätösesityksen asiasta, jos

1) keskeinen toimija on olennaisesti ja vakavasti laiminlyönyt toteuttaa kyberturvallisuuden riskienhallinnan toimintamallin tai riskienhallinnan edellyttämät hallintatoimenpiteet; tai
2) keskeinen toimija on jättänyt olennaisesti ja vakavasti noudattamatta muita sille tässä laissa, tämän lain nojalla annetuissa määräyksissä tai NIS 2-direktiivin nojalla annetuissa säädöksissä asetettuja velvoitteita.

Valvovan viranomaisen on ennen 1 momentissa tarkoitetun päätöksen tai päätösesityksen tekemistä annettava keskeiselle toimijalle huomautus tai varoitus sekä varattava kohtuullinen määräaika puutteen tai laiminlyönnin korjaamiseksi.

Toiminnan rajoittaminen taikka luvan tai sertifioinnin peruuttaminen määrätään olemaan voimassa toiminnassa esiintyneiden puutteiden tai laiminlyöntien vakavuuteen suhteutetun määräajan kuitenkin enintään, kunnes tarvittavat toimet puutteen tai laiminlyönnin korjaamiseksi on toteutettu. Jos puutteita tai laiminlyöntejä ei ole korjattu määräajassa, valvova viranomainen voi määräajan päättymisen jälkeen päättää tai esittää päätettäväksi luvan ehtojen muuttamista toiminnan rajoittamiseksi tai luvan taikka sertifioinnin peruuttamista pysyvästi.

33 §

Johdon toiminnan rajoittaminen

Valvova viranomainen voi määräajaksi, enintään viideksi vuodeksi, kieltää henkilöä toimimasta keskeisen toimijan hallituksen jäsenenä ja varajäsenenä, hallintoneuvoston jäsenenä ja varajäsenenä, toimitusjohtajana tai muussa siihen rinnastettavassa asemassa, sekä toimitusjohtajan välittömään alaisuuteen kuuluvissa tehtävissä, jotka ovat keskeisen toimijan ylimpiä johtotehtäviä tai joissa tosiasiallisesti johdetaan sen toimintaa, jos tämä on toistuvasti ja vakavasti rikkonut 10 §:ssä säädettyjä velvoitteita. Valvovan viranomaisen on ennen päätöksen tekemistä annettava keskeiselle toimijalle huomautus tai varoitus sekä varattava kohtuullinen määräaika puutteen tai laiminlyönnin korjaamiseksi.

Edellä 1 momentista poiketen johdon toimintaa ei voida rajoittaa, jos kyse on valtion viranomaisesta, valtion liikelaitoksesta, kunnallisesta viranomaisesta, itsenäisestä julkisoikeudellisesta laitoksesta, eduskunnan virastosta, tasavallan presidentin kansliasta, Suomen evankelisluterilaisesta kirkosta, Suomen ortodoksisesta kirkosta tai niiden seurakunnista, seurakuntayhtymistä tai muista elimistä.

34 §

Ilmoitus tietosuojavaltuutetulle

Jos valvova viranomainen saa tässä laissa tarkoitettujen tehtävien hoitamisen yhteydessä tietoonsa, että 2 luvussa säädettyjen velvoitteiden laiminlyönti voi johtaa tai on johtanut yleisessä tietosuoja-asetuksessa tarkoitettuun henkilötietojen tietoturvaloukkaukseen, josta on yleisen tietosuoja-asetuksen 33 artiklan nojalla ilmoitettava yleisen tietosuoja-asetuksen mukaiselle valvontaviranomaiselle, valvovan viranomaisen on ilmoitettava asiasta tietosuojavaltuutetulle.

Jos yleisen tietosuoja-asetuksen nojalla toimivaltainen valvontaviranomainen on sijoittunut toiseen jäsenvaltioon, valvova viranomainen tekee 1 momentissa tarkoitetun ilmoituksen tietosuojavaltuutetulle.

35 §

Uhkasakko, teettämisuhka ja keskeyttämisuhka

Valvova viranomainen voi asettaa tämän lain nojalla antamansa päätöksen tehosteeksi uhkasakon, teettämisuhan tai keskeyttämisuhan, joihin sovelletaan, mitä uhkasakkolaissa (1113/1990) säädetään.

36 §

Oikaisuvaatimus

Valvovan viranomaisen 30-33 §:n nojalla tekemään päätökseen saa vaatia oikaisua. Oikaisuvaatimuksesta säädetään hallintolaissa.

Valvova viranomainen voi päätöksessään määrätä, että päätöstä on noudatettava muutoksenhausta huolimatta, jollei muutoksenhakuviranomainen toisin määrää.

5 luku

Seuraamusmaksu

37 §

Hallinnollinen seuraamusmaksu

Hallinnollinen seuraamusmaksu voidaan määrätä toimijalle, joka tahallaan tai törkeästä huolimattomuudesta:

1) laiminlyö 7 §:ssä tarkoitetun riskienhallintavelvoitteen, 8 §:ssä tarkoitetun kyberturvallisuuden riskienhallinnan toimintamallin laatimisen tai 9 §:n 1 momentissa tarkoitettujen osa-alueiden huomioimisen osana kyberturvallisuuden riskienhallinnan toimintamallia;
2) laiminlyö toteuttaa 9 §:n 2 momentissa tarkoitetut toimenpiteet;
3) laiminlyö antaa 11 §:ssä tarkoitetun poikkeamailmoituksen taikka 12 §:ssä tarkoitetun väliraportin tai 13 §:ssä tarkoitetun loppuraportin valvovalle viranomaiselle;
4) laiminlyö antaa 43 §:ssä tarkoitetut tiedot valvovalle viranomaiselle.

Seuraamusmaksua ei voida määrätä valtion viranomaisille, valtion liikelaitoksille, kunnallisille viranomaisille, itsenäisille julkisoikeudellisille laitoksille, eduskunnan virastoille, tasavallan presidentin kanslialle eikä Suomen evankelisluterilaiselle kirkolle ja Suomen ortodoksiselle kirkolle eikä niiden seurakunnille, seurakuntayhtymille ja muille elimille.

38 §

Seuraamusmaksulautakunta

Hallinnollisen seuraamusmaksun määrää seuraamusmaksulautakunta valvovan viranomaisen esityksestä. Hallinnollinen seuraamusmaksu määrätään maksettavaksi valtiolle.

Seuraamusmaksulautakunnan puheenjohtajan ja varapuheenjohtajan nimeää Liikenne- ja viestintävirasto. Kukin valvova viranomainen nimeää lautakuntaan jäsenen ja hänelle henkilökohtaisen varajäsenen. Lautakunnan jäseneltä ja varajäseneltä edellytetään perehtyneisyyttä kyberturvallisuuden riskienhallintaan sekä NIS 2-direktiiviin ja sitä täytäntöönpanevan sääntelyn asettamiin velvoitteisiin nimeävän viranomaisen valvontatoimialalla. Lautakunnan puheenjohtajalla ja varapuheenjohtajalla tulee olla tehtävän edellyttämä riittävä oikeudellinen asiantuntemus. Lautakunnan jäsenet nimetään kolmen vuoden määräajaksi. Lautakunnan jäsen toimii tehtävässään riippumattomasti ja puolueettomasti.

Seuraamusmaksulautakunnan päätös tehdään esittelystä. Esittelijänä toimii sen valvovan viranomaisen virkamies, jonka valvontatoimivaltaan kohdistuva asia on ratkaistavana. Lautakunta on päätösvaltainen, kun paikalla on puheenjohtaja tai varapuheenjohtaja ja vähintään kaksi muuta jäsentä tai varajäsentä. Päätökseksi tulee se kanta, jota enemmistö on kannattanut. Äänten mennessä tasan päätökseksi tulee se kanta, joka on lievempi sille, johon seuraamus kohdistuu.

Seuraamusmaksulautakunnalla on oikeus salassapitosäännösten estämättä saada maksutta tehtäviensä hoidon kannalta välttämättömät tiedot.

39 §

Seuraamusmaksun määrääminen

Hallinnollisen seuraamusmaksun määrä perustuu kokonaisarviointiin, jossa otetaan huomioon tapauksen olosuhteet sekä vähintään seuraavat seikat:

1) rikkomisen vakavuus ja rikottujen säännösten tärkeys siten, että rikkomisen vakavuutta osoittaa
    a) väärinkäytösten toistuvuus
    b) merkittävien poikkeamien jättäminen ilmoittamatta tai korjaamatta
    c) havaittujenpuutteiden jättäminen korjaamatta valvovan viranomaisen päätöksistä, huomautuksista tai varoituksista huolimatta
    d) valvovan viranomaisen tarkastuksen estäminen tai määrätyn auditoinnin teettämättä jättäminen
    e) riskienhallinnasta tai merkittävistä poikkeamista viranomaiselle liittyvien väärien tai harhaanjohtavien tietojen antaminen.
2) rikkomisen kesto;
3) toimijan mahdolliset vastaavat aiemmat rikkomiset;
4) aiheutunut vahinko, mukaan lukien rahoitukseen liittyvät tai taloudelliset tappiot, vaikutukset muihin palveluihin sekä niiden käyttäjien lukumäärä, joihin rikkominen vaikuttaa;
5) tahallisuuden aste;
6) toimenpiteet, jotka toimija on toteuttanut vahingon ehkäisemiseksi tai lieventämiseksi;
7) hyväksyttyjen käytännesääntöjen tai hyväksyttyjen sertifiointimekanismien noudattaminen;
8) toimijan halukkuus tehdä yhteistyötä valvovan viranomaisen kanssa.

40 §

Seuraamusmaksun enimmäismäärä

Hallinnollisen seuraamusmaksun enimmäismäärä 26 §:ssä tarkoitetulle keskeiselle toimijalle on 10 000 000 euroa tai 2 prosenttia toimijan edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

Hallinnollisen seuraamusmaksun enimmäismäärä muulle kuin keskeiselle toimijalle on 7 000 000 euroa tai 1,4 prosenttia toimijan edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

41 §

Seuraamusmaksun määräämättä jättäminen ja täytäntöönpano

Seuraamusmaksu jätetään määräämättä, jos

1) toimija on oma-aloitteisesti ryhtynyt riittäviin toimenpiteisiin rikkomuksen tai laiminlyönnin korjaamiseksi välittömästi sen havaitsemisen jälkeen ja ilmoittanut siitä viivytyksettä valvovalle viranomaiselle sekä toiminut yhteistyössä valvovan viranomaisen kanssa eikä rikkomus tai laiminlyönti ole vakava tai toistuva;
2) rikkomusta tai laiminlyöntiä on pidettävä vähäisenä; tai
3) seuraamusmaksun määräämistä on pidettävä ilmeisen kohtuuttomana muutoin kuin 1 tai 2 kohdassa tarkoitetulla perusteella.

Seuraamusmaksua ei saa määrätä, jos on kulunut yli viisi vuotta siitä, kun rikkomus tai laiminlyönti on tapahtunut. Jos rikkomus tai laiminlyönti on ollut luonteeltaan jatkuvaa, määräaika lasketaan siitä, kun rikkomus tai laiminlyönti on päättynyt.

Seuraamusmaksua ei saa määrätä sille, jota epäillään samasta teosta esitutkinnassa, syyteharkinnassa tai tuomioistuimessa vireillä olevassa rikosasiassa. Seuraamusmaksua ei saa määrätä myöskään sille, jolle on samasta teosta annettu lainvoimainen tuomio.

Seuraamusmaksua ei saa määrätä sille, jolle on määrätty samasta teosta yleisen tietosuoja-asetuksen 83 artiklassa tarkoitettu seuraamusmaksu.

Seuraamusmaksun täytäntöönpanosta säädetään sakon täytäntöönpanosta annetussa laissa (672/2002). Seuraamusmaksu vanhenee viiden vuoden kuluttua lainvoiman saaneen päätöksen tekemisestä.

42 §

Muutoksenhaku

Muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).

6 luku

Muut säännökset

43 §

Toimijaluettelo

Toimijoiden on ilmoitettava valvovalle viranomaiselle seuraavat tiedot toimijaluettelon ylläpitämiseksi:

a) toimijan nimi;
b) osoite, sähköpostiosoite, puhelinnumero ja muut ajantasaiset yhteystiedot;
c) toimijan IP-osoitealueet;
d) NIS 2-direktiivin liitteessä I tai II tarkoitettu asiaankuuluva toimiala ja toimialan osa;
e) tieto siitä, onko toimija 26 §:ssä tarkoitettu keskeinen toimija;
f) luettelo EU-jäsenvaltioista, joissa toimija tarjoaa NIS 2 -direktiivin soveltamisalaan kuuluvia palveluja; ja
g) osallistumisesta 22 §:ssä tarkoitettuun kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn.

DNS-palveluntarjoajien, aluetunnusrekisterien, pilvipalvelujen tarjoajien, datakeskuspalvelujen tarjoajien, sisällönjakeluverkkojen tarjoajien, hallintapalvelun tarjoajien, tietoturvapalveluntarjoajien sekä verkossa toimivien markkinapaikkojen tarjoajien, verkossa toimivien hakukoneiden tarjoajien ja verkkoyhteisöalustojen tarjoajien on ilmoitettava valvovalle viranomaiselle edellä 1 momentissa tarkoitettujen tietojen lisäksi:

a) NIS 2-direktiivin liitteessä I tai II tarkoitettu toimijatyyppi;
b) toimijan päätoimipaikan ja muiden unionissa sijaitsevien laillisten toimipaikkojen osoite tai, jos toimija ei ole sijoittautunut Euroopan unioniin, sen Euroopan unioniin nimetyn edustajan osoite, sähköpostiosoite, puhelinnumero ja muut ajantasaiset yhteystiedot; ja
c) luettelo EU-jäsenvaltioista, joissa toimija tarjoaa palveluita.

Toimijoiden on ilmoitettava muutoksista tässä pykälässä tarkoitettuihin tietoihin viipymättä. Muutoksesta 1 momentissa tarkoitettuihin tietoihin on ilmoitettava valvovalle viranomaiselle kahden viikon kuluessa ja 2 momentissa tarkoitettuihin tietoihin on ilmoitettava kolmen kuukauden kuluessa muutoshetkestä. Valvova viranomainen voi antaa tarkempia teknisiä määräyksiä tietojen ilmoittamisesta.

Valvova viranomainen ylläpitää valvontatoimialansa osalta toimijaluetteloa 1 ja 2 momentin nojalla toimitetuista tiedoista. Valvovan viranomaisen on toimitettava NIS 2-direktiivin 3 artiklan 5 kohdassa ja 27 artiklan 4 kohdassa tarkoitettujen ilmoituksien tekemiseksi tarpeelliset tiedot toimijaluettelosta keskitetylle yhteyspisteelle. Keskitetty yhteyspiste vastaa NIS 2-direktiivin 3 artiklan 5 kohdassa ja 27 artiklan 4 kohdassa tarkoitettujen ilmoituksien tekemisestä Euroopan komissiolle, NIS-yhteistyöryhmälle ja Euroopan unionin kyberturvallisuusvirasto ENISA:lle.

44 §

Kansallinen kyberturvallisuusstrategia

Valtioneuvosto hyväksyy kansallisen kyberturvallisuusstrategian sekä vastaa kansallisen kyberturvallisuusstrategian päivittämisestä säännöllisesti vähintään viiden vuoden välein.

Kansalliseen kyberturvallisuusstrategiaan on sisällytettävä vähintään NIS 2-direktiivin 7 artiklan 1 kohdassa tarkoitetut osa-alueet ja 7 artiklan 2 kohdassa tarkoitetut toimintaperiaatteet.

Valtioneuvosto antaa kansallisen kyberturvallisuusstrategian tiedoksi Euroopan komissiolle kolmen kuukauden kuluessa sen hyväksymisestä. Kyberturvallisuusstrategiasta voidaan jättää antamatta tietoja, joiden luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin siihen liittyvää tärkeää etua.

45 §

Laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintasuunnitelma

Liikenne- ja viestintävirasto vastaa kansallisen laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallintasuunnitelman laatimisesta yhteistoiminnassa 25 §:ssä tarkoitettujen valvovien viranomaisten, poliisihallituksen, suojelupoliisin, Puolustusvoimien ja huoltovarmuuskeskuksen kanssa.

Kansallisen laajamittaisten kyberturvallisuuspoikkeamien ja –kriisien hallintasuunnitelman tulee sisältää NIS 2 -direktiivin 9 artiklan 3 ja 4 kohdassa tarkoitetut tiedot. NIS 2 -direktiivin 9 artiklan 1 kohdan tarkoittamana kyberkriisinhallintaviranomaisena toimii kukin viranomainen sille laissa säädettyjen tehtävien mukaisesti. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus toimii koordinaattorina laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallinnassa.

Edellä 2 momentissa tarkoitetut tiedot on annettava tiedoksi Euroopan komissiolle ja NIS 2 -direktiivin 16 artiklassa tarkoitetulle Euroopan kyberkriisien yhteysorganisaatioiden verkostolle kolmen kuukauden kuluessa sen hyväksymisestä. Tietoja voidaan olla antamatta siltä osin, jos niiden luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoi siihen liittyvää tärkeää etua.

46 §

Viranomaisten yhteistyö

Valvovien viranomaisten, CSIRT-yksikön ja keskitetyn yhteyspisteen on toimittava yhteistyössä tässä laissa ja NIS 2-direktiivin nojalla säädettyjen tehtävien täyttämiseksi.

Valvovien viranomaisten, CSIRT-yksikön ja keskitetyn yhteyspisteen on toimittava tarvittaessa yhteistyössä poliisin tai muun esitutkintaviranomaisen, tietosuojavaltuutetun, yhteisistä siviili-ilmailun turvaamista koskevista säännöistä ja asetuksen (EY) N:o 2320/2002 kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 300/2008 toimivaltaisen viranomaisen, yhteisistä siviili-ilmailua koskevista säännöistä ja Euroopan unionin lentoturvallisuusviraston perustamisesta, Euroopan parlamentin ja neuvoston asetusten (EY) N:o 2111/2005, (EY) N:o 1008/2008, (EU) N:o 996/2010, (EU) N:o 376/2014 ja direktiivien 2014/30/EU ja 2014/53/EU muuttamisesta sekä Euroopan parlamentin ja neuvoston asetusten (EY) N:o 552/2004, (EY) N:o 216/2008 ja neuvoston asetuksen (ETY) N:o 3922/91 kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1139 toimivaltaisen viranomaisen, eIDAS-asetuksen mukaisten valvontaelinten, DORA-asetuksen toimivaltaisen viranomaisen, teledirektiivin mukaisen kansallisen sääntelyviranomaisen ja CER-direktiivin mukaisen toimivaltaisen viranomaisen kanssa.

Valvovien viranomaisten ja CER-direktiivin mukaisen toimivaltaisen viranomaisen on vaihdettava keskenään säännöllisesti tietoja kriittisten toimijoiden määrittämisestä sekä riskeistä, kyberuhkista ja poikkeamista ja muista kuin kyberturvallisuuteen liittyvistä riskeistä, uhkista ja poikkeamista, jotka vaikuttavat CER-direktiivin nojalla kriittisiksi toimijoiksi määriteltyihin toimijoihin, sekä näiden riskien, uhkien ja poikkeamien hallintatoimenpiteistä. Valvovien viranomaisten on ilmoitettava CER-direktiivin mukaiselle toimivaltaiselle viranomaiselle kun se käyttää 4 luvussa säädettyjä toimivaltuuksia CER-direktiivin nojalla kriittiseksi tunnistettuun toimijaan. Valvova viranomainen voi CER-direktiivin mukaisen toimivaltaisen viranomaisen perustellusta pyynnöstä kohdistaa 4 luvussa säädettyjä toimivaltuuksia CER-direktiivin nojalla kriittiseksi tunnistettuun toimijaan.

Valvovien viranomaisten on ilmoitettava DORA-asetuksen 32 artiklan 1 kohdan nojalla perustetulle valvontafoorumille, kun ne käyttävät valvonta- ja täytäntöönpanovaltuuksiaan toimijaan, joka on nimetty kriittiseksi TVT-palveluntarjoajana olevaksi kolmanneksi osapuoleksi DORA-asetuksen 31 artiklan nojalla.

Valvovien viranomaisten ja eIDAS-asetuksen mukaisten valvontaelinten, DORA-asetuksen toimivaltaisen viranomaisen ja teledirektiivin mukaisen kansallisen sääntelyviranomaisen on vaihdettava keskenään säännöllisesti tietoja merkittävistä poikkeamista ja kyberuhkista.

47 §

Voimaantulo

Tämä laki tulee voimaan 18 päivänä lokakuuta 2024.
Tämän lain 43 § tulee voimaan 1 päivänä tammikuuta 2025.

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

Liite I

1. Ilmaliikenne:
   a) Yhteisistä siviili-ilmailun turvaamista koskevista säännöistä ja asetuksen (EY) N:o 2320/2002 kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 300/2008 3 artiklan 4 alakohdassa määritellyt lentoliikenteen harjoittajat, joiden toiminta on kaupallista
   b) Lentoasemaverkoista ja –maksuista annetun lain (210/2011) 3 §:n 1 momentin 2 kohdassa tarkoitetut lentoaseman pitäjät
   c) Yhtenäisen eurooppalaisen ilmatilan toteuttamisen puitteista annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 549/2004 2 artiklan 1 alakohdassa määriteltyä lennonjohtopalvelua tarjoavat lennonjohtopalvelun tarjoajat
2. Raideliikenne:
   a) Raideliikennelain (1302/2018) 4 §:n 1 momentin 29 kohdassa tarkoitetut rataverkon haltijat ja liikenteenohjauspalvelua tarjoavat yhtiöt
   b) Raideliikennelain 4 §:n 1 momentin 34 kohdassa tarkoitetut rautatieyritykset
   c) Raideliikennelain 4 §:n 1 momentin 23 kohdassa tarkoitetut palvelupaikan ylläpitäjät
3. Vesiliikenne:
   a) Alusten ja satamarakenteiden turvatoimien parantamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 725/2004 liitteessä I merenkulun osalta määritellyt sisävesillä, merillä ja rannikoilla matkustaja- ja rahtiliikennettä hoitavat yhtiöt, lukuun ottamatta tällaisten yhtiöiden liikennöimiä yksittäisiä aluksia

b) Eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain (485/2004) 2 §:n 2 kohdassa tarkoitetut satamanpitäjät sekä toimijat, jotka huolehtivat rakenteista ja varusteista sataman alueella.
c) Alusliikennepalvelulain (623/2005) 2 §:n 1 momentin 5 kohdassa tarkoitetut VTS-palveluntarjoajat

4. Tieliikenne:
   a) Euroopan parlamentin ja neuvoston direktiivin 2010/40/EU täydentämisestä EU:n laajuisten tosiaikaisten liikennetietopalvelujen tarjoamisen osalta annetun Komission delegoidun asetuksen (EU) 2015/962 2 artiklan 12 alakohdassa tarkoitetut, liikenteenhallinnasta vastaavat tieviranomaiset, lukuun ottamatta julkishallinnon toimijoita, joille liikenteenhallinta tai älykkäiden liikennejärjestelmien ylläpitäminen ei ole keskeinen osa niiden yleistä toimintaa
   b) Liikenteen palveluista annetun lain (320/2017) 160 §:ssä tarkoitettujen älykkäiden liikennejärjestelmien ylläpitäjät
5. Maa-asemista ja eräistä tutkista annetun lain (96/2023) 2 §:n 1 momentin 5 kohdassa tarkoitetut toiminnanharjoittajat; tai muut avaruuspohjaisten palvelujen tarjoamista tukevan, jäsenvaltioiden tai yksityisten tahojen omistaman, hallinnoiman ja operoiman maassa sijaitsevan infrastruktuurin ylläpitäjät, lukuun ottamatta yleisten sähköisten viestintäverkkojen tarjoajia
6. Digitaalinen infrastruktuuri:
   a) Internetin yhdysliikennepisteiden, eli sellaisen verkkoinfrastruktuurin osan, joka mahdollistaa useamman kuin kahden riippumattoman verkon (autonomisen järjestelmän) yhdistämisen pääasiassa internetliikenteen välittämisen helpottamiseksi, joka tarjoaa yhteenliitäntää ainoastaan autonomisille järjestelmille ja joka ei edellytä minkään yhteenliittämänsä kahden autonomisen järjestelmän väliseltä internetliikenteeltä kulkemista minkään kolmannen autonomisen järjestelmän kautta eikä muokkaa tällaista liikennettä tai muutoin puutu siihen, ylläpitäjät
   b) DNS-palveluntarjoajat
   c) Aluetunnusrekisterit
   d) Pilvipalvelun tarjoajat
   e) Datakeskuspalvelun tarjoajat
   f) Sisällönjakeluverkon tarjoajat
   g) Luottamuspalvelun tarjoajat
   h) Yleisten sähköisten viestintäverkkojen tarjoajat
   i) Yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat
7. TVT-palvelujen hallinta:
   a) Hallintapalvelun tarjoajat
   b) Tietoturvapalveluntarjoajat
8. Sähkö:
   a) Sähkömarkkinalain (588/2013) 3 §:n 1 momentin 21 kohdassa tarkoitetut sähköalan yritykset, jotka harjoittavat momentin 11 kohdassa tarkoitettua sähköntoimitusta
   b) Sähkömarkkinalain 3 §:n 1 momentin 10 kohdassa tarkoitetut jakeluverkonhaltijat
   c) Sähkömarkkinalain 7 §:n mukaiset kantaverkonhaltijat
   d) Sähkömarkkinalain 3 §:n 1 momentin 15 kohdassa tarkoitetut tuottajat
   e) Sähkön sisämarkkinoista annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/943 2 artiklan 8 alakohdassa määritellyt nimitetyt sähkömarkkinaoperaattorit
   f) Sähkömarkkinalain 3 §:n 1 momentin 37 kohdassa tarkoitetut sähkömarkkinoiden osapuolet, jotka tarjoavat sähkömarkkinalain 3 §:n 1 momentin 21 a kohdassa tarkoitettua aggregointia, 30 a kohdassa tarkoitettua kulutusjoustoa tai 21 c kohdassa tarkoitettua energian varastointia

g) Latauspisteiden operaattorit, jotka vastaavat latauspalvelua loppukäyttäjille tarjoavan latauspisteen hallinnoinnista ja toiminnasta, myös liikennepalvelun tarjoajan nimissä ja puolesta

9. Uusiutuvista lähteistä peräisin olevan energian käytön edistämisestä annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2018/2001 2 kohdan 19 alakohdassa määritellyn kaukolämmityksen tai kaukojäähdytyksen haltijat
10. Kaasu:
    a) Maakaasumarkkinalain 3 §:n 1 momentin 10 kohdassa tarkoitetut jakeluverkonhaltijat
    b) Maakaasumarkkinalain 3 §:n 1 momentin 9 kohdassa tarkoitetut siirtoverkonhaltijat
    c) Maakaasumarkkinalain (587/2017) 3 §:n 1 momentin 14 kohdassa tarkoitetut maakaasun toimittajat
    d) Maakaasumarkkinalain 3 §:n 1 momentin 20 kohdassa tarkoitetut varastointilaitteiston haltijat
    e) Maakaasumarkkinalain 3 §:n 1 momentin 22 kohdassa tarkoitetut nesteytetyn maakaasun käsittelylaitteiston haltijat
    f) Maakaasumarkkinalain 3 §:n 1 momentin 18 kohdassa tarkoitetut maakaasualan yritykset
    g) Maakaasun jalostus- ja käsittelylaitteistojen haltijat
11. Öljy:
    a) Öljynsiirtoputkistojen haltijat
    b) Öljyn tuotanto-, jalostus- ja käsittelylaitteistojen haltijat sekä öljyn varastointia ja siirtoa hoitavat operaattorit
    c) Jäsenvaltioiden velvollisuudesta ylläpitää raakaöljy- ja/tai öljytuotevarastojen vähimmäistasoa annetun Neuvoston direktiivin 2009/119/EY 2 kohdan f alakohdassa määritellyt keskusvarastointiyksiköt
12. Vedyn tuotantoa, varastointia ja siirtoa harjoittavat toimijat
13. Terveys:
    a) Potilaiden oikeuksien soveltamisesta rajatylittävässä terveydenhuollossa annetun Euroopan parlamentin ja neuvoston direktiivin 2011/24/EU 3 artiklan g alakohdassa määritellyt terveydenhuollon tarjoajat
    b) Rajatylittävistä vakavista terveysuhkista ja päätöksen N:o 1082/2013/EU kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2371 15 artiklassa tarkoitetut EU:n vertailulaboratoriot
    c) Ihmisille tarkoitettuja lääkkeitä koskevista yhteisön säännöistä annetun Euroopan parlamentin ja neuvoston direktiivin 2001/83/EY 1 artiklan 2 alakohdassa määriteltyjen lääkkeiden tutkimusta ja kehitystä harjoittavat toimijat
    d) NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 21 tarkoitettua lääkeaineiden ja lääkkeiden valmistusta harjoittavat toimijat
    e) Euroopan lääkeviraston roolin vahvistamisesta kriisivalmiudessa ja -hallinnassa lääkkeiden ja lääkinnällisten laitteiden osalta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/123 22 artiklassa tarkoitettuja vakavan kansanterveysuhan aikana kriittisiksi katsottuja lääkinnällisiä laitteita (kansanterveysuhan aikana kriittisten lääkinnällisten laitteiden luettelo) valmistavat toimijat
14. Ihmisten käyttöön tarkoitetun veden laadusta annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2020/2184 2 artiklan 1 alakohdan a alakohdassa määritellyn ihmisten käyttöön tarkoitetun veden toimittajat ja jakelijat, lukuun ottamatta jakelijoita, joille ihmisten käyttöön tarkoitetun veden jakelu ei ole keskeinen osa niiden yleistä toimintaa, joka muodostuu muiden hyödykkeiden ja tavaroiden jakelusta

15. Yhdyskuntajätevesien käsittelystä annetun Neuvoston direktiivin 91/271/ETY 2 artiklan 1, 2 ja 3 alakohdassa määriteltyä yhdyskuntajätevettä, talousjätevettä tai teollisuusjätevettä keräävät, hävittävät tai käsittelevät yritykset, lukuun ottamatta yrityksiä, joille yhdyskuntajäteveden, talousjäteveden tai teollisuusjäteveden kerääminen, hävittäminen tai käsittely ei ole keskeinen osa niiden yleistä toimintaa

Liite II

1. Kuriiripalvelun tarjoajat ja postilain (415/2011) 2 §:n 1 momentin 2 kohdassa tarkoitetun postipalvelun tarjoajat
2. Digitaalisen palvelun tarjoajat:
   a) Verkossa toimivien markkinapaikkojen tarjoajat
   b) Verkossa toimivien hakukoneiden tarjoajat
   c) Verkkoyhteisöalustojen tarjoajat
3. NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 29 tarkoitettua moottoriajoneuvojen, perävaunujen ja puoliperävaunujen valmistusta harjoittavat toimijat
4. NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 30 tarkoitettua muiden kulkuneuvojen valmistusta harjoittavat toimijat
5. Tutkimusorganisaatiot, joiden ensisijaisena tavoitteena on harjoittaa soveltavaa tutkimusta tai kokeellista kehitystyötä kyseisen tutkimuksen tulosten hyödyntämiseksi kaupallisiin tarkoituksiin mutta joka ei ole korkeakoulu tai muu opetus- ja koulutusalan laitos.
6. Kemikaalien rekisteröinnistä, arvioinnista, lupamenettelyistä ja rajoituksista (REACH), Euroopan kemikaaliviraston perustamisesta, direktiivin 1999/45/EY muuttamisesta sekä neuvoston asetuksen (ETY) N:o 793/93, komission asetuksen (EY) N:o 1488/94, neuvoston direktiivin 76/769/ETY ja komission direktiivien 91/155/ETY, 93/67/ETY, 93/105/EY ja 2000/21/EY kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 1907/2006 3 artiklan 9 alakohdassa tarkoitettua aineiden valmistusta ja 14 alakohdassa tarkoitettua aineiden tai seosten jakelua harjoittavat yritykset sekä yritykset, jotka tuottavat mainitun asetuksen 3 artiklan 3 alakohdassa määriteltyjä esineitä aineista tai seoksista
7. Elintarvikelainsäädäntöä koskevista yleisistä periaatteista ja vaatimuksista, Euroopan elintarviketurvallisuusviranomaisen perustamisesta sekä elintarvikkeiden turvallisuuteen liittyvistä menettelyistä annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 178/2002 3 artiklan 2 alakohdassa määritellyt elintarvikeyritykset, jotka harjoittavat tukkukauppaa, teollista tuotantoa tai jalostusta
8. Jätteistä ja tiettyjen direktiivien kumoamisesta annetun Euroopan parlamentin ja neuvoston direktiivin 2008/98/EY 3 artiklan 9 alakohdassa määriteltyä jätehuoltoa harjoittavat yritykset, lukuun ottamatta yrityksiä, joille jätehuolto ei ole niiden pääasiallista taloudellista toimintaa
9. Lääkinnällisistä laitteista, direktiivin 2001/83/EY, asetuksen (EY) N:o 178/2002 ja asetuksen (EY) N:o 1223/2009 muuttamisesta sekä neuvoston direktiivien 90/385/ETY ja 93/42/ETY kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2017/745 2 artiklan 1 alakohdassa määriteltyjä lääkinnällisiä laitteita valmistavat toimijat
10. In vitro -diagnostiikkaan tarkoitetuista lääkinnällisistä laitteista sekä direktiivin 98/79/EY ja komission päätöksen 2010/227/EU kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2017/746 2 artiklan 2 alakohdassa määriteltyjä in vitro -diagnostiikkaan tarkoitettuja lääkinnällisiä laitteita valmistavat toimijat,

lukuun ottamatta tämän lain liitteessä I olevan 13 kohdan e-alakohdassa tarkoitettuja toimijoita
11. NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 26 tarkoitettua tietokoneiden sekä elektronisten ja optisten tuotteiden valmistusta harjoittavat yritykset.
12. NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 27 tarkoitettua sähkölaitteiden valmistusta harjoittavat yritykset
13. NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 28 tarkoitettua muiden koneiden ja laitteiden valmistusta harjoittavat yritykset

2.

Laki

julkisen hallinnon tiedonhallinnasta annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 2 §:n 16 kohta, 3 §, 10 §:n 1 momentin 2 kohta, 18 §:n 1 momentti, sekä

lisätään 1 §:ään uusi 2 momentti, 2 §:ään uusi 17 – 26 kohta sekä lakiin uusi 4 a luku seuraavasti:

1 §

Lain tarkoitus

— —

Tällä lailla pannaan julkishallinnon toimialalla täytäntöön toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 (NIS 2 – direktiivi). NIS 2 – direktiivin täytäntöönpanosta säädetään lisäksi kyberturvallisuuden riskienhallinnasta annetussa laissa (/).

2 §

Määritelmät

Tässä laissa tarkoitetaan:

— —

16) *käsittelysäännöillä* luonnollisen henkilön ennalta laatimia automaattisen tietojenkäsittelyn ohjaamiseen tarkoitettuja sääntöjä;

17) *viestintäverkolla ja tietojärjestelmällä*

a) direktiivin (EU) 2018/1972 2 artiklan 1 alakohdassa määriteltyä sähköistä viestintäverkkoa;

b) laitetta taikka yhteen kytkettyjen tai toisiinsa yhteydessä olevien laitteiden ryhmää, joista yksi tai useampi suorittaa ohjelman avulla digitaalisten tietojen automaattista käsittelyä; tai

c) digitaalisia tietoja, joita a ja b alakohdassa tarkoitetuissa järjestelmissä säilytetään, käsitellään, haetaan tai siirretään näiden järjestelmien toimintaa, käyttöä, suojausta tai ylläpitoa varten;

18) *viestintäverkon ja tietojärjestelmän turvallisuudella* viestintäverkon ja tietojärjestelmien kykyä suojautua tietyllä varmuudella tapahtumilta, jotka saattavat vaarantaa kyseisissä viestintäverkoissa ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden;

19) *kyberturvallisuudella* toimia, joita tarvitaan viestintäverkkojen ja tietojärjestelmien, niiden käyttäjien ja muiden asianosaisten henkilöiden suojaamiseksi kyberuhilta;

20) *kyberuhkalla* potentiaalista tilannetta, tapahtumaa tai toimintaa, joka voi vahingoittaa tai häiritä viestintäverkkoja ja tietojärjestelmiä, tällaisten järjestelmien käyttäjiä ja muita henkilöitä tai muulla tavoin vaikuttaa näihin haitallisesti

21) *merkittävällä kyberuhkalla* kyberuhkaa, jonka voidaan sen teknisten ominaisuuksien perusteella olettaa vaikuttavan mahdollisesti vakavasti viranomaisen verkko- ja tietojärjestelmiin tai sen palvelujen käyttäjiin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa;

22) *riskillä* poikkeaman aiheuttamien menetysten tai häiriön mahdollisuutta, joka ilmaistaan tällaisten menetysten tai häiriön suuruuden ja kyseisen poikkeaman toteutumisen todennäköisyyden yhdistelmänä;

23) *läheltä piti -tilanteella* tapahtumaa, joka olisi voinut vaarantaa verkko- ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden mutta jonka toteutuminen onnistuttiin estämään tai joka ei toteutunut;

24) *poikkeamalla* tapahtumaa, joka vaarantaa viestintäverkoissa ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden;

25) *merkittävällä poikkeamalla* poikkeamaa, joka:

a) on aiheuttanut tai voi aiheuttaa palvelujen vakavan toimintahäiriön tai viranomaiselle taloudellisia tappioita;

b) on vaikuttanut tai voi vaikuttaa luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa;

26) *poikkeaman käsittelyllä* mitä tahansa toimia ja menettelyjä, joilla pyritään ehkäisemään ja havaitsemaan poikkeama, analysoimaan, rajoittamaan tai hallitsemaan sitä ja palautumaan siitä.

3 §

Lain soveltamisala ja sen rajoitukset

Tätä lakia sovelletaan tiedonhallintaan ja tietojärjestelmien käyttöön, kun viranomaiset käsittelevät tietoaineistoja, jollei muualla laissa toisin säädetä. Tämän lain 6 a lukua sovelletaan automaattisen ratkaisumenettelyn käyttöönottoon ja käyttöön. Mitä tässä laissa säädetään viranomaisesta, sovelletaan myös yliopistolaissa (558/2009) tarkoitettuihin yliopistoihin ja ammattikorkeakoululaissa (932/2014) tarkoitettuihin ammattikorkeakouluihin.

Tämän lain 4 a lukua sovelletaan 4 §:n 1 momentin 1 kohdassa tarkoitettuihin valtion virastoihin ja laitoksiin, valtion liikelaitoksiin, 4 §:n 1 momentin 9 kohdassa tarkoitettuihin itsenäisiin julkisoikeudellisiin laitoksiin sekä hyvinvointialueisiin, hyvinvointiyhtymiin ja Helsingin kaupunkiin niiden hoitaessa laissa hyvinvointialueiden järjestämisvastuulle säädettyjä tehtäviä. Lisäksi 4 a lukua sovelletaan [CER-lain] nojalla julkishallinnon toimialan kriittisiksi toimijoiksi määriteltyihin toimijoihin. Tämän lain 4 a lukua ei kuitenkaan sovelleta Puolustusvoimiin, Puolustuskiinteistöihin, poliisin hallinnosta annetussa laissa (110/1992) tarkoitettuihin poliisiyksikköihin, Rajavartiolaitokseen, Tullin rikostorjuntaan, Syyttäjälaitokseen, Suomen Pankkiin eikä

julkisen hallinnon turvallisuusverkkotoiminnasta annetussa laissa (10/2015), jäljempänä *turvallisuusverkkolaki*, tarkoitettuun turvallisuusverkon palvelutuotantoon ja palvelujen käyttöön. Tämän lain 4 a luvun 18 h-18 l §:ää ei sovelleta tasavallan presidentin kansliaan, valtioneuvoston oikeuskanslerin toimintaan eikä Kansaneläkelaitokseen.

Asiankäsittelyssä ja palvelujen tuottamisessa noudatettavista menettelyistä, salassapidosta ja tiedonsaantioikeudesta viranomaisten asiakirjoihin sekä asiakirjojen arkistoinnista säädetään erikseen. Tiedonhallinnasta ja tietojärjestelmien käytöstä Suomen evankelis-luterilaisessa kirkossa säädetään kirkkolaissa (1054/1993).

Tämän lain 19, 20, 26 ja 27 §:ää ei sovelleta tuomioistuimien eikä valitusasioita käsittelemään perustettujen lautakuntien lainkäyttöön. Tämän lain 3 lukua ei sovelleta eduskunnan oikeusasiamiehen eikä valtioneuvoston oikeuskanslerin toimintaan, tuomioistuimien eikä valitusasioita käsittelemään perustettujen lautakuntien toimintaan, tasavallan presidentin kansliaan, eduskunnan virastoihin, Kansaneläkelaitokseen, Suomen Pankkiin, muihin itsenäisiin julkisoikeudellisiin laitoksiin, yliopistolaissa tarkoitettuihin yliopistoihin eikä ammattikorkeakoululaissa tarkoitettuihin ammattikorkeakouluihin. Tämän lain 3 lukua sovelletaan hyvinvointialueisiin, hyvinvointiyhtymiin, kuntiin ja kuntayhtymiin niiden hoitaessa laissa säädettyjä tehtäviä.

Mitä tämän lain 4 luvussa, 22–24 ja 25–27 §:ssä sekä 6 a luvussa säädetään tiedonhallintayksiköstä ja viranomaisesta, sovelletaan yksityisiin henkilöihin tai yhteisöihin taikka muihin kuin viranomaisena toimiviin julkisoikeudellisiin yhteisöihin siltä osin kuin ne hoitavat julkista hallintotehtävää. Yksityisiin henkilöihin ja yhteisöihin sekä muihin kuin viranomaisena toimiviin julkisoikeudellisiin yhteisöihin sovelletaan lisäksi, mitä 4 ja 28 §:ssä säädetään tiedonhallintayksiköstä, niiden käyttäessä julkista valtaa viranomaisten toiminnan julkisuudesta annetun lain 4 §:n 2 momentissa tarkoitetulla tavalla tai kun mainittu laki on säädetty erikseen sovellettavaksi niiden toiminnassa. Edelleen yksityisiin yhteisöihin ja muihin kuin viranomaisena toimiviin julkisoikeudellisiin yhteisöihin sovelletaan, mitä tämän lain 19 §:n 2 momentissa sekä 24 a ja 24 b §:ssä säädetään viranomaisesta niiden käyttäessä julkista valtaa viranomaisten toiminnan julkisuudesta annetun lain 4 §:n 2 momentissa tarkoitetulla tavalla.

Tätä lakia ei sovelleta Ahvenanmaan maakunnassa toimiviin valtion viranomaisiin. Tämän lain 13 a §:ää ja 6 a lukua sovelletaan kuitenkin Ahvenanmaalla toimiviin valtion viranomaisiin niiden hoitaessa sellaisia valtakunnan lainsäädäntövaltaan kuuluvia viranomaistehtäviä, joissa tehdään hallintolain 53 e §:ssä tarkoitettuja asian automaattisia ratkaisuja. Myös 4 a lukua sovelletaan Ahvenanmaan maakunnassa toimiviin valtion viranomaisiin, ellei 2 momentista muuta johdu.

10 §

Julkisen hallinnon tiedonhallintalautakunta

Valtiovarainministeriön yhteydessä toimii julkisen hallinnon tiedonhallintalautakunta (tiedonhallintalautakunta), jonka tehtävänä on:

— —

2) edistää tässä laissa säädettyjen tiedonhallinnan ja tietoturvallisuuden menettelytapojen ja tämän lain vaatimusten toteuttamista, lukuun ottamatta 4 a luvussa säädettyä.

— —

18 §

Turvallisuusluokiteltavat asiakirjat valtionhallinnossa

Valtion virastoissa, laitoksissa ja valtion liikelaitoksissa toimivien viranomaisten, tuomioistuimien ja valitusasioita käsittelemään perustettujen lautakuntien sekä Suomen Erillisverkot

Oy:n ja sen kokonaan omistaman tytäryhtiön niiden hoitaessa turvallisuusverkkolaissa tarkoitettuja tehtäviä on turvallisuusluokiteltava asiakirjat ja tehtävä niihin turvallisuusluokkaa koskeva merkintä sen osoittamiseksi, minkälaisia tietoturvallisuustoimenpiteitä asiakirjaa käsiteltäessä noudatetaan. Turvallisuusluokkaa koskeva merkintä on tehtävä, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2, 5 tai 7–11 kohdan perusteella ja asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle.

— —

4a Luku

Kyberturvallisuusvelvoitteet ja niiden noudattamisen valvonta

18 a §

Toimijajaottelu ja toimintaa koskeva ilmoitus

Tämän luvun soveltamisalaan kuuluvat tiedonhallintayksiköt ovat NIS 2 – direktiivin liitteen I 10 kohdassa tarkoitetun julkishallinnon toimialan (*julkishallinnon toimiala*) keskeisiä toimijoita, lukuun ottamatta hyvinvointialueita ja hyvinvointiyhtymiä sekä Helsingin kaupunkia, jotka ovat tärkeitä toimijoita.

Tiedonhallintayksikön on ilmoitettava Liikenne- ja viestintävirastolle:

1) tiedonhallintayksikön nimi;
2) tiedonhallintayksikön osoite ja ajantasaiset yhteystiedot, mukaan lukien sähköpostiosoite ja puhelinnumero;
3) tiedonhallintayksikön IP-osoitealueet;
4) onko se julkishallinnon toimialan keskeinen vai tärkeä toimija;
5) luettelo muista Euroopan unionin jäsenvaltioista, joissa se tarjoaa palvelujaan;
6) osallistumisesta kyberturvallisuuden riskienhallinnasta annetun lain 22 §:ssä tarkoitettuun kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn.

Tiedonhallintayksikön on viipymättä ja, viimeistään kahden viikon kuluessa muutoksesta ilmoitettava kaikista muutoksista 1 momentin nojalla annettuihin tietoihin.

18 b §

Kyberturvallisuuden riskienhallintavelvoite ja riskienhallinnan toimintamalli

Tiedonhallintayksikön on tunnistettava, arvioitava ja hallittava riskejä, joita kohdistuu sen toiminnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Kyberturvallisuuden riskienhallinnan tarkoitus on suojata viestintäverkkoja ja tietojärjestelmiä, niiden käyttäjiä ja muita henkilöitä kyberuhilta.

Tiedonhallintayksikön on laadittava kyberturvallisuuden riskienhallinnan toimintamalli ja ylläpidettävä sitä. Toimintamallissa tunnistetaan tiedonhallintayksikön viestintäverkkoihin ja tietojärjestelmiin sekä niiden fyysiseen ympäristöön kohdistuvat riskit kaikki vaaratekijät huomioivan lähestymistavan mukaisesti. Lisäksi toimintamallissa on kuvattava kyberturvallisuuden riskienhallinnan tavoitteet, menettelyt ja vastuut sekä 18 c §:ssä tarkoitetut tekniset, operatiiviset ja organisatoriset kyberturvallisuuden riskienhallintatoimenpiteet.

Tiedonhallintayksikön johto vastaa kyberturvallisuuden riskienhallinnan toteuttamisen ja valvonnan järjestämisestä sekä hyväksyy kyberturvallisuuden riskienhallinnan toimintamallin ja

valvoo sen toteuttamista. Tiedonhallintayksikön johdolla tulee olla riittävä perehtyneisyys kyberturvallisuuden riskienhallintaan.

18 c §

Kyberturvallisuuden riskienhallintatoimenpiteet

Tiedonhallintayksikön on toteuttava kyberturvallisuuden riskienhallintatoimenpiteet, jotka ovat asianmukaiset ja oikeasuhtaiset suhteessa käytetyille viestintäverkoille ja tietojärjestelmille aiheutuviin riskeihin, viestintäverkon tai tietojärjestelmän merkitykseen tiedonhallintayksikön toiminnalle sekä niissä ilmenevän poikkeaman yhteiskunnallisiin ja taloudellisiin vaikutuksiin. Lisäksi toimenpiteiden mitoittamisessa on otettava huomioon tiedonhallintayksikön koko, sen toiminnan laatu, poikkeaman todennäköisyys ja vakavuus, toimenpiteistä aiheutuvat kustannukset sekä ajantasainen kehitys huomioiden käytettävissä olevat tekniset mahdollisuudet torjua kyberuhka.

Kyberturvallisuuden riskienhallintatoimenpiteillä tunnistetaan poikkeamariskit, ehkäistään, havaitaan ja hallitaan poikkeamia, palaudutaan niistä ja lievennetään niiden vaikutuksia. Kyberturvallisuuden riskienhallintatoimenpiteillä suojataan viestintäverkkoja ja tietojärjestelmiä ja niiden fyysistä ympäristöä kyberuhkilta ja poikkeamilta sekä minimoidaan poikkeamien vaikutus tiedonhallintayksikön toimintaan, sen palvelujen vastaanottajiin ja muihin palveluihin. Kyberturvallisuuden riskienhallintatoimenpiteisiin on sisällyttävä ainakin seuraavat toimenpidekokonaisuudet:

1) kyberturvallisuuden riskienhallinnan toimintaperiaatteet ja kyberturvallisuuden riskienhallintatoimenpiteiden vaikuttavuuden arviointi;
2) viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet;
3) viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus sekä tarvittavat menettelyt haavoittuvuuksien käsittelyyn ja julkistamiseen;
4) toimitusketjun toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt;
5) omaisuudenhallinta ja turvallisuuden kannalta tärkeiden toimintojen tunnistaminen;
6) henkilöstöturvallisuus ja kyberturvallisuuskoulutus
7) pääsynhallinnan ja todentamisen menettelyt;
8) salausmenetelmien käyttämistä koskevat toimintaperiaatteet ja menettelyt sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttöön;
9) poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden ylläpitämiseksi ja palauttamiseksi;
10) varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan jatkuvuuden hallinta ja tarvittaessa suojattujen varaviestintäjärjestelmien käyttö;
11) perustason kyberhygieniakäytännöt toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi;
12) toimenpiteet viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön suojaamiseksi ja tilaturvallisuuden varmistamiseksi sekä välttämättömien resurssien varmistamiseksi.

[Mahdollinen asetuksenantovaltuus NIS 2 – direktiivin 21 artiklan 5 kohdan 2 alakohdan sekä 24 ja 25 artiklan täytäntöön panemiseksi.

- komission täytäntöönpanosäännökset koskien riskienhallintatoimenpiteitä
- komission täytäntöönpanosäännökset tiettyjen kyberturvallisuusasetuksen mukaisesti sertifioitujen tuotteiden käyttöön velvoittamisesta
- standardien käyttö]

18 d §

Ilmoitusvelvollisuus merkittävästä poikkeamasta

Viranomaisen on ilman aiheetonta viivytystä, viimeistään 24 tunnin kuluessa siitä, kun se on tullut tietoiseksi merkittävästä poikkeamasta, toimitettava Liikenne ja viestintävirastolle poikkeamaa koskeva ensi-ilmoitus, jossa on ilmoitettava, epäilläänkö poikkeaman johtuvan rikoksesta taikka muusta lainvastaisesta tai vihamielisestä teosta ja voiko sillä olla rajat ylittäviä vaikutuksia sekä näiden vaikutusten todennäköisyys.

Viranomaisen on ilman aiheetonta viivytystä, viimeistään 72 tunnin kuluessa siitä, kun se on tullut tietoiseksi merkittävästä poikkeamasta, toimitettava Liikenne- ja viestintävirastolle poikkeamaa koskeva jatkoilmoitus, jossa on ajantasaistettava 1 momentissa tarkoitetut tiedot ja esitettävä ensimmäinen arvio merkittävän poikkeaman laadusta, vakavuudesta ja vaikutuksista sekä vaarantumisindikaattorit, jos sellaisia on saatavilla.

Viranomaisen on viimeistään kuukauden kuluttua jatkoilmoituksesta toimitettava Liikenne- ja viestintävirastolle poikkeamaa koskeva loppuraportti, joka sisältää seuraavat tiedot:

1) yksityiskohtainen kuvaus poikkeamasta, sen vakavuus ja vaikutukset mukaan lukien;
2) poikkeaman todennäköisesti aiheuttaneen uhkan tai juurisyyn tyyppi;
3) toteutetut ja meneillään olevat toimenpiteet vaikutusten lieventämiseksi;
4) mahdolliset rajat ylittävät vaikutukset.

Jos poikkeama on edelleen meneillään, kun 3 momentissa tarkoitettu loppuraportti pitäisi toimittaa, on loppuraportin sijaan toimitettava väliraportti. Loppuraportti on tällöin toimitettava kuukauden kuluessa siitä, kun viranomainen on käsitellyt poikkeaman. Liikenne- ja viestintävirastolla on oikeus poikkeaman kestäessä saada viranomaiselta lisätietoja tai väliraportti asiaan liittyvistä tilannepäivityksistä ja käsittelyn edistymisestä.

[Mahdollinen asetuksenantovaltuus NIS 2 – direktiivin 23 artikla 11 kohdan täytäntöön panemiseksi:

- Komissio voi hyväksyä täytäntöönpanosäädöksiä, joissa täsmennetään tämän artiklan 1 kohdan (ilmoitusvelvollisuus merkittävästä poikkeamasta valvovalle viranomaiselle ja palvelujen käyttäjille) ja 30 artiklan nojalla tehtävän (vapaaehtoisen) ilmoituksen sekä tämän artiklan 2 kohdan nojalla annettavan tiedonannon (tiedotusvelvollisuus palvelujen vastaanottajille merkittävästä kyberuhkasta) tietosisältö, muoto ja ilmoitusmenettely.]

18 e §

Poikkeamailmoituksen vastaanottaminen

Liikenne- ja viestintäviraston on ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 24 tunnin kuluessa 18 d §:n 1 momentissa tarkoitetun ensi-ilmoituksen vastaanottamisesta annettava viranomaiselle vastaus. Vastauksessa on oltava alustava palaute merkittävästä poikkeamasta, viranomaisen pyynnöstä ohjeita tai operatiivisia neuvoja koskien poikkeaman käsittelyä sekä ohjeet merkittävän poikkeaman ilmoittamisesta esitutkintaviranomaiselle, jos asiassa epäillään rikosta.

18 f §

Vapaaehtoinen ilmoittaminen

Viranomainen voi ilmoittaa Liikenne- ja viestintävirastolle myös muista kuin merkittävistä poikkeamista sekä kyberuhkista ja läheltä piti –tilanteista. Myös muut tämän lain 3 §:ssä mainitut, joihin tätä lukua ei sovelleta, voivat ilmoittaa poikkeamista, kyberuhkista ja läheltä piti –tilanteista Liikenne- ja viestintävirastolle.

Liikenne- ja viestintäviraston on käsiteltävä 1 momentissa tarkoitetut vapaaehtoiset ilmoitukset 18 e §:ssä säädettyä menettelyä noudattaen. Liikenne- ja viestintävirasto voi asettaa 18 d §:ssä tarkoitettujen ilmoitusten käsittelyn etusijalle vapaaehtoisten ilmoitusten käsittelyyn nähden.

Viranomainen ja muut lain 3 §:ssä mainitut voivat vapaaehtoisen ilmoituksen yhteydessä luovuttaa Liikenne- ja viestintävirastolle tietoja, jotka Liikenne- ja viestintävirastolla on oikeus saada 18 i §:n 1 ja 2 momentin nojalla. Tietojen luovuttamiseen sovelletaan myös, mitä 18 i §:n 3 momentissa säädetään.

18 g §

Tiedotusvelvollisuus merkittävästä kyberuhkasta ja poikkeamasta

Viranomaisen on ilmoitettava viipymättä merkittävästä poikkeamasta palvelujensa vastaanottajille, jos merkittävä poikkeama todennäköisesti haittaa sen palvelujen tarjoamista.

Viranomaisen on ilmoitettava viipymättä merkittävästä kyberuhkasta sekä kyberuhkan hallitsemiseksi käytettävissä olevista toimenpiteistä niille palvelujensa vastaanottajille, joihin merkittävä kyberuhka saattaa vaikuttaa.

Jos merkittävän poikkeaman julkistaminen on yleisen edun mukaista, Liikenne- ja viestintävirasto voi velvoittaa viranomaisen tiedottamaan merkittävästä poikkeamasta tai kuultuaan viranomaista tiedottaa asiasta itse.

18 h §

Toimivaltainen viranomainen

Liikenne- ja viestintävirasto on NIS 2 – direktiivin 8 artiklan 1 kohdassa tarkoitettu toimivaltainen viranomainen julkishallinnon toimialalla. Liikenne- ja viestintäviraston tehtävänä on sen lisäksi mitä edellä tässä luvussa säädetään poikkeamailmoitusten käsittelystä, valvoa tässä luvussa ja tämän luvun tai NIS 2 – direktiivin nojalla annetuissa säädöksissä säädettyjen velvoitteiden noudattamista julkishallinnon toimialalla sekä ylläpitää julkishallinnon toimialan toimijaluetteloa 18 a §:n nojalla toimitetuista tiedoista.

Liikenne- ja viestintäviraston on valvontatoimiaan suorittaessaan ja 18 l §:ssä tarkoitettua valvontapäätöstä tehdessään otettava huomioon NIS 2 – direktiivin 32 artiklan 7 kohdassa säädetyt seikat. Liikenne- ja viestintävirasto voi asettaa tässä laissa säädetyt valvontatehtävänsä tärkeysjärjestykseen soveltaen riskiperusteista lähestymistapaa. Liikenne- ja viestintävirasto voi kohdistaa valvontaa hyvinvointialueeseen, hyvinvointiyhtymään tai Helsingin kaupunkiin vain, jos on perusteltu syy epäillä, että mainittu ei ole noudattanut tässä luvussa taikka tämän luvun tai NIS 2 – direktiivin nojalla annetuissa säädöksissä säädettyä.

Ellei tässä luvussa toisin säädetä, Liikenne- ja viestintäviraston on 18 a §:ssä tarkoitettujen toimintaa koskevien ilmoitusten, 18 d ja f §:ssä tarkoitettujen poikkeamailmoitusten ja muiden valvontatehtävässä saatujen tietojen käsittelyssä sekä yhteistyössä NIS 2 – direktiivissä tarkoitettujen muiden viranomaisten, Euroopan unionin toimielinten, erillisvirastojen ja yhteistyöelinten kanssa sekä tietojen luovuttamisessa niille noudatettava mitä kyberturvallisuuden riskienhallinnasta annetun lain [6 §:n 4 momentissa, 15 §:n 3 momentissa, 17 §:ssä, 25 §:n 3 momentissa, 27 §:n 2 momentissa, 34 §:ssä, 43 §:n 4 momentissa ja 46 §:ssä] säädetään tietojen käsittelystä valvovassa viranomaisessa sekä valvovan viranomaisen yhteistyöstä NIS 2 – direktiivissä tarkoitettujen muiden viranomaisten, Euroopan unionin toimielinten, erillisvirastojen ja yhteistyöelinten kanssa sekä tietojen luovuttamisesta niille. NIS 2 – direktiivissä tarkoitetusta keskistetystä yhteyspisteestä ja CSIRT-yksiköstä ja niiden tehtävistä, tietojen käsittelystä sekä

yhteistyöstä NIS 2 – direktiivissä tarkoitettujen muiden viranomaisten, Euroopan unionin toimielinten, erillisvirastojen ja yhteistyöelinten kanssa säädetään kyberturvallisuuden riskienhallinnasta annetussa laissa.

18 i §

Toimivaltaisen viranomaisen tiedonsaantioikeus

Liikenne- ja viestintävirastolla on tämän luvun mukaisia tehtäviä suorittaessaan oikeus saada salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä tehtäviensä suorittamiseksi välttämättömät tiedot viranomaiselta, johon sovelletaan tätä lukua. Viranomaisen on luovutettava tiedot viipymättä, pyydetyssä muodossa ja maksutta.

Liikenne- ja viestintävirastolla on oikeus saada salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä viranomaiselta välitystieto, sijaintitieto tai haitallisen tietokoneohjelman tai käskyn sisältävä viesti, jos se on välttämätöntä 18 b ja c §:ssä säädettyjen kyberturvallisuuden riskienhallintavelvoitteiden noudattamisen valvomiseksi tai merkittävän poikkeaman selvittämiseksi. Mainittujen tietojen käsittelyyn Liikenne- ja viestintävirastossa sovelletaan mitä sähköisen viestinnän palveluista annetun lain (917/2014) 316 §:n 4 momentissa ja 319 §:ssä säädetään Liikenne- ja viestintäviraston viestistä, välitystiedosta, sijaintitiedosta sekä luottamuksellisen radiolähetyksen sisällöstä ja olemassaolosta saamien ja hankkimien tietojen salassapidosta, luovuttamisesta ja hävittämisestä.

Tässä pykälässä säädetty tiedonsaantioikeus ei velvoita luovuttamaan Liikenne- ja viestintävirastolle tietoja turvallisuusverkkolaissa tarkoitetusta turvallisuusverkon palvelutuotannosta tai palvelujen käytöstä eikä tietoja, joiden luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin niihin liittyvää tärkeää etua. Viranomainen voi viranomaisten toiminnan julkisuudesta annetun lain julkisuus- tai salassapito-olettaman sisältävän salassapitosäännöksen osoittamissa rajoissa luovuttaa Liikenne- ja viestintävirastolle tietoja myös turvallisuusverkon palvelutuotannosta ja palvelujen käytöstä sekä maanpuolustukseen ja kansalliseen turvallisuuteen liittyviä tietoja, jotka ovat yleisöltä salassa pidettäviä. Jos tällainen asiakirja tai siihen sisältyvä tieto on turvallisuusluokiteltu, asiakirjan tai tiedon antamisesta päättää asiakirjan laatinut viranomainen tai viranomainen, jonka käsiteltäväksi asia kokonaisuudessaan kuuluu. Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitetun erityissuojattavan tietoaineiston käsittelyssä on noudatettava mitä mainitussa laissa säädetään.

18 j §

Tarkastusoikeus

Liikenne- ja viestintävirastolla on siinä laajuudessa kuin se on tarpeen, oikeus tehdä tässä luvussa taikka tämän luvun tai NIS 2 – direktiivin nojalla annetuissa säädöksissä säädettyjen velvoitteiden noudattamisen valvomiseksi viranomaiseen kohdistuva tarkastus.

Tarkastuksen suorittajalla on oltava tarkastuksen laatuun ja laajuuteen nähden riittävä koulutus ja kokemus.

Tarkastusta suorittavalla on tarkastuksen suorittamiseksi oikeus päästä muihin kuin pysyväisluonteiseen asumiseen tarkoitettuihin tiloihin ja tarkastuksen kohteena olevaan viestintäverkkoon tai tietojärjestelmään sekä oikeus salassapitosäännösten estämättä saada tutkittavakseen tarkastustehtävän kannalta tarpeelliset tiedot, asiakirjat, laitteet ja ohjelmistot, suorittaa tarvittavia testejä ja mittauksia sekä tarkastaa viranomaisen toteuttamat turvallisuusjärjestelyt. Tarkastuksessa noudatettavaan menettelyyn sovelletaan, mitä hallintolain 39 §:ssä säädetään tarkastuksesta.

Tarkastuksen suorittajan tarkastus- ja tiedonsaantioikeuteen sovelletaan mitä 18 i §:n 3 momentissa säädetään tiedonsaantioikeuden rajoituksista.

18 k §

Avustavan tehtävän antaminen hyväksytylle arviointilaitokselle ja arvioinnin teettäminen

Liikenne- ja viestintävirasto voi antaa 18 j §:ssä tarkoitettuun tarkastustehtävään liittyvän avustavan tehtävän tietoturvallisuuden arviointilaitoksista annetussa laissa (1405/2011) tarkoitetulle hyväksytylle tietoturvallisuuden arviointilaitokselle (*hyväksytty arviointilaitos*).

Liikenne- ja viestintävirasto voi valvonnan toteuttamiseksi velvoittaa viranomaisen teettämään hyväksytyn arviointilaitoksen suorittaman kyberturvallisuuden riskienhallintaan kohdistuvan arvioinnin, jos

1) viranomaiseen on kohdistunut merkittävä poikkeama, joka on aiheuttanut palvelujen vakavan toimintahäiriön tai huomattavaa aineellista tai aineetonta vahinkoa; tai

2) viranomainen on olennaisesti ja vakavasti laiminlyönyt 18 b tai c §:ssä tarkoitettujen kyberturvallisuuden riskienhallintavelvoitteiden noudattamisen.

Hyväksytyn arviointilaitoksen palveluksessa olevaan tarkastuksen tai arvioinnin suorittajaan sovelletaan, mitä 18 j §:n 2–4 momentissa säädetään tarkastuksen suorittajan kokemuksesta ja koulutuksesta sekä tarkastuksen suorittajan oikeuksista. Hyväksytyn arviointilaitoksen palveluksessa olevaan henkilöön sovelletaan hänen tässä pykälässä tarkoitettuja tehtäviä hoitaessaan virkamiehen rikosoikeudellista virkavastuuta koskevia säännöksiä, viraltapanoseuraamusta lukuun ottamatta. Vahingonkorvausvastuusta säädetään vahingonkorvauslaissa.

18 l §

Seuraamukset

Liikenne- ja viestintävirasto voi päätöksellään velvoittaa viranomaisen määräajassa korjaamaan puutteet tässä luvussa taikka tämän luvun tai NIS 2 – direktiivin nojalla annetuissa säädöksissä säädettyjen velvoitteiden noudattamisessa. Liikenne- ja viestintävirasto voi velvoittaa viranomaisen julkistamaan kyseiset puutteet tai muut seikat, jotka liittyvät mainittujen säännösten rikkomiseen.

Liikenne- ja viestintävirasto voi antaa viranomaiselle huomautuksen tai varoituksen. Varoituksen voi antaa, jos huomautusta ei asiasta ilmenevät seikat kokonaisuudessaan huomioiden voida pitää riittävänä.

Liikenne- ja viestintävirasto voi asettaa uhkasakon 1 momentissa tarkoitetun päätöksen toteuttamisen tehosteeksi. Uhkasakosta säädetään uhkasakkolaissa (1113/1990).

18 m §

Muutoksenhaku

Liikenne- ja viestintäviraston tämän luvun nojalla tekemään päätökseen saa vaatia oikaisua. Oikaisuvaatimusmenettelystä säädetään hallintolain 7 a luvussa.

Muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).

Tämä laki tulee voimaan [18] päivänä [loka]kuuta 2024.

Tämän lain 18 a §:n 2 momentissa tarkoitettu ilmoitus on tehtävä viimeistään 31 päivänä joulukuuta 2024.

_____

3.

Laki

sähköisen viestinnän palveluista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan sähköisen viestinnän palveluista annetun lain (917/2014) 1 luvun 2 §:n 2 momentti ja 29 luvun 247 a §, sellaisina kuin ne ovat, 1 luvun 2 §:n 2 momentti laissa 1207/2020 ja 29 luvun 247 a § laissa 281/2018, sekä

muutetaan 21 luvun 165 §:n 1 momentti, 167 ja 170 §, 33 luvun 275 §, 38 luvun 308 §:n 3 momentti, 39 luvun 313 §:n 2 momentin 2 kohta, 40 luvun 318 §:n 4 momentti, sellaisina kuin ne ovat, 21 luvun 165 §:n 1 momentti ja 170 §, 38 luvun 308 §:n 3 momentti sekä 39 luvun 313 §:n 2 momentin 2 kohta laissa 1003/2018, 21 luvun 167 § laeissa 1003/2018 ja 1207/2020 sekä 33 luvun 275 § ja 40 luvun 318 §:n 4 momentti laissa 1207/2020, sekä

lisätään 21 luvun 165 §:ään uusi 4 momentti ja 29 luvun 247 §:ään uusi 5 momentti seuraavasti:

165 §

Verkkotunnusvälittäjän ilmoitusvelvollisuudet

Verkkotunnusvälittäjän on ennen toimintansa aloittamista tehtävä ilmoitus verkkotunnusrekisteriä hallinnoivalle viranomaiselle. Ilmoituksessa on oltava seuraavat tiedot:

a) verkkotunnusvälittäjän nimi, y-tunnus tai sellaisen puuttuessa muu yksilöivä tieto sekä kuulemisiin ja tiedoksiantoihin käytettävä sähköpostiosoite;
b) verkkotunnusvälittäjän päätoimipaikan ja muiden unionissa sijaitsevien laillisten toimipaikkojen osoite ja ajantasaiset yhteystiedot tai, jos verkkotunnusvälittäjä ei ole sijoittautunut Euroopan unioniin, sen Euroopan unioniin nimetyn edustajan osoite, sähköpostiosoitteet, puhelinnumerot ja muut ajantasaiset yhteystiedot;
c) verkkotunnusvälittäjän IP-osoitealueet;
d) luettelo EU-jäsenvaltioista, joissa verkkotunnusvälittäjä tarjoaa palveluja; ja
e) muut valvonnan kannalta tarpeelliset tiedot.

Verkkotunnusvälittäjän ilmoittamissa tiedoissa tapahtuneista muutoksista on viipymättä ilmoitettava Liikenne- ja viestintävirastolle. Toiminnan lopettamisesta on ilmoitettava Liikenne- ja viestintävirastolle ja asiakkaille viimeistään kaksi viikkoa etukäteen. Liikenne- ja viestintäviraston 171 §:n 2 momentin nojalla tekemästä kieltopäätöksestä on ilmoitettava asiakkaille viipymättä.

Tarkempia määräyksiä ilmoituksen tekemisestä ja sen sisällöstä voidaan antaa Liikenne- ja viestintäviraston määräyksellä.

Liikenne- ja viestintäviraston on toimitettava toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2022/2555 (jäljempänä *NIS 2-direktiivi*) 27 artiklan 4 kohdassa tarkoitetun ilmoituksen tekemiseksi tarpeelliset tiedot verkkotunnusvälittäjien ilmoituksista kyberturvallisuuden riskienhallinnasta annetun lain (/) 18 §:ssä tarkoitetulle keskitetylle yhteyspisteelle.

— —

167 §

Tietojen merkitseminen verkkotunnusrekisteriin ja tietojen julkaiseminen

Verkkotunnus on merkittävä verkkotunnuksen käyttäjän nimiin. Verkkotunnuksen käyttäjän on ilmoitettava verkkotunnusvälittäjälle oikeat, ajantasaiset ja yksilöivät käyttäjä- ja yhteystiedot sekä niissä tapahtuvat muutokset. Verkkotunnusvälittäjän tai sen puolesta toimivan, on merkittävä verkkotunnusrekisteriin verkkotunnuksen käyttäjää sekä rekisteröityä verkkotunnusta koskevat oikeat, ajantasaiset ja yksilöivät tiedot sekä kuulemisiin ja tiedoksiantoihin käytettävä sähköpostiosoite.

Liikenne- ja viestintävirasto voi estää verkkotunnuksen rekisteröinnin verkkotunnusrekisteriin, jos se epäilee 1 momentissa tarkoitettujen tietojen olevan puutteellisia tai virheellisiä eikä verkkotunnusvälittäjä kehotuksesta huolimatta todenna tietoja oikeiksi määräajassa. Liikenne- ja viestintävirasto asettaa julkisesti saataville käytössään olevat käyttäjätietojen oikeellisuuden varmistamista koskevat toimintaperiaatteet ja menettelyt.

Liikenne- ja viestintävirasto julkaisee ilman aiheetonta viivytystä internet-sivuillaan tai muussa sähköisessä palvelussa verkkotunnusrekisterin tiedot. Henkilötietojen suojasta säädetään luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) 2016/679 (yleinen tietosuoja-asetus) ja sitä täydentävässä tietosuojalaissa. Liikenne- ja viestintäviraston on vastattava verkkotunnusten rekisteritietoihin pääsyä koskevaan pyyntöön ilman aiheetonta viivytystä ja viimeistään 72 tunnin kuluessa pyynnön vastaanottamisesta. Rekisterin tietojen luovuttamiseen sovelletaan muutoin viranomaisten toiminnan julkisuudesta annetun lain 16 §:ää. Liikenne- ja viestintävirasto asettaa julkisesti saataville käytössään olevat toimintaperiaatteet ja menettelyt verkkotunnusten rekisteröintitietojen luovuttamisesta.

Verkkotunnusrekisteriin merkitty verkkotunnus on voimassa enintään viisi vuotta. Verkkotunnusvälittäjä voi uudistaa verkkotunnusta koskevan merkinnän enintään viideksi vuodeksi kerrallaan.

Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä merkitsemisen teknisestä toteuttamistavasta ja merkitsemisen yhteydessä ilmoitettavista tiedoista sekä verkkotunnuksen käyttäjän tunnistamisesta ja verkkotunnuksen käyttäjän tietojen varmistamisesta.

— —

170 §

Verkkotunnusvälittäjän muut velvollisuudet

Verkkotunnusvälittäjän on:

1) tarjottava ennen verkkotunnuksen merkitsemistä tämän lain mukaiset tarvittavat tiedot verkkotunnuksen sisältöön ja muotoon liittyvistä edellytyksistä;

2) pidettävä verkkotunnusrekisteriin merkityt tiedot ajantasaisina;

3) kyettävä merkitsemään tietoja verkkotunnusrekisteriin Liikenne- ja viestintäviraston määrittelemällä teknisellä järjestelyllä;

4) tiedotettava verkkotunnuksen käyttäjää riittävästi ja tehokkaasti verkkotunnuksen voimassaoloajan päättymisestä;

5) poistettava verkkotunnus verkkotunnusrekisteristä verkkotunnuksen käyttäjän pyynnöstä ennen voimassaoloajan päättymistä;

6) huolehdittava toimintansa tietoturvasta;
7) ilmoitettava viipymättä Liikenne- ja viestintävirastolle, jos sen verkkotunnusten välitystoimintaan kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus taikka muu tapahtuma, joka estää tai häiritsee sitä olennaisesti; samalla on myös ilmoitettava häiriön tai sen uhan arvioitu kesto ja vaikutukset, korjaustoimenpiteet sekä ne toimenpiteet, joilla häiriön toistuminen pyritään estämään;
8) asetettava julkisesti saataville toimintaperiaatteet ja menettelyt, joilla varmistetaan verkkotunnusrekisterin tietojen olevan 167 §:n 1 momentin mukaiset;
9) asetettava muut verkkotunnuksen rekisteröintitiedot kuin henkilötiedot julkisesti saataville ilman aiheetonta viivytystä;
10) annettava pääsy verkkotunnusten rekisteröintitietoihin tietosuojalainsäädännön mukaisesti ja maksuttomasti sekä vastattava rekisteritietoihin pääsyä oikeutetusti pyytävälle ilman aiheetonta viivytystä ja viimeistään 72 tunnin kuluessa lainmukaisen ja asianmukaisesti perustellun pyynnön vastaanottamisesta;
11) asetettava julkisesti saataville toimintaperiaatteet ja menettelyt verkkotunnusten rekisteröintitietojen luovuttamisesta.

Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä verkkotunnuksen käyttäjälle annettavista tiedoista, julkisesti saataville asetettavista tiedoista, pääsyn antamisesta tietoihin sekä toimintaperiaatteista ja menettelyistä, toiminnan tietoturvallisuudesta sekä siitä, milloin 1 momentin 7 kohdassa tarkoitettu häiriö on merkittävä sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

DNS-palveluntarjoajan velvollisuudesta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja poikkeamien ilmoittamisesta säädetään kyberturvallisuuden riskienhallinnasta annetussa laissa (/).

— —

247 §

Viestinnän välittäjän ja lisäarvopalvelun tarjoajan velvollisuus huolehtia tietoturvasta

— —

Tietoturvasta huolehtimiseen sovelletaan lisäksi, mitä kyberturvallisuuden riskienhallinnasta annetussa laissa (/) säädetään sellaisen viestinnän välittäjän ja lisäarvopalvelun tarjoajan osalta, joka kuuluu NIS 2-direktiivin soveltamisalaan.

275 §

Häiriöilmoitukset Liikenne- ja viestintävirastolle

Teleyrityksen on ilmoitettava viipymättä Liikenne- ja viestintävirastolle, jos sen palveluun kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus taikka muu tapahtuma, joka estää viestintäpalvelun toimivuuden tai häiritsee sitä olennaisesti. Teleyrityksen on ilmoitettava myös ilman aiheetonta viivästystä häiriön tai sen uhan arvioitu kesto ja vaikutukset, korjaustoimenpiteet sekä ne toimenpiteet, joilla häiriön toistuminen pyritään estämään.

Jos häiriöistä ilmoittaminen on yleisen edun mukaista, Liikenne- ja viestintävirasto voi velvoittaa teleyrityksen tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.

Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä 1 momentissa tarkoitettujen ilmoitusten sisällöstä, muodosta ja toimittamisesta.

Liikenne- ja viestintäviraston on arvioitava, koskeeko 1 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille. Edellä 1 momentissa tarkoitetusta häiriöstä on lisäksi tarvittaessa ilmoitettava Euroopan unionin kyberturvallisuusvirastolle. Häiriöilmoituksiin sovelletaan lisäksi, mitä kyberturvallisuuden riskienhallinnasta annetussa laissa säädetään poikkeamailmoituksista.

308 §

Yhteistyö eri viranomaisten kanssa

— —

Liikenne- ja viestintäviraston on toimittava yhteistyössä muiden Euroopan unionin jäsenvaltioiden verkko- ja tietoturvallisuutta valvovien viranomaisten, tietoturvaloukkauksiin reagoivien yksiköiden sekä NIS 2-direktiivin 14–16 artiklassa tarkoitetun yhteistyöryhmän, CSIRT-verkoston ja Euroopan kyberkriisien yhteysorganisaatioiden verkoston kanssa.

313 §

Valvonta-asioiden käsittely Liikenne- ja viestintävirastossa

— —

2) asialla on epäillystä virheestä tai laiminlyönnistä huolimatta viestintämarkkinoiden toimivuuden, viestintäpalvelujen luotettavuuden tai sähköisen viestinnän häiriöttömyyden turvaamisen ja palveluja käyttävien edun kannalta vain vähäinen merkitys; tai

— —

318 §

Tietojen luovuttaminen viranomaisesta

— —

Liikenne- ja viestintäministeriöllä ja Liikenne- ja viestintävirastolla on oikeus luovuttaa salassa pidettävä asiakirja sekä ilmaista salassa pidettävä tieto komissiolle, Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelimelle ja toisen ETA-valtion valvontaviranomaiselle, jos se on viestintämarkkinoiden valvonnan kannalta välttämätöntä. Liikenne- ja viestintävirastolla on oikeus luovuttaa 170 §:n 1 momentin 7 kohdan, 171 §:n ja 275 §:n 1 momentin nojalla saamansa salassa pidettävä asiakirja sekä ilmaista salassa pidettävä tieto toisen ETA-valtion valvontaviranomaiselle, NIS 2-direktiivin 14 artiklassa tarkoitetulle yhteistyöryhmälle ja NIS 2-direktiivin 15 artiklassa tarkoitetulle CSIRT-verkostolle, jos se on verkko- ja tietoturvallisuuden valvonnan kannalta välttämätöntä, eikä luovuttaminen vaaranna mainituissa pykälissä tarkoitettujen toimijoiden turvallisuuteen ja liikesalaisuuksiin liittyviä etuja tai annettujen tietojen luottamuksellisuutta.

— —

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

4.

Laki

ilmailulain 128 a §:n ja 128 b §:n kumoamisesta

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Tällä lailla kumotaan ilmailulain (864/2014) 128 a § ja 128 b §.

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

5.

Laki

raideliikennelain 169 §:n kumoamisesta

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Tällä lailla kumotaan raideliikennelain (1302/2018) 169 §.

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

6.

Laki

liikenteen palveluista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan liikenteen palveluista annetun lain (320/2017) 18 luvun 161 §, sellaisena kuin se on laissa 1256/2020, sekä

muutetaan 15 luvun 140 §, sellaisena kuin se on laeissa 579/2018, 984/2018 ja 371/2019 seuraavasti:

140 §

Tietoturva tieliikenteen ohjaus- ja hallintapalvelussa

Tieliikenteen ohjaus- ja hallintapalvelun tarjoajan velvollisuudesta huolehtia käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja poikkeamien ilmoittamisesta säädetään kyberturvallisuuden riskienhallinnasta annetussa laissa (/)

Tieliikenteen ohjaus- ja hallintapalvelun tarjoajan on tallennettava ja säilytettävä tieliikenteen tilannekuva tavalla, joka turvaa tallenteet oikeudettomalta puuttumiselta. Tallenteita on säilytettävä 14 vuorokautta.

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

7.

Laki

alusliikennepalvelulain 18 a §:n kumoamisesta

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Tällä lailla kumotaan alusliikennepalvelulain (/) 18 a §.

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

8.

Laki

eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain 7 e ja 7 f §:n kumoamisesta.

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Tällä lailla kumotaan eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain (485/2004) 7 e ja 7 f §.

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

9.

Laki

sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain (703/2023) 90 §:n 4 momentti, sekä

muutetaan 2 §:n 3 momentti ja 90 §:n 2 ja 3 momentti

seuraavasti:

2 §

Soveltamisala ja suhde muuhun lainsäädäntöön

— —

Tässä lailla annetaan toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta annettua Euroopan parlamentin ja neuvoston direktiiviä (EU) 2022/2555 (*NIS 2 –direktiivi*) ja kyberturvallisuuden riskienhallinnasta annettua lakia (/) täydentävät ja täsmentävät säännökset käsiteltäessä sosiaali- ja terveydenhuollon asiakastietoja ja asiakkaan itsensä tuottamia hyvinvointitietoja sosiaali- ja terveyspalveluiden järjestämisen ja toteuttamisen käyttötarkoituksissa.

90 §

Ilmoittaminen tietojärjestelmän ja hyvinvointisovelluksen olennaisten vaatimusten poikkeamista sekä tietoverkkoihin kohdistuvista tietoturvallisuuden häiriöistä

— —

Terveydenhuollon palvelunantajan velvoitteista ilmoittaa tietoturvallisuuden häiriöstä säädetään kyberturvallisuuden riskienhallinnasta annetun lain 11–14 §:ssä. Sosiaalihuollon palvelunantajan, apteekin, Kansaneläkelaitoksen ja tietojärjestelmäpalvelun tuottajan tai tietojärjestelmän valmistajan tai välittäjän on ilmoitettava viipymättä Sosiaali- ja terveysalan lupa- ja valvontavirastolle sellaisesta sen käyttämiin käyttöympäristöihin ja tietoverkkoihin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena tietojärjestelmien käyttö ja sosiaalipalveluiden toteuttaminen voi merkittävästi vaarantua. Terveyden ja hyvinvoinnin laitos voi antaa tarkempia määräyksiä siitä, milloin häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

Jos 1 ja 2 momentissa tarkoitetusta tietoturvallisuuteen liittyvästä poikkeamasta tai häiriöstä ilmoittaminen on yleisen edun mukaista, Sosiaali- ja terveysalan lupa- ja valvontavirasto voi velvoittaa sosiaalihuollon palvelunantajan, apteekin, Kansaneläkelaitoksen, tietojärjestelmäpalvelun tuottajan tai tietojärjestelmän valmistajan taikka välittäjän tiedottamaan yleisölle asiasta taikka kuultuaan ilmoitusvelvollista tiedottaa asiasta itse

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

10.

Laki

sähkömarkkinalain muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan sähkömarkkinalain (588/2013) 29 a § sekä 49 a §:n 5 momentti, sellaisena kuin ne ovat, 29 a § laissa 287/2018 ja 49 a §:n 5 momentti laissa 108/2019, sekä

muutetaan 62 §:n 1 momentti, sellaisena kuin se on laissa 497/2023

seuraavasti:

62 §

Suljettua jakeluverkkoa koskevat erityissäännökset

Suljettuun jakeluverkkoon ja suljetun jakeluverkonhaltijaan ei sovelleta 23 eikä 26 a §:ää, 27 §:n 3 momenttia, 28, 29, 50–53, 53 a, 54–57, 57 a, 58 eikä 59 §:ää.

— —

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

11.

Laki

maakaasumarkkinalain 34 a §:n kumoamisesta

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Tällä lailla kumotaan maakaasumarkkinalain (587/2017) 34 a §.

———

Tämä laki tulee voimaan päivänä kuuta 20 .

—————

12.

Laki

Energiavirastosta annetun lain 1 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

lisätään Energiavirastosta annetun lain (870/2013) 1 §:n 2 momenttiin, sellaisena kuin se on osaksi laeissa 634/2020, 804/2020, 606/2021 ja 500/2023, uusi 21 kohta

seuraavasti:

1 §

Tehtävät

— —

Energiavirasto hoitaa tehtävät, jotka sille on annettu:

— —

21) kyberturvallisuuden riskienhallinnasta annetussa laissa (/);

— —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

—————

13.

Laki

sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain 28 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain (590/2013) 28 §:n 1 momentin 1 kohta, sellaisena kuin se on laissa 1002/2018

seuraavasti:

28 §

Energiaviraston oikeus luovuttaa tietoja toiselle viranomaiselle

— —

1) Finanssivalvonnalle, Kilpailu- ja kuluttajavirastolle ja kuluttaja-asiamiehelle niiden tehtävien hoitamista varten;

— —

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

14.

Laki

vesihuoltolain 35 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Tällä lailla kumotaan vesihuoltolain (119/2001) 35 §:n 2 momentin 3 kohta.

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

Helsingissä x.x.20xx

Pääministeri

Etunimi Sukunimi

..ministeri Etunimi Sukunimi