HE 57/2024 vp

Hallituksen esitys eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan säädettäväksi kyberturvallisuuslaki. 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 maakaasumarkkinoiden valvonnasta annettua lakia, vesihuoltolakia, sakon täytäntöönpanosta annettua lakia, maa-asemista ja eräistä tutkista annettua lakia ja vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annettua lakia.

Ehdotetuilla laeilla pantaisiin täytäntöön EU:n kyberturvallisuusdirektiivi. 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.

Direktiivi ehdotetaan pantavaksi täytäntöön säätämällä edellytetyistä velvollisuuksista keskitetysti uudessa kyberturvallisuuslaissa. Julkisen sektorin osalta velvoitteista säädettäisiin myös julkisen hallinnon tiedonhallinnasta annetussa laissa. Samalla kumottaisiin nykyisin voimassa olevat kumotun verkko- ja tietoturvallisuusdirektiivin täytäntöönpanosäännökset useista laeista. Valvonnan järjestämisessä jatkettaisiin sektorikohtaisesti hajautettua mallia. Laissa säädettäisiin myös tietoturvaloukkauksia tutkivasta ja niihin reagoivasta yksiköstä, joka sijaitsisi Liikenne- ja viestintävirastossa, sekä kansallisesta kyberturvallisuusstrategiasta ja kyberkriisinhallintakehyksestä. Direktiivin täytäntöönpano ehdotetaan tehtäväksi sen vähimmäistason mukaisesti ja kansallinen liikkumavara täysimääräisesti hyödyntäen.

Pääministeri Petteri Orpon hallituksen hallitusohjelman mukaan kyberturvallisuutta ja sitä koskevaa yhteistyötä viranomaisten ja elinkeinoelämän välillä vahvistetaan, hallitus parantaa tietoturvaa kriittisillä toimialoilla ja EU-lainsäädännön toimeenpanon yhteydessä vältetään kansallista lisäsääntelyä.

Lait on tarkoitettu tulemaan voimaan 18.10.2024.

SISÄLLYS

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ 1
PERUSTELUT 7
1 Asian tausta ja valmistelu 7
1.1 Tausta 7
1.2 Valmistelu 8
1.2.1 EU-säädöksen valmistelu 8
1.2.2 Hallituksen esityksen valmistelu 9
2 EU-säädöksen tavoitteet ja pääasiallinen sisältö 10
2.1 Tavoitteet 10
2.2 Soveltamisala 11
2.3 Keskeiset ja tärkeät toimijat 13
2.4 Toimijaluettelo ja toimijoiden rekisteri 14
2.5 Riskienhallintavelvoitteet 14
2.6 Raportointivelvoitteet 16
2.7 Valvonta ja hallinnolliset sanktiot 19
2.8 Viranomaisyhteistyö 20
2.8.1 CSIRT-yksiköt 20
2.8.2 Koordinoitu haavoittuvuuden julkistaminen ja haavoittuvuustietokanta 20
2.8.3 Keskitetty yhteyspiste 21
2.8.4 CSIRT-verkosto, NIS yhteistyöryhmä ja EU-CyCLONe 21
2.9 Kyberturvallisuusstrategia ja kansalliset kyberkriisinhallintakehykset 21
2.10 Verkkotunnusten rekisteröintitietojen tietokanta 22
2.11 Kyberturvallisuustietojen jakamisjärjestelyt 22
2.12 Kansallinen liikkumavara 23
3 Nykytila ja sen arviointi 24
3.1 NIS1-direktiivin täytäntöönpano 24
3.2 Energia 25
3.2.1 Sähkö 25
3.2.2 Öljy 26
3.2.3 Maakaasu 26
3.2.4 Kaukolämmitys ja –jäähdytys 26
3.2.5 Vety 27
3.3 Liikenne 27
3.3.1 Ilmaliikenne 27
3.3.2 Rautatieliikenne 28
3.3.3 Tieliikenne 29
3.3.4 Vesiliikenne 30
3.4 Pankkitoiminta ja finanssimarkkinoiden infrastruktuuri 30
3.4.1 Kansallinen sääntely 30
3.4.2 DORA-asetus 32
3.5 Terveydenhuoltoala 33
3.5.1 Terveydenhuollon tarjoajat 33
3.5.2 EU:n vertailulaboratoriot 34
3.5.3 Lääkkeiden tutkimusta, kehitystä ja valmistusta harjoittavat toimijat 35

3.5.4 Vakavan kansanterveysuhan aikana kriittisiksi katsottuja lääkinnällisiä laitteita valmistavat toimijat 35
3.6 Juomavesi ja jätevesi 36
3.7 Digitaalinen infrastruktuuri ja digitaalisen palvelun tarjoajat 37
3.7.1 Digitaalisen palvelun tarjoajat 37
3.7.2 Verkkotunnustoiminta 37
3.7.3 Viestintäverkot ja –palvelut 38
3.7.4 Sähköiset luottamuspalvelut 38
3.8 Tieto- ja viestintätekniikan palvelujen (TVT-palvelut) hallinta 38
3.9 Avaruus 39
3.10 Posti- ja kuriiripalvelut 40
3.11 Jätehuolto 40
3.12 Kemikaalien valmistus, tuotanto ja jakelu 41
3.12.1 Kemikaalit ja räjähteet 41
3.12.2 Painelaitesääntely 42
3.13 Elintarvikkeiden teollinen tuotanto, jalostus ja tukkukauppa 43
3.14 Valmistussektori 45
3.14.1 Lääkinnällisten laitteiden valmistus 45
3.14.2 Tietokoneiden sekä elektronisten ja optisten tuotteiden valmistus 46
3.14.3 Sähkölaitteiden valmistus 47
3.14.4 Muiden koneiden ja laitteiden valmistus 48
3.14.5 Moottoriajoneuvojen ja perävaunujen valmistus 49
3.14.6 Muiden kulkuneuvojen valmistus 50
3.15 Tutkimusorganisaatiot 51
3.16 Julkishallinnon toimiala 51
3.16.1 NIS2-direktiivin sääntelyn soveltaminen julkishallinnon toimialalla 51
3.16.2 Käsitteet ja määritelmät 52
3.16.3 Kyberturvallisuutta koskevat riskienhallintatoimenpiteet 53
3.16.4 Johdon (hallintoelimen) vastuu 53
3.16.5 Ilmoitusvelvollisuudet ja valvonta 54
3.16.6 Julkishallinnon toimialaa koskevan sääntelyn sijoittaminen tiedonhallintalakiin 54
3.17 Kyberturvallisuusstrategia 54
3.18 Toimilupa- ja sertifiointisääntely 55
4 Ehdotukset ja niiden vaikutukset 57
4.1 Keskeiset ehdotukset 57
4.2 Pääasialliset vaikutukset 60
4.2.1 Ehdotuksen pääasialliset vaikutukset 60
4.2.2 Riskienhallinta- ja raportointivelvoitteiden soveltamisalaan kuuluvat toimijat 63
4.2.3 Vaikutukset verkkotunnusvälittäjiin ja verkkotunnusrekisterin ylläpitäjään 82
4.3 Taloudelliset vaikutukset 83
4.3.1 Vaikutukset yrityksiin 83
4.3.1.1 Yhteenveto yritysvaikutuksista 83
4.3.1.2 Riskienhallintavelvoite 88
4.3.2 Vaikutukset kansantalouteen 100
4.4 Vaikutukset viranomaisten toimintaan 102

4.4.1 Vaikutukset viranomaisten tehtäviin ja julkistalouteen 102
4.4.2 Tiedonhallinnan muutosvaikutukset 113
4.5 Muut ihmisiin kohdistuvat ja yhteiskunnalliset vaikutukset 117
4.5.1 Vaikutukset turvallisuuteen 117
4.5.2 Vaikutukset tietoyhteiskuntaan ja tietosuojaan 119
4.5.3 Ympäristövaikutukset 119
5 Muut toteuttamisvaihtoehdot 120
5.1 Vaihtoehdot ja niiden vaikutukset 120
5.1.1 Riskienhallinta- ja raportointivelvoitteiden kansalliset laajennukset 120
5.1.2 Sääntelymalli muuten kuin julkishallinnon toimialalla 120
5.1.3 Julkishallinnon toimialan NIS2 -sääntely ja soveltaminen julkishallinnon toimialalla 121
5.1.4 Valvonnan järjestäminen 123
5.1.5 Julkishallinnon toimialan valvova viranomainen 126
5.1.6 Seuraamusmaksu 128
5.2 Muiden jäsenvaltioiden suunnittelemat tai toteuttamat keinot 129
5.2.1 Ruotsi 129
5.2.2 Viro 129
5.2.3 Tanska 130
5.2.4 Saksa 130
5.2.5 Ranska 131
6 Lausuntopalaute 131
6.1 Lausuntokierros 131
6.2 Muu kuuleminen 134
6.3 Lainsäädännön arviointineuvoston lausunto 135
7 Säännöskohtaiset perustelut 136
7.1 Kyberturvallisuuslaki 136
7.2 Laki julkisen hallinnon tiedonhallinnasta annetun lain muuttamisesta 203
7.3 Laki sähköisen viestinnän palveluista annetun lain muuttamisesta 227
7.4 Laki ilmailulain 128 a §:n ja 128 b §:n kumoamisesta 231
7.5 Laki raideliikennelain 169 §:n kumoamisesta 231
7.6 Laki liikenteen palveluista annetun lain muuttamisesta 231
7.7 Laki alusliikennepalvelulain 18 a §:n kumoamisesta. 232
7.8 Laki eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain 7 e ja 7 f §:n kumoamisesta 232
7.9 Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain muuttamisesta 232
7.10 Laki sähkömarkkinalain muuttamisesta 234
7.11 Laki maakaasumarkkinalain 34 a §:n kumoamisesta 234
7.12 Laki energiavirastosta annetun lain 1 §:n muuttamisesta 234
7.13 Laki sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain muuttamisesta 234
7.14 Laki vesihuoltolain 35 §:n muuttamisesta 235
7.15 Laki sakon täytäntöönpanosta annetun lain 1 §:n muuttamisesta. 235
7.16 Laki maa-asemista ja eräistä tutkista annetun lain 8 §:n muuttamisesta 235

7.17 Laki vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annetun lain muuttamisesta 235
8 Lakia alemman asteinen sääntely 236
8.1 Esityksellä ehdotettavat uudet valtuudet lakia alemman asteisen sääntelyn antamiseksi 236
8.2 Esityksellä kumottavat valtuudet antaa lakia alemman asteisia säännöksiä....239
9 Voimaantulo 240
10 Toimeenpano ja seuranta....240
11 Suhde muihin esityksiin 241
12 Suhde perustuslakiin ja säätämisjärjestys....242
12.1 Luottamuksellisen viestinnän suoja....242
12.2 Julkisen hallintotehtävän antaminen muulle kuin viranomaiselle ja viranomaisen suoritteen maksullisuus....250
12.3 Elinkeinonvapaus....252
12.4 Omaisuudensuoja....256
12.5 Hallinnollinen seuraamusmaksu....256
12.6 Valtion toimielinten yleiset perusteet 258
12.7 Lainsäädäntövallan siirtäminen 259
12.8 Julkisuusperiaate....261
12.9 Eräiden valtioelinten ja viranomaisten asema 262
12.10 Ahvenanmaan asema ja suhde itsehallintoon 265
LAKIEHDOTUKSET 267
1. Kyberturvallisuuslaki 267
LIITE I....287
LIITE II 290
2. Laki julkisen hallinnon tiedonhallinnasta annetun lain muuttamisesta 292
3. Laki sähköisen viestinnän palveluista annetun lain muuttamisesta....301
4. Laki ilmailulain 128 a ja 128 b §:n kumoamisesta 306
5. Laki raideliikennelain 169 §:n kumoamisesta 307
6. Laki liikenteen palveluista annetun lain muuttamisesta 308
7. Laki alusliikennepalvelulain 18 a §:n kumoamisesta 309
8. Laki eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain 7 e ja 7 f §:n kumoamisesta....310
9. Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain 2 ja 90 §:n muuttamisesta 311
10. Laki sähkömarkkinalain muuttamisesta 313
11. Laki maakaasumarkkinalain 34 a §:n kumoamisesta 314
12. Laki Energiavirastosta annetun lain 1 §:n muuttamisesta 315
13. Laki sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain muuttamisesta....316
14. Laki vesihuoltolain 35 §:n muuttamisesta 318
15. Laki sakon täytäntöönpanosta annetun lain 1 §:n muuttamisesta....319
16. Laki maa-asemista ja eräistä tutkista annetun lain 8 §:n muuttamisesta 320
17. Laki vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annetun lain muuttamisesta 321
LIITE 323
RINNAKKAISTEKSTIT 323

2. Laki julkisen hallinnon tiedonhallinnasta annetun lain muuttamisesta 323
3. Laki sähköisen viestinnän palveluista annetun lain muuttamisesta.....340
4. Laki ilmailulain 128 a ja 128 b §:n kumoamisesta 349
5. Laki raideliikennelain 169 §:n kumoamisesta 351
6. Laki liikenteen palveluista annetun lain muuttamisesta 352
7. Laki alusliikennepalvelulain 18 a §:n kumoamisesta 354
8. Laki eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain 7 e ja 7 f §:n kumoamisesta.....355
9. Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain 2 ja 90 §:n muuttamisesta 357
10. Laki sähkömarkkinalain muuttamisesta 360
11. Laki maakaasumarkkinalain 34 a §:n kumoamisesta 362
12. Laki Energiavirastosta annetun lain 1 §:n muuttamisesta 364
13. Laki sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain muuttamisesta....365
14. Laki vesihuoltolain 35 §:n muuttamisesta 367
15. Laki sakon täytäntöönpanosta annetun lain 1 §:n muuttamisesta.....368
16. Laki maa-asemista ja eräistä tutkista annetun lain 8 §:n muuttamisesta 369
17. Laki vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annetun lain muuttamisesta 370

PERUSTELUT

1 Asian tausta ja valmistelu

1.1 Tausta

Tieto- ja viestintäteknologia sekä niihin liittyvät palvelut ovat keskeinen osa nykyaikaista yhteiskuntaa ja sen kriittistä infrastruktuuria. Kehittyneet tieto- ja viestintäteknologiset ratkaisut mahdollistavat uusia innovaatioita, toimintatapoja ja palveluita yhteiskunnassa. Samaan aikaan yhä useammat palvelut ja toiminnot ovat kasvavassa määrin riippuvaisia viestintäverkkojen ja tietojärjestelmien luotettavasta toiminnasta. Viestintäverkkojen ja tietojärjestelmien kyberturvallisuuteen voi kohdistua monenlaisia riskejä, jotka voivat aiheuttaa monenlaista häiriötä ja haittaa erilaisten syy-yhteyksien seurauksena. Kyberturvallisuuteen kohdistuvan riskin toteutuminen voi olla seurausta tahattomasta vahingosta tai tahallisesta oikeudettomasta teosta, jonka taustalla olevat motiivit vaihtelevat. Suomi on tietoyhteiskuntana riippuvainen viestintäverkkojen ja tietojärjestelmien toiminnasta ja näin ollen myös haavoittuvainen niihin kohdistuville häiriöille. Yhteiskunnan kokonaisturvallisuuden kannalta on tärkeää kasvattaa kyberturvallisuuden tasoa viestintäverkoissa ja tietojärjestelmissä.

Kyberturvallisuuteen liittyvistä häiriöistä voi lisäksi aiheutua merkittäviä taloudellisia seurauksia, niin yhteiskunnalle kuin yksityisille kansalaisille, yrityksille ja muille yhteisöille. Yksittäisten kansalaisten ja yritysten kannalta erityisen merkityksellisiä ovat häiriöt, joiden seurauksena ulkopuolinen taho, kuten tietoverkkorikolliset, voisivat päästä käsiksi heidän luottamuksellisiin tietoihinsa, kuten henkilötietoihin, viestintään tai verkkopalveluiden salasanoihin. Palveluiden toiminnan kannalta erityisen haitallisia voivat olla häiriöt, joiden seurauksena palvelut tai niissä säilytetyt tiedot, eivät olisi käyttäjiensä käytettävissä. Häiriön aiheuttama taloudellinen vahinko voi johtua esimerkiksi omaisuuden vahingoittumisesta, yrityksen liiketoiminnan keskeytymisestä tai kuluista, jotka syntyvät vahingoilta suojautumisesta. Yhteiskunnan toiminnan kannalta on tärkeää huolehtia kyberturvallisuudesta sellaisissa tietojärjestelmissä ja viestintäverkoissa, joiden avulla tuotetaan palveluita ja harjoitetaan toimintaa, joka on osa yhteiskunnan kriittistä infrastruktuuria.

Tämän esityksen keskeinen tavoite on vahvistaa ja kehittää kyberturvallisuuden tasoa yhteiskunnan toiminnan kannalta keskeisillä toimialoilla. 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 (NIS 2 -direktiivi), jäljempänä *NIS 2 -direktiivi*. Tähän esitykseen sisältyvät NIS2-direktiivin kansallisen toimeenpanon edellyttämät lainsäädäntömuutokset on valmisteltu liikenne- ja viestintäministeriön asettamassa poikkihallinnollisessa valmisteluhankkeessa.

NIS 2 -direktiivi korvaa aiemman EU:n verkko- ja tietoturvadirektiivin, eli Euroopan parlamentin ja neuvoston 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).

NIS 2 -direktiivi on julkaistu 14.12.2022 ja tullut voimaan 16.1.2023. NIS 2 –direktiivin säännökset on saatettava osaksi kansallista lainsäädäntöä 17.10.2024 mennessä ja sen soveltamisalaan kuuluviin toimijoihin kohdistuvia velvoitteita on sovellettava kansallisesti viimeistään 18.10.2024 alkaen.

Esitys toteuttaa myös pääministeri Petteri Orpon hallitusohjelman kirjauksia kyberturvallisuuden ja sitä koskevan yhteistyön vahvistamisesta viranomaisten ja elinkeinoelämän välillä. Hallitusohjelman mukaan 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). Kuntien toiminnan ja tehtävien mitoitusta ja toteutustapojen yksityiskohtaista sääntelyä karsitaan (3.1). Lisäksi EU-lainsäädännön toimeenpanon yhteydessä vältetään kansallista lisäsääntelyä (6.1).

Esitys toteuttaa osaltaan myös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla annetun valtioneuvoston periaatepäätöksen tavoitteita ja toimenpiteitä. Periaatepäätös on annettu 10.6.2021 ja vahvistettu linjauksineen voimassa olevaksi 21.3.2024. Periaatepäätöksen linjausten mukaisesti lainsäädännössä on oltava riittävät tietoturvaa koskevat vaatimukset ja –velvoitteet, toimijoilla riittävä tietämys ja osaaminen velvoitteiden noudattamisessa, sekä viranomaisilla riittävät toimivaltuudet ja resurssit valvoa tietoturvan ja tietosuojan toteutumista ja tehdä toimialarajat ylittävää yhteistyötä. Periaatepäätöksen tavoitteena on tietoturvan ja tietosuojan tason kehittäminen kaikilla yhteiskunnan kriittisillä sektoreilla.

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 20.12.2021. 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 14 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 10 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 ja 9.10.2023. 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.

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.

Hallituksen esityksen valmistelun aikana liikenne- ja viestintäministeriö on osallistunut NIS 2 –direktiivin nojalla perustetun EU:n NIS-yhteistyöryhmän toimintaan direktiivin kansallisen täytäntöönpanon tukemiseksi. Liikenne- ja viestintäministeriö on selvittänyt Euroopan komission tarkentavia tulkintoja NIS 2 –direktiivin sisällöstä erityisesti soveltamisalan osalta. Lisäksi liikenne- ja viestintäministeriö on ollut yhteydessä muihin EU-jäsenvaltioihin kansainvälisen vertailun ja muiden jäsenvaltioiden soveltamisalaa koskevien tulkintojen selvittämiseksi.

Esitys on arvioitu lainsäädännön arviointineuvostossa, joka antoi asiasta lausunnon 29.2.2024.

Esityksestä on käyty kuntalain 11 §:n mukainen neuvottelu ja asia on käsitelty kuntatalouden ja –hallinnon neuvottelukunnassa 5.3.2024.

Esitystä on käsitelty yhteiskunnan uudistamisen ministerityöryhmässä 15.3.2024.

Esitys on käynyt valtioneuvoston oikeuskanslerin ennakkotarkastuksessa. Ennakkotarkastuksen johdosta esityksen perusteluita on selkeytetty ja täydennetty keskeisten huomioiden osalta.

2 EU-säädöksen tavoitteet ja pääasiallinen sisältö

2.1 Tavoitteet

NIS2-direktiivin tavoitteena on vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa yhteiskunnan toiminnan kannalta keskeisten ja tärkeiden toimialojen ja toimijatyyppien osalta. Jäsenvaltiot velvoitetaan asettamaan direktiivin soveltamisalaan kuuluville toimijoille velvoite riskienhallintatoimiin kyberturvallisuushäiriöiden varalta sekä järjestämään kyberturvallisuushäiriöiden hallintaan liittyviä viranomaistoimintoja kansallisella tasolla. Lisäksi direktiivissä säädetään kansainvälisestä ja unionin tason yhteistyöstä, jonka tavoitteena on kyberturvallisuuden korkean tason ylläpitäminen.

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

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

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.

NIS1-direktiivin uudelleentarkastelussa todettiin sen vauhdittaneen institutionaalista ja sääntelyyn perustuvaa lähestymistapaa kyberturvallisuuden varmistamiseksi EU:ssa. NIS1-direktiivin uudelleentarkastelussa tuli kuitenkin esiin siihen liittyviä puutteita suhteessa nykyisiin kyberturvallisuushaasteisiin. Uudelleentarkastelussa havaittiin muun ohella merkittäviä eroja jäsenvaltioiden välillä NIS1-direktiivin täytäntöönpanossa ja sen soveltamisalaan kuuluvien toimijoiden määrittämisessä. Lisäksi NIS1-direktiiviin liittyvä erottelu palvelujen tarjoajien välillä on osoittautunut vanhanaikaiseksi. Direktiivin tavoitteiden saavuttamiseksi sen soveltamisalan tulisi olla laajempi. NIS2-direktiivin tavoitteena on vastata muuttuneeseen kyberturvallisuusympäristöön ja NIS1-direktiivin uudelleenarvioinnissa havaittuihin haasteisiin.

NIS2-direktiivin täytäntöönpano edellyttää sen soveltamisalaan kuuluville toimijoille kohdistuvista riskienhallinta- ja raportointivelvoitteista säätämistä. Lisäksi täytäntöönpano edellyttää direktiivissä tarkoitetuista viranomaistehtävistä ja em. velvoitteiden valvonnasta säätämistä. Direktiivin verkkotunnusten rekisteröintitietoja koskevan 28 artiklan täytäntöönpano edellyttäisi sähköisen viestinnän palveluista annetun lain muuttamista.

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 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 teollinen tuotanto, jalostus ja tukkukauppa, 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 jonka 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. CER-direktiivi koskee yhteiskunnan toiminnan kannalta kriittisten toimijoiden häiriönsietokykyä. CER-direktiivillä asetetaan muita kuin kyberturvallisuutta koskevia riskienhallintavelvoitteita ja poikkeamaraportointivelvoitteita direktiivin mukaisesti kriittiseksi tunnistetuille toimijoille. Kyberturvallisuutta koskevan riskienhallinnan ja poikkeamaraportoinnin osalta näihin toimijoihin olisi sovellettava NIS2-direktiivin mukaisia velvoitteita. CER-direktiivin mukaiset kriittiset toimijat olisi määritettävä ensimmäisen kerran vuonna 2026.

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. Direktiivin johdanto-osan perustelukappaleen 8 mukaisesti kansainvälisen sopimuksen mukaisesti kolmannen maan kanssa perustetut julkishallinnon toimijat eivät kuulu direktiivin soveltamisalaan eikä direktiiviä olisi sovellettava kolmansissa maissa sijaitseviin diplomaattisiin edustustoihin ja konsuliedustustoihin siltä osin kun verkko- ja tietojärjestelmät sijaitsevat edustuston tiloissa tai niitä ylläpidetään kolmannessa maassa olevia käyttäjiä varten.

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, jäljempänä *DORA-asetus*) soveltamisalan ulkopuolelle mainitun asetuksen 2 artiklan 4 kohdan mukaisesti. NIS 2 – direktiivin soveltamista DORA-asetuksen soveltamisalaan kuuluviin toimijoihin käsitellään jäljempänä Nykytila-osiossa.

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 3 artiklan 1 kohdan a-g alakohdassa tarkoitetut toimijat. Keskeisiä toimijoita ovat a-alakohdan direktiivin liitteessä I tarkoitetut toimijat jotka ylittävät keskisuuren yrityksen (suositus 2003/361/EY liitteessä olevan 2 artiklan 1 kohta) määrittelyssä käytetyt kynnysarvot. Keskisuuren yrityksen määrittelyssä käytettävät kynnysarvot ylittävä yritys on yritys, jonka palveluksessa on vähintään 250 työntekijää tai jonka vuosiliikevaihto ylittää 50 miljoonaa euroa ja taseen loppusumma ylittää 43 miljoonaa euroa. Lisäksi keskeisiä toimijoita ovat b-alakohdan nojalla hyväksytyt luottamuspalvelun tarjoajat ja aluetunnusrekisterit sekä DNS-palveluntarjoajat niiden koosta riippumatta. Keskeisiä toimijoita ovat c-alakohdan nojalla yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat, jotka täyttävät suosituksen 2003/361/EY liitteessä olevan 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset, eli ovat muita kuin mikro- tai pienyrityksiä. Lisäksi keskeisiä toimijoita ovat 3 artiklan 1 kohdan d-alakohdan nojalla keskustason julkishallinnon toimijat ja f-alakohdan nojalla CER-direktiivin nojalla kriittiseksi määritetyt toimijat.

Keskeisen toimijan määritelmän osalta 3 artiklan 1 kohdan e ja g alakohtiin liittyy kansallista liikkumavaraa. E-alakohdan nojalla keskeisiä toimijoita ovat myös sellaiset toimijat, jotka jäsenvaltio on määrittänyt keskeiseksi 2 artiklan 2 kohdan b-e alakohdan nojalla. G-alakohdan

nojalla jäsenvaltio voi säätää NIS1-direktiivin nojalla määritettyjä keskeisten palvelujen tarjoajia keskeisiksi toimijoiksi.

Tärkeinä toimijoina pidetään 3 artiklan 2 kohdan nojalla niitä toimijoita, jotka eivät täytä keskeisen toimijan määritelmää, mutta kuuluvat direktiivin soveltamisalaan ja ovat liitteissä I tai II tarkoitettua toimijatyyppiä. Tärkeitä toimijoita ovat myös sellaiset toimijat, jotka jäsenvaltiot ovat määrittäneet soveltamisalaan 2 artiklan 2 kohdan b-e alakohdan nojalla tärkeinä toimijoina. Näin ollen kaikki riskienhallinta- ja raportointivelvoitteiden soveltamisalaan kuuluvat toimijat ovat joko keskeisiä tai tärkeitä toimijoita.

2.4 Toimijaluettelo ja toimijoiden rekisteri

NIS2-direktiivin 3 artiklan 3 kohta velvoittaa jäsenvaltiot laatimaan luettelon keskeisistä ja tärkeistä toimijoista sekä verkkotunnusten rekisteröintipalveluja tarjoavista toimijoista. Luettelo on laadittava 17.4.2025 mennessä. Luettelon laatimiseksi jäsenvaltion on vaadittava, että keskeisten ja tärkeiden toimijoiden sekä verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden on toimitettava toimivaltaisille viranomaisille 3 artiklan 4 kohdassa tarkoitetut tiedot sekä ilmoitettava muutoksista tietoihin viipymättä ja enintään kahden viikon kuluessa muutospäivästä. Jäsenvaltio voi perustaa järjestelyitä, joiden avulla toimija voi itse kirjautua luetteloon. Jäsenvaltion on tarkasteltava luetteloa uudelleen säännöllisesti ja vähintään kahden vuoden välein ja saatettava se tarvittaessa ajan tasalle. Toimivaltaisten viranomaisten on viimeistään 17.4.2025 ja sen jälkeen kahden vuoden välein ilmoitettava komissiolle ja NIS-yhteistyöryhmälle luetteloon kirjattujen keskeisten ja tärkeiden toimijoiden lukumäärä kullakin direktiivin liitteissä tarkoitetulla toimialalla ja toimialan osalla. Lisäksi komissiolle on ilmoitettava 5 kohdan b alakohdassa tarkoitetut tiedot 2 artiklan 2 kohdan b-e alakohdan nojalla soveltamisalaan saatetuista toimijoista.

Lisäksi NIS2-direktiivin 27 artiklassa säädetään Euroopan unionin kyberturvallisuusvirasto ENISA:n perustamasta 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 rekisteristä. ENISA tarjoaa pyynnöstä toimivaltaisille viranomaisille pääsyn rekisteriin ja varmistaa tarvittaessa tietojen luottamuksellisuuden suojaamisen. Tätä rekisteriä varten jäsenvaltioiden on edellytettävä, että nämä toimijat ilmoittavat 17.1.2025 mennessä toimivaltaisille viranomaisille NIS2-direktiivin 27 artiklan 2 kohdassa tarkoitetut tiedot sekä ilmoittavat muutoksista tietoihin viipymättä ja enintään kolmen kuukauden kuluessa muutospäivästä. Kansallisen keskitetyn yhteyspisteen tulee toimittaa ENISA:lle nämä tiedot ilman aiheetonta viivytystä, lukuun ottamatta tietoa toimijan IP-osoitealueista.

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 artiklan nojalla jäsenvaltion on varmistettava, että keskeiset ja tärkeät 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. Riskienhallintatoimenpiteillä on varmistettava, että verkko- ja tietojärjestelmien turvallisuuden taso on oikeassa suhteessa riskeihin.

Direktiivin 21 artiklassa määritellään osa-alueet, joita keskeisen ja tärkeän toimijan on otettava riskienhallinnassa ja riskienhallintatoimenpiteissä huomioon. 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 viivytyksettä ja 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.

NIS2-direktiivin 22 artiklan nojalla voidaan tehdä Euroopan unionin tason koordinoituja turvallisuusriskinarviointeja tietyistä kriittisistä TVT-palvelujen, TVT-järjestelmien tai TVT-tuotteiden toimitusketjuista ottaen huomioon tekniset ja tarvittaessa muut kuin tekniset riskitekijät. Jäsenvaltioiden on varmistettava, että näiden riskiarviointien tulokset otetaan huomioon toimitusketjun turvallisuutta koskevassa riskinhallinnassa NIS2-direktiivin 21 artiklan 3 kohdan nojalla.

NIS2-direktiivin 21 artiklan 5 kohdan nojalla komissio hyväksyy viimeistään 17 päivänä lokakuuta 2024 täytäntöönpanosäädöksiä, joilla vahvistetaan 21 artiklan 2 kohdan riskienhallinnassa tarkoitettujen toimenpiteiden tekniset ja menetelmiin liittyvät vaatimukset, 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.

NIS2-direktiivin 21 artiklan 5 kohdan nojalla komissio voi hyväksyä täytäntöönpanosäädöksiä, joilla vahvistetaan 21 artiklan 2 kohdan riskienhallinnassa tarkoitettujen toimenpiteiden tekniset ja menetelmiin liittyvät vaatimukset sekä tarvittaessa alakohtaiset vaatimukset, jotka koskevat myös muita kuin edellä tarkoitettuja toimijoita.

NIS2-direktiivin 24 artiklan 1 momentin nojalla jäsenvaltio voi vaatia riskienhallintavelvoitteen vaatimusten noudattamisen osoittamiseksi, että keskeiset ja tärkeät toimijat käyttävät TVT-tuotteita, TVT-palveluja ja TVT-prosesseja, jotka on sertifioitu EU:n kyberturvallisuusasetuksen (EU) 2019/881[2] 49 artiklan nojalla hyväksyttyjen eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukaisesti. Lisäksi jäsenvaltioiden on kannustettava keskeisiä ja tärkeitä toimijoita käyttämään hyväksyttyjä luottamuspalveluja. Keskeisten ja tärkeiden toimijoiden vaatiminen riskienhallintavelvoitteen noudattamisen osoittamista siten, että ne käyttävät EU:n kyberturvallisuusasetuksen mukaisesti sertifioitua TVT-tuotetta, TVT-palvelua tai TVT-prosessia, on lähtökohtaisesti kokonaan kansallisen liikkumavaran alassa.

NIS2-direktiivin 24 artiklan 2 momentin nojalla komissiolla on valta antaa delegoituja säädöksiä, joilla täydennetään NIS2-direktiiviä täsmentämällä, mitä keskeisten ja tärkeiden toimijoiden luokkia on vaadittava käyttämään tiettyjä sertifioituja TVT-tuotteita, TVT-palveluja ja TVT-prosesseja tai hankkimaan sertifiointi asetuksen (EU) 2019/881 49 artiklan nojalla hyväksytyn eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti. Siltä osin, jos tällaisia delegoituja säädöksiä annetaan, ei asian osalta ole kansallista liikkumavaraa.

NIS2-direktiivin 25 artiklan nojalla jäsenvaltioiden on riskienhallintavelvoitteen yhdenmukaisen täytäntöönpanon edistämiseksi kannustettava käyttämään verkko- ja tietojärjestelmien turvallisuuden kannalta merkityksellisiä eurooppalaisia ja kansainvälisiä standardeja ja teknisiä eritelmiä ilman, että ne määräävät käyttämään jotain tiettyä teknologiaa tai harjoittavat syrjintää jonkin tietyn teknologian käytön suosimiseksi.

2.6 Raportointivelvoitteet

Toimijoihin kohdistuvista raportointivelvoitteista säädetään NIS2-direktiivin 23 artiklassa ja vapaaehtoisesta ilmoittamisesta 30 artiklassa.

NIS2-direktiivin 23 artiklan 1 kohdan nojalla keskeisten ja tärkeiden toimijoiden tulee raportoida merkittävästä poikkeamasta CSIRT-yksikölle tai toimivaltaiselle valvovalle

[2] Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus)

viranomaiselle. Jos raportti tehdään toimivaltaiselle viranomaiselle, jäsenvaltion on varmistettava, että kyseinen toimivaltainen viranomainen heti ilmoituksen saatuaan toimittaa sen eteenpäin CSIRT-yksikölle.

Merkittävällä poikkeamalla tarkoitetaan NIS2-direktiivin 23 artiklan 1 kohdan mukaisesti poikkeamaa, jolla on merkittävä vaikutus palvelujen tarjoamiseen NIS2-direktiivin 23 artiklan 3 kohdan mukaisesti. NIS2-direktiivin 23 artiklan 3 kohdan nojalla poikkeama katsotaan merkittäväksi, jos

a) se on aiheuttanut tai voi aiheuttaa palvelujen vakavan toimintahäiriön tai asianomaiselle toimijalle taloudellisia tappioita; tai

b) jos poikkeama on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa.

Raportointivelvoite merkittävästä poikkeamasta on kolmiportainen (NIS2-artiklan 23 artiklan 4 kohta). 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 lainvastaisista 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. Poikkeuksena tälle luottamuspalvelun tarjoajan tulisi ilmoittaa luottamuspalvelun tarjontaan vaikuttavasta merkittävästä poikkeamasta 24 tunnin kuluessa.

Loppuraportti laaditaan viimeistään kuukauden kuluttua poikkeamailmoituksen toimittamisesta ja sen tulee sisältää yksityiskohtainen kuvaus poikkeamasta, sen vakavuudesta 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 tai tilannepäivitys asian käsittelyn edistymisestä on toimitettava CSIRT-yksikön tai toimivaltaisen viranomaisen pyynnöstä. Jos poikkeama on edelleen meneillään silloin, kun loppuraportti pitäisi toimittaa, jäsenvaltioiden on varmistettava, että asianomaiset toimijat toimittavat tuolloin edistymisraportin ja lopullisen raportin kuukauden kuluessa siitä, kun ne ovat käsitelleet poikkeaman.

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 tai operatiivisia neuvoja mahdollisten vaikutuksia lieventävien toimenpiteiden täytäntöönpanoa varten. Jos CSIRT-yksikkö ei ole ilmoituksen alkuperäinen vastaanottaja, toimivaltaisen viranomaisen on annettava ohjeet yhteistyössä CSIRT-yksikön kanssa. CSIRT-yksikkö antaa täydentävää teknistä tukea, jos asianomainen toimija sitä pyytää. Jos merkittävää poikkeamaa epäillään

rikokseksi, CSIRT-yksikön tai toimivaltaisen viranomaisen on myös annettava ohjeita merkittävän poikkeaman ilmoittamisesta lainvalvontaviranomaisille.

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 viranomaisella 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 ilmoittamisen lisäksi keskeisen tai tärkeän toimijan on tarvittaessa ilmoitettava ilman aiheetonta viivytystä palvelujensa vastaanottajille merkittävistä poikkeamista, jotka todennäköisesti vaikuttavat haitallisesti kyseisten palvelujen tarjoamiseen (NIS2-direktiivin 23 artiklan 1 kohta). NIS2-direktiivin 23 artiklan 2 kohdan nojalla jäsenvaltion on tapauksen mukaan varmistettava, että keskeiset ja tärkeät toimijat tiedottavat ilman aiheetonta viivytystä niille palvelujensa vastaanottajille, joihin merkittävä kyberuhka saattaa vaikuttaa, kaikista toimenpiteistä tai korjaavista toimista, joita kyseiset palvelun vastaanottajat voivat uhkan hallitsemiseksi toteuttaa. Toimijoiden on tarvittaessa myös tiedotettava kyseisille palvelun vastaanottajille merkittävästä kyberuhkasta itsestään. NIS2-direktiivin 23 artiklan 7 kohdan nojalla silloin, jos yleinen tietoisuus on tarpeen merkittävän poikkeaman estämiseksi tai meneillään olevan merkittävän poikkeaman käsittelemiseksi tai jos merkittävän poikkeaman julkistaminen on muutoin yleisen edun mukaista, 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 itseään tekemään niin.

NIS2-direktiivin 23 artiklan 6 kohdan nojalla CSIRT-yksikön, toimivaltaisen viranomaisen tai keskitetyn yhteyspisteen on tarvittaessa ja erityisesti silloin, kun merkittävä poikkeama koskee vähintään kahta jäsenvaltiota, tiedotettava merkittävästä poikkeamasta ilman aiheetonta viivytystä niille muille jäsenvaltioille, joihin poikkeama vaikuttaa, ja ENISA:lle. Tällöin annettaviin tietoihin on sisällyttävä sen tyyppisiä tietoja kuin on vastaanotettu 4 kohdan mukaisesti. Näin tehdessään CSIRT-yksikön, toimivaltaisen viranomaisen tai keskitetyn yhteyspisteen on unionin oikeuden tai kansallisen lainsäädännön mukaisesti säilytettävä toimijan turvallisuusedut ja kaupalliset edut sekä annettujen tietojen luottamuksellisuus.

Keskitetyn yhteyspisteen on CSIRT-yksikön tai toimivaltaisen viranomaisen pyynnöstä toimitettava ilmoitukset eteenpäin niiden muiden jäsenvaltioiden keskitetyille yhteyspisteille, joihin poikkeama vaikuttaa (23 artiklan 8 kohta). Lisäksi keskitetyn yhteyspisteen on toimitettava ENISA:lle kolmen kuukauden välein yhteenvetoraportti, joka sisältää anonymisoidut koontitiedot merkittävistä poikkeamista, poikkeamista, kyberuhkista ja läheltä piti -tilanteista, joista on ilmoitettu.

NIS2-direktiivin 23 artiklan 10 kohdan nojalla CSIRT-yksiköiden tai tapauksen mukaan toimivaltaisten viranomaisten on toimitettava CER-direktiivin mukaisille toimivaltaisille

viranomaisille tietoa merkittävistä poikkeamista, poikkeamista, kyberuhkista ja läheltä piti -tilanteista, joista CER-direktiivin kriittisiksi toimijoiksi määritetyt toimijat ovat ilmoittaneet.

NIS2-direktiivin 23 artiklan 11 kohdan nojalla komissio voi hyväksyä täytäntöönpanosäädöksiä, joissa täsmennetään pakollista tai vapaaehtoista ilmoitusta sekä palvelujen vastaanottajiin kohdistuvaa tiedottamista koskeva tietosisältö, muoto ja ilmoitusmenettely.

NIS2-direktiivin 23 artiklan 11 kohdan nojalla komissio hyväksyy viimeistään 17.10.2024 DNS-palveluntarjoajia, aluetunnusrekistereitä, pilvipalvelujen tarjoajia, datakeskuspalvelujen tarjoajia, sisällönjakeluverkkojen tarjoajia, hallintapalvelun tarjoajia, tietoturvapalveluntarjoajia sekä verkossa toimivien markkinapaikkojen tarjoajia, verkossa toimivien hakukoneiden tarjoajia ja verkkoyhteisöalustojen tarjoajia koskevia täytäntöönpanosäädöksiä, joissa täsmennetään tapaukset, joissa poikkeama katsotaan merkittäväksi 3 kohdan mukaisesti.

NIS2-direktiivin 23 artiklan 11 kohdan nojalla komissio voi hyväksyä myös muita kuin edellä tarkoitettuja toimijoita koskevia täytäntöönpanosäädöksiä, joilla täsmennetään tapaukset, joissa poikkeama katsotaan merkittäväksi.

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 perustelukappaleen 122 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 noudattamisesta, vaan valvovan viranomaisen olisi tärkeiden toimijoiden osalta harjoitettava yleisen valvonnan sijasta jälkikäteisvalvontaa. Kansallisessa harkinnassa olisi tärkeiden toimijoiden valvominen enemmälti tai saattaminen etukäteisvalvonnan piiriin.

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 toimijoille määrättävistä hallinnollisista sakoista 21 artiklassa tarkoitetun riskienhallintavelvoitteen tai 23 artiklassa tarkoitetun raportointivelvoitteen laiminlyönnistä sekä asetettu vähimmäisvaatimus kansallisesti määrättävien 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 keskeisiin toimijoihin kohdistetut 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 koskeva sertifiointi tai lupa 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 kuin keskeisiin toimijoihin. Keskeisimpänä erona direktiivi ei edellytä tärkeiden toimijoiden kohdalla, toisin kuin keskeisten toimijoiden kohdalla, että valvova viranomainen voisi kohdistaa niihin tietoturva-auditointeja, perua toimintaa koskevan luvan tai sertifioinnin taikka kieltää toimijan johdossa toimivaa henkilöä toimimasta johtotehtävässä. Tärkeisiin toimijoihin direktiivi edellyttää edellä kuvatulla valvontatoimenpiteiden kohdistamista vain, jos jäsenvaltiot saavat näyttöä, viitteitä tai tietoja, joiden mukaan tärkeä toimija ei väitetysti noudata direktiiviä ja erityisesti sen 21 ja 23 artiklaa, eli ne ovat niin kuvatusti jälkikäteisvalvonnan piirissä.

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. CSIRT-yksikön tehtävistä ja vaatimuksista säädetään NIS 2 –direktiivin 10 ja 11 artikloissa. CSIRT-yksiköillä tulee olla tekniset valmiudet suorittaa niille annetut tehtävät. Toimijoiden velvollisuus raportoida merkittävistä poikkeamista voidaan osoittaa joko CSIRT-yksikölle tai toimivaltaiselle viranomaiselle jäsenvaltion kansallisen liikkumavaran sisällä.

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 Keskitetty yhteyspiste

NIS 2 –direktiivin 8 artikla edellyttää jäsenvaltiota nimeämään tai perustamaan keskitetyn yhteyspisteen. Kunkin keskitetyn yhteyspisteen on huolehdittava yhteydenpidosta ja varmistettava jäsenvaltionsa viranomaisten rajat ylittävä yhteistyö muiden jäsenvaltioiden asiaankuuluvien viranomaisten ja tarvittaessa komission ja ENISA:n kanssa sekä varmistettava toimialarajat ylittävä yhteistyö jäsenvaltionsa muiden toimivaltaisten viranomaisten kanssa.

2.8.4 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 kyberturvallisuus-strategian 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 Verkkotunnusten rekisteröintitietojen tietokanta

NIS2-direktiivin 28 artiklassa säädetään verkkotunnusten rekisteröintitietojen tietokannasta. Artiklan 1 kohdan nojalla jäsenvaltioiden on edellytettävä DNS-järjestelmän turvallisuuden, vakauden ja häiriönsietokyvyn edistämiseksi, että aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat keräävät ja ylläpitävät tarkkoja ja täydellisiä verkkotunnusten rekisteröintitietoja erityisessä tietokannassa noudattaen unionin tietosuojalainsäädännön mukaisesti asianmukaista huolellisuutta henkilötietojen suhteen.

NIS2-direktiivin 28 artiklan 2 kohdan nojalla jäsenvaltion tulisi edellyttää, että verkkotunnusten rekisteröintitietojen tietokanta sisältää tarvittavat tiedot, jotta verkkotunnusten haltijat ja aluetunnusrekistereissä verkkotunnuksia hallinnoivat yhteyspisteet voidaan tunnistaa ja niihin voidaan ottaa yhteyttä. Näihin tietoihin olisi sisällyttävä verkkotunnus; rekisteröintipäivä; verkkotunnuksen rekisteröijän nimi, yhteyssähköpostiosoite ja puhelinnumero; verkkotunnusta hallinnoivan yhteyspisteen yhteyssähköpostiosoite ja puhelinnumero, jos ne eivät ole samat kuin verkkotunnuksen rekisteröijän.

NIS2-direktiivin 28 artiklan 3 kohdan nojalla jäsenvaltioiden on edellytettävä, että aluetunnusrekistereillä ja verkkotunnusten rekisteröintipalveluja tarjoavilla toimijoilla on käytössä toimintaperiaatteet ja menettelyt, myös tarkastusmenettelyt, joilla varmistetaan, että tietokannat sisältävät tarkat ja täydelliset tiedot. Jäsenvaltioiden on edellytettävä, että tiedot tällaisista toimintaperiaatteista ja menettelyistä asetetaan julkisesti saataville.

NIS2-direktiivin 28 artiklan 4 ja 5 kohdan nojalla jäsenvaltioiden on edellytettävä, että aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat asettavat julkisesti saataville ilman aiheetonta viivytystä verkkotunnuksen rekisteröinnin jälkeen muut verkkotunnuksen rekisteröintitiedot kuin henkilötiedot. Jäsenvaltioiden on edellytettävä, että aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat antavat pääsyn tarkasti määrättyihin verkkotunnusten rekisteröintitietoihin unionin tietosuojalainsäädännön mukaisesti, kun pääsyä oikeutetusti pyytävä esittää lainmukaisen ja asianmukaisesti perustellun pyynnön. Jäsenvaltioiden on edellytettävä, että aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat vastaavat tietoihin pääsyä koskeviin pyyntöihin ilman aiheetonta viivytystä ja joka tapauksessa 72 tunnin kuluessa pyynnön vastaanottamisesta. Jäsenvaltioiden on edellytettävä, että tällaisten tietojen luovuttamista koskevat toimintaperiaatteet ja menettelyt asetetaan julkisesti saataville.

2.11 Kyberturvallisuustietojen jakamisjärjestelyt

NIS2-direktiivin 29 artikla edellyttää jäsenvaltiota varmistamaan, että NIS2-direktiivin soveltamisalaan kuuluvat toimijat ja tapauksen mukaan soveltamisalan ulkopuolella olevat toimijat voivat vaihtaa keskenään asiaankuuluvia kyberturvallisuustietoja, mukaan lukien tietoja kyberuhkista, läheltä piti -tilanteista, haavoittuvuuksista, tekniikoista ja menettelyistä, vaarantumisindikaattoreista, kyberhyökkäystaktiikoista, yksittäisistä uhkatoimijoista, kyberturvallisuushälytyksistä ja suosituksista, jotka koskevat kyberhyökkäysten havaitsemiseen käytettävien kyberturvallisuustyökalujen konfigurointia, kun tällaisella tietojenvaihdolla

a) pyritään ehkäisemään, havaitsemaan ja hallitsemaan poikkeamia tai palautumaan niistä tai lieventämään niiden vaikutuksia; tai

b) parannetaan kyberturvallisuuden tasoa erityisesti lisäämällä tietoisuutta kyberuhkista, rajoittamalla tai estämällä tällaisten uhkien kykyä levitä, tukemalla erilaisia puolustusvalmiuksia, haavoittuvuuden korjaamista ja julkistamista, uhkien havaitsemis-, rajoittamis- ja ehkäisemistekniikoita, lieventämisstrategioita tai hallinta- ja palautumisvaiheita tai edistämällä julkisten ja yksityisten toimijoiden yhteistyöhön perustuvaa kyberuhkatutkimusta.

NIS2-direktiivin 29 artiklan nojalla jäsenvaltion on helpotettava ja edistettävä kyberturvallisuustietojen jakamisjärjestelyiden perustamista. Jakamisjärjestelyissä voidaan asettaa ehtoja viranomaisten saataville asettamille tiedoille. 29 artiklan 4 kohdan nojalla jäsenvaltioiden on varmistettava, että keskeiset ja tärkeät toimijat ilmoittavat toimivaltaisille viranomaisille osallistumisestaan 2 kohdassa tarkoitettuihin kyberturvallisuustietojen jakamisjärjestelyihin, kun ne liittyvät tällaisiin järjestelyihin, tai tapauksen mukaan vetäytymisestään tällaisista järjestelyistä, kun vetäytyminen tulee voimaan.

2.12 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). Lisäksi jäsenvaltioilla on kansallista liikkumavaraa direktiivin soveltamisalan laajentamisen sekä sen edellyttämää korkeatasoisempien kyberturvallisuuden riskinhallinta- ja raportointivelvoitteiden osalta.

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). Lisäksi jäsenvaltio voi määrittää NIS2-direktiivin 2 artiklan 2 kohdan b-e alakohdassa tarkoitetut toimijat keskeisiksi tai tärkeiksi toimijoiksi (3 artiklan 1 kohdan e-alakohta ja 2 kohta).

NIS 2 –direktiivi jättää kansallista liikkumavaraa sille, miten direktiivin valvonta jäsenvaltiossa järjestetään. Direktiivi edellyttää nimettäväksi vähintään yhden tai useamman toimivaltaisen viranomaisen, joka valvoo sen noudattamista kansallisella tasolla. Lisäksi NIS 2 –direktiivi edellyttää nimettäväksi tai perustettavaksi yhden tai useamman keskitetyn yhteyspisteen EU-tason yhteistyötä varten. Lisäksi NIS 2 –direktiivi edellyttää kansallisesti nimettävän tai perustettavan vähintään yksi tai useampi tietoturvaloukkauksiin reagoiva ja niitä tutkiva CSIRT-yksikkö.

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 EU-sertifioituja TVT-tuotteita, -palveluja tai –prosesseja, mutta jäsenvaltiot voivat 24 artiklan 1 kohdan mukaan vaatia keskeisiä ja tärkeitä toimijoita käyttämään Euroopan unionin kyberturvallisuusvirasto ENISA:sta 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. Kansallisen liikkumavaran lisäksi NIS 2 -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 21 artiklassa tarkoitetun riskienhallintavelvoitteen ja 23 artiklassa tarkoitetun raportointivelvoitteen vastaisesta toiminnasta. Kansallinen liikkumavara koskee hallinnollisten seuraamusmaksujen tasoa, kuitenkin siten, että direktiivissä säädetään alimmasta sallitusta tasosta, jolla keskeisille ja tärkeille toimijoille määrättävän hallinnollisen seuraamusmaksun enimmäismäärän tulee vähintään olla. 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). Lisäksi 32 artiklan 5 kohdan mukaisia seuraamuksia (sertifioinnin tai luvan peruuttaminen sekä kieltäminen toimimaan toimijan johtotehtävissä) ei sovelleta direktiivin soveltamisalaan kuuluviin julkishallinnon toimijoihin.

3 Nykytila ja sen arviointi

3.1 NIS1-direktiivin täytäntöönpano

NIS2-direktiiviä edeltävä EU:n verkko- ja tietoturvadirektiivi eli NIS1-direktiivi saatettiin pääosin voimaan kansallisesti 9. toukokuuta 2018 voimaan tulleilla sektorikohtaisilla 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 NIS1-vaatimusten osalta. 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 NIS1-direktiivin täytäntöönpanosäädöksiä tarkasteltava NIS2-direktiivin täytäntöönpanon yhteydessä tarpeettoman ja päällekkäisen sääntelyn välttämiseksi sekä tarkoituksenmukaisen sääntelykokonaisuuden laatimiseksi.

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 tehtävät sähköntoimitusten mittauksessa (22 §), verkonhaltijan varautumissuunnittelu (28 §), verkonhaltijan yhteistoimintavelvollisuus häiriötilanteissa (29 §), kantaverkon toiminnan laatuvaatimukset (40 §), sähkökaupan keskitetyn tiedonvaihdon palvelut (49 a §), suurjännitteisen jakeluverkon toiminnan laatuvaatimukset (50 §), jakeluverkon toiminnan laatuvaatimukset (51 §),jakeluverkonhaltijan velvoite tiedottaa verkon käyttäjille häiriötilanteissa (59 §), sähkökaupan markkinaprosesseihin liittyvän tiedon hallinta (75 b §) sekä maakaapeleita vaarantava työ ja maakaapeleiden sijainnin selvittäminen (110 §). 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 perustelukappaleessa 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 riskeihin varautumissuunnitelmissa.” Kyberturvallisuutta koskevia erityisiä sääntöjä sähkötoimialalla voidaan antaa sähkön sisämarkkinoista annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) 2019/943 vahvistetussa verkkosäännössä.

NIS2-direktiivin soveltamisalaan sähkötoimijoiden osalta kuuluu uusia toimijatyyppejä, joita ei ollut NIS1-direktiivissä tai, joita ei NIS1-direktiivin täytäntöönpanossa ole tunnistettu keskeisten palveluiden tarjoajiksi.

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, painelaitelaissa (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 myös maakaasumarkkinalaissa kemikaaliturvallisuuslainsäädännön lisäksi. 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 §), verkonhaltijan yhteistoimintavelvollisuutta häiriötilanteissa (28 §), maakaasukaupan ja taseselvityksen edellyttämää tiedonvaihdon kehittämistä (32 a §) sekä maakaasukaupan keskitetyn tiedonvaihdon palveluita (32 b §) 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:

Taulukko 1

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 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.	Sovelletaan 16.10.2025 alkaen eräisiin tuotanto- ja suunnitteluorganisaatioihin, lentopaikkojen pitäjiin sekä asematasovalvontapalvelujen tarjoajiin.

Ilmailun tietoturvallisuutta koskeva EU-sääntely soveltuu laajempaan toimijajoukkoon kuin NIS2-direktiivi, ja toimijoille asetettavat velvoitteet vastaavat pitkälti NIS2-vaatimuksia.

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 annetussa 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 ohjauspalvelun sekä älykkäiden tieliikennejärjestelmien ylläpitäjien osalta soveltamisalaan kuuluvat toimialan toimijatyypit ovat NIS1- ja NIS2-direktiivissä olleet pääosin samat. Erona direktiivien välillä on NIS2-direktiivin soveltamisalan ulkopuolelle rajatut julkishallinnon toimijat, joille liikenteenhallinta tai älykkäiden liikennejärjestelmien ylläpitäminen ei ole keskeinen osa niiden yleistä toimintaa.

Tieliikenteen hallinta- ja ohjauspalveluja tarjoavien toimijoiden NIS1-direktiivin mukaisista riskienhallinta- ja raportointivelvoitteista on säädetty liikenteen palveluista annetussa laissa, jonka 140 § koskee tietoturvaa tieliikenteen ohjaus- ja hallintapalvelussa sekä 141 § tietoturvaa tieliikenteen ohjaus- ja hallintapalveluiden poikkeamailmoitusten laatimisvelvoitetta koskien. Liikenteen palveluista annetun lain 140 § olisi tarpeen muuttaa NIS2-direktiivin kansallisen toimeenpanon johdosta. Soveltamisalaan kuuluvien toimijoiden, eli tieliikenteen ohjaus- ja hallintapalvelun tarjoajien, määritelmää ei olisi tarpeen muuttaa.

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. Soveltamisalaan kuuluvien toimijoiden, eli älykkään liikennejärjestelmän ylläpitäjän määritelmää ei olisi tarpeen muuttaa.

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

operatiivisia 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 perustelukappale 16 ja NIS2-direktiivin johdanto-osan perustelukappale 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.

Euroopan komissio on julkaissut 13.9.2023 ohjeistuksen (C(2023) 6068 final), jonka nojalla DORA-asetus on NIS 2 –direktiivin 4 artiklassa tarkoitettu alakohtainen unionin säädös. Näin ollen jäsenvaltioiden ei pitäisi soveltaa direktiivin (EU) 2022/2555 säännöksiä, jotka koskevat kyberturvallisuusriskien hallintaa ja raportointivelvoitteita sekä valvontaa ja täytäntöönpanoa, asetuksen (EU) 2022/2554 soveltamisalaan kuuluviin finanssialan toimijoihin. Koska NIS 2 –direktiivin finanssisektorin toimijat kuuluvat DORA-asetuksen soveltamisalaan, ei kyberturvallisuuslaissa olisi tarve säätää NIS 2 –velvoitteista finanssisektorin toimijoille.

Lisäksi NIS2-direktiivin 2 artiklan 10 kohdan nojalla direktiiviä ei sovellettaisi toimijaan, johon DORA-asetusta ei sovelleta sen 2 artiklan 4 kohdan nojalla. Näitä toimijoita Suomessa ovat Finnvera Oyj ja Teollisen yhteistyön rahasto Oy (Finnfund). Laissa olisi tarpeen säätää tältä osin direktiiviä vastaavasta soveltamisalarajauksesta.

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 potilaiden oikeuksien soveltamisesta rajatylittävässä terveydenhuollossa (jäljempänä *potilasdirektiivi*) 3 artiklan g alakohdassa määritellyt terveydenhuollon tarjoajat. Potilasdirektiivin 3 artiklan g alakohdassa 'terveydenhuollon tarjoajalla' tarkoitetaan luonnollista henkilöä tai oikeushenkilöä tai muuta kokonaisuutta, joka tarjoaa laillisesti terveydenhuoltoa jonkin jäsenvaltion alueella. Potilasdirektiivin 3 artiklan a alakohdassa terveydenhuollolla tarkoitetaan terveydenhuollon ammattihenkilön potilaalle antamia terveyspalveluita potilaan terveydentilan arvioimiseksi, ylläpitämiseksi tai palauttamiseksi, mukaan lukien lääkkeiden ja lääkinnällisten laitteiden määrääminen, toimittaminen ja tarjoaminen.

Potilasdirektiivi on pantu täytäntöön rajat ylittävästä terveydenhuollosta annetulla lailla (1201/2013). Lisäksi 1.1.2024 on pääosin tullut voimaan sosiaali- ja terveydenhuollon valvonnasta annettu laki (741/2023), jonka 4 §:n 1-4 kohdassa määritellään sosiaali- ja terveydenhuollon palvelunjärjestäjä, palveluntuottaja, sosiaalipalvelu ja terveyspalvelu. NIS 2 –direktiivin terveydenhuollon vähimmäissoveltamisala kattaisi sosiaali- ja terveydenhuollon valvonnasta annetun lain 4 §:n 1 kohdassa tarkoitetut palvelunjärjestäjät, 2 kohdassa tarkoitetut palveluntuottajat, jotka tarjoavat terveyspalvelua, sekä veripalvelulain (197/2005) mukaiset veripalvelulaitokset, apteekit ja muut potilasdirektiivin mukaiset lääkkeitä ja lääkinnällisiä laitteita toimittavat ja tarjoavat toimijat. Hyvinvointialueisiin, Helsingin kaupunkiin ja HUS-yhtymään lakia sovelletaan niiden järjestämän ja tuottaman sosiaali- ja terveydenhuollon osalta sekä lisäksi julkishallinnon toimialan osalta. Lääkkeiden ja lääkinnällisten laitteiden määrääminen, toimittaminen ja tarjoaminen kuuluu potilasdirektiivin alaan silloin, kun lääkkeitä ja lääkinnällisiä laitteita määrää, toimittaa tai tarjoaa terveydenhuollon ammattihenkilö tai oikeushenkilö, jonka toiminta perustuu terveydenhuollon ammattihenkilöiden tarjoamaan palveluun. NIS 2 –direktiivin riskienhallinta- ja raportointivelvoitteesta olisi tarpeen säätää näitä toimijoita koskien. Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa (703/2023, jäljempänä *asiakastietolaki*) säädetään sosiaali- ja terveydenhuollon tietojärjestelmistä ja niiden turvallisuusvaatimuksista. Lain 67 § 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 66 § edellyttää, että arkistointipalvelu tulee suojata valtion viranomaisten tietoturvallisuutta koskevien velvoitteiden mukaisesti. Näistä velvoitteista säädetään julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019, jäljempänä *tiedonhallintalaki*), jonka 4 luku sisältää tietoturvaa koskevat säännökset, erityisesti 13 § tietoaineistojen ja tietojärjestelmien tietoturvallisuudesta ja 13 a § häiriötilanteista tiedottamisesta ja niihin varautumisesta.

Asiakastietolain 77 §:ssä säädetään palvelunantajalle, apteekille, välittäjälle ja Kansaneläkelaitokselle velvoite laatia tietoturvasuunnitelma, jossa käsitellään organisaation tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyviä keskeisiä asioita. Säännös velvoittaa palvelunantajan, välittäjän ja Kansaneläkelaitoksen laatimaan tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvän tietoturvasuunnitelman. Lain 97 §:n mukaan Terveyden- ja hyvinvoinnin laitos vastaa valtakunnallisten tietojärjestelmäpalvelujen suunnittelusta, ohjauksesta ja seurannasta. Terveyden- ja hyvinvoinnin laitokselle annetaan lisäksi valtuudet antaa tarkentavia turvallisuusmääräyksiä.

Asiakastietolain 77 § lisättiin lakiin sen päivityksen yhteydessä (HE 246/2022 vp, laki 703/2023). Lisäksi lakiin lisättiin uusi 90 §, jossa säädetään toimijoiden velvoitteesta ilmoittaa

tietojärjestelmän ja hyvinvointisovelluksen olennaisten vaatimusten poikkeamista sekä tietoverkkoihin kohdistuvasta tietoturvallisuuden häiriöstä. Muutokset tulivat 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 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 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 1 artiklan 2 alakohdassa määriteltyjen lääkkeiden tutkimusta ja kehitystä harjoittavat toimijat. Direktiivin 2001/83/EY 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 muuttamiseksi 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 lääkinnällisisistä 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 täydentävää 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 §). Yhdyskuntajätevesien käsittelyä säännellään ympäristönsuojelulailla (527/2014), valtioneuvoston asetuksella ympäristönsuojelusta (713/2014) ja valtioneuvoston asetuksella yhdyskuntajätevesistä (888/2006). Jäteveden käsittely on ympäristönsuojelulain nojalla ympäristöluvanvaraista toimintaa ja puhdistamoita koskevia varautumis- ja riskienhallintavelvoitteita on määrätty puhdistamojen ympäristölupapäätöksissä. Nämä velvoitteet eivät kuitenkaan erityisesti kohdistu tieto- tai kyberturvallisuuskysymyksiin.

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 kuutiometrin määritelmästä luovutaan. Soveltamisalan olisi määräydyttävä 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 tulisivat 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 sähköisen viestinnän palveluista annetun 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 sekä maa-asema- ja tutkatoiminnan harjoittaminen ovat 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 postin yleispalvelusta ja eräistä muista postipalveluista säädetään postilaissa

(415/2011). Kansallinen sääntely postipalvelujen osalta on perinteisesti keskittynyt postimarkkinoiden avaamiseen ja datan avoimuuteen eikä turvallisuusnäkökohtiin. Postipalveluista säädetään lisäksi yhteisön postipalvelujen sisämarkkinoiden kehittämistä ja palvelun laadun parantamista koskevista yhteisistä säännöistä annetussa Euroopan parlamentin ja neuvoston direktiivissä 97/67/EY (sellaisena kuin se on muutettuna direktiiveillä 2002/39/EY ja 2008/6/EY, jäljempänä *postidirektiivi*) sekä rajat ylittävistä 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 tarjoamisesta ei ole Suomessa erityissääntelyä, ja toiminta on siviilioikeudellisten yleissäännösten varassa.

Postilakiin 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 on valmisteltu 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. Valmistelu ei etene tällä hetkellä.

Kemikaaliturvallisuuslakiin lisättäisiin edellä mainitun hankkeen yhteydessä 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 teollinen tuotanto, jalostus ja tukkukauppa

Elintarvikkeiden teollinen tuotanto, jalostus ja tukkukauppa 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 a-luokan 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.

Taulukko 2: 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. Sähköturvallisuussääntelyssä 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.

Taulukko 3: 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 sektorikohtaistasääntelyä.

Taulukko 4: 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.

Taulukko 5: 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.

Taulukko 6: 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 kyberturvallisuuslakiin. 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 voisi kuulua NIS2-sääntelyn piiriin ehdotetun kyberturvallisuuslain nojalla. Kyberturvallisuuslailla 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 tietojenkäsittelylaitteista, 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 Kyberturvallisuutta koskevat 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. Direktiivin 20 artiklan edellyttämä johdon vastuu on myös rajattavissa rikosoikeudellisen laillisuusperiaatteen kannalta riittävän selkeästi ja tarkkarajaisesti kyberturvallisuusriskien hallintatoimenpiteiden hyväksymiseen ja valvomiseen.

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.

3.17 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).

3.18 Toimilupa- ja sertifiointisääntely

NIS2-direktiivin 32 artiklan 5 kohdan ensimmäisen alakohdan a-alakohdassa edellytetään, että toimivaltaisilla viranomaisilla olisi oltava toimivalta keskeyttää väliaikaisesti tai pyytää toista tahoa keskeyttämään väliaikaisesti kansallisen lainsäädännön mukaisesti sertifiointi tai lupa, joka koskee keskeisen toimijan tarjoamia asiaankuuluvia palveluja tai toimintoja taikka osaa niistä. Toimiluvan tai sertifioinnin keskeyttäminen tulisi kuitenkin kyseeseen vain, jos lievemmän puuttumiskeinot eivät ole olleet tuloksekkaita, ja jos toimivaltainen viranomainen on ensin asettanut toimijalle määräajan, jonka kuluessa havaitut puutteet olisi korjattava, mutta toimija ei olisi korjannut havaittuja puutteita määräajan kuluessa. Määrättyjä keskeyttämisiä olisi sovellettava siihen asti, kunnes toimija toteuttaa tarvittavat toimet korjatakseen ne puutteet tai noudattaakseen niitä toimivaltaisen viranomaisen vaatimuksia, joiden johdosta seuraamukset määrättiin. Toimiluvan peruuttamista koskeva säännös ei soveltuisi julkishallinnon toimijoihin.

NIS2-direktiivin säännös kohdistuu vain keskeisiin toimijoihin, eli vastaavaa toimivaltuutta ei olisi tarvetta säätää muiden kuin keskeisten toimijoiden osalta. Säännös kohdistuu lisäksi vain luvanvaraiseen tai sertifioituun toimintaan, eli vastaavaa toimivaltuutta ei olisi tarvetta säätää esimerkiksi ilmoituksen- tai rekisteröinninvaraisen toiminnan osalta. Edelleen, säännös kohdistuisi sertifioinnin tai luvan keskeyttämiseen kansallisen lainsäädännön mukaisesti, eli se ei kohdistuisi sellaisiin toimilupiin tai sertifiointeihin, joista on säädetty suoraan soveltuvassa EU-lainsäädännössä.

NIS2-direktiivin soveltamisalaan kuuluvia, keskeisiä toimijoita koskevaa kansallista toimilupa- tai sertifiointisääntelyä on tunnistettu maa-asema- tai tutkatoimintaa harjoittavien toimijoiden, teleyritysten, sähkö- ja maakaasuverkkojen haltijoiden, öljyn tai vedyn käsittelyä tai varastointia harjoittavien toimijoiden sekä lääkkeitä tai lääkeaineita valmistavien toimijoiden osalta.

Maa-asema- ja tutkatoimintaa harjoittavilta toimijoilta edellytetään maa-asemalain 4 §:ssä tarkoitettua toimilupaa. Luvan myöntää Liikenne- ja viestintävirasto, paitsi jos luvan myöntäminen ilmeisesti vaikuttaisi kansalliseen turvallisuuteen, jolloin luvan myöntää valtioneuvosto. Luvan myöntämisen edellytyksistä on säädetty maa-asemalain 4 §:ssä, ja luvan muuttamisesta ja peruuttamisesta on säädetty maa-asemalain 8 §:ssä. Luvan myöntänyt viranomainen voi muuttaa myönnettyä lupaa tai peruuttaa luvan, jos esimerkiksi toiminnanharjoittaja tai maa-asema- tai tutkatoiminta ei enää täytä luvan myöntämisen ehtoja, tai jos toiminnanharjoittaja on olennaisella tavalla laiminlyönyt tai rikkonut maa-asemalaissa säädettyä velvollisuutta tai rajoitusta taikka luvan ehtoja. Luvan peruuttamisen edellytyksenä on lisäksi, että luvan haltija ei viranomaisen kehotuksesta huolimatta ole kohtuullisessa määräajassa korjannut puutetta, virhettä, rikkomusta tai laiminlyöntiä. Lupa voitaisiin lisäksi peruuttaa vain erityisen painavista syistä tilanteissa, joissa luvan muuttaminen ei ole mahdollista. Luvan peruuttaminen ei vaikuttaisi olevan mahdollista sillä perusteella, että toiminnanharjoittaja on laiminlyönyt muussa kuin maa-asemalaissa säädettyjä velvollisuuksia. Maa-asemalain 8 §:ään onkin katsottu tarpeelliseksi lisätä maininta ehdotetun kyberturvallisuuslain velvoitteiden olennaisesta rikkomisesta luvan peruuttamisen perusteena.

Yleisten sähköisten viestintäverkkojen tarjoajien sekä yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajien, eli teleyritysten toiminta edellyttää sähköisen viestinnän palveluista annetun lain 3 luvussa tarkoitettua verkkotoimilupaa. Teletoimintaan verkkotoimiluvan myöntää valtioneuvosto. Teletoiminnan osalta NIS-sääntelyä valvova viranomainen olisi kuitenkin Liikenne- ja viestintävirasto. Sähköisen viestinnän palveluista annettuun lakiin ei ole tunnistettu tarpeelliseksi tehdä muutoksia toimilupasääntelyn osalta, sillä kyse ei olisi valvovan viranomaisen myöntämän luvan peruuttamisesta.

Sähköverkkotoimintaa saa eräin poikkeuksin harjoittaa Suomessa sijaitsevassa sähköverkossa vain Energiaviraston myöntämällä sähköverkkoluvalla. Sähköverkkoluvan myöntämisestä on säädetty sähkömarkkinalain 5 §:ssä. NIS2-direktiivin soveltamisalaan kuuluvista keskeisistä toimijoista ainakin sähkön jakelu- tai kantaverkon haltijoilla tulisi olla sähkömarkkinalain mukainen sähköverkkolupa. Samoin maakaasuverkkotoimintaa saa eräin poikkeuksin harjoittaa Suomessa sijaitsevassa maakaasuverkossa vain Energiaviraston myöntämällä maakaasuverkkoluvalla. Maakaasuverkkoluvan myöntämisestä on säädetty maakaasumarkkinalain 5 §:ssä. NIS2-direktiivin soveltamisalaan kuuluvista keskeisistä toimijoista ainakin maakaasun siirto- tai jakeluverkon haltijoilla tulisi olla maakaasumarkkinalain mukainen maakaasuverkkolupa. Sähkö- ja maakaasuverkkoluvan peruuttamisesta säädetään sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain (590/2013) 23 §:ssä. Sen mukaan Energiavirasto voi peruuttaa sähkö- tai maakaasuverkkoluvan, jos luvanhaltija lopettaa verkkotoiminnan, ei enää täytä luvan myöntämisen edellytyksiä tai toistuvasti ja oleellisesti rikkoo lupaehtoja, tai eräitä sähkö- tai maakaasuverkkotoimintaa koskevia säädöksiä, eikä luvanhaltijalle etukäteen annettu varoitus luvan peruuttamisesta ole johtanut toiminnassa esiintyneiden puutteiden korjaamiseen. Luvan peruuttaminen ei vaikuttaisi olevan mahdollista sillä perusteella, että luvanhaltija on laiminlyönyt ehdotetussa kyberturvallisuuslaissa säädettyjä velvollisuuksia. sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain 23 §:ään onkin katsottu tarpeelliseksi lisätä maininta ehdotetun kyberturvallisuuslain velvoitteiden toistuvasta ja olennaisesta rikkomisesta luvan peruuttamisen perusteena.

Kemikaaliturvallisuuslain 23 §:n mukaan vaarallisen kemikaalin laajamittaista teollista käsittelyä ja varastointia saa harjoittaa vain Turvallisuus- ja kemikaaliviraston luvalla. Kyseinen toimilupavaatimus saattaa koskea NIS2-soveltamisalaan kuuluvista keskeisistä toimijoista etenkin öljy- ja vetyalan toimijoita. Luvan myöntämisestä säädetään kemikaaliturvallisuuslain 23 a §:ssä ja peruuttamisesta 109 §:ssä. Valvontaviranomaisen tulee peruuttaa toiminnanharjoittamista koskeva lupa osittain tai kokonaan, jos toiminnanharjoittajan toteuttamissa toimenpiteissä onnettomuuksien estämiseksi ja rajoittamiseksi on todettu olevan vakavia puutteita. Sama koskee myös vaarallisten kemikaalien siirtoa. Lisäksi valvontaviranomainen voi peruuttaa toiminnanharjoittamista koskevan luvan, jos toiminnanharjoittaja ei ole määräajassa toimittanut vaadittua ilmoitusta tai selvityksiä taikka muita kemikaaliturvallisuuslain nojalla annettujen säännösten edellyttämiä tietoja toimenpiteistään onnettomuuksien estämiseksi tai rajoittamiseksi tai jos toiminnasta on todettu muutoin aiheutuvan kemikaaliturvallisuuslain 109 §:n 1 momentissa tarkoitettua vaaraa vähäisempää vaaraa. Luvan peruuttaminen ei vaikuttaisi olevan mahdollista sillä perusteella, että toiminnanharjoittaja on laiminlyönyt ehdotetussa kyberturvallisuuslaissa säädettyjä velvollisuuksia. Kemikaaliturvallisuuslain 109 §:ään onkin katsottu tarpeelliseksi lisätä maininta ehdotetun kyberturvallisuuslain velvoitteiden olennaisesta ja vakavasta rikkomisesta luvan peruuttamisen perusteena. Lääkkeiden valmistus edellyttää lääkelain 8 §:n mukaista lupaa (niin kutsuttu lääketehdaslupa). Lääkelain 8 §:n mukaisen luvan myöntää Lääkealan turvallisuus- ja kehittämiskeskus. Lääkelain 101 a §:ssä säädetään tilanteista, jolloin Lääkealan turvallisuus- ja kehittämiskeskus voi peruuttaa lääkkeiden valmistustoiminnan harjoittamiseen myönnetyn luvan väliaikaisesti tai kokonaan. Luvan voisi peruuttaa, jos jokin luvan myöntämiseen liittyvä vaatimus ei enää täyty tai jos jotakin turvallisuuden tai laadun kannalta olennaista velvoitetta ei ole täytetty. Ehdotetun kyberturvallisuuslain velvoitteiden on arvioitu olevan sellaisia turvallisuuden kannalta olennaisia vaatimuksia, että niiden laiminlyönti voisi täyttää toimiluvan peruuttamisen edellytykset. Lääkelakiin ei ole tunnistettu tarpeelliseksi tehdä muutoksia toimilupasääntelyn osalta.

NIS 2 –direktiivin 32 artiklan 5 kohdan a-alakohdan täytäntöönpano edellyttäisi edellä arvioituja muutoksia kansalliseen toimilupasääntelyyn.

4 Ehdotukset ja niiden vaikutukset

4.1 Keskeiset ehdotukset

Esityksessä ehdotetaan säädettäväksi uusi kyberturvallisuuslaki. Laki sisältäisi kootusti NIS2-direktiivin edellyttämät kyberturvallisuuden riskienhallintaa ja poikkeamaraportointia koskevat vähimmäisvelvoitteet sen soveltamisalaan kuuluville toimijoille. Laissa noudatettaisiin NIS2-direktiivin edellyttämää vähimmäistasoa velvoitteiden soveltamisalan, laajuuden ja valvonnan suhteen. Lisäksi laissa säädettäisiin direktiivin edellyttämällä tavalla viranomaistehtävistä, eli valvovasta viranomaisesta, velvoitteiden noudattamisen valvonnasta ja valvontatoimivaltuuksista sekä hallinnollisesta seuraamusmaksusta, jonka määräisi uusi Liikenne- ja viestintäviraston yhteyteen perustettava seuraamusmaksulautakunta. Laissa säädettäisiin myös tietoturvaloukkauksiin reagoivasta ja niitä tutkivasta yksiköstä (CSIRT-yksikkö) ja sen tehtävistä. CSIRT-yksikkö sijoitettaisiin Liikenne- ja viestintäviraston Kyberturvallisuuskeskukseen. Direktiivin pääasiallinen täytäntöönpanomenetelmä olisi uudelleenkirjoittaminen. Direktiivin velvoitteet ja vaatimukset uudelleen kirjoitettaisiin kansalliseen lainsäädäntöön erityisesti siltä osin, kun ne kohdistuvat toimijoihin. Täytäntöönpano tehtäisiin direktiivin vähimmäisvaatimusten mukaisesti ja kansallista liikkumavaraa hyödyntäen.

Yksinomaan julkishallinnon toimialaan kohdistuvista velvoitteista ja niiden noudattamisen valvonnasta säädettäisiin erikseen tiedonhallintalaissa. 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 kyberturvallisuuslain 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 kyberturvallisuuslain perusteella, mikäli se harjoittaisi lain liitteessä I tai II tarkoitettua toimintaa tai CER-direktiivin nojalla kriittiseksi tunnistettua toimintaa ja täyttäisi sen toiminnan osalta toimijan määritelmän. Paikallistason julkishallintoa koskevan kansallisen liikkumavaran mukaisesti velvoitteita ei sovellettaisi muilta osin kuntiin.

Finanssialan toimijoita ei ehdoteta sisällytettävän kyberturvallisuuslain 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 verkkotunnusten rekisteröintitietojen tietokantaa koskevan NIS2-direktiivin 27 ja 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:

Taulukko 7:

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 ja maakaasun toimittajat) ja vedyn siirtoa harjoittavat toimijat.
Turvallisuus- ja kemikaalivirasto	Kaasu (varastointilaitteiston haltijat, käsittelylaitteiston haltijat, maakaasualan yritykset sekä maakaasun jalostus- ja käsittelylaitteistojen haltijat), öljy, vedyn tuotanto ja varastointi, 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	Terveyspalvelun tuottajat ja EU:n vertailulaboratoriot
Etelä-Savon ELY-keskus	Juomavesi, jätevesi ja jätehuolto
Ruokavirasto	Elintarvikeyritykset, jotka harjoittavat tukkukauppaa, teollista tuotantoa tai jalostusta
Lääkealan turvallisuus ja kehittämiskeskus	Lääkkeiden tutkimus ja kehitys, lääkeaineita, lääkkeitä ja lääkinnällisiä laitteita valmistavat toimijat, In vitro – diagnostiikkaan tarkoitettuja lääkinnällisiä laitteita valmistavat toimijat, veripalvelulaitokset, apteekit ja terveydenhuollon ammattihenkilönä lääkkeitä ja lääkinnällisiä laitteita toimittavat ja tarjoavat toimijat.

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 parannetaan yhteiskunnan toiminnan kannalta keskeisten toimialojen ja palveluiden kyberturvallisuutta sekä kykyä sietää, vastustaa ja palautua kyberhäiriöistä, kyberhyökkäyksistä ja 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 esityksellä pyritään välttämään ja joiden realisoitumisen estämisellä saavutetaan esityksen merkittävin hyöty sekä yhteiskunnan että soveltamisalaan kuuluvien organisaatioiden kannalta.

Kyberturvallisuuslain mukaiset velvoitteet aiheuttavat sääntelyn kohteena oleville toimijoille kustannuksia velvoitteiden noudattamisesta. Kustannuksien määrään vaikuttaa olennaisesti sääntelyn kohteena olevan toimijan ennestään suorittaman riskienhallinnan taso, toiminnan laatu ja laajuus, toimintaan kohdistuvien riskien taso ja toimijan tarpeelliseksi arvioimien riskienhallintatoimenpiteiden laatu. Kustannuksia velvoitteiden noudattamiseksi syntyy erityisesti toimialoilla, jotka eivät ole ennestään NIS1-direktiivin velvoitteiden piirissä. Niille toimijoille, joilla kyberturvallisuuden riskienhallinnan taso on entuudestaan lain edellyttämällä vähimmäistasolla, lain voimaantulosta aiheutuu vain vähäisiä kustannuksia.

Julkisen sektorin organisaatioille tiedonhallintalain mukaisten velvoitteiden noudattamisesta arvioidaan aiheutuvan jonkin verran kustannuksia, jotka katetaan olemassa olevien määrärahojen puitteissa. Sellaiselle julkishallinnon toimijalle, joka ylläpitää useiden viranomaisten hyödyntämiä tai laajasti käytössä olevia tietojärjestelmiä, esityksestä aiheutuvien kustannuksien määrä on suurempi, kuin muussa julkishallinnossa.

Vaikka velvoitteiden kohteille aiheutuisi kustannuksia niiden noudattamisesta, saavutetaan velvoitteiden myötä paremmalla kyberhyökkäyksiin varautumisella, reagoinnilla ja tiedonvaihdolla 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.

Julkiselle sektorille ja julkistaloudelle aiheutuu kustannuksia NIS2-direktiivin täytäntöönpanon edellyttämistä viranomaistehtävistä erityisesti velvoitteiden valvonnasta ja CSIRT-yksikön toiminnasta, mistä säädettäisiin kyberturvallisuuslaissa sekä julkishallinnon toimialan osalta tiedonhallintalaissa. Velvoitteiden valvonnasta ja CSIRT-yksikön toiminnasta aiheutuisi lisäresurssitarpeita niille viranomaisille, joille näitä tehtäviä osoitetaan. Lisäksi esityksellä olisi vaikutuksia Tietosuojavaltuutetun toimistolle.

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 teollinen tuotanto, jalostus ja tukkukauppa, 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 kuten jaksossa 4.2.2 esitetään. Toimijoiden määrä ja vaikutukset vaihtelevat toimialoittain.

Ehdotuksella olisi vaikutuksia julkishallintoon sääntelyn valvojana ja sen kohteena. NIS2-direktiivin edellyttämät riskienhallintaa ja poikkeamaraportointia koskevat vaatimukset koskisivat tiedonhallintalakiin esitettyjen muutoksien myötä 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 kasvavat 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 kolmiportaiseksi. 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

Yhteenveto

Kyberturvallisuuslain soveltamisalan arvioidaan kattavan yhteensä noin 2500–5000 toimijaa. Näistä organisaatioista noin 10–20 % on kuulunut NIS1-direktiiviä täytäntöönpanevien velvoitteiden alaan. Näistä organisaatioista keskeisiä toimijoita arvioidaan olevan noin 10 % eli 250–500 kappaletta. Tiedonhallintalain uuden 4 a luvun soveltamisalaan arvioidaan tulevan noin 160 julkishallinnon organisaatiota, jotka ovat pääosin keskeisiä toimijoita.

Kyberturvallisuuslain soveltamisalaan kuuluvien toimijoiden määrän arviossa merkittävää epävarmuutta liittyy erityisesti energia-, kemikaali- ja valmistustoimialojen osalta soveltamisalaan uusina tulevien organisaatioiden määrään, joka voi olla huomattava. Ilman näitä toimialoja soveltamisalaan arvioidaan kuuluvan noin 1700 – 2200 toimijaa. Merkittävää epävarmuutta arvioon toimijoiden kokonaismäärästä aiheuttaa myös eroavaisuudet siinä, millä tavalla konsernirakenteiset organisaatiot ovat järjestäneet toimintaansa erillisiin yhtiöihin. Lisäksi epävarmuutta arviossa kokonaismäärästä liittyy soveltamisalaa koskevan yleisen kokorajoituksen poikkeuksiin ja poikkeuksien johdosta soveltamisalaan kuuluvien pien- ja mikroyritysten määrään. Soveltamisalaan kuuluvien toimijoiden määrästä saataisiin tilastotietoa lain voimaantulon jälkeen toimijailmoituksiin perustuen.

Soveltamisalaan kuuluvien ja erityisesti keskeisten toimijoiden määrään vaikuttaa myös se, minkä verran organisaatioita tunnistetaan CER-direktiivin tarkoittamalla tavalla kriittiseksi Suomessa. Tämä tunnistaminen tehdään lakiehdotuksen voimaantulon jälkeen ja perustuisi CER-direktiivin kansallista täytäntöönpanoa koskevaan lakiehdotukseen. Oletettavaa on, että merkittävä osa näistä toimijoista kuuluisi jo ennalta velvoitteiden soveltamisalaan, mutta osa toimijoista tulee uutena, sillä NIS2- ja CER-direktiivien soveltamisalaan liittyy eroavaisuuksia. Lisäksi CER-kriittiseksi määrittely voi määrittää keskeisiksi toimijoiksi sellaisia toimijoita, jotka eivät niitä muuten kokonsa tai toimialansa vuoksi olisi.

NIS1-direktiiviä täytäntöönpanevien velvoitteiden alaan on kuulunut noin 800–1000 toimijaa painottuen määrällisesti terveys-, finanssi- ja digitaalisen infrastruktuurin toimialoille. Lisäksi terveydenhuollon toimialalla sääntelyn alaan on lainsäädäntöteknisesti kuulunut määrällisesti merkittävä joukko pieniä toimijoita, joiden osalta kriittisyyden määrittäminen on ollut täsmentymätöntä. Osa NIS1-velvoitteiden alaan kuuluneista toimijoista ei kuuluisi kyberturvallisuuslain soveltamisalaan, erityisesti soveltamisen yleisen kokorajoituksen vuoksi. Lisäksi kyberturvallisuuslaki ei koskisi finanssisektorin toimialan yrityksiä, joita koskevista

vaatimuksista säädettäisiin EU:n DORA-asetuksella ja sitä täydentävällä kansallisella lainsäädännöllä.

Vuonna 2022 kaikilla toimialoilla Suomessa on toiminut yhteensä noin 3.800 yritystä, jotka työllistävät 50 henkeä tai enemmän. Lain soveltamisalaan voisi tulla myös edellä kuvatulla tavalla yritysten ohella muita oikeushenkilöitä tai luonnollisia henkilöitä, mukaan lukien julkishallinnon organisaatioita, niiden oikeudellisesta muodosta riippumatta, jos ne harjoittaisivat lain liitteissä tarkoitettua toimintaa. Lisäksi lain soveltamisalaan voisi tulla vähemmän kuin 50 henkeä työllistäviä yrityksiä, jos ne täyttävät keskisuuren toimijan määritelmän liikevaihtonsa ja taseensa koon johdosta taikka jos niiden kynnysarvojen laskennassa huomioidaan omistusyhteyksiensä johdosta myös omistavan yrityksen tunnuslukuja. Vuonna 2022 kaikilla toimialoilla Suomessa on ollut rekisteröitynä yhteensä 571 742 yritystä, joista 37 931 on työllistänyt 5 henkeä tai enemmän. Pien- ja mikroyritykset eivät kuuluisi esityksen soveltamisalaan eräitä NIS2-direktiivin vähimmäissoveltamisalan edellyttämiä poikkeuksia lukuun ottamatta. [3]

Kyberturvallisuuslain 3 §:n 3 momentissa säädettäisiin NIS2-direktiivin 2 artiklan 2 kohdan b-e alakohtaa vastaavista erityiskriteereistä, joiden alaan kuuluva organisaatio kuuluisi velvoitteiden soveltamisalaan sen koosta riippumatta. Näitä organisaatioita arvioidaan olevan määrällisesti alle 10 kappaletta.

NIS2-direktiivin ja kyberturvallisuuslain 27 §:n 2 momentissa tarkoitettuja keskeisiä toimijoita arvioidaan olevan noin 250 – 500 kappaletta. Keskeisiä toimijoita olisivat eräillä toimialoilla toimivat yritykset, jotka ylittävät keskisuuren toimijan kriteerit. Lisäksi keskeisiä toimijoita olisivat 27 §:n 2 momentissa tarkoitetut toimijat niiden koosta riippumatta sekä CER-direktiivin nojalla kriittiseksi tunnistettavat toimijat. Kokonaismääräarvioon liittyy samoja epävarmuuksia, joita edellä on kuvattu. Keskeisten toimijoiden määrästä saataisiin tilastotietoa lain voimaantulon jälkeen toimijailmoituksiin perustuen. Vuonna 2022 kaikilla toimialoilla Suomessa on toiminut yhteensä noin 669 yritystä, jotka työllistävät 250 henkeä tai enemmän, eli ylittävät keskisuuren toimijan kriteerin henkilöstömäärän perusteella.[4] Lisäksi soveltamisalaan voisi tulla alle 250 henkeä työllistäviä yrityksiä, jos ne ylittävät keskisuuren yrityksen määritelmän liikevaihdon tai taseen laajuuden perusteella.

Soveltamisala toimialoittain

Kyberturvallisuuslain soveltamisala kattaisi yritykset, yhteisöt, julkishallinnon organisaatiot ja muut oikeushenkilöt niiden oikeudellista muodosta riippumatta, 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.

---

[3] Lähde yrityksien määrälle: Tilastokeskus, yritysten rakenne- ja tilinpäätöstilasto, yritykset toimialoittain ja henkilöstön suuruusluokittain 2018-2022 (13w1).

[4] Lähde yrityksien määrälle: Tilastokeskus, yritysten rakenne- ja tilinpäätöstilasto, yritykset toimialoittain ja henkilöstön suuruusluokittain 2018-2022 (13w1).

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 tiedonhallintalaissa määriteltävät julkishallinnon sektorin toimijat sekä toimijat silloin, jos toimijat ovat yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajia; luottamuspalvelun tarjoajia; aluetunnusrekisterien ylläpitäjiä; 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 rajat ylittäviä 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.

NIS 2 –direktiivissä säädettyjä riskienhallinta- ja raportointivelvoitteita sovellettaisiin sen liitteissä määriteltyihin toimijatyyppeihin seuraavilla toimialoilla.

Taulukko 8:

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 teollinen tuotanto, jalostus ja tukkukauppa
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. Pankkitoiminta ja finanssimarkkinoiden infrastruktuuri –toimialan osalta NIS 2 –direktiivin velvoitteet pantaisiin täytäntöön DORA-asetuksella ja sitä täydentävällä kansallisella sääntelyllä. Muilta osin velvoitteet pantaisiin täytäntöön kyberturvallisuuslailla.

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:

Taulukko 9:

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.

Liikennesektorin osalta soveltamisalaan kuuluisivat seuraavat toimijatyypit:

Taulukko 10:

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 olemassa olevaa 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 myös tiedonhallintalaissa osana julkishallinnon toimialan velvoitteita. Yksityiset sosiaali- ja terveydenhuollon toimijat kuuluisivat ainoastaan kyberturvallisuuslain soveltamisalaan. Yksityisiä terveydenhuollon toimijoita, joilla on vähintään 50 työntekijää, arvioidaan olevan tällä hetkellä noin 150 kpl ja määrä on edelleen kasvussa. Valvovana viranomaisena on toiminut ja toimisi jatkossakin NIS1-velvoitteiden osalta Valvira.

Tällä hetkellä julkisen ja yksityisen terveydenhuollon yksiköillä sekä apteekeilla on velvollisuus liittyä Kanta-palveluihin. Tämä edellyttää käyttämään turvallisuusvaatimukset täyttäviä tietojärjestelmiä, jotka sertifioidaan ulkopuolisen tahon puolesta. Organisaatioiden on myös tehtävä asiakastietolain 77 §:ssä tarkoitettu tietoturvasuunnitelma. Asiakastietolaissa on säädetty Kanta-palveluihin liittymisestä, sertifioinnista sekä annettu Terveyden- ja

hyvinvoinnin laitokselle valtuudet antaa määräyksiä vaadittavista turvallisuusominaisuuksista sekä tietoturvasuunnitelman sisällöstä. Lisäksi on säädetty velvollisuudesta ilmoittaa poikkeamista Valviralle. NIS2-direktiivi ei aiheuta terveydenhuollon palveluntarjoajille merkittäviä lisätoimenpiteitä.

Uusina toimijoina NIS2-direktiivin myötä soveltamisalaan tulevat veripalvelulaitokset, apteekit ja muut lääkkeitä ja lääkinnällisiä laitteita toimittavat ja tarjoavat toimijat, EU:n vertailulaboratoriot, lääkkeiden tutkimus ja kehitystoiminta sekä lääkkeiden, lääkeaineiden tai lääkinnällisten laitteiden valmistus.

Veripalvelun osalta Suomessa toimii vain yksi toimiluvallinen veripalvelutoimija, jolla on päätoimipisteen lisäksi 10 toimipistettä eri puolilla maata. Apteekkien osalta Suomessa toimii yhteensä 630 pääapteekkia sekä 190 sivuapteekkia. Avohuollon apteekkien lisäksi sääntely kattaisi lääkekeskukset sekä laitosten lääkehuollosta vastaavat sairaala-apteekit, joita on yhteensä 24 kappaletta. Hyvinvointialueiden sairaala-apteekkitoiminta ja yksityisten palveluntuottajien lääkekeskukset olisivat kuitenkin lain soveltamisalan piirissä jo sen vuoksi, että apteekkitoiminta on osa toimijan terveyspalveluita. Lisäksi Suomessa on tällä hetkellä noin 100 lääketukkukauppatoimiluvan haltijaa, joista ainakin osa kuuluisi todennäköisesti sääntelyn soveltamisalaan. EU:n vertailulaboratorioita ei ole Suomessa toistaiseksi vielä ollenkaan.

Lääkkeiden tutkimus- ja kehitystoimintaa harjoittavia laboratorioita on arvioitu olevan Suomessa vain muutamia. Lääkkeiden valmistuksen osalta Suomessa toimii yhteensä 35 teollisen lääkevalmistuksen toimiluvan haltijaa, joiden toiminta vaihtelee paljon valmistettavan lääkevalikoiman ja valmistusvolyymien osalta. Lääkinnällisiä laitteita valmistavia toimijoita on Suomessa satoja, mutta vakavan kansanterveysuhan aikana kriittisiksi katsottuja lääkinnällisiä laitteita valmistavia toimijoita on arvioitu olevan noin 30.

Terveyssektorilla NIS2-direktiivin laajeneva soveltamisala toisi velvoitteiden alaan uusia toimijatyyppejä ja siten kasvattaisi valvottavien toimijoiden määrää. Valvovana viranomaisena toimisi EU:n vertailulaboratorioiden osalta Valvira. Sen sijaan lääkkeiden tutkimus- ja kehitystoiminnan sekä lääkeaineiden, lääkkeiden ja lääkinnällisten laitteiden valmistuksen, veripalvelulaitosten, apteekkien ja muiden lääkkeitä ja lääkinnällisiä laitteita toimittavien ja tarjoavien toimijoiden osalta valvovana viranomaisena toimisi Fimea.

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 voimaan 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 täytäntöönpanon 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. 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 kappaletta ja keskeisen toimijan kokokriteerin ylittäviä toimijoita alle 5 kappaletta.

Mikäli NIS2-velvoitteiden täytäntöönpanoa koskevaan lakiin ei sisältyisi soveltamisen rajausta kuntia koskien, johtaisi tämä Suomessa siihen, että pienimuotoistakin vesihuoltotoimintaa harjoittava kunta tulisi kunnan koko toiminnan osalta NIS2-velvoitteiden soveltamisalaan, mikäli kunta ei ole eriyttänyt vesihuoltoa tai muuta NIS2-direktiivin liitteessä tarkoitetun toiminnan harjoittamista kunnasta erilliseen oikeushenkilöön. Tämän vaikutuksen ei odoteta realisoituvan, koska laissa säädettäisiin NIS2-direktiivin kansallisen liikkumavaran sallimalla tavalla kunnan rajaamisesta soveltamisalan ulkopuolelle muun kuin NIS2-direktiivin liitteessä tarkoitetun toiminnan osalta.

Valvovana viranomaisena juoma- ja jätevesisektorin osalta on toiminut Etelä-Savon 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, aluetunnusrekisterien

ylläpitäjät 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, jonka mukaan toimija kuuluisi soveltamisalaan sen koosta riippumatta (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, aluetunnusrekisterien ylläpitäjät, pilvipalvelujen tarjoajat, datakeskuspalvelujen tarjoajat, sisällönjakeluverkkojen tarjoajat sekä verkossa toimivien markkinapaikkojen tarjoajat, verkossa toimivien hakukoneiden tarjoajat 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 soveltamisalaan kuulumiselle 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 toimijoille. Valvovana viranomaisena toimisi Liikenne- ja viestintävirasto.

Avaruus

Avaruus on uusi sektori NIS2-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 NIS2-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 postipalvelun 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 2022 postimarkkinaselvityksessä[5] 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 posti- ja kuriiripalvelujen tarjoajista jäisi kuitenkin soveltamisalan kokorajauksen myötä todennäköisesti sääntelyn soveltamisalan ulkopuolelle. Postipalvelujen osalta soveltamisalan piiriin kuuluisi Suomesta ainakin Posti Group Oyj, jonka tytäryhtiö Posti Jakelu Oy toimii tällä hetkellä postilain mukaisena yleispalvelun tarjoajana. Suomessa toimivista postipalvelujen tarjoajista useiden on arvioitu jäävän kokorajoituksen myötä lain soveltamisalan ulkopuolelle. Soveltamisalan piiriin on arvioitu kuuluvan Posti Group Oyj:n ohella vain yksittäisiä toimijoita posti- ja kuriiripalveluiden toimialalla. Valvovana viranomaisena toimisi Liikenne- ja viestintävirasto.

Jätehuolto

Jätehuolto on uusi toimiala 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.

[5] Postimarkkinaselvitys, Liikenne- ja viestintävirasto (2022).

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 §: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. Joukossa on useita kuntien omistamia yrityksiä tai kuntayhtymiä. Suurimmat toimijat ovat osa yrityskonserneja, jotka voivat kuulua sääntelyn soveltamisalaan myös muun toiminnan kuin jätehuollon osalta.

Mikäli NIS2-velvoitteiden täytäntöönpanoa koskevaan lakiin ei sisältyisi soveltamisen rajausta kuntia koskien, johtaisi tämä Suomessa siihen, että pienimuotoistakin jätehuoltotoimintaa harjoittava kunta tulisi kunnan koko toiminnan osalta NIS2-velvoitteiden soveltamisalaan, mikäli kunta ei ole eriyttänyt jätehuoltoa tai muuta NIS2-direktiivin liitteessä tarkoitetun toiminnan harjoittamista kunnasta erilliseen oikeushenkilöön. Tämän vaikutuksen ei odoteta realisoituvan, koska laissa säädettäisiin NIS2-direktiivin kansallisen liikkumavaran sallimalla tavalla kunnan rajaamisesta soveltamisalan ulkopuolelle muun kuin NIS2-direktiivin liitteessä tarkoitetun toiminnan 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 teollinen tuotanto, jalostus ja tukkukauppa

Elintarvikkeiden teollinen tuotanto, jalostus ja tukkukauppa on uusi toimiala NIS-sääntelyn piirissä. Soveltamisalaan kuuluisivat elintarvikeyritykset, jotka harjoittavat teollista tuotantoa tai jalostusta taikka tukkukauppaa. Elintarvikesektorilla Suomessa suurten yritysten rooli on keskeinen sekä valmistavassa teollisuudessa että tukkukaupassa. 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. ruokaöljyjä 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. Elintarvikesektorin toimijoita valvoisi NIS2-velvoitteiden osalta Ruokavirasto. Kyberturvallisuuteen liittyvät valvontatehtävät ovat uusia Ruokavirastolle. Elintarvikesektorin toimijoihin kohdistuvaa muuta elintarvikevalvontaa 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. Elintarvikesektorilla toiminnan ominaispiirteenä on toimitus- ja tukkuketjun korostunut rooli toiminnan jatkuvuuden kannalta.

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 työntekijämäärän tai vuosiliikevaihdon ja taseen perusteella tai siksi, että ne ovat CER-direktiivin perusteella kriittisiä toimijoita.

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-tukkukauppiaiden mukaan noin 85–90 % julkisista toimijoista tekee elintarviketilauksensa konekielisinä. Foodservice on verkostoitunutta toimintaa, jossa jokaisella on oma roolinsa, jolloin toiminta voi olla altis kyberhäiriöille.

Elintarvikevalvontaviranomaisen valvonnassa olevien elintarvikealan yritysten rakennetta on kuvattu taulukossa 11. 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. Keskeiset sairaaloille, vanhainkoteihin, kouluihin ja päiväkoteihin ruokaa valmistavat ruokapalvelutoimijat tulevat NIS2-direktiivin soveltamisen piiriin, koska ne ovat CER-direktiivin mukaisia kriittisiä toimijoita.

Elintarvikepakkaukset ovat kriittisen tärkeitä elintarvikkeiden tuotannon, jalostuksen ja jakelun kannalta. Ruokaviraston 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 yhteensä noin 160 kappaletta. Näistä keskeisiä toimijoita arvioidaan olevan lähes 50.

Taulukko 11: Elintarvikevalvontaviranomaisen rekisterissä vuonna 2022 olleiden toimipaikkojen perusteella tehty arvio NIS2-direktiivin mukaisista tärkeistä ja keskeisistä toimijoista

Toimiala	Arvio muista kuin NIS2 keskeisistä 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 kasvisala	4	2
Tukkukauppa	7	
Ruokapalvelutoimijat	-	3
Elintarvikepakkausten valmistus	-	5
Yhteensä	159	46

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.

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

Taulukko 12:

Lääkinnälliset laitteet	Lääkinnällisten laitteiden ja in vitro -diagnostiikkaan tarkoitettujen lääkinnällisten laitteiden valmistus
Tietokoneiden sekä elektronisten ja optisten tuotteiden valmistus	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 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 digitalisaatio on johtanut yhä kasvavaan kyberhyökkäyspinta-alaan ja toimijoiden tarpeeseen kehittää kyberturvallisuuden riskienhallintaa ja häiriötilanteisiin varautumista oma-aloitteisesti. Valmistustoimintaa harjoittavista yrityksistä merkittävä osa on 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.

Julkishallinnon toimiala

Julkishallinnon toimialan toimijat tulisivat uutena toimijatyyppinä NIS-velvoitteiden soveltamisalaan, sillä julkishallinto ei toimialana ole kuulunut NIS1-direktiivin soveltamisalaan. Julkishallinnon toimialan toimijoihin ei sovellettaisi kokokriteeriä ja soveltamisala määräytyisi tiedonhallintalaissa säädetyn mukaisesti. Velvoitteet olisivat julkishallinnon toimialalla uusia ja niiden valvominen uusi tehtävä. Valvovana viranomaisena toimisi Liikenne- ja viestintävirasto.

Julkishallinnon toimialan toimijoina tiedonhallintalain uuden 4 a luvun soveltamisalaan tulisi yhteensä noin 160 julkishallinnon toimijaa. Luku sisältää valtion keskushallinnon, virastot ja

laitokset, valtion liikelaitokset sekä itsenäiset julkisoikeudelliset laitokset ja hyvinvointialueet ja –yhtymät mukaan luettuna Helsingin kaupungin. Määrä ei sisällä niitä viranomaisia, joihin tiedonhallintalakiin ehdotettua velvoitteiden täytäntöönpanoa koskevaa uutta lukua ei sovellettaisi, kuten esimerkiksi ulkomaanedustustoja.

Keskeiset ja tärkeät toimijat

NIS2-direktiivi jakaa velvoitteiden soveltamisalaan kuuluvat toimijat keskeisiin ja tärkeisiin toimijoihin. Edellä jaksossa 2 esitetyllä tavalla direktiivi edellyttää keskeisiin toimijoihin kohdistuvaa ennakkovalvontaa ja tärkeiden toimijoiden osalta vain jälkikäteisvalvontaa. Lisäksi direktiivin edellyttää keskeisiin toimijoihin kohdistuvia eräitä valvontatoimivaltuuksia, joita tärkeiden toimijoiden osalta ei edellytetä. Lisäksi direktiivi asettaa keskeisiin toimijoihin kohdistuvan seuraamusmaksun alimman sallitun enimmäismäärän korkeammalle tasolle kuin tärkeiden toimijoiden osalla.

Kyberturvallisuuslain 27 §:ssä määritettäisiin keskeiset toimijat. Toimijat, joita ei erikseen määriteltäisi keskeisiksi, olisivat NIS2-direktiivin tarkoittamia tärkeitä toimijoita, eli muita kuin keskeisiä toimijoita. Jos toimija olisi joltain osin keskeinen, koko toimijaa olisi pidettävä keskeisenä toimijana. Tiedonhallintalain 4 a luvun soveltamisalaan kuuluvat tiedonhallintayksiköt olisivat julkishallinnon toimialan keskeisiä toimijoita., lukuun ottamatta hyvinvointialueita ja hyvinvointiyhtymiä sekä Helsingin kaupunkia, jotka olisivat tärkeitä toimijoita.

Alla olevassa taulukossa havainnollistetaan eroa keskeisten ja tärkeiden toimijoiden välillä.

Taulukko 13:

Keskeinen toimija	Muu kuin keskeinen toimija (tärkeä toimija)
Kyberturvallisuuslain liitteessä I tarkoitettu toimija (joka ylittää keskisuuren kriteerin eli on kooltaan suuri) Luottamuspalvelun tarjoaja, aluetunnusrekisterin ylläpitäjä, DNS-palveluntarjoaja (koosta riippumatta) yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat (keskisuuri tai suuryritys) CER-direktiivin ja sitä täytäntöönpanevan lainsäädännön nojalla kriittiseksi määritetty toimija (koosta riippumatta) 3 §:n 3 momentissa tarkoitetut erityistoimijat (koosta riippumatta) Julkisen hallinnon tiedonhallinnasta annetun lain 4 a luvun soveltamisalaan kuuluva	Kyberturvallisuuslain liitteessä I tarkoitettu toimija (joka on kooltaan keskisuuri tai pienempi) Kyberturvallisuuslain liitteessä II tarkoitettu toimija (koosta riippumatta) yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat (mikro- tai pienyritys)

viranomainen pois lukien hyvinvointialueet ja hyvinvointiyhtymät sekä Helsingin kaupunki.	Hyvinvointialueet ja hyvinvointiyhtymät sekä Helsingin kaupunki (tiedonhallintalain soveltamisen osalta)
Suuntaa-antava arvio kokonaismäärästä: 250 – 500 toimijaa.	Suuntaa-antava arvio kokonaismäärästä: 2250 – 4500 toimijaa.

Alla olevassa taulukossa havainnollistetaan sääntelyn eroavaisuuksia keskeisten ja muiden toimijoiden välillä kyberturvallisuuslaissa. Julkishallintoa koskisi lisäksi eräät poikkeukset valvontatoimivaltuuksien soveltamisen ja seuraamusmaksun määräämisen osalta, joita ei havainnollistamisen selkeyttämiseksi ole sisällytetty tähän taulukkoon.

Taulukko 14:

Keskeinen toimija	Muu kuin keskeinen toimija (tärkeä toimija)
Riskienhallinta- ja raportointivelvoite: Ei eroa keskeisen ja muun toimijan välillä.	Riskienhallinta- ja raportointivelvoite: Ei eroa keskeisen ja muun toimijan välillä.
Valvonnan kynnys: Valvonta kohdistetaan keskeisiin toimijoihin	Valvonnan kynnys: Valvontaa voi kohdistaa, jos on perusteltu syy epäillä, että toimija ei ole noudattanut sääntelyä.
Valvontatoimivaltuudet: Tiedonsaanti- ja tarkastusoikeus, turvallisuusauditointi, valvontapäätös ja –varoitus. Johdon toiminnan rajoittaminen.	Valvontatoimivaltuudet: Tiedonsaanti- ja tarkastusoikeus, turvallisuusauditointi, valvontapäätös ja –varoitus.
Seuraamusmaksun enimmäismäärä: 10 000 000 euroa.	Seuraamusmaksun enimmäismäärä: 7 000 000 euroa.
Toimijaluetteloon ilmoittautuminen: Ei eroa keskeisen ja muun toimijan välillä.	Toimijaluetteloon ilmoittautuminen: Ei eroa keskeisen ja muun toimijan välillä.

4.2.3 Vaikutukset verkkotunnusvälittäjiin ja verkkotunnusrekisterin ylläpitäjään

Verkkotunnusvälittäjiin sekä verkkotunnusrekisterin ylläpitäjään kohdistuu vaikutuksia verkkotunnusten rekisteröintitietojen tietokantaa koskevan NIS2-direktiivin 28 artiklan

täytäntöönpanosta. Sitä koskevista ehdotuksista säädettäisiin sähköisen viestinnän palveluista annetussa laissa.

Verkkotunnusvälittäjiä ei koskisi NIS2-direktiivin mukaisten riskienhallinta- ja raportointivelvoitteet eivätkä verkkotunnusvälittäjät kuuluisi kyberturvallisuuslain soveltamisalaan. Verkkotunnusvälittäjä voisi kuulua soveltamisalaan silloin, jos se tarjoaa verkkotunnusten välittämisen ohella myös jotain muuta lain liitteessä palvelua. Tällaista palvelua on esimerkiksi DNS-palvelu.

Fi-verkkotunnusvälittäjiä on noin 3200. Liikenne- ja viestintävirasto toimii fi-verkkotunnusrekisterin ylläpitäjänä. Rekisteröityjä fi-verkkotunnuksia on ollut 1.3.2024 yhteensä 547 481 kappaletta, joista kymmenen suurimman verkkotunnusvälittäjän verkkotunnuksien määrä on ollut yhteensä 309 412 kappaletta. Fi-verkkotunnuksia rekisteröidään päivittäin tavanomaisesti 100-250 kappaletta. Ax-verkkotunnusvälittäjiä on noin 100 kappaletta ja ax-verkkotunnusrekisterin ylläpitäjänä toimii Ahvenanmaan maakuntahallitus.

Verkkotunnusvälittäjille asetetaan sähköisen viestinnän palveluista annettua lakia koskevassa ehdotuksessa eräitä velvoitteita, joilla on vaikutuksia niiden toimintaan. Keskeisin on velvollisuus laatia ja julkaista verkkotunnusrekisterin tietojen oikeellisuuden varmistamista sekä verkkotunnusten rekisteröintitietojen luovuttamista koskevat toimintaperiaatteet ja menettelyt, jonka toteuttamisesta aiheutuu verkkotunnusvälittäjälle hallinnollista taakkaa, jonka määrän vaikuttaa keskeiseltä osin toiminnan laajuus. 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 sääntelyn soveltamisen alkaessa kertaluontoisia kustannuksia, jotka koostuvat sääntelyn noudattamisen edellyttämien menettelyiden käyttöönotosta sekä vaatimustenmukaisuuden osoittamiseen liittyvästä hallinnollisesta taakasta.

Verkkotunnusrekisterin ylläpitäjään kohdistuu vaikutuksia sähköisen viestinnän palveluista annettua lakia koskevassa ehdotuksessa erityisesti velvoitteesta vastata verkkotunnusten rekisteröintitietoa koskevaan pyyntöön ilman aiheetonta viivytystä ja viimeistään 72 tunnin kuluessa pyynnön vastaanottamisesta. Lisäksi vaikutuksia kohdistuu velvoitteesta estää verkkotunnuksen rekisteröinti verkkotunnusrekisteriin silloin, jos verkkotunnusrekisterin ylläpitäjä epäilee tietojen olevan puutteellisia tai virheellisiä eikä niitä kehotuksesta huolimatta todenneta oikeaksi. Nämä ehdotukset lisäävät verkkotunnusrekisterin ylläpidosta aiheutuvaa hallinnollista työtä. Lisäksi sähköisen viestinnän palveluista annetussa laissa säädettäisiin mahdollisuudesta hakea oikaisua verkkotunnuksen rekisteröinnin estämistä tai poistamista koskevaan verkkotunnusrekisterin ylläpitäjän päätökseen. Oikaisuvaatimusmenettelyn arvioidaan kokonaisuutena alentavan näistä päätöksistä aiheutuvia muutoksenhakumenettelyyn liittyviä kustannuksia viranomaisessa ja hallintotuomioistuimissa.

4.3 Taloudelliset vaikutukset

4.3.1 Vaikutukset yrityksiin

4.3.1.1 Yhteenveto yritysvaikutuksista

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 yritysten toimintavarmuutta ja edistää liiketoimintaa digitalisoituvassa yhteiskunnassa. Kyberturvallisuushäiriöiden vähentyminen säästäisi toimijoita häiriöiden haitallisista vaikutuksista aiheutuvilta kustannuksilta. Kyberturvallisuuden häiriöiden sietokyvyn parantamisella vältetään niitä haitallisia vaikutuksia ja kustannuksia, joita yrityksen toimintaan tai palveluntarjontaan aiheutuvista merkittävistä poikkeamista aiheutuisi. Haitalliset vaikutukset kyberhäiriön toteutumisesta voivat olla erittäin merkittäviä sekä yrityksen että sen palveluiden käyttäjien kannalta. Kyberpoikkeamien määrä, laajuus, kehittyneisyys, esiintymistiheys ja vaikutukset lisääntyvät, ja ne muodostavat riskejä liiketoiminnan harjoittamiselle.

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. Riskienhallinnan kustannukset ovat sitä suurempia, mitä suurempaa ja laajempaa yrityksen toiminta on. Yrityskohtaiset erot IT- ja kyberturvallisuuskustannuksissa ovat merkittäviä ja olennaisessa suhteessa yrityksen toimintaan. Pienelle yritykselle, jonka toiminnassa käytetään vain vähän IT-järjestelmiä, riskienhallintavelvoitteesta aiheutuvat kustannukset voivat olla vain vähäisiä. Toisaalta myös pienelle yritykselle voi aiheutua olennaisia kustannuksia, jos sen liiketoiminnassa on erityispiirteitä, joihin liittyy erityisiä riskejä.

Yleisesti IT-kustannukset ovat keskimäärin noin 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.[6] Komission arvion mukaan kyberturvallisuuskustannusten on arvioitu olevan keskimäärin eri toimialoilla 0,52 % vuotuisesta liikevaihdosta. Yksin kyberturvallisuuteen tai –riskienhallintaan liittyviä

[6] [6] Insta (2023) Selvitys kyberturvallisuusdirektiivin (NIS2-direktiivi) riskienhallintavelvoitteiden taloudellisista vaikutuksista elintarvike- ja valmistussekotoreille

kustannuksia on haastavaa erottaa yrityksen muista IT- tai riskienhallintakustannuksista. Kyberturvallisuuslain soveltamisalassa olevalle yritykselle arvioidaan suuntaa-antavasti aiheuttavan kustannuksia kyberturvallisuuden riskienhallinnasta lain edellyttämällä vähimmäistasolla noin 0,2 – 0,8 % vuotuisesta liikevaihdosta, jos vertailukohtana on taso, jossa yritys ei toteuttaisi ennalta lainkaan kyberturvallisuuden riskienhallintatoimenpiteitä. Arvioihin liittyy merkittävää epävarmuutta yrityskohtaisten erojen osalta.

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.[7] Arvio on vertailukelpoinen myös Suomessa, sillä NIS2-direktiivin mukaisista velvoitteista ehdotetaan säädettäväksi kyberturvallisuuslaissa velvoitteiden edellyttämällä vähimmäistasolla. Näin ollen kyberturvallisuuden riskienhallintavelvoitteella arvioidaan suuntaa-antavasti olevan keskimäärin noin 12-22 % yrityksen IT-kustannuksia korottava vaikutus. Julkisella sektorilla ja muilla toimialoilla, joihin on ennalta kohdistunut tietoturvallisuuden varmistamista kohdistuvaa yksityiskohtaista sääntelyä, tätä arviota ei voida pitää luotettavana. Näillä sektoreilla korottavan vaikutuksen määrä arvioidaan tätä matalammaksi.

Edellä esitettyihin arvioihin liittyy merkittäviä epävarmuustekijöitä. Kyberturvallisuuslain voimaantulosta ja lain mukaisen riskienhallintavelvoitteen noudattamisesta yrityksessä aiheutuvaan kustannukseen vaikuttaa ratkaisevasti se, missä laajuudessa yritys on ennestään toteuttanut kyberturvallisuuden riskienhallintaa liiketaloudellisin perustein tai toimialakohtaisen sääntelyn velvoittamana. Kustannukseen vaikuttaa ratkaisevasti myös se, miten ja millaisia viestintäverkkoja ja tietojärjestelmiä yritys toiminnassaan käyttää. Koska yrityskohtaiset erot IT-kustannusten ja kyberturvallisuuteen luettavien kustannusten välillä ovat niin suuria, ei tarkkaa ja yleistettävissä olevaa luotettavaa arviota ole esitettävissä.

Kyberturvallisuuslakiin sisältyvästä velvoitteesta ilmoittaa merkittävästä poikkeamasta valvovalle viranomaiselle arvioidaan aiheutuvan vain vähäisiä kustannuksia. Kustannukset koostuvat ilmoituksen tai raportin tekemiseen kuluvasta työajasta yksittäisen merkittävän poikkeaman tapahtuessa. Kustannuksia madaltaa mahdollisuus tehdä poikkeamailmoitukset ja –raportit kaikille valvoville viranomaisille keskitetyn sähköisen järjestelmän kautta. Kustannuksia kasvattaa velvoite tehdä ensi- ja jatkoilmoitukset tiukoissa määräajoissa, eli 24 ja 72 tunnin määräajoissa poikkeaman havaitsemisesta.

Merkittävällä poikkeamalla, joka kuuluisi raportointivelvoitteen alaan, tarkoitettaisiin poikkeamaa, joka on aiheuttanut tai voi aiheuttaa vakavan palvelujen toimintahäiriön, huomattavia taloudellisia tappioita tai huomattavaa aineellista tai aineetonta vahinkoa muille tahoille. Merkittävän poikkeaman kynnyksen täyttäisi esimerkiksi tapahtuma, joka aiheuttaisi viestintäverkon tai tietojärjestelmän välityksellä tarjottavan palvelun pitkäkestoisen toimintahäiriön.

Vaikka kyberhäiriöt ja –uhkat yleistyvät, velvoittavan ilmoittamiskynnyksen ylittävien merkittävien poikkeamien toteutuminen on harvinaisempaa. NIS1-direktiiviä täytäntöönpanevan sääntelyn nojalla Suomessa on tehty vuosittain muutamia kymmeniä ilmoituksia merkittävistä poikkeamista. Nämä ilmoitukset ovat koskeneet vakavimpia

[7] 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

kyberpoikkeamatilanteita NIS1-direktiivin velvoitteiden alaan kuuluvissa yrityksissä. Tämän lisäksi on tavanomaista, että osana varautumista kyberhäiriötilanteisiin yritykset ilmoittavat kyberhäiriöistä ja -uhkista vapaaehtoisesti Kyberturvallisuuskeskukselle.

Merkittäviä poikkeamia koskevien ilmoitusten määrän ennakoidaan kasvavan sääntelyn täytäntöönpanon myötä. Ilmoittamisvelvoitteen ala laajenee merkittävästi kyberturvallisuuslain ja tiedonhallintalakiin esitettyjen muutosten johdosta. Lisäksi yleisellä tasolla erilaisten viestintäverkkoihin ja tietojärjestelmiin kohdistuvien poikkeamien määrä on ollut jatkuvasti kasvussa yhteiskunnassa. Ilmoittamiskynnys merkittävästä poikkeamasta säilyisi NIS1-direktiivin sääntelyä vastaavana.

Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen Tietoturvan vuosi 2022 –julkaisun mukaan kyberuhkataso on noussut vuoden 2022 aikana. Vuoden 2022 aikana kiristyshaittaohjelmat, kohdistettu tietojenkalastelu ja haitallinen liikenne lisääntyivät niin valtionhallintoon kuin huoltovarmuuskriittisiin organisaatioihin. Palvelunestohyökkäykset ovat arkipäiväistyneet ja niitä todetaan vuosittain yli 10 000 kappaletta. Palvelunestohyökkäyksestä aiheutuva haitta on yleensä lyhytaikainen eikä sen toteuttaminen vaadi erityistä teknistä osaamista, vaan sen voi tilata rikollisilta kaupallisena palveluna. Vuonna 2022 palvelunestohyökkäyksien määrä lisääntyi ja niiden kohteena olivat erityisesti valtionhallinnon sekä sote-sektorin, finanssialan, liikenne- ja logistiikka-alan ja media-alan toimijat, joiden palveluihin kohdistuvilla katkoksilla sai suoraa näkyvyyttä kansalaisille, vaikka organisaatioiden sisäisiin järjestelmiin niillä ei vaikutusta ollutkaan ja vaikutukset ulkoisiinkin palveluihin olivat valtaosin lyhytaikaisia. Kiristyshaittaohjelmien uhriksi joutumisesta ilmoitettiin vuonna 2022 Kyberturvallisuuskeskukselle edellisvuotta useammin. Kiristyshaittaohjelmien levittäminen Suomessa nähtiin aiempaa kohdennetumpana ja uhriorganisaatioon selvästi kohdennettuja hyökkäyksiä kohdistui muun muassa suuriin ja merkittäviin yrityksiin sekä huoltovarmuuden kannalta kriittisiin organisaatioihin. Suuri osa kiristyshaittaohjelmiin johtaneista hyökkäyksistä aiheutui sähköpostitse välitetyn tietojenkalasteluviestin avulla. Myös muiden tavanomaisten suojausmenetelmien, kuten hyvien salasanakäytänteiden tai ohjelmistopäivitysten puuttumista käytettiin kiristyshaittaohjelmahyökkäyksissä hyväksi. Tietojenkalastelu- ja huijausyritykset jatkuivat aktiivisina ja Kyberturvallisuuskeskus käsitteli vuonna 2022 kuukausittain keskimäärin 500-1000 ilmoitusta aiheeseen liittyen. Varoituksia viestintäverkkoihin ja tietojärjestelmiin liittyvistä haavoittuvuuksista Kyberturvallisuuskeskus julkaisee vuosittain keskimäärin 1-3 kappaletta; vuonna 2022 yhden varoituksen ja vuonna 2021 viisi varoitusta. Vuonna 2022 Kyberturvallisuuskeskus käsitteli yhteensä 12 946 erillistä tapausta. Merkittäviä, vakavia ja kriittisiä häiriöitä Kyberturvallisuuskeskus on käsitellyt vuonna 2022 yhteensä 45 kappaletta.[8]

Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen Tietoturvan vuosi 2023 –julkaisun mukaan kyberuhkataso on pysynyt kohonneena ja sen arvioidaan pysyvän kohonneena myös vuonna 2024. Kyberturvallisuuskeskukselle raportoitujen poikkeamatapauksien määrä kasvoi noin 44 % verrattuna edellisvuoteen. Kyberturvallisuuskeskus käsitteli vuonna 2023 yhteensä 211 ilmoitusta palvelunestohyökkäyksistä, jotka painottuivat määrällisesti syys-joulukuun väliselle ajanjaksolle. Maailmassa julkaistiin yli 20 000 uniikkia CVE-haavoittuvuustunnisteen omaavaa haavoittuvuutta, joista osa on vakavampia ja osa vähemmän vakavia. Kyberturvallisuuskeskus julkaisee vuosittain noin 30-40 haavoittuvuustiedotetta kriittisimmistä haavoittuvuuksista, jotka koskevat suomalaisia käyttäjiä.[9]

[8] Liikenne- ja viestintävirasto Traficomin julkaisuja 16/2023. Tietoturvan vuosi 2022.
[9] Liikenne- ja viestintävirasto Traficomin julkaisuja 10/2024. Tietoturvan vuosi 2024.

Kyberturvallisuuskeskuksen tietoon tuli vuoden 2023 aikana 4 963 huijausta, 9 266 kalastelua, 111 tietovuotoa, 1014 tietomurtoa ja 383 tietomurron yritystä. Kyberturvallisuuskeskuksen tietoon tuli vuoden 2023 aikana yhteensä 18 625 erilaista tietoturvapoikkeamaa. Vuonna 2022 Kyberturvallisuuskeskuksen tietoon tuli 3 519 huijausta, 5 787 kalastelua, 104 tietovuotoa, 1026 tietomurtoaja 127 tietomurron yritystä, yhteensä erilaista 12 947 tietoturvapoikkeamaa. Virossa kansallisen kyberturvallisuuskeskuksen (NCSC-EE) tietoon tuli 3 314 tietoturvapoikkeamaa, joista suurimpina kalasteluja oli 1 722, petoksia 546 ja palveluhäiriöitä 312 kappaletta. Vuonna 2023 palvelunestohyökkäyksiä (DDoS) tuli tietoon Suomessa 211 kappaletta ja Virossa 139 kappaletta. Tietoturvapoikkeamia sekä huijaus-, kalastelu- ja tietomurtojen yrityksien tapahtuminen on raportoitujen lukujen perusteella yleistä ja yleistymässä. [10]

Kyberturvallisuuslain soveltamisalaan kuuluville yrityksille aiheutuu vähäisiä kustannuksia valvovan viranomaisen toimijaluetteloon ilmoittautumisesta. Kustannukset ovat pääasiassa kertaluonteisia silloin, kun yritys tulee lain soveltamisalaan. Kustannuksia voi aiheutua myös toimijaluettelossa olevien tietojen päivittämisestä, jos tiedot muuttuvat. Kustannukset koostuvat ilmoitukseen käytettävästä työajasta ja arvioidaan määrältään vähäisiksi.

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 voivat 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.[11] 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. [12] Solarwinds -yritykselle koitui tapauksesta vuoden 2021 aikana ainakin 40 miljoonan dollarin kustannukset. Tämän lisäksi yritykselle arvioitiin aiheutuvan merkittävä mainehaitta, joten kustannusten voidaan arvioida

[10] Liikenne- ja viestintävirasto Traficomin julkaisuja 10/2024. Tietoturvan vuosi 2024.
Cyber Security in Estonia 2024. Publisher: Republic of Estonia, Information System Authority (NCSC-EE).
[11] YLE (2019) Kyberhyökkäys on maksanut Lahden kaupungille lähes 690 000 euroa
https://yle.fi/a/3-10914550
[12] Cybersecurity Impact Report 2021
https://www.ironnet.com/resource-library/2021-cybersecurity-impact-report

olevan paljon suuremmat.[13] 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, että esityksellä saavutettaisiin 11,3 miljardin euron kyberturvallisuushäiriöiden aiheuttamien kustannusten alenema EU:n tasolla kymmenen vuoden aikana. EU:n tasolla kyberturvallisuushäiriöistä ja –kriiseistä aiheutuneiksi kustannuksiksi yhteensä 118 miljardia euroa kymmenen vuoden ajanjakson aikana.

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

Ehdotettavan sääntelyn toimeenpanoon liittyy riskejä ja epävarmuuksia erityisesti laajan soveltamisalan vuoksi. Sääntelyn valmistelun aikana on ilmennyt yritysten ja muiden soveltamisalaan kuuluvien organisaatioiden tarve viranomaisneuvonnalle ja –ohjaukselle soveltamisalan osalta ja riskienhallintavelvoitteen sisällön osalta. Sääntelyn täytäntöönpanon yhteydessä valvovilla viranomaisilla sekä Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksella olisi keskeinen rooli viranomaisneuvonnan ja –ohjeistuksen tarjoamisessa soveltamisalaan kuuluville toimijoille.

Riskienhallintavelvoitteen osalta soveltamisalaan kuuluvilla yrityksillä ja muilla toimijoilla on lähtökohtaisesti paras kyky ennakoida ja tunnistaa omaan toimintaansa liittyviä riskejä myös kyberturvallisuuden osalta, mutta kyberturvallisuusasioihin liittyvän osaamisen taso yrityksissä vaihtelee. Esityksen välillisenä vaikutuksena arvioidaan kehittyvän myös kyberturvallisuuteen liittyvän osaamisen ja sen kysynnän kasvua yhteiskunnassa.

Riskienhallinta- ja poikkeamaraportointivelvoitteiden osalta Euroopan komission antamat täytäntöönpanosäädökset tai delegoidut säädökset voivat vaikuttaa toimijoille aiheutuviin kustannuksiin. Täytäntöönpanosäädöksellä voitaisiin esimerkiksi edellyttää tietyillä toimialoilla toimijoilta yksityiskohtaisempia toimenpiteitä riskienhallinnassa tai täsmentää merkittävän poikkeaman ilmoituskynnystä, millä olisi vaikutuksia yrityksille.

4.3.1.2 Riskienhallintavelvoite

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 soveltamisalaan tulee uutena huomattava lukumäärä yrityksiä. Selvityksen toteutti Insta Advance Oy (jäljempänä ”Insta”).

[13] 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/

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 artiklan mukaan riskienhallinnassa ja riskienhallintatoimenpiteissä huomioitaviin osa-alueisiin. Kyberturvallisuuslakia koskevan ehdotuksen 7–9 §:n nojalla riskienhallinnassa huomioitavat osa-alueet vastaavat NIS2-direktiivin 21 artiklaa. Selvityksessä pyrittiin selvittämään velvoitteiden toteuttamisesta aiheutuvia henkilöstötyövuosia ja muita kustannuksia, joita aiheutuu kertaluontoisesti ja jatkuvasti vuosittain. Näitä tietoja hyödynnettiin Sääntelytaakkalaskurilla[14] tehtyihin arvioihin yrityskohtaisista kustannuksista. Kyselytutkimukseen osallistui 20 yritystä ja saadut tulokset ovat näiden yritysten arvioita vuotuisista kyberturvallisuuskustannuksista. Selvityksen tulokset eivät ole sellaisenaan yleistettävissä koskemaan koko sektorin tuloksia, johtuen muun muassa pienestä otoskoosta. Kustannusten suuruuteen vaikuttaa yrityssektorilla merkittävästi myös yrityksen koko sekä yritys- ja konsernirakenteet, joiden vaikutusta ei selvityksessä pystytty erittelemään.

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 tulevan 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.

Koska kyberturvallisuuslaissa säädettäisiin riskienhallintavelvoitteen sisällöstä NIS2-direktiivin velvoitteiden edellyttämällä vähimmäistasolla, arviot vastaisivat lain voimaantulosta yrityksille aiheutuvia kustannuksia. Selvityksen perusteella voidaan arvioida, että riskienhallinnasta aiheutuvat kustannukset jakautuvat yrityksissä keskimäärin suuntaa-antavasti siten, että noin ¼ kustannuksista on työkustannuksia ja ¾ muita kustannuksia, kuten tietojärjestelmäinvestointeja.

Riskienhallinnassa huomioitavista osa-alueista kustannuksia arvioitiin aiheutuvan 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

[14] Sääntelytaakkalaskuri on työ- ja elinkeinoministeriön ylläpitämä standardikustannusmalliin perustuva Excel-työkalu, joka sisältää muun muassa tiedot hinta- ja palkkakehityksestä, vakiopalkkaluokat eri tasoisiin tehtäviin, palkkojen sivu- ja yleiskulut, keskimääräisen vuosityöajan ja yritystilastoja. (https://tem.fi/yksi-yhdesta-periaate).

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 todennäköisyyteen sekä vakavuuteen 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 riskienhallinnan toteuttamisesta aiheutuvia henkilötyöpäivien määrän lisäyksiä ja muista kustannuksista johtuvia kustannustenlisäyksiä toimijoille elintarvike- ja valmistussektoreilla.

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 toteuttamiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 10-20 henkilötyöpäivää. Vuosittain toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen toteuttamiseen kertaluonteisesti käytettävien muiden kustannusten määrän olevan 30 001-50 000 euroa. Jatkuvaluonteisia muita kustannuksia arvioitiin aiheutuvan 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 velvoitteen toteuttamisesta ensimmäisenä vuotena ja 11 400 euroa vuosittain tämän jälkeen.

Selvityksen mukaan valmistussektorilla yritysten arvio velvoitteen toteuttamiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 21-50 henkilötyöpäivää. Vuosittain toistuvia henkilötyöpäiviä arvioitiin aiheutuvan 10-20 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen toteuttamiseen kertaluonteisesti käytettävien muiden kustannusten määrän olevan 5 000-30 000 euroa. Jatkuvaluonteisia muita kustannuksia arvioitiin aiheutuvan korkeintaan 5 000- 30 000 euroa. Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille valmistussektorin yrityksille aiheutuu kertakustannuksena keskimäärin 52 900 euroa velvoitteeseen toteuttamisesta 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.

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.

Asiantuntija-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 toteuttamiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 10-20 henkilötyöpäivää. Vuosittain toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen toteuttamiseen kertaluonteisesti käytettävien muiden kustannusten määrän olevan 30 001-50 000 euroa. Jatkuvaluonteisia muita kustannuksia arvioitiin tulevan korkeintaan 5 000- 15 000 euroa. Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 47 200 euroa velvoitteen toteuttamisesta ensimmäisenä vuotena ja 19 700 euroa vuosittain tämän jälkeen.

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

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.

Asiantuntija-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 (Insta 2023).

Selvityksen mukaan elintarvikesektorilla yritysten arvio velvoitteen toteuttamiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 10-20 henkilötyöpäivää. Vuosittain toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen toteuttamisen kertaluonteisesti käytettävien muiden kustannusten määrän olevan 15 001-30 000 euroa. Jatkuvaluonteisia muita kustannuksia arvioitiin aiheutuvan korkeintaan 5 000- 15 000 euroa. Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 31 200 euroa velvoitteen toteuttamisesta ensimmäisenä vuotena ja 19 400 euroa vuosittain tämän jälkeen.

Selvityksen mukaan valmistussektorilla yritysten arvio velvoitteen toteuttamiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 10-20 henkilötyöpäivää. Vuosittain toistuvia henkilötyöpäiviä arvioitiin aiheutuvan 10-20 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen toteuttamiseen kertaluonteisesti käytettävien muiden kustannusten määrän olevan 5 000-15 000 euroa. Jatkuvaluonteisia muita kustannuksia arvioitiin aiheutuvan korkeintaan 15 001- 30 000 euroa. Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille valmistussektorin yrityksille aiheutuu kertakustannuksena keskimäärin 32 100 euroa velvoitteeseen toteuttamisesta ensimmäisenä vuotena ja 29 500 euroa vuosittain tämän jälkeen.

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 perustelukappaleen 85 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 asiantuntija-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 toteuttamiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 10-20 henkilötyöpäivää. Vuosittain toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen toteuttamiseen 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 velvoitteen toteuttamisesta ensimmäisenä vuotena ja 23 200 euroa vuosittain tämän jälkeen.

Selvityksen mukaan valmistussektorilla yritysten arvio velvoitteen toteuttamiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 10-100 henkilötyöpäivää. Vuosittain toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen toteuttamiseen kertaluonteisesti käytettävien muiden kustannusten määrän olevan 5 000-15 000 euroa. Jatkuvaluonteisia muita kustannuksia arvioitiin aiheutuvan 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 valmistussektorin yrityksille aiheutuu kertakustannuksena keskimäärin 46 500 euroa velvoitteen toteuttamisesta ensimmäisenä vuotena ja 31 700 euroa vuosittain tämän jälkeen.

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 perustelukappaleen 80 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 perustelukappaleen 78 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 asiantuntija-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 toteuttamiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 10-20 henkilötyöpäivää. Vuosittain toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat, että velvoitteen toteuttamisesta ei aiheudu kertaluonteisia tai jatkuvaluonteisia muita kustannuksia. Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 30 800 euroa velvoitteen toteuttamisesta ensimmäisenä vuotena ja 21 900 euroa vuosittain tämän jälkeen.

Selvityksen mukaan valmistussektorilla yritysten arvio velvoitteen toteuttamiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 10-20 henkilötyöpäivää. Vuosittain toistuvia henkilötyöpäiviä arvioitiin aiheutuvan korkeintaan 10-20 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen toteuttamisen kertaluonteisesti käytettävien muiden kustannusten määrän olevan 5 000-30 000 euroa, mutta monet arvioivat myös, että velvoitteen toteuttamisesta ei aiheudu muita kertaluonteisia kustannuksia. Jatkuvaluonteisia muita kustannuksia ei arvioitu aiheutuvan. Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille valmistussektorin yrityksille aiheutuu kertakustannuksena keskimäärin 34 200 euroa velvoitteeseen sopeutumisesta ensimmäisenä vuotena ja 25 100 euroa vuosittain tämän jälkeen.

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.

Asiantuntija-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 toteuttamisesta käytettävistä kertaluonteisista henkilötyöpäivistä oli alle 10 henkilötyöpäivää. Vuosittain toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen toteutumisen 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 velvoitteen toteuttamisesta ensimmäisenä vuotena ja 4 500 euroa vuosittain tämän jälkeen.

Selvityksen mukaan valmistussektorilla yritysten arvio velvoitteen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 10-50 henkilötyöpäivää. Vuosittain toistuvia henkilötyöpäiviä arvioitiin aiheutuvan 10-20 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen toteuttamisen 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

valmistussektorin yrityksille aiheutuu kertakustannuksena keskimäärin 34 700 euroa velvoitteen toteuttamisesta ensimmäisenä vuotena ja 27 600 euroa vuosittain tämän jälkeen.

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 perustelukappaleen 89 mukaan yritysten olisi otettava käyttöön monenlaisia perustason kyberhygieniakäytäntöjä, kuten nollaluottamuksen periaate, ohjelmistopäivitykset, laitteiden konfigurointi eli asetusten määrittely, verkon segmentointi, identiteetin- ja pääsynhallinta ja käyttäjien tietoisuuden lisääminen, ja järjestettävä henkilöstölleen koulutusta kyberuhkista, verkkourkinnasta ja käyttäjän manipuloinnista. Selvityksen yhteydessä tehdyissä 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 (Zero Trust).

Selvityksen mukaan elintarvikesektorilla yritykset arvioivat, että velvoitteen toteuttamisesta ei aiheudu kertaluonteisia henkilötyöpäiviä. Vuosittain toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen toteuttamisen kertaluonteisesti käytettävien muiden kustannusten määrän olevan korkeintaan 30 001-50 000 euroa. Kuitenkin useat arvioivat myös, että kertaluonteisia muita kustannuksia ei velvoitteen toteuttamisesta aiheudu. Jatkuvaluonteisia muita kustannuksia arvioitiin aiheutuvan 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 velvoitteen toteuttamisesta ensimmäisenä vuotena ja 19 500 euroa vuosittain tämän jälkeen.

Selvityksen mukaan valmistussektorilla yritysten arvio velvoitteen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä on alle 10 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioitiin aiheutuvan 10-20 henkilötyöpäivää. Tämän lisäksi yritykset arvioivat velvoitteen toteuttamisesta kertaluonteisesti käytettävien muiden kustannusten olevan korkeintaan 5 000-15 000 euroa, mutta monet arvioivat myös, että velvoitteen täyttämisestä ei aiheudu muita kertaluonteisia kustannuksia. Jatkuvaluonteisia muita kustannuksia arvioitiin aiheutuvan 5 000- 15 000 euroa. Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille valmistussektorin yrityksille aiheutuu kertakustannuksena keskimäärin 37 100 euroa velvoitteen toteuttamisesta ensimmäisenä vuotena ja 26 700 euroa vuosittain tämän jälkeen.

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.

Asiantuntija-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. (Insta 2023).

Selvityksen mukaan elintarvikesektorilla yritykset arvioivat, että velvoitteen toteuttamisesta 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 velvoitteen toteuttamisesta ensimmäisenä vuotena ja 10 200 euroa vuosittain tämän jälkeen.

Selvityksen mukaan valmistussektorilla yritysten arvio velvoitteen toteuttamiseen käytettävistä kertaluonteisista 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 valmistussektorin yrityksille aiheutuu kertakustannuksena keskimäärin 30 900 euroa velvoitteen toteuttamisesta ensimmäisenä vuotena ja 23 500 euroa vuosittain tämän jälkeen.

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 perustelukappaleen 79 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 asiantuntija-arvion 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. (Insta 2023).

Selvityksen yhteydessä havaittiin, että vaatimus omaisuudenhallinnasta on osittain tulkinnanvarainen, koska NIS2-direktiivissä ei määritellä omaisuudenhallintaa terminä 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. Selvityksessä omaisuudenhallinnan osalta käytettiin ISO 27001 -standardin mukaista määritelmää.

Selvityksen mukaan elintarvikesektorilla yritykset arvioivat, että velvoitteen toteuttamisesta aiheutuu alle 10 henkilötyöpäivää. Vuosittain toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää, mutta monet arvioivat, että vuosittain toistuvia henkilötyöpäiviä ei velvoitteen toteuttamisesta aiheudu. Velvoitteista ei arvioitu aiheutuvan kertaluontoisia tai jatkuvia muita kustannuksia. Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 12 000 euroa velvoitteen toteuttamisesta ensimmäisenä vuotena ja 8 500 euroa vuosittain tämän jälkeen.

Selvityksen mukaan valmistussektorilla yritysten arvio velvoitteen toteuttamiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli korkeintaan 10-20 henkilötyöpäivää, mutta monet arvioivat velvoitteen toteuttamisen aiheuttavan alle 10 henkilötyöpäivää. Vuosittain toistuvia henkilötyöpäiviä arvioitiin aiheutuvan alle 10 henkilötyöpäivää. Velvoitteista ei arvioitu aiheutuvan kertaluontoisia tai jatkuvia muita kustannuksia. Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille valmistussektorin yrityksille aiheutuu kertakustannuksena keskimäärin 18 000 euroa velvoitteen toteuttamisesta ensimmäisenä vuotena ja 11 00 euroa vuosittain tämän jälkeen.

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.

Selvityksen mukaan elintarvikesektorilla yritykset arvioivat, että velvoitteen toteuttamisesta aiheutuu korkeintaan 10-20 henkilötyöpäivää. Monet arvioivat kuitenkin, että velvoitteen toteuttamisesta ei aiheudu henkilötyöpäiviä. Vuosittain toistuvia henkilötyöpäiviä arvioitiin aiheutuvan korkeintaan alle 10 henkilötyöpäivää, mutta monet arvioivat, että vuosittain aiheutuvia toistuvia henkilötyöpäiviä ei velvoitteen toteuttamisesta aiheudu. Velvoitteista ei arvioitu aiheutuvan kertaluontoisia tai jatkuvia muita kustannuksia. Sääntelytaakkalaskurilla tehdyn arvion mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 24 700 euroa velvoitteen toteuttamisesta ensimmäisenä vuotena ja 10 100 euroa vuosittain tämän jälkeen.

Selvityksen mukaan valmistussektorilla yritysten arvio velvoitteen toteuttamiseen käytettävistä kertaluonteisia henkilötyöpäivistä oli 10-20 henkilötyöpäivää. Vuosittain toistuvia henkilötyöpäiviä arvioitiin aiheutuvan korkeintaan alle 10 henkilötyöpäivää. Monet arvioivat,

että toistuvia henkilötyöpäiviä ei velvoitteen toteuttamisesta 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 velvoitteen toteuttamisesta ensimmäisenä vuotena ja 27 700 euroa vuosittain tämän jälkeen.

Seuraavassa taulukossa on koottu sääntelytaakkalaskurilla tehdyt arviot NIS2-direktiivin 21 artiklan mukaisten riskienhallintavaatimusten täyttämisestä aiheutuvat keskimääräiset yrityskohtaiset kustannukset toimijoille elintarvike- ja valmistussektoreilla.

Taulukko 15:

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 ensimmäisestä, toisesta ja neljännestä velvoitteesta eli 1. riskianalyysi ja tietojärjestelmän turvallisuus, 2. poikkeamien käsittely sekä 4. toimitusketjujen turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuuskohdat. Huomioitavaa on, että tarkasteluun valitut sektorit eivät ole olleet aikaisemmin NIS-sääntelyn piirissä, joten lukujen voidaan arvioida olevan eräänlaisia maksimeja sääntelystä koituvista kustannuksista. Huoltovarmuuskeskus[15] 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

[15] Huoltovarmuuskeskus (2022) Toimialojen kyberkypsyyden selvitys 2022. https://www.huoltovarmuuskeskus.fi/files/29b11d0af56a115126ad490af444f1c4fd7885af/hvk-toimialojen-kyberkypsyyden-selvitys-2022.pdf

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 (2022) toimesta. 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 arvioitiin yleisesti hyväksi ja erilaisiin uhkiin on toimialoilla varauduttu. Toimiala jakautuu kuitenkin korkean ja matalan kypsyystason toimijoihin ja tietoturvakulttuuri on vaihtelevaa toimijoiden välillä. Lisäksi selvityksessä 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.

Terveydenhuollon toimialalla NIS2-direktiivin soveltamisalan piiriin kuuluvat hyvinvointialueet ja uusina direktiivin soveltamisalaan kuuluvat myös jotkin tutkimuslaitokset ja laboratoriot. Selvityksessä 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 arvioitiin selvityksessä nousevaksi. Kokonaiskypsyys jäi toimialalla alle hyvän perustason ja alan keskeinen rooli yhteiskunnan

toimivuudessa arvioitiin merkittäväksi. Tämän johdosta arvioidaan, että investointeja kyberturvallisuuteen tulee toimialalla tehdä, jotta nykyisiin uhkakuviin on tarpeeksi varauduttu. Erityisesti heikkoudeksi selvityksessä 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 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 toimialalla uhkatason merkitys toimialalle arvioitiin selvityksessä 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 toimialojen uhkatason merkitys toimialalle arviointiin neutraaliksi. Kaupan ja jakelun toimialan kokonaiskypsyys jäi selvityksessä alle hyvän perustason, jolloin varautuminen kyberuhkiin ei ole toimialalla 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. Toimialoille arvioidaan koituvan kustannuksia NIS2-velvoitteiden täyttymisestä muun muassa kyberturvallisuusmaturiteetin suuren hajonnan takia.

Satamat ja merenkulku toimialalle uhkatason merkitys toimialalle arvioitiin neutraaliksi. Toimialan kyberturvallisuusmaturiteetti 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. Tutkimuksen perusteella on kuitenkin selvää, että kybermaturiteetin lähtötaso vaihtelee toimialakohtaisesti.

4.3.2 Vaikutukset kansantalouteen

Esityksellä pyritään parantamaan kriittisten toimialojen kyberturvallisuutta ja tätä kautta parantamaan markkinoiden luottamusta ja kansantaloutta. Esityksen vaikutukset kansantalouteen ovat välillisiä. Esityksellä on vaikutuksia julkistaloudelle. Julkistaloudelliset vaikutukset kuvataan jaksossa 4.4.

Esityksen tuoma suurempi sääntelytaakka tarkoittaa, että toimijat joutuvat käyttämään lisää resursseja kyberturvallisuuteen. Tämä voi lyhyellä aikavälillä pienentää yritysten voittoja, ja on myös mahdollista, että tietoturvaan ja tietosuojaan kohdennetut lisäresurssit ovat pois muusta toiminnasta. Hyvästä tietoturvasta ja tietosuojan tasosta huolehtiminen voi tarjota kuitenkin yrityksille 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 tai tietoturvan tai tietosuojan häiriötilanne aiheuttaa kustannuksia sekä tuotannon tai palveluntarjonnan keskeytymisen, että 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 euron 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.

Esityksellä ei arvioida olevan vaikutusta hieman keskisuuren yrityksen määritelmän alle jäävien pienyritysten kasvun edellytyksiin ja sitä kautta kansantalouteen. Soveltamisalaan kuuluvilla yrityksillä arvioidaan pääsääntöisesti olevan liiketaloudellinen intressi toteuttaa kyberturvallisuuden riskienhallintaa lähellä lain edellyttämää tasoa, vaikka ne eivät täyttäisi kyberturvallisuuslain soveltamisalaa koskevaa kokokriteeriä. Näin ollen kasvaminen hieman alle keskisuuresta yrityksestä keskisuureksi yritykseksi aiheuttaisi lähtökohtaisesti vain vähäisiä kustannuksia, joiden ei arvioida vaikuttavan yrityksen kannustimiin laajentaa toimintaansa. Esityksellä voi olla vaikutuksia yrityksien kannustimiin laajentaa toimintaansa ulkomaille EU:n sisällä, mikäli EU:n tasolla NIS2-direktiivin kansallinen toimeenpano, -vaatimukset tai -

raportointi eriäisi merkittävästi jäsenvaltioiden välillä. Vaikutukset arvioidaan kansantalouden kannalta vähäisiksi.

4.4 Vaikutukset viranomaisten toimintaan

4.4.1 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 omaksutun kriittisten toimijoiden tunnistamisen sijaan 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. Kasvavaa tarvetta viranomaisen neuvonnalle voi edellyttää erityisesti soveltamisalasäännöksen tulkintaa koskevan tuen tarve.

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.

Taulukko 16:

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 (moottoriajoneuvojen, perävaunujen ja puoliperävaunujen valmistusta harjoittavat toimijat, muiden kulkuneuvojen valmistusta harjoittavat toimijat), tutkimusorganisaatiot, julkishallinto.	- 8,5 htv - tietojärjestelmäinvestoinnit 0,4 M€ vuodelle 2024 ja 0,15 M€ vuodesta 2025 alkaen	Kyllä
Energiavirasto	Sähkö, kaukolämmityksen tai kaukojäähdytyksen haltijat, kaasu (jakelu- ja siirtoverkonhaltijat), vedyn siirtoa harjoittavat toimijat	- 2 htv - tietojärjestelmäinvestoinnit 0,42 M€ vuodelle 2024 ja 0,0625 M€ vuodesta 2025 eteenpäin.	Kyllä
Turvallisuus- ja kemikaalivirasto	Kaasu (maakaasun toimittajat, varastointilaitteiston haltijat, maakaasun käsittelylaitteiston haltijat, maakaasualan yritykset sekä maakaasun jalostus- ja käsittelylaitteistojen haltijat), öljy, vedyn tuotantoa ja varastointia	- 6 htv - tietojärjestelmäinvestoinnit 0,2 M€ vuodelle 2024 ja 0,06 M€ vuodesta 2025 alkaen.	Ei

	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).		
Sosiaali- ja terveysalan lupa- ja valvontavirasto	Terveyspalvelun tuottajat ja EU:n vertailulaboratoriot	- 3 htv - tietojärjestelmäinvestoinnit kertaluontoisesti noin 0,15 M€ ja 60 000 euroa vuosittain 2025 alkaen.	Kyllä
Etelä-Savon ELY-keskus	Jätehuolto	- 2,5 htv - tietojärjestelmäkehitys 0,2 M€, 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 - tietojärjestelmäinvestoinnit 0,1 M€ vuonna 2025 sekä noin 100.000€ vuosittainen ostopalvelumääräraha.	Kyllä
Ruokavirasto	Elintarvikeyritykset, jotka harjoittavat tukkukauppaa,	- 5 htv	Ei

	teollista tuotantoa tai jalostusta	- tietojärjestelmäkustannus 0,6 M€ vuodelle 2024 ja 0,1 M€ vuodesta 2025 alkaen	
Lääkealan turvallisuus ja kehittämiskeskus	Lääkkeiden tutkimus ja kehitys, lääkeaineita, lääkkeitä ja lääkinnällisiä laitteita valmistavat toimijat, In vitro –diagnostiikkaan tarkoitettuja lääkinnällisiä laitteita valmistavat toimijat, veripalvelulaitokset, apteekit ja terveydenhuollon ammattihenkilönä lääkkeitä ja lääkinnällisiä laitteita toimittavat ja tarjoavat toimijat	- 4 htv - tietojärjestelmäinvestoinnit 0,5M€	Ei
Finanssivalvonta	Pankkitoiminta ja finanssimarkkinoiden infrastruktuuri	Ei vaikutuksia	Kyllä
Tietosuojavaltuutettu	-	2,5 htv.	-
Oikeusrekisterikeskus	Hallinnollisen seuraamusmaksun täytäntöönpano	Vähäisiä vaikutuksia, ei lisäresurssitarpeita.	-

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 pysyvän lisäresurssitarpeen vuodesta 2025 alkaen. 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 45 §: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 39 §: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

Energiavirasto on toiminut NIS1-direktiivin mukaisena valvovana viranomaisena jo aiemmin, mutta NIS2-direktiivin myötä valvottavien toimijoiden ja toimijatyyppien määrä kasvaisi merkittävästi. Lisäksi valvonnan arvioidaan muuttuvan yksityiskohtaisemmaksi ja laajemmaksi. Uudet valvontatehtävät edellyttävät Energiavirastolta lisäresursseja, koulutusta ja osaamisen kehittämistä. Lisäresursointitarvetta saattaa aiheutua myös toimijoiden neuvonnasta sekä vapaaehtoisten poikkeamailmoitusten käsittelystä, mikäli ilmoituskanavaa hyödynnetään laajasti. Energiaviraston on arvioitu tarvitsevan uusien tehtävien hoitamiseen kaksi henkilötyövuotta (2 htv). Resurssiarviossa on huomioitu valvottavien toimijoiden lukumäärän kasvu, valvonnan laajeneminen ja yksityiskohtaistuminen sekä nykytila, jossa Energiavirastolle resursoitu kyberturvallisuusosaaminen ei ole riittävällä tasolla NIS2-direktiivin mukaisten tehtävien asianmukaiseen hoitamiseen. Arviossa on huomioitu myös se, että NIS2- ja CER-direktiivien sekä sektorikohtaisen sääntelyn täytäntöönpanon myötä Energiavirastolle tulevat tehtävät tukevat toisiaan ja niistä on saatavissa synergiahyötyjä.

Lisäresurssien ohella uusien tehtävien toimeenpano sekä uusien toimijoiden valvonta edellyttäisi Energiavirastolta myös järjestelmäkehitystä sekä mahdollisesti ulkopuolisen asiantuntijaselvitysten teettämistä esimerkiksi kyberturvallisuuden alkukartoituksen muodossa. Energiaviraston olisi on otettava käyttöön erillinen asiankäsittelyjärjestelmä, jossa voidaan käsitellä ja arkistoida sähköisesti TL III-luokiteltua materiaalia. Energiavirasto arvioi käsittelyjärjestelmän kertaluontoisen kustannusarvion olevan noin 0,4 M€ vuodelle 2024 sekä järjestelmän vuosittaiset ylläpitokustannukset 0,06 M€ vuodesta 2025 eteenpäin. Lisäksi Energiavirasto arvioi, että toimijaluettelon vaatiman järjestelmän kehittäminen edellyttää kertaluontoista 20 000 € kustannusta vuonna 2024 ja vuodesta 2025 eteenpäin järjestelmän ylläpitokustannuksia 2500 € per vuosi olettaen, ettei toimijaluettelon ylläpito vaadi koodaustöitä.

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 kuusi asiantuntijahenkilötyövuotta (6 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 600 000 euroa (6 htv 540 000 ja 60 000 Vallu-järjestelmän ylläpitokustannuksiin). Lisäksi esitetään kertaluonteisesti vuodelle 2024 Vallu-järjestelmän uudistamiseen 200 000 euroa.

Taulukko 17: (tuhatta euroa)

	2024	2025	2026	2027
Henkilöstökulut (6 htv)	540	540	540	540
Investointimenot (VALLU)	200 (kertaluontoinen)	0	0	0
Edelliseen liittyvät ylläpitokustannukset	0	60	60	60
TAE-lisäys yhteensä	740	600	600	600

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.

Etelä-Savon ELY-keskukselle vesihuollon osalta 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 tarkastuksissa käytetään apuna ulkopuolisen tietotekniikan asiantuntijoiden palveluita. 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 artiklan 1 kohdan a alakohdan nojalla 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 0,2 M€ 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 0,6 M€ vuodelle 2024 ja 0,1 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.

Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira

Sosiaali- ja terveysalan lupa- ja valvontavirasto Valviralle esitys toisi uusia valvontatehtäviä ja laajentaisi nykyistä valvontaa. Lisäksi erityisesti ilmoitusmenettelyyn liittyen on odotettavissa,

että toimijat tarvitsevat viranomaisen ohjeistusta ja koulutusta. 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 3 htv:n lisäresurssitarpeen valvontaa varten. Uusien rekrytointien lisäksi on arvioitu tarvittavan jatkuvaa asiantuntijoiden kouluttautumista ja alan seuraamista. Lisäksi Valvira tarvitsee toimijaluettelon toteuttamista ja ylläpitoa varten tietojärjestelmiin kertaluontoisen investoinnin n. 0,15 M€ ja jatkuviin kustannuksiin 60 000 euroa vuodessa.

Lääkealan turvallisuus- ja kehittämiskeskus Fimea

Esitys toisi Lääkealan turvallisuus- ja kehittämiskeskus Fimealle uusia valvontatehtäviä. Valvonnan järjestäminen edellyttää Fimeassa uudenlaista osaamista ja kouluttautumista, laatujärjestelmän ohjeistuksen täydentämistä sekä toimijoiden ohjausta ja neuvontaa. Valvontaan arvioidaan tarvittavan yhteensä neljän henkilötyövuoden (4 htv) asiantuntijaresurssit pysyvästi. Lisäksi Fimean on arvioitu tarvitsevan valvontaa tukevan tietojärjestelmän, jonka kehittämiseen on arvioitu tarvittavan 0,5M €.

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, jotka katetaan olemassa olevien määrärahojen puitteissa.

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.

Esityksestä voi aiheutua vähäisiä vaikutuksia Oikeusrekisterikeskukselle, joka vastaisi seuraamusmaksun täytäntöönpanosta. Vaikutusten määrä riippuisi täytäntöönpantavien hallinnollisten seuraamusmaksujen lukumäärästä. Seuraamusmaksuja ennakoidaan määrättävän määrällisesti harvoin. Toisaalta sääntelyn alaan kuuluisi edellä kuvatulla tavalla määrällisesti olennainen joukko toimijoita, joille seuraamusmaksu voitaisiin määrätä. Seuraamusmaksun täytäntöönpanoa koskeva tehtävä vastaisi olennaisesti Oikeusrekisterikeskuksella olevia nykyisiä ja vastaavia seuraamusmaksun täytäntöönpanoa koskevia tehtäviä. Oikeusrekisterikeskukselle arvioidaan aiheutuvan esityksestä vähäistä lisätyön tarvetta. Oikeusrekisterikeskukselle aiheutuviin kustannuksiin vaikuttaa täytäntöönpantavien seuraamusmaksujen määrä, minkä vaikutusta on tarpeen seurata tulosohjausmenettelyssä yhdessä muiden Oikeusrekisterikeskuksen tehtävien kanssa. Kokonaisuutena Oikeusrekisterikeskukselle esityksestä aiheutuvat vaikutukset arvioidaan

vähäisiksi. Esityksestä aiheutuva työmäärän lisäys olisi katettava olemassa olevista valtion talouden kehyspäätösten ja valtion talousarvion mukaisista määrärahoista.

Vaikutukset julkishallinnon toimijoille riskienhallinta- ja raportointivelvoitteiden kohteena

Riskienhallinta- ja raportointivelvoitteita olisi sovellettava myös julkishallinnon toimialan toimijoissa NIS2-direktiivin toimeenpanemiseksi. Näin ollen soveltamisen kohteena oleville julkishallinnon toimialan toimijoille aiheutuisi esityksestä vaikutuksia myös velvoitteiden noudattamisesta. Velvoitteista ja niiden soveltamisalasta ehdotetaan säädettäväksi julkishallinnon toimialan osalta tiedonhallintalaissa. Lisäksi siltä osin kun julkishallinnon toimija harjoittaisi kyberturvallisuuslain liitteessä tarkoitettua toimintaa, esimerkiksi hyvinvointialue terveyspalvelun tarjoajana, julkishallinnon toimijaan soveltuisivat myös mainitun lain vastaavat säännökset.

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 ja hyvinvointiyhtymille sekä Helsingin kaupungille sen 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 viranomaisella 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 viranomainen 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 ja tiedonhallintayksikön tulisikin arvioida riskiarvionsa mukaisesti, miten se olemassa olevilla resursseillaan järjestää tarvittavat toimet poikkeamien havaitsemiseksi ja niistä ilmoittamiseksi.

Tiedonhallintayksikköihin kohdistuva valvontatehtävä olisi Liikenne- ja viestintävirastolla. Valvonta-asetelmaa ei ole arvioitu lainsäädännön kannalta muodollisesti ongelmalliseksi. Liikenne- ja viestintävirasto tehtävänä olisi valvoa lain noudattamista, jota se käytännössä voisi toteuttaa esimerkiksi tiedonhallintayksikköön kohdistuvalla tietopyynnöllä tai tarkastuksella.

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. Viranomaisten käyttämiin tietojärjestelmiin on kohdistunut ennestäänkin tietoturvavaatimuksia, joten yleisesti viranomaiselle aiheutuvien kustannuksien arvioidaan olevan yrityksille aiheutuvia kustannuksia matalammalla tasolla. Velvoitteiden noudattamisesta ei pääsääntöisesti aiheutuisi merkittäviä kustannuksia sen kohteena oleville viranomaisille. Poikkeuksen voisi muodostaa julkishallinnon toimija, joka ylläpitää useiden viranomaisten hyödyntämiä tai laajasti käytössä olevia tietojärjestelmiä. Lisäksi esityksellä voisi olla välillisiä vaikutuksia uusilta tietojärjestelmiltä edellytettyyn tietoturvan tasoon. Sääntelyn noudattamisesta aiheutuvat kustannukset olisi katettava valtion talouden kehyspäätösten ja valtion talousarvion mukaisista määrärahoista.

NIS1-sääntelyä valvovilta viranomaisilta saatujen tietojen mukaan osa kuntien liikelaitoksista ja kuntaomisteisista yhtiöistä on kuulunut NIS1–sääntelyn soveltamisalaan esimerkiksi vesihuollon sektorilla ja satamien osalta. Näissä toiminnoissa on myös saatettu hyödyntää kunnan tarjoamia IT-palveluja siten, että valvonnan kohteena oleva yritys tai liikelaitos on ollut velvollinen ilmoittamaan näissä ilmenneistä poikkeamista ja huolehtimaan myös alihankittujen palvelujen tietoturvasta, vaikkakin sääntely on koskenut vain palvelua tarjoavia laitoksia ja yritystä, eikä kuntaa kokonaisuudessaan. Kyberturvallisuuslakiin esitetään kuntia koskevaa poikkeusta niin, että lakia ei sen 4 §:n 6 momentin mukaisesti sovellettaisi kuntalaissa (410/2015) tarkoitettuun kuntaan muuten kuin liitteessä I tai II tarkoitetun toiminnan osalta. Tavoitteena sääntelyllä on mahdollisimman pitkälti ollut säilyttää nykytila kuntiin kohdistuvien kyberturvallisuusvelvoitteiden osalta niin, että koko kunta ei tulisi velvoitteiden piiriin

tilanteessa, jossa kunnan taseyksikkö harjoittaa toimintaa NIS2-direktiivin liitteissä kuvatulla toimialalla. Myös toiminnan laajuutta arvioitaisiin vain siihen liittyvän henkilöstön, taseen ja liikevaihdon perusteella eikö koko kunnan henkilöstön ja budjetin perusteella.

4.4.2 Tiedonhallinnan muutosvaikutukset

Tiedonhallintalain 8 §:n 2 momentin mukaan toimialasta vastaavan ministeriön on laadittava lain 5 §:n 3 momentin mukainen arviointi, kun valmisteltavat säännökset vaikuttavat (viranomaisten tai tiedonhallintayksiköiden) tietoaineistoihin ja tietojärjestelmiin. Lisäksi ministeriön on arvioitava suunniteltujen säännösten vaikutukset asiakirjojen julkisuuteen ja salassapitoon. Säännöksen perustelujen mukaan tarkoituksena olisi varmistaa, että lainsäädännön valmisteluvaiheessa tunnistetaan tiedonhallintaan kohdistuvien säännösten vaikutukset viranomaisten toimintaan ja että arvioinnin perusteella voidaan ryhtyä suunnittelemaan kohdealueen tiedonhallinnan muutoksia tarkemmin. Arvioinnin avulla lainvalmistelussa tunnistetaan nykytila ja suoritetaan arvio tavoitetilasta valmisteltavan lain näkökulmasta.

Muutosvaikutukset sääntelyn kohteena oleville julkishallinnon toimialan viranomaisille

Julkishallinnon toimialan toimijoina tiedonhallintalain soveltamisalan kautta NIS2-velvoitteiden alaan tulisi yhteensä noin 160 toimijaa.

Sääntelyn kohteena oleville tiedonhallintayksiköille tulisi velvoite ilmoittaa tietyt toimintaa koskevat tiedot valvovalle viranomaiselle (ehdotettu tiedonhallintalain 18 a §). Ilmoitukset voitaisiin kerätä sähköisesti joko jo muissa tehtävissä käytössä olevilla teknisillä lomakealustoilla tai uudella järjestelmällä, johon voidaan järjestää myös pääsynhallinta. Lisäksi olisi huomioitava tiedon tallennus ja tietokannan suojaaminen.

Lisäksi tiedonhallintayksiköiden tulisi huolehtia kyberturvallisuuden riskienhallinnasta. Riskienhallinnan velvoitteet aiheuttavat jonkin verran muutoksia tiedonhallintaan. Tiedonhallintayksikön olisi laadittava kyberturvallisuuden riskienhallinnan toimintamalli ja käytävä läpi tietojärjestelmien ja niiden fyysisen ympäristön suojaamiseksi säädetyt riskienhallintatoimenpiteet ja toteutettava ne riskienhallinnan perusteella omassa toiminnassaan. Lisäksi nämä toimenpiteet tulee dokumentoida riskienhallinnan toimintamalliin. Toimintamallin muodostavista asiakirjoista ja muista tiedoista muodostuu tiedonhallintayksikölle uusi hallittava tietoaineisto ja velvollisuus ylläpitää tietoaineistoa. Velvoitteen vaikutukset riippuvat osittain myös siitä, onko riskienhallinnan toimintamallin laadintaan saatavilla tarkempaa ohjeistusta tai mallipohjia esimerkiksi valvovalta viranomaiselta.

Esityksessä ei ehdoteta säädettäväksi tietojärjestelmästä, jolla tiedonhallintayksiköt ylläpitäisivät kyberturvallisuuden riskienhallinnan toimintamallin tietoaineistoja tai joilla poikkeamailmoitukset toteutetaan. Ehdotukseen sisältyvien tietoaineistojen käsittelyssä käytettävien tietojärjestelmien järjestäminen jää kunkin tiedonhallintayksikön tehtäväksi. Ehdotukseen ei sisälly sääntelyä, joka edellyttäisi tietojen käsittelyssä käytettäviltä tietojärjestelmiltä muuta, kuin mitä tiedonhallintalain 4 luvussa tietoaineistojen ja tietojärjestelmien tietoturvallisuudesta on säädetty.

Kyberturvallisuuden riskienhallinnassa muodostuvat tietoaineistot vastaavat pitkälti tietoaineistoja, joita viranomaiset ylläpitävät tiedonhallintalain 4 §:n 2 momentissa ja 4 luvussa säädettyjen tietoturvallisuusvelvollisuuksien osalta. Tämän vuoksi, ei ehdotuksesta arvioida

muodostuvan viranomaisille sellaisia uusia tietojen käsittelyyn kohdistuvia riskejä, jotka edellyttäisivät voimassa olevasta sääntelystä poikkeavien tietoturvallisuustoimenpiteiden toteuttamista. On kuitenkin mahdollista, että osalle viranomaisista voi siitä huolimatta aiheutua merkittäviäkin vaikutuksia, etenkin sellaisten viranomaisten osalta, joiden riskienhallintakyvykkyys on matala, ja jotka eivät ole aiemmin tehneet esimerkiksi vapaaehtoisia poikkeamailmoituksia.

Ehdotuksen vaikutuksesta ylläpidettävistä tietoaineistoista muodostettaviin asiakirjoihin sovellettaisiin tiedonhallintalain 25 ja 26 §:ssä säädettyä. Viranomaisen valvontaviranomaiselle toimittamat poikkeamailmoitukset ovat julkisuuslain tarkoittamia viranomaisen asiakirjoja, joista sen on rekisteriöitävä tiedonhallintalain 26 §:ssä säädetyt tiedot. Lisäksi soveltamisalaan kuuluvien viranomaisten tulisi yksilöidä kyberturvallisuuden riskienhallinnan toimintamallissa ylläpidettävät tietoaineistot tiedonhallintalain 27 §:ssä säädetyn mukaisesti.

Ehdotuksen vaikutuksesta muodostuvien uusien tietoaineistojen ylläpito edellyttää, että tiedonhallintayksiköt ja niihin kuuluvat viranomaiset varmistavat, että tietoaineistojen käsittelyssä käytettävien tietojärjestelmien käytöstä ja niistä mahdollisesti tehtävistä tietojen luovutuksista (poikkeamailmoitukset valvontaviranomaiselle, valvonnan ja seurannan perusteella luovutettavat tiedot) kerätään tarvittavat lokitiedot siten kuin tiedonhallintalain 17 §:ssä edellytetään.

Tiedonhallintalaissa säädettäisiin tiedonhallintayksikön johdon uusista tiedonhallinnan vastuista: kyberturvallisuuden riskienhallinnan toteuttaminen ja valvonnan järjestäminen sekä kyberturvallisuuden riskienhallinnan toimintamallin hyväksyminen ja sen toteuttamisen valvonta. Näiden velvollisuuksien toteuttamiseksi säädettäisiin ehdotuksessa myös johdon osaamisvaatimuksesta (riittävä perehtyneisyys), joka aiheuttaa tiedonhallintayksikölle mm. uuden tarpeen huolehtia, että johto saa tarvittavan koulutuksen ja johdolla on ajantasaiset ohjeet asiasta. Uudet säännökset edellyttäisivät, että tiedonhallintayksikön johto määrittää kyberturvallisuuden riskienhallinnan toteuttamiseen liittyvien tehtävien vastuut. Soveltamisalaan kuuluvien tiedonhallintayksiköiden tulisikin tarkentaa riskienhallintaa ja tiedonhallintaan liittyvien säädösten, määräysten ja ohjeiden noudattamista koskevia ohjeita sekä tarkastella ja tarkentaa tiedonhallintayksikön tekemien palvelusopimusten ehtoja. Tiedonhallintayksikön johdon tulisi myös huolehtia tarvittavan koulutuksen järjestämisestä määriteltyjä vastuita toteuttaville henkilöille. Vaatimukset kohdistuisivat jokaiseen tiedonhallintalain 4 a luvun soveltamisalaan kuuluvaan tiedonhallintayksikköön.

Ehdotetun 18 b §:n mukaan tiedonhallintayksiköllä olisi myös oltava dokumentoituna 18 b ja c §:ssä tarkoitetut kyberturvallisuuden riskienhallintaan liittyvät asiat (kyberturvallisuuden riskienhallinnan toimintamalli). Kyseiset toimenpiteet olisivat käytännössä osin vastaavia, jotka viranomaisen on jo otettava huomioon osana 4 luvun mukaisia tietoturvallisuustoimenpiteitä. Ehdotetun 4 a luvun soveltamisalaan kuuluvan tiedonhallintayksikön tulisi sisällyttää tai liittää kyberturvallisuuden riskienhallinnan toimintamalli osaksi tiedonhallintamalliaan. Tämä hyödyttäisi myös viranomaista, kun sen tiedonhallintaa määrittelevä ja kuvaava aineisto olisi koottuna samaan dokumentaatioon. Sääntely mahdollistaisi tiedonhallintayksiköiden ja niiden kyberturvallisuuden kannalta tarkoituksenmukaisen toteutusmallin, jossa lain 4 luvun edellyttämiä tiedonhallintamaliin sisällytettäviä yleisiä tietoturvallisuustoimenpiteitä voidaan täydentää ehdotetun 4 a luvun edellyttämillä riskinhallintatoimenpiteillä ja tiedonhallintayksikkö voi itse harkita kokonaisuuden suunnittelu- ja dokumentointirakenteen.

Viranomaisten tulisi myös ilmoittaa merkittävistä poikkeamista valvovalle viranomaiselle sekä hallinnon asiakkaille. Tarkoituksena on, että ilmoitukset tehtäisiin Kyberturvallisuuskeskuksen verkkosivuilta löytyvällä ilmoituslomakkeella. Poikkeaman käsittelystä muodostuisi

viranomaiselle velvollisuus ylläpitää poikkeamaa koskevia tietoja ja tietoja valvovalle viranomaiselle tehdyistä poikkeamailmoituksista myös omassa järjestelmässään (uusi tietoaineisto tai olemassa olevan tietoaineiston muokkaaminen). Viranomaisen tulisi myös ilmoittaa merkittävästä kyberuhkasta sekä kyberuhkan hallitsemiseksi käytettävissä olevista toimenpiteistä niille palvelujensa vastaanottajille, joihin merkittävä kyberuhka saattaa vaikuttaa.

Valvovan viranomaisen uusi tiedonsaantioikeus muodostaa valvottaville viranomaisille uuden velvollisuuden luovuttaa tietoja valvovalle viranomaiselle. Uusi tietojen luovutusvelvollisuus koskee kaikkia valvottavia viranomaisia. Valvovan viranomaisen tiedonsaantioikeutta ehdotetaan rajattavaksi siten, että se ei koske tiettyä osaa salassa pidettävistä tiedoista. Valvottavalle viranomaiselle muodostuukin velvollisuus arvioida tiedonsaantioikeuden laajuus, jota on kuvattu tarkemmin tiedonsaantioikeutta koskevan säännöksen (tiedonhallintalain 18 i §) yksityiskohtaisissa perusteluissa. Tiedonsaantioikeuden laajuus vaikuttaa myös poikkeamailmoituksissa toimitettaviin tietoihin.

Ehdotuksen vaikutuksesta tiedonhallintayksikön on ylläpidettävä tiedonhallintalain 5 §:ssä tarkoitettua tiedonhallintamallia ehdotuksesta muodostuvien uusien toimintaprosessien ja niissä hyödynnettävien tietoaineistojen ja tietojärjestelmien sekä näihin liittyvien vastuiden osalta. Lisäksi tiedonhallintayksikön on arvioitava ehdotuksista sen tiedonhallintaan kohdistuvat vaikutukset tiedonhallintalain 5 §:n 3 momentin mukaisesti.

Muutosvaikutukset valvoville viranomaisille, CSIRT-yksikölle ja keskitetylle yhteyspisteelle

Valvovien viranomaisten uudet valvontatehtävät, keskitetyn yhteyspisteen tehtävät, CSIRT-yksikön tehtävät sekä viranomaisten välinen yhteistyö, yhteistyö EU:n yhteistyöelimien kanssa sekä näihin liittyvä tiedon keruu ja tietojen luovuttaminen aiheuttavat muutoksia näiden viranomaisten tiedonhallintaan ja aiheuttavat myös muutostarpeita niiden tietojärjestelmiin sekä tietovarantoihin.

NIS2-direktiivin myötä tiedonhallintayksikölle syntyy uusia tehtäviä, tietoaineistoja ja mahdollisesti tietojärjestelmiä. Syntyvissä tehtävissä käsiteltävän tiedon salassa pidettävyys ja tietovirrat täytyy selvittää ja arvioida, jotta voidaan suunnitella tiedonhallintaa ja järjestelmätoteutuksia sekä laatia näihin liittyvää dokumentaatiota.

Kaikkiin mainittuihin tehtäviin niin valvontaviranomaisena, CSIRT-yksikön tehtävissä kuin keskitettynä yhteyspisteenä liittyy määrittely- ja arviointitehtäviä luokittelun ja pääsynhallinnan kannalta sen mukaan, mitä tietotyyppejä käsitellään julkisuuslain ja sähköisen viestinnän palveluista annetun lain, sähköisen viestinnän luottamuksellisuuden suojan sekä yleisen tietosuoja-asetuksen valossa, miltä tahoilta tietoa tulee, mihin tarkoituksiin tietoa saa käyttää ja keille ja millä perusteilla ja menettelyillä tietoa voi luovuttaa.

Valvova viranomainen

Erityisesti NIS1-sääntelyn valvovina viranomaisina toimineiden viranomaisten tiedonhallintamallit ovat pääosin valvontaviranomaisen toiminnan kannalta eri tietotyypeille ja eri tahoilta tuleville tiedoille pitkälti olemassa ja tiedonkäsittelyn olennaisin muutos on volyymien kasvu, kun valvottavat toimijat ja sääntelyn edellyttämät ennakoivat ja mahdollisesti myös jälkikäteiset valvontatoimenpiteet lisääntyvät.

Valvontaviranomaisten olisi toteutettava toimijoiden ilmoitusten vastaanotto, toimijarekisteri ja tarvittaessa tiedon toimittaminen keskitetylle yhteyspisteelle (ehdotetus kyberturvallisuuslaiksi, 15-17 § ja 41 §:n 4 mom) Lisäksi eräillä Liikenne- ja viestintäviraston valvontatoimivaltaan ehdotetuilla toimialoilla olisi järjestettävä NIS2-direktiivin 27 artiklan 1-4 kohdan tietojen ja niiden muutosten vastaanotto sekä kyseisten tietojen toimittaminen keskitetylle yhteyspisteelle (ehdotettu kyberturvallisuuslaki, 41 §:n 4 mom)

Viranomaisilla on entuudestaan sähköisiä ilmoitusalustoja ja toimijatietovarantoja, mutta niiden soveltuvuus uuteen tehtävään täytyy selvittää. Ilmoitusten kerääminen voitaisiin tehdä sähköisesti joko ennestään muissa tehtävissä käytössä olevilla teknisillä lomakealustoilla tai uudella järjestelmällä. Jos mahdollistettaisiin toimijalle tietojen päivittäminen suoraan rekisteriin, tulisi järjestelyssä toteuttaa ilmoittajien todentaminen. Tiedon verifiointia esimerkiksi suhteessa kaupparekisterissä oleviin oikeushenkilöihin olisi punnittava. Rekisteritiedon suojaaminen tulisi järjestää.

Poikkeamailmoitusten vastaanotto, jakaminen CSIRT-yksikölle ja käsittely tulee järjestää. Tarkoituksena on kehittää Kyberturvallisuuskeskuksen verkkosivuilta löytyvää ilmoitussovellusta siten, että sitä voisi hyödyntää esimerkiksi poikkeamailmoituksen jakamiseen CSIRT-yksikölle.

Suojattujen kanavien kuten turvapostin tarve ja tehokkuus valvontatehtävissä toimijoiden ja viranomaisen tiedonvaihdossa täytyy arvioida. Muutoin kuin paikan päällä tehtävät tarkastukset toimijoihin sekä tarkastuksista ja muiden valvontatoimivaltuuksien käytöstä kertyvän tiedon käsittely tulee suunnitella.

Viranomaisten välisen tiedonvaihdon todennäköisesti lisääntyessä niin kansallisesti kuin kansainvälisesti sähköiset tiedonvaihtojärjestelyt voivat edellyttää kehittämistä.

CSIRT-yksikkö

Ehdotettu sääntely aiheuttaisi muutoksia CSIRT-yksikön tiedonhallintaan. CSIRT-yksikön teknisistä ja toiminnallisista vaatimuksista säädettäisiin jatkossa lailla (NIS2-direktiivin 10 artikla ja 11 artiklan 1 kohta sekä ehdotettu kyberturvallisuuslaki, 19 §), CSIRT-yksikölle annettaisiin uusia tehtäviä (NIS2-direktiivin 11 artiklan 3 kohta ja kyberturvallisuuslaki, 19-20 §) ja edellä mainittujen uusien tehtävien johdosta CSIRT-yksikön tulee ottaa käyttöön uusia tietojärjestelmiä.

Eräät CSIRT-yksikölle säädettävistä tehtävistä ovat sellaisia, joita Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen CERT-toiminta on hoitanut ja tuottanut jo ennen NIS2-direktiivin voimaantuloa ja joiden ei ole arvioitu aiheuttavan merkittäviä muutoksia tiedonhallintaan. Tästä huolimatta uusista tehtävistä seuraa eräitä prosessimuutoksia ja tietovirtojen muutoksia, jotka tulee dokumentoida sääntelyn täytäntöönpanon edetessä. Lisäksi uusien tehtävien hoitaminen edellyttää investointeja uusiin tietojärjestelmiin sekä olemassa olevien tietojärjestelmien ja palvelujen kehittämistä.

Uutena tiedonhallinnallisena muutoksena CSIRT-yksikön tulee muun muassa luoda prosessi uudenlaisten poikkeamailmoitusten käsittelyyn, joita valvovat viranomaiset toimittavat CSIRT-yksikölle. Todennäköisesti kasvava ilmoitusmäärä edellyttää jatkovalmistelussa tarkempien tiedonhallinnallisten muutosten arviointia.

Keskitetty yhteyspiste

Liikenne- ja viestintävirasto on toiminut jo NIS1-sääntelyn aikana keskitettynä yhteyspisteenä, mutta nyt ehdotettavalla sääntelyllä arvioidaan olevan tiedonhallintavaikutuksia myös sille säädettävien tehtävien osalta.

Keskitetyn yhteyspisteen olisi toimitettava ENISA:lle kolmen kuukauden välein yhteenvetoraportti, joka sisältää anonymisoidut koontitiedot merkittävistä poikkeamista, poikkeamista, kyberuhkista ja läheltä piti -tilanteista, joista on ilmoitettu kyberturvallisuuden riskienhallinnasta annetun lain mukaisesti (ehdotettu kyberturvallisuuslaki, 18 §:n 3 mom). Tehtävä edellyttäisi keskitetyltä yhteyspisteeltä aikaisempaa useammin tapahtuvaa raportointia, sillä tällä hetkellä tietoja ilmoitetaan kerran vuodessa. Lisäksi ilmoitettavien tietojen joukko on laajempi kuin aikaisemmin.

Lisäksi keskitetty yhteyspiste vastaisi NIS 2-direktiivin 3 artiklan 5 kohdassa ja 27 artiklan 4 kohdassa tarkoitettujen ilmoitusten tekemisestä Euroopan komissiolle, NIS-yhteistyöryhmälle ja Euroopan unionin kyberturvallisuusvirasto ENISA:lle. Keskitetyn yhteyspisteen olisi siis ilmoitettava kahden vuoden välein komissiolle ja NIS yhteistyöryhmälle toimijaluetteloa koskevia tietoja. Lisäksi keskitetyn yhteyspisteen olisi toimitettava ENISA:lle eräiden Liikenne- ja viestintäviraston valvontatoimivaltaan ehdotettujen toimialojen osalta NIS2-direktiivin 27 artiklan 4 kohdassa tarkoitetut tiedot.

Kun toimijat ovat ensin toimittaneet tiedot valvoville viranomaisille, on ratkaistava, miten ja missä laajuudessa valvovat viranomaiset toimittavat tiedot keskitetylle yhteyspisteelle, joka puolestaan vastaa tietojen toimittamisesta EU:n yhteistyöelimille. Valittu ratkaisu vaikuttaa osaltaan tiedonhallinnan muutosvaikutusten arviointiin.

Toimitettaessa tietoja EU:n yhteistyöelimille, eli ENISA:lle, komissiolle ja NIS yhteistyöryhmälle, tulee selvittää, tarjoavatko ne jonkin teknisen järjestelyn tätä tarkoitusta varten.

4.5 Muut ihmisiin kohdistuvat ja yhteiskunnalliset vaikutukset

4.5.1 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 toimintaedellytyksiä 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.

Esityksellä arvioidaan olevan yhteiskunnan häiriöttömän toiminnan edistämisen kautta välillisesti myönteisiä vaikutuksia kansalaisten turvallisuudelle. Edistämällä yhteiskunnan keskeisten toimialojen ja -palveluiden kykyä sietää kyberhäiriöitä parannetaan välillisesti kansalaisten turvallisuutta erityisesti silloin, kun toimialassa tai palvelussa kyse on kansalaisten turvallisuuteen vaikuttavista, yhteiskunnan toiminnan kannalta kriittiseen infrastruktuurin liittyvistä seikoista. Esityksellä tavoitteena on vähentää kyberhäiriöiden määrää. Näkyvien kyberhäiriöiden yleistyminen olisi omiaan vaikuttamaan kansalaisten kokemukseen turvallisuudesta yhteiskunnassa.

4.5.2 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 asianmukainen suojaus edellyttää järjestelmien tietoturvaominaisuuksien kehittämistä. Toimenpiteet tietojärjestelmien ja viestintäverkkojen kyberturvallisuuden parantamiseksi vaikuttavat myös niissä käsiteltävien henkilötietojen tietosuojaan sitä parantavasti. Esityksellä olisi siten tietoturvan kohentumisen myötä myönteisiä vaikutuksia myös tietosuojan parantumiseen. Viestintäverkkojen ja tietojärjestelmien kyberturvallisuuden kehittämisellä pyritään muun ohella parantamaan ja suojaamaan myös henkilötietojentietosuojaan liittyviä oikeushyviä. Toisaalta esitykseen sisältyy viranomaisten tiedonsaantia sekä viranomaisten välistä tiedonvaihtoa koskevia uusia säännöksiä. Tällaisten säännösten voidaan ajatella myös heikentävän tietosuojaa. Ehdotuksen nojalla tehtävien viranomaistoimien tarkoituksena on kuitenkin kyberturvallisuuden kehittäminen ja sitä kautta myös tietosuojaan liittyvien oikeushyvien edistäminen tietojärjestelmissä ja viestintäverkoissa. Ehdotetut säännökset on laadittu yksityiselämän suojaan liittyvät perustuslailliset näkökohdat huomioon ottaen ja pyritty rajoittamaan vain välttämättömään esityksen tarkoituksen toteuttamiseksi. Ehdotuksen nojalla tehtävien viranomaistoimien tarkoituksena on kuitenkin muun ohella tietosuojaan liittyvien oikeushyvien edistäminen tietojärjestelmissä ja viestintäverkoissa ja myönteisen vaikutuksen näille oikeushyville arvioidaan olevan merkittäviä.

4.5.3 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 2.12.

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 keskitetyllä 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 on vaikuttanut myös kyberturvallisuuden merkityksen kasvu toimialarajat ylittäen. 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 hajautettua sääntelyä paremmin ja yhdenmukaisemmin NIS2-direktiivin tavoitteen, eli osoittaisi kyberturvallisuusvelvoitteiden vähimmäistason kaikille soveltamisalaan kuuluville toimijoille. 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 -sääntely 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 toimialalla toimijan määrittely on myös poikkeava muista direktiivin liitteiden toimialoista. Muilla toimialoilla soveltaminen määrittyy lähtökohtaisesti ns. kokokriteerin täyttymisen perusteella, kun taas julkishallinnon toimialalla soveltamisalaan kuuluvat direktiivin liitteen I kohdan 10 mukaisesti keskustason ja aluetason julkishallinnon toimijat sellaisina kuin jäsenvaltio on ne kansallisen lainsäädännön mukaisesti määrittänyt.

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 noudattamisen valvonta olisi järjestetty julkishallinnon toimialan osalta. Sektorikohtaisen valvonnan ja julkishallinnon tilannetietoisuuden osalta on myös tarkoituksenmukaista, että julkishallinnon toimialan toimijoilla on erikseen säädetty valvonta ja valvova viranomainen suhteessa muihin toimialoihin, joilla toimii myös julkisia toimijoita. Julkinen toimija voi harjoittamansa toiminnan osalta kuulua ehdotetun kyberturvallisuuslain soveltamisalaan (esim. hyvinvointialueiden ja hyvinvointiyhtymien terveydenhuolto). Julkinen toimija voisi myös kuulua yksinomaan kyberturvallisuuslain soveltamisalaan, koska tiedonhallintalain NIS2-sääntelyä 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 ehdotetun kyberturvallisuuslain 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 julkisiin 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 toimialalla 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 tehtävät ja toimivaltuudet tukevat monessa suhteessa yleisemminkin 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-yksikölle 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. Valmistelussa ei niin ikään ole tunnistettu olemassa olevaa viranomaista, jonka olemassa oleviin tehtäviin NIS2-direktiivin velvoitteiden keskitetty valvonta olisi luontevasti sopiva osa. Valmistelussa on tunnistettu, että ehdotettujen valvontatehtävien tapaisia tehtäviä on osoitettu useille eri viranomaisille. Valmistelussa on tunnistettu, että toimialakohtaista riskienhallintaa tai erityisiä toimialakohtaisia toimintaan kohdistuvia turvallisuusvaatimuksia valvotaan sektorikohtaisissa asiantuntijaviranmaisissa. Nykyisistä NIS1-direktiiviä valvovista viranomaisista yhdelläkään ole ehdotetun sääntelyn edellyttämää laaja-alaista osaamista eri toimialojen erityispiirteistä.

Valvonnan keskittämisen näkökulmasta vaihtoehtoina on arvioitu tehtävien keskittämistä uudelle valvontataholle tai Liikenne- ja viestintävirastolle, 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. Liikenne- ja viestintävirastolle tehtävän osoittaminen edellyttäisi käytännössä uuden toiminnallisen yksikön ja sen edellyttämän osaamisen perustamista. Liikenne- ja viestintävirastossa ei ole toimialakohtaista osaamista NIS2-direktiivin laajasta soveltamisalasta muuten kuin liikenteen ja viestinnän toimijoiden osalta. Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksessa on olemassaolevaa korkeatasoista tietoturvaosaamista, mutta Kyberturvallisuuskeskuksen osalta rooli samanaikaisesti sekä keskitettynä valvovana viranomaisena jokaisella sektorilla että tietoturvaloukkauksia tutkivana ja ohjaavana CSIRT-yksikkönä, jota vastaavia tehtäviä sille on nykyisin osoitettu, yhdistettynä Kyberturvallisuuskeskuksen muihin nykyisiin tehtäviin loisi laajan tehtäväkokonaisuuden, joka olisi epätarkoituksenmukainen sekä soveltamisalaan kuuluvien toimijoiden että viranomaisen toimintaedellytyksien kannalta. Vastaava haaste tulisi epätarkoituksenmukaisen laaja-alaisesta valvonnasta ja sen edellyttämän toimialakohtaisen osaamisen hankkimisesta tulisi myös muulle viranomaiselle, jolle valvontaa keskitettäisiin. Yhteenvetona valmistelussa on päädytty arvioon siitä, että mikäli valvonta keskitettäisiin, olisi 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. Hajautetussa mallissa näihin toimijoihin voisi kohdistua useamman viranomaisen valvontatoimenpiteitä. Keskitetty valvontamalli keskittäisi myös kyberturvallisuuden riskienhallintavelvoitteisiin liittyvää osaamista viranomaisessa. Keskitetty valvontamalli parantaisi myös toimialojen välisen valvonta- ja tulkintakäytännön yhtenäisyyttä verrattuna toimialakohtaisesti hajautettuun malliin ja voisi siten vaikuttaa toimijoiden oikeusturvaa parantavasti. 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, velvoitteiden soveltamisala ei ole yleinen ja toimintaan liittyvä, kuten henkilötietojen käsittely, vaan NIS2-direktiivin soveltamisalaan kuuluvat direktiivissä säädetyt kriteerit täyttävät toimijat säädetyillä toimialoilla. Lisäksi sääntely ei kohdistu henkilötietojen käsittelyä vastaavalla tavalla toiminnan osaan, vaan kokonaisvaltaisesti kyberturvallisuusriskien hallintaan ja merkittävien poikkeamien raportointiin soveltamisalaan kuuluvissa organisaatioissa. Toimijoiden määrä ja laatu sekä toiminnan yhteiskunnallinen merkittävyys vaihtelevat toimialakohtaisesti. Nämä seikat puoltavat valvontamallia, jossa toimialakohtaiset erityispiirteet sekä toimialakohtaisen muuta kuin kyberturvallisuutta koskevan turvallisuuden ja riskienhallinnan sääntely voidaan yhteen sovittaa 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.

Lisäksi on todettava, että sisällöllisesti NIS2-direktiivin riskienhallintavelvoite edellyttää valvontamallista riippumatta valvovalta viranomaiselta sekä kyseisen toimialan markkinatuntemusta, että sektorikohtaisten erityispiirteiden sekä muun relevantin toimialakohtaisen lainsäädännön tuntemusta. Valvonnan toteuttaminen täysin ilman toimialakohtaista ymmärrystä ei ole viranomaisessa mahdollista. Valvovan viranomaisen olisi tunnettava valvottavaa toimialaa, 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. Riskin, riskienhallinnan ja riskinhallintatoimenpiteiden oikeasuhtaisuuden arvioinnissa merkityksellistä on riskin toteutumisen todennäköisyys suhteessa siitä aiheutuviin haitallisiin vaikutuksiin.

Edellä esitetyt seikat huomioiden valmistelun aikana on vaihtoehtoarvioinnin lopputuloksena päädytty siihen, että kansallisesti NIS 2 –direktiivin mukaisten velvoitteiden valvonta olisi tarkoituksenmukaista järjestää siten, että valvonta osoitettaisiin toimialakohtaiselle valvovalle viranomaiselle. 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 kyvykkyys 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 kyberturvallisuudesta. 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 täytäntöönpanossa olisi kiinnitettävä huomiota valvovien viranomaisten välisten tulkintojen ja toimenpiteiden yhteismitallisuuteen valvottavilla toimialoilla.

Valvontatoiminnon perustamisesta toimialakohtaisesti hajautettuihin viranomaisiin aiheutuisi kustannuksia, koska tehtävä olisi viranomaisille joko uusi tai laajenisi merkittävästi NIS1-direktiivin valvonnasta. Vastaavasti 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. Julkistaloudelle aiheutuvien kustannusten osalta katsotaan myös perustellummaksi, että kyberturvallisuusvelvoitteita valvoisivat sektorikohtaisesti samat viranomaiset, jotka valvovat sääntelyn kohteena olevia toimijoita muiltakin osin. Jos valvonta keskitettäisiin pääosin yhdelle viranomaiselle, uuden valvontaa toteuttavan keskitetyn viranomaistahon arvioidaan aiheuttavan noin 10-25 % hajautettua mallia korkeammat kokonaiskustannukset valvontatoiminnan järjestämiseksi samalla kyvykkyystasolla kuin hajautetussa mallissa.

Edellä esitetyn lisäksi NIS1-direktiivin täytäntöönpanossa omaksuttu sektorikohtainen valvontamalli on koettu pääosin toimivaksi. Niillä toimialoilla, jotka ovat kuuluneet NIS1-direktiivin velvoitteiden alaan, 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 toimivaa yhteistyötä ole tarkoituksenmukaista kaventaa NIS2-direktiivin täytäntöönpanon yhteydessä.

5.1.5 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 julkishallinnon toimialalla. 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. Maa- ja metsätalousministeriön mukaan valvovien viranomanomaisten määrää ei pitäisi lisätä eriyttämällä valvontaa valtionhallinnon ja aluehallinnon tasolla, vaan julkishallinnon valvonta tulisi keskittää olemassa olevien kyberturvallisuustoimintojen yhteyteen tai uudelle riippumattomalle poikkihallinnolliselle elimelle, jotta se olisi systemaattista, yhtenäistä ja saataisiin parhaat resurssit laajaan käyttöön. Ministeriön rooli hallinnonalansa toimijoiden valvontatoiminnan tuessa voitaisiin myös määritellä. Julkishallinnon valvonnan tulisi myös tukea muuta sektorikohtaista valvontaa, ainakin kun toimija on osa julkista hallintoa. 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.

Julkishallinnossa on nykyisinkin eri sektoreilla valvonta-asetelmia, joissa virasto valvoo ylempiä tahojaan, kuten ministeriöitä, eikä niitä ole pidetty lainsäädännössä muodollisesti ongelmallisina. Asetelma ei siten muodostaisi estettä valvontatehtävän osoittamiseksi Liikenne- ja viestintävirastolle. Liikenne- ja viestintävirastolla olisi myös tosiasiallisesti mahdollisuus valvoa myös ministeriöitä käyttäen laissa säädettyjä tiedonsaanti- ja tarkastustoimivaltuuksia. Asetelma kuitenkin edellyttää, että valvonnasta säädettäessä huomioidaan asianmukaisesti valtioneuvoston oikeuskanslerin ja eduskunnan oikeusasiamiehen toiminta ylimpinä laillisuusvalvojina.

5.1.6 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 tieto- ja 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 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

6.1 Lausuntokierros

Esitys on ollut lausuntokierroksella suomeksi kahdeksan viikkoa ajalla 3.10.–29.11.2023. Esitys on ollut lausuntokierroksella ruotsiksi yhteensä kahdeksan viikkoa ajalla 6.10.–1.11. (pykälät ja osa perusteluista) ja 1.11.–4.12.2023 (kokonaisuudessaan). Esitys on ollut lausuttavana Ahvenanmaan maakuntahallituksella kahdeksan viikkoa ajalla 2.11. – 29.12.2023.

Esityksestä vastaanotettiin yhteensä 131 lausuntoa.

Lausuntopalautteesta on laadittu lausuntoyhteenveto, jossa kuvataan lausuntojen keskeisin palaute ja merkityksellisimmät näkökannat. Lausuntopalaute ja lausuntoyhteenveto on saatavilla Valtioneuvoston hankeikkunasta hanketunnuksella LVM027:00/2023 (linkki: https://valtioneuvosto.fi/hanke?tunnus=LVM027:00/2023).

Lausuntopalautteessa pidettiin yleisesti tärkeänä ja kannatettavana esityksen tavoitteita kyberturvallisuuden vahvistamiseksi yhteiskunnassa. Kyberturvallisuuden riskienhallinta- ja raportointivelvoitteiden asettamista lain tasolla pidettiin kannatettavana. Velvoitteista säätämistä keskitetysti uudella toimialarajat ylittävällä lailla pidettiin kannatettavana. Lausunnoissa kannatettiin niin ikään NIS2-direktiivin täytäntöönpanoa sen velvoitteiden vähimmäistasolla ja kansallinen liikkumavara esitetyllä tavalla hyödyntäen. Lausunnoissa esitettiin runsaasti yksityiskohtaisia ja teknisiä huomioita esitetystä sääntelystä.

Toimialakohtaisesti hajautettua valvontamallia ja valvonnan yhdistämistä muuhun toimijoihin kohdistuvaan valvontaan pääosin kannatettiin lausuntopalautteessa. Oikeusministeriö arvioi lausunnossaan keskitetyn valvontamallin toimialakohtaista hajautusta perustellummaksi tavaksi järjestää valvonta. Eräisiin toimijoihin kohdistuisi valvontaa useamman viranomaisen toimesta, esimerkiksi hyvinvointialueet, jotka kuuluisivat sekä julkishallinnon että terveyssektorin määritelmien alaan.

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

Tiedonhallintalakia koskevien lausuntojen perusteella turvallisuusluokitteluvelvoitteen piiriin kuuluvia viranomaisia ja muita tahoja tulisi selvittää laajempana kokonaisuutena eikä pistemäisesti lisätä sääntelyn piiriin vain yhtä toimijaa. Lausuntopalautteen johdosta on poistettu tiedonhallintalain 18 §:n 1 momenttia eli turvallisuusluokitteluvelvollisuutta koskenut muutosehdotus.

Lausuntopalautteen johdosta esitykseen on tehty muutoksia, täsmennyksiä ja täydennyksiä. Esityksen keskeisiä ehdotuksia sääntelytavasta, -tasosta tai viranomaistehtävistä ei ole muutettu

lausuntopalautteen johdosta. Lausuntopalautteen johdosta esitykseen on tehty seuraavia muutoksia.

Soveltamisalan osalta esityksessä on pyritty tarkentamaan toimijan määritelmää ja siihen liittyvää kokokriteeriä. Perusteluihin on tarkennettu kokokriteerin soveltumista sekä toimijan määritelmän käsittämistä oikeushenkilökohtaisesti. Perusteluissa on selkiytetty lain soveltumista koko oikeushenkilöön, vaikka vain osa toiminnasta olisi liitteessä I tai II tarkoitettua toimintaa. sekä koko oikeushenkilön toiminnan huomioimista arvioitaessa kokoedellytyksen täyttymistä. Toimijan määritelmän kokoedellytyksestä poikkeamiseen liittyvää valtioneuvoston asetuksenantovaltuutta on tarkennettu siten, että se koskisi toimijan sijaan laissa säädettyjen kriteerien tarkentamista. Lisäksi soveltamisalaan on lisätty kansallinen rajaus lain soveltumisesta kuntalaissa tarkoitettuun kuntaan vain siltä osin, kun kunta harjoittaa liitteessä I tai II tarkoitettua taikka CER-direktiivin nojalla kriittiseksi määritettyä toimintaa. Lisäksi soveltamisalaan on lisätty selventävä rajaus siitä, ettei lakia olisi sovellettava vähäiseen ja satunnaiseen liitteessä I tai II tarkoitettuun toimintaan.

Toimialakohtaisesti soveltamisalaa on täsmennetty postipalveluiden, tieliikenteen ja terveyssektorin osalta. Postipalveluiden osalta soveltamisalaan kuuluisivat postidirektiivissä tarkoitetut postipalvelujen tarjoajat. Tieliikenteen osalta soveltamisalaan kuuluisivat liikenteen palveluista annetun lain 15 luvussa tarkoitetun tieliikenteen ohjaus- ja hallintapalvelun tarjoajat.

Terveyssektorilla terveydenhuollon tarjoajan määritelmää on tarkennettu siten, että soveltamisalaan kuuluisivat sosiaali- ja terveydenhuollon valvonnasta annetussa laissa tarkoitetut palveluntuottajat, jotka tuottavat terveyspalvelua, sekä veripalvelulain mukaiset veripalvelulaitokset, apteekit ja muut potilasdirektiivin mukaiset terveydenhuollon ammattihenkilöt, jotka toimittavat tai tarjoavat lääkkeitä tai lääkinnällisiä laitteita. Soveltamisala vastaisi terveyssektorilla potilasdirektiivin mukaista NIS 2 –direktiivin edellyttämää vähimmäissoveltamisalaa yhdessä tiedonhallintalain soveltamisalan kanssa.

Tiedonhallintalaissa uuden 4 a luvun soveltamisalaa koskeva 3 § on lausuntokierroksen johdosta muotoiltu uudelleen ja sisällöllisesti muutettu siten, että tasavallan presidentin kanslia ja kolmansissa maissa sijaitsevat edustustot eivät kuuluisi sääntelyn soveltamisalaan. Muutamien julkisten toimijoiden asemaa on selkeytetty perusteluissa. Eduskunnan virastojen osalta sääntelyä muutettiin siten, että virastot kuuluisivat soveltamisalaan. Soveltamisalaa on myös täsmennetty sen osalta, että CER-direktiivin nojalla kriittiseksi toimijaksi määritettyyn julkishallinnon toimialan toimijaan sovellettaisiin 3 §:n rajauksista huolimatta 4 a lukua. Lakiehdotukseen lisättiin myös kriittisen toimijan määritelmä. Soveltamista täsmennettiin myös niiden viranomaisten osalta, joihin ei sovellettaisi valvovan viranomaisen toimivaltuuksia koskevia säännöksiä.

Kyberturvallisuuslain ja tiedonhallintalain välistä suhdetta selkeytettiin määrittelemällä laeissa (tiedonhallintalaki 1 § 2 mom ja kyberturvallisuuslaki 1 §) selkeämmin, mitä osin NIS2-direktiivi täytäntöönpannaan tiedonhallintalailla ja miltä osin kyberturvallisuuslailla. Tiedonhallintalain 18 h §:n viittaussäännöksiä sekä valvovan viranomaisen toimivaltaa koskevia pykäliä muotoiltiin lakien välisen suhteen selkeyttämiseksi.

Toimijoihin kohdistuvan riskienhallinta- ja raportointivelvoitteen osalta sekä kyberturvallisuuslaissa että tiedonhallintalaissa on täsmennetty merkittävän poikkeaman määritelmää. Merkittävä poikkeama edellyttäisi taloudellisen haitan osalta huomattavuutta. Riskienhallinta- ja raportointivelvoiteisiin liittyvän valvovan viranomaisen määräyksenantovaltuuden alaa on kavennettu. Valvova viranomainen voisi määräyksellä täsmentää toimialakohtaisia seikkoja riskinhallinnassa, toimitusketjujen unionin tason

riskiarviointien huomioimista, sekä poikkamailmoituksiin ja – raportteihin liittyviä teknisiä menettelytapoja ja tietosisältöjä. Liikenne- ja viestintävirasto voisi antaa ohjeistusta riskienhallintavelvoitteeseen ja riskienhallintatoimenpiteisiin liittyvistä seikoista. Lakiin on lisätty viittaussäännökset Euroopan komission antamien täytäntöönpanosäädösten soveltamisesta riskienhallinnassa ja merkittävän poikkeaman määritelmässä. Lisäksi riskinhallintavelvoitetta koskevia perusteluita on tarkennettu ja täsmennetty erityisesti toimitusketjun huomioimista koskevan osa-alueen osalta, joka kattaisi toimijan välittömät toimitusketjut. Merkittävistä poikkeamista raportointia koskien lakiin on lisätty säännös valvovan viranomaisen velvollisuudesta ilmoittaa merkittävästä poikkeamasta poliisille, jos merkittävän poikkeaman epäillään aiheutuvan rikoksesta, josta säädetty enimmäisrangaistus olisi vähintään kolme vuotta vankeutta.

Myös tiedonhallintalakiin lisättiin tarpeelliset viittaukset komission täytäntöönpanosäädöksiin ja delegoituihin säädöksiin.

Tiedonhallintalain 4 a luvun riskienhallintaan liittyviä velvoitteita yhtenäistettiin kyberturvallisuuslain vastaavien velvoitteiden kanssa. Tiedonhallintalaissa riskin määritelmä kuitenkin muutettiin kyberriskiksi, koska tiedonhallintalaki sisältää muitakin riskienhallintavelvoitteita, joihin NIS2-direktiivn riskin määritelmä ei täysin sovellu.

CSIRT-yksikön osalta laissa säädettäisiin täsmällisemmin sille asetettavista vaatimuksista. Haavoittuvuuskartoitusta koskevaan ehdotukseen on tarkennettu, ettei kartoituksessa käsitellä luottamuksellisen viestinnän suojan alaan kuuluvia tietoja. Vapaaehtoisten kyberturvallisuustietojen jakamisjärjestelyiden osalta lakiin on tehty täsmennyksiä koskien tiedonvaihtoa jakamisjärjestelyssä. CSIRT-yksiköllä olevien tietojen palomuurisäännöstä suhteessa lain valvontaan on tarkennettu.

Valvontavastuun osalta valvontatehtävien jakoa on tarkennettu vety- ja maakaasualan toimijoiden osalta Energiaviraston ja Turvallisuus- ja kemikaaliviraston välillä. Terveyssektorilla ehdotettua valvontatehtävien jakoa on tarkennettu Sosiaali- ja terveysalan lupa- ja valvontavirasto Valviran ja Lääkealan turvallisuus- ja kehittämiskeskus Fimean välillä. Valvontatoimivaltuuksien osalta esityksestä on poistettu säännös huomautuksen antamisesta ja tarkennettu varoituksen antaminen kirjallisena. Valvovan viranomaisen tiedonsaantioikeutta koskevia säännöksiä on täsmennetty ja säännökset yhdistetty. Tarkastustoimivaltuutta on tarkennettu siten, että valvova viranomainen voisi käyttää tarkastuksessa vain apuna ulkopuolista, mutta ei ulkoistaa tarkastusta. Johdon vastuuta ja johdon toiminnan kieltämistä koskevista säännöksistä on poistettu viittaus johdon välittömässä alaisuudessa toimiviin henkilöihin sekä tarkennettu johdon toiminnan kieltämisen liittymistä kiellon perusteena olevan puutteen tai laiminlyönnin jatkumiseen.

Oikaisuvaatimusmenettelyn sijasta muutosta valvovan viranomaisen päätökseen haettaisiin suoraan oikeudenkäynnistä hallintoasioissa annetussa laissa säädetyssä järjestyksessä, Lausuntopalautteen perusteella oikaisuvaatimusmenettely olisi epätarkoituksenmukainen osa muutoksenhakumenettelyä, sillä valvontapäätökset perustuisivat valvovassa viranomaisessa tapauskohtaiseen harkintaan.

Luvan tai sertifioinnin peruuttamista tai toimijan toiminnan rajoittamista koskeva toimivaltasäännös on poistettu kyberturvallisuuslaista. Sen sijasta esitykseen on lisätty säännökset, joissa kyberturvallisuuslain velvoitteiden rikkominen lisättäisiin luvan peruuttamisperusteeksi eräiden toimilupien osalta. Kyseiset muutokset on lisätty liitelakeina maa-asemalakiin, sähkö- ja maakaasumarkkinoiden valvonnasta annettuun lakiin ja kemikaaliturvallisuuslakiin.

Esityksessä olevia vaikutusarviointeja sekä vaikutuksia viranomaistoiminnalle ja julkistaloudelle on täydennetty ja päivitetty lausuntokierroksen aikana ja lausuntokierroksella esitettyjen arvioiden johdosta. Vaikutusarviointiin on lisätty tiedonhallinnan muutosvaikutuksia koskeva arvio.

Lisäksi esityksen säätämisjärjestysperusteluita on tarkennettu ja laajennettu lausuntokierroksen johdosta. Esityksen säätämisjärjestystä koskeviin perusteluihin on lisätty arvio esityksen suhteesta omaisuudensuojaan, valtion toimielinten yleisistä perusteista säätämiseen, eräiden valtioelinten ja viranomaisten asemaan sekä Ahvenanmaan itsehallintoon.

Verkkotunnusten rekisteröintiä koskien sähköisen viestinnän palveluista annettuun lakiin on lisätty säännös oikaisuvaatimuksesta muutoksenhakukeinona viranomaisen päätökseen, joka koskee verkkotunnuksen rekisteröinnin estämistä tai rekisteröinnin poistamista.

Esitykseen on tehty myös lausuntopalautteen johdosta muita, pienempiä ja lainsäädäntöteknisiä muutoksia, täsmennyksiä ja täydennyksiä.

6.2 Muu kuuleminen

Esityksen valmistelusta on viestitty aktiivisesti sidosryhmille ja sidosryhmiä on kuultu valmistelun aikana myös muutoin kuin lausuntokierroksen aikana.

Esityksen valmistelun aikana on järjestetty avoimet kuulemistilaisuudet 30.3.2023 ja 9.10.2023 NIS2-direktiivin kansallisesta toimeenpanosta Suomessa. Lisäksi 4.5.2023 on järjestetty avoin webinaari koskien NIS2-direktiivin kansallista toimeenpanoa julkishallinnon sektorilla. Kuulemistilaisuuksien aineisto on saatavilla Valtioneuvoston hankeikkunassa hanketunnuksella LVM044:00/2022 (linkki: https://valtioneuvosto.fi/hanke?tunnus=LVM044:00/2022).

NIS2-direktiivin toimeenpanoa tukeva päätyöryhmä on kutsunut keskeisten sidosryhmien edustajia kuultavaksi päätyöryhmän kokouksiin 18.4.2023 ja 25.5.2023. Kokouksissa kuultavat sidosryhmät ovat olleet FiCom ry, FISC – Kyberala ry, Finanssiala ry, Elinkeinoelämän keskusliitto ry, Energiateollisuus ry, Teknologiateollisuus ry, Kemianteollisuus ry, Elintarviketeollisuusliitto ja Päivittäistavarakauppa ry.

Esityksen valmistelua on edeltänyt Euroopan komission verkko- ja tietoturvadirektiivistä (NIS-direktiivi) ja sen soveltamisesta eri jäsenvaltioissa tekemä uudelleenarviointi vuonna 2020. Komissio on järjestänyt direktiivistä julkisen kuulemisen vuoden 2020 aikana. Suomikin vastasi osaltaan julkiseen kuulemiseen ennakkovaikuttamislinjausten perusteella (E 107/2020 vp).

Kansallisesti sidosryhmiä on kuultu NIS2-direktiivin ennakkovaikuttamisen ja EU-neuvotteluiden aikana muun muassa EU-jaostoissa pidettyjen esitysten kautta, sidosryhmille erikseen pidettyjen useiden esitysten kautta sekä epävirallisen kansallisen seurantaryhmäjakelun kautta. Hallituksen esityksen valmistelun aikana on lisäksi pidetty useita esityksiä NIS2-direktiivistä ja sen kansallisesta täytäntöönpanosta sidosryhmille sekä käyty keskustelua ja kuultu näkemyksiä näiden tilaisuuksien yhteydessä.

6.3 Lainsäädännön arviointineuvoston lausunto

Lainsäädännön arviointineuvosto on antanut luonnoksesta hallituksen esitykseksi lausunnon 29.2.2024 asianumerolla VN/5157/2024-VNK-2. Lausumanaan arviointineuvosto katsoi, että hallituksen esitysluonnos noudattaa välttävästi lainvalmistelun vaikutusarviointiohjetta. Hallituksen esitysluonnoksessa on olennaisia puutteita ja esitysluonnosta tulee korjata

neuvoston lausunnon mukaisesti ennen hallituksen esityksen antamista. Esityksen vaikutusarviointia on täydennetty lainsäädännön arviointineuvoston lausunnon johdosta.

Arviointineuvosto katsoi, että esitysluonnos sisältää laajan kuvauksen täytäntöönpantavasta direktiivistä, mutta esitysluonnos on hajanainen ja vaikealukuinen. Arvioneuvosto katsoi, että kokonaiskuvan saaminen vaikutuksista edellyttäisi tiivistelmää keskeisistä vaikutuksista. Keskeisimpinä puutteina ja kehityskohteina arviointineuvosto katsoi, että esityksessä tulisi antaa suuntaa-antava arvio soveltamisalan piiriin tulevien toimijoiden kokonaismäärästä, arvioida tarkemmin yritysten kustannuksia suhteessa liikevaihtoon, IT-kustannuksiin ja yrityskokoon, selkeyttää esimerkein raportointivelvollisuuden piiriin kuuluvia tilanteita ja raportoinnista yrityksille aiheutuvia kustannuksia sekä kiinnittää paremmin huomiota sääntelykokonaisuuden ymmärrettävyyteen esimerkiksi havainnollistamalla keskeisten ja muiden toimijoiden eroa ja sääntelyn eroavaisuuksia niiden välillä kaaviolla tai taulukolla. Lisäksi arviointineuvosto katsoi, että jos esityksellä arvioidaan olevan yhteiskunnan häiriöttömän toiminnan kautta olennaisia vaikutuksia kansalaisille, niitä tulisi käsitellä esityksessä. Arviointineuvosto katsoo, että vaikutusten ymmärrettävyyden parantamiseksi tulisi laatia tiivistelmä, josta saisi kokonaiskuvan olennaisista määrällisistä ja laadullisista vaikutuksista. Lisäksi arviointineuvosto katsoi, että esitystä tulisi muutenkin tiivistää. Arviointineuvosto katsoi myös, että esityksessä tulisi kuvata selvemmin täytäntöönpantavan direktiivin tavoitteet ja siitä seuraavat sääntelyvelvoitteet sekä direktiivin linkittyminen muuhun EU-lainsäädäntöön sekä kuvata nykyisiä ja ennakoituja ongelmia kyberturvallisuudessa. Arviointineuvosto katsoi myös, että sääntelyn toimeenpanoon liittyviä riskejä ja epävarmuuksia voisi käsitellä laajemmin vaikutusarviointien yhteydessä. Lisäksi arviointineuvosto katsoi, että julkishallinnolle velvoitteiden noudattamisesta aiheutuvia kustannuksia tulisi arvioida vielä euromääräisesti, jos mahdollista.

Arviointineuvosto piti myönteisenä, että esityksestä käy hyvin ilmi sen kansallinen liikkumavara ja sen käyttöä koskevat ehdotukset. Arviointineuvosto piti myönteisenä, että valmistelua on tehty poikkihallinnollisesti työryhmätyönä ja siinä on hankittu tietoa sidosryhmien näkemyksistä ja vaikutuksista muun muassa teettämällä erillinen selvitys sekä haastattelemalla ehdotettavan sääntelyn piiriin tulevia toimijoita. Arviointineuvosto pitää myönteisenä, että esitysluonnoksen vaikutusarviointien tekemisessä on hyödynnetty sääntelytaakkalaskuria ja laskelmia on havainnollistettu taulukon avulla.

Arviointineuvoston lausunnon johdosta esitykseen on lisätty suuntaa-antava arvio sääntelyn piiriin tulevien toimijoiden kokonaismäärästä sekä arvio siitä osuudesta toimijoita, joka tulisi sääntelyn piiriin uusina. Lisäksi esitykseen on lisätty suuntaa-antava arvio keskeisten toimijoiden kokonaismäärästä. Esitykseen on täydennetty myös arviota riskienhallintavelvoitteesta aiheutuviin kustannuksiin suhteessa yritysten liikevaihtoon tai IT-kustannuksiin. Näihin arvioihin liittyy jaksossa 4 kuvattuja merkittäviä epävarmuustekijöitä, sillä yritys- ja toimintakohtaiset erot tekevät soveltamisalan laajuus huomioiden yleistettävien arvioiden esittämisen erittäin haastavaksi. Riskienhallinnasta aiheutuva kustannus on lähtökohtaisesti suhteessa toiminnan laatuun ja laajuuteen, mutta on keskeisessä yhteydessä yrityskohtaisiin yksittäisiin ratkaisuihin ja toiminnan luonteeseen. Soveltamisalaan kuuluvien toimijoiden ja keskeisten toimijoiden määrän osalta on lain voimaantulon jälkeen mahdollista muodostaa täsmällinen tieto sääntelyn alaan toimijoiden valvoville viranomaisille tekemien ilmoituksien perusteella.

Esitystä on pyritty selkeyttämään lisäämällä vaikutusarviointeihin yhteenveto yritysvaikutuksista ja yhteenveto velvoitteiden soveltamisalasta. Vaikutuksia yrityksille aiheuttavat kyberturvallisuuslaissa säädetty riskienhallintavelvoite, merkittävien poikkeamien raportointia koskeva velvoite ja toimijaluetteloon ilmoittautuminen. Arvioitaessa

kyberturvallisuuden riskienhallintavelvoitteesta eri kokoisille yrityksille aiheutuvia kustannuksia on otettava huomioon, että yrityskohtaiset erot IT-kustannuksien ja kyberturvallisuuden riskienhallintaan liittyvien kustannuksien osalta ovat erittäin merkittäviä, kuten edellä kuvataan. Lisäksi esitykseen on lisätty taulukko keskeisen toimijan kriteereistä sekä taulukko sääntelyn eroista keskeisen ja muun kuin keskeisen toimijan välillä. Esitykseen on lisätty tiivis arvio sääntelyn toimeenpanoon liittyvistä riskeistä.

Jatkovalmistelun ja NIS2-direktiivin täytäntöönpanon aikataulun johdosta ja esityksen laajuus huomioiden sääntelyn tiivistämiselle, täydentämiselle tai jäsentelylle enemmälti arviointineuvoston esittämällä tavalla ei ole ollut mahdollisuutta. Vaikutustenarviointia on täydennetty ja täsmennetty arviointineuvoston esittämien keskeisimpien puutteiden ja kehityskohtien osalta.

7 Säännöskohtaiset perustelut

7.1 Kyberturvallisuuslaki

1 §. *Soveltamisala*. Laissa säädettäisiin kyberturvallisuutta koskevien riskien hallinnasta ja poikkeamista raportoimisesta. Velvoitteista säädettäisiin NIS 2 -direktiivin edellyttämällä tavalla sen soveltamisalaan kuuluville toimijoille. Lain soveltamisalaan kuuluvat toimijat määriteltäisiin 3 §:ssä. Laissa säädettäisiin myös velvoitteiden noudattamisen valvonnasta sekä NIS 2 –direktiivin täytäntöönpanon edellyttämistä viranomaistehtävistä ja -yhteistyöstä.

Pykälän *2 momentissa* olisi informatiivinen viittaussäännös siitä, että 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).

Pykälän *3 momentissa* olisi informatiivinen viittaussäännös tiedonhallintalakiin, jolla pantaisiin täytäntöön NIS2 –direktiivi sen liitteen I kohdassa 10 tarkoitetulla julkishallinnon toimialalla.

Tiedonhallintalaissa säädettäisiin NIS 2 –direktiivin edellyttämistä velvoitteista direktiivin liitteen I kohdassa 10 tarkoitetuille julkishallinnon toimijoille. Toiminta julkishallinnon toimialalla ei kuuluisi kyberturvallisuuslain liitteisiin I tai II ja julkishallinnon toimialan toimijat eivät siten kuuluisi kyberturvallisuuslaissa säädettävien velvoitteiden alaan.

Tiedonhallintalain soveltamisalaan kuuluva viranomainen voisi kuitenkin kuulua myös kyberturvallisuuslain soveltamisalaan, mikäli se harjoittaisi toimintaa NIS 2 –direktiivin ja kyberturvallisuuslain liitteessä tarkoitetulla toimialalla. Julkishallinnon organisaatio tulisi myös kyberturvallisuuslain soveltamisalaan, mikäli se harjoittaisi lain liitteessä I tai II tarkoitettua toimintaa tai olisi niissä tarkoitettua toimijatyyppiä ja siten täyttäisi 3 §:ssä tarkoitetun toimijan määritelmän (esimerkiksi hyvinvointialue terveyspalvelun tuottajana). Viranomainen tai osa sen toiminnasta (esimerkiksi osa kunnan toiminnasta) voisi kuulua myös ainoastaan kyberturvallisuuslain soveltamisalaan, jos viranomaiseen (esimerkiksi kunnallinen viranomainen) ei tiedonhallintalain 3 §:n 3 momentin perusteella sovellettaisi tiedonhallintalain 4 a luvun julkishallinnon toimialan NIS 2 -säännöksiä.

Mikäli julkishallinnon organisaatio kuuluisi samanaikaisesti sekä tiedonhallintalain että kyberturvallisuuslain soveltamisalaan, tulisi sen noudattaa sekä tiedonhallintalain 4 a lukua että kyberturvallisuuslaissa toimijalle asetettavia velvoitteita, jotka ovat keskeiseltä osin vastaavia. Kyberturvallisuuslaissa tarkoitettua hallinnollista seuraamusmaksua ei voitaisi määrätä lain 35

§:ssä tarkoitetulle julkishallinnon organisaatiolle, vaikka se kuuluisi muutoin lain soveltamisalaan.

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

Pykälän *1 kohdassa* säädettäisiin aluetunnusrekisterin ylläpitäjän määritelmästä. Aluetunnusrekisterin ylläpitäjän määritelmä vastaisi NIS2-direktiivin 6 artiklan 21 kohdan määritelmää aluetunnusrekisteristä. Aluetunnusrekisterin ylläpitäjällä tarkoitettaisiin siten tahoa, jolle on myönnetty oikeus hallinnoida tiettyä aluetunnusta ja joka kyseistä aluetunnusta hallinnoidessaan vastaa 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. Aluetunnusrekisterin ylläpitäjä olisi esimerkiksi sähköisen viestinnän palveluista annetun lain 21 luvussa tarkoitettua verkkotunnusrekisteriä hallinnoiva viranomainen.

Pykälän *2 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 laitteiden 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 ja datakeskuspalvelun määritelmää ei tulisi käyttää toimijan omistamista ja omiin sisäisiin käyttötarkoituksiinsa operoimista datakeskuksista.

Pykälän *3 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 *4 kohdassa* säädettäisiin haavoittuvuuden määritelmästä. Haavoittuvuudella tarkoitettaisiin tuotteen tai palvelun heikkoutta, alttiutta tai vikaa, joka voi aiheuttaa kyberuhkan tai poikkeaman. Haavoittuvuuden määritelmä vastaisi sisällöllisesti NIS2-direktiivin 6 artiklan 15 kohtaa, jonka nojalla haavoittuvuudella tarkoitetaan 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 *5 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 *6 kohdassa* säädettäisiin hyväksytyn luottamuspalvelun tarjoajan määritelmästä. Hyväksytyllä luottamuspalvelun tarjoajalla tarkoitettaisiin eIDAS-asetuksen 3 artiklan 20 kohdassa tarkoitettua 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 *7 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 *8 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 siten tilannetta, tapahtumaa tai toimintaa, joka toteutuessaan voisi vahingoittaa tai häiritä viestintäverkkoja tai tietojärjestelmiä, tällaisten järjestelmien käyttäjiä ja muita henkilöitä tai muulla tavoin vaikuttaa näihin haitallisesti. Kyberuhka voisi aiheutua esimerkiksi haavoittuvuudesta tai tietojärjestelmän tai viestintäverkon puutteellisesta suojauksesta. Kyberuhkan olemassaoloon riittäisi uhka, eli määritelmä ei edellyttäisi tilanteen, tapahtuman tai toiminnan toteutumista.

Pykälän *9 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 *10 kohdassa* säädettäisiin pilvipalvelun määritelmästä NIS2-direktiivin 6 artiklan 30 kohtaa ja johdanto-osan perustelukappaletta 33 ja 34 vastaavasti. Pilvipalvelulla tarkoitettaisiin digitaalista palvelua, joka tarjoaa laajaan etäkäyttöön skaalattavan ja joustavan joukon jaettavissa olevia ja tarveperusteisesti ohjattavia tietoteknisiä resursseja, myös sijainniltaan hajautettuja resursseja.

Pilvipalvelun määritelmää tarkennetaan NIS2-direktiivin johdanto-osan perustelukappaleessa 33 ja 34. 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 johdanto-osan perustelukappaletta 33 vastaavasti samaa kuin standardissa ISO/IEC 17788:2014 määritellyillä palvelu- ja toimintamalleilla. Standardi on korvattu standardeilla ISO/IEC 22123-1:2023 ja 22123-2:2023.

Pykälän *11 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 *12 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 *13 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 *14 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 *15 kohdassa* säädettäisiin NIS2-direktiivin 6 artiklan 40 kohtaa vastaavasti tietoturvapalveluntarjoajan määritelmästä. Tietoturvapalveluntarjoajalla tarkoitettaisiin 5 kohdassa tarkoitettua hallintapalvelun tarjoajaa, joka toimii kyberturvallisuusriskien hallitsemiseksi tai antaa tukea sitä varten toteuttamalla kyberturvallisuusriskien hallintatoimia tai antamalla muuten tukea sitä varten.

Pykälän *16 kohdassa* säädettäisiin TVT-palvelun määritelmästä. TVT-palvelun määritelmä vastaa sisällöllisesti kyberturvallisuusasetuksen (EU) 2019/881 2 artiklan 13 kohdassa tarkoitettua 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 *17 kohdassa* säädettäisiin TVT-tuotteen määritelmästä. TVT-tuotteen määritelmä vastaisi sisällöllisesti kyberturvallisuusasetuksen (EU) 2019/881 2 artiklan 12 kohdassa tarkoitettua tieto- ja viestintätekniikan tuotetta. TVT-tuotteella tarkoitettaisiin mitä tahansa viestintäverkkojen ja tietojärjestelmien elementtiä ja elementtien ryhmää.

Pykälän *18 kohdassa* säädettäisiin valvovan viranomaisen määritelmästä. Valvovalla viranomaisella tarkoitettaisiin 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 *19 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 *20 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 *21 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 *22 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 teledirektiiviin sekä NIS2-direktiivin verkko- ja tietojärjestelmän määritelmän tulkintaan.

Pykälän *23 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 *24 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 *25 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 toimijan määritelmästä eli siitä, mitkä tahot olisivat lain soveltamisalaan kuuluvia toimijoita. Pykälän *1 momentissa* säädettäisiin toimijan yleisestä määritelmästä, joka olisi kaksiosainen liittyen toimijan toiminnan laatuun tai tyyppiin ja toimijan kokoon. Pykälän *2 ja 3 momentissa* säädettäisiin erikoistapauksista, joissa toimija kuuluisi lain soveltamisalaan sen koosta riippumatta. Eräiden toimijoiden osalta rajauksista lain soveltamisalaan säädettäisiin jäljempänä 4 §:ssä. Kansainvälisten toimijoiden osalta lainkäyttövallasta ja alueellisuudesta säädettäisiin 6 §:ssä.

Lain soveltamisalan ja toimijan määritelmän 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, pois lukien julkishallinnon

sektori, jonka osalta NIS2-direktiivin mukaisten velvoitteiden täytäntöönpanosta säädettäisiin julkisen hallinnon tiedonhallinnasta annetussa laissa.

Ehdotetussa *1 momentissa* säädettäisiin toimijan yleismääritelmästä. Toimijalla tarkoitettaisiin oikeushenkilöä tai luonnollista henkilöä, joka harjoittaa lain liitteissä I ja II tarkoitettua toimintaa tai on niissä tarkoitettua toimijatyyppiä. Lisäksi edellytyksenä on, että toimija täyttää tai ylittää komission suosituksen 2003/361/EY liitteessä olevan 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset ja tarjoaa palvelujaan tai harjoittaa toimintaansa unionissa. Suosituksen liitteessä olevan 3 artiklan 4 kohtaa ei sovelleta toimijan määrittelyssä 5 momentin nojalla.

Toimijan määritelmän kannalta ei olisi merkitystä toimijan oikeudellisella muodolla, vaan ainoastaan sillä, että toimija harjoittaa pykälässä tarkoitettua toimintaa tai on siinä tarkoitettua toimijatyyppiä sekä täyttää 1 momentissa säädetyn kokoedellytyksen tai sitä koskee 2 tai 3 momentissa säädetty poikkeus soveltamisesta toimijan koosta riippumatta. Lisäksi edellytyksenä on, että toimija tarjoaa palvelua tai harjoittaa toimintaansa Euroopan unionissa.

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.

Komission suosituksen mukaisen keskisuuren yrityksen kynnyksen voisi ylittää tai täyttää joko julkinen tai yksityinen organisaatio, joka täyttää tai ylittää komission suosituksen 2003/361/EY liitteessä olevan 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset. Kynnys määräytyisi muutoin 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.

Keskisuurta yritystä koskevien edellytysten täyttymisessä olisi otettava huomioon toimijan koko toiminta. Mikäli toimija toimii usealla eri toimialalla ja vain osa sen toiminnasta on liitteessä I tai II tarkoitettua toimintaa, kokorajoitusta arvioitaessa olisi otettava huomioon toimijan toiminta kokonaisuudessaan, eli kokorajoituksen ylittymistä koskevaa arviota ei olisi rajoitettava vain liitteessä I tai II tarkoitetun toiminnan laajuuteen. Näin ollen liikevaihtoa, tasetta ja henkilöstömäärää arvioidaan koko toimijan osalta, mikä kattaisi myös muun kuin liitteessä I tai II tarkoitetun toiminnan laajuuden. Arviointi tehdään toimijakohtaisesti. Poikkeuksena tästä olisi kuitenkin myöhemmin 4 §:ssä säädetty rajoitus silloin, jos liitteessä I tai II tarkoitettua toimintaa harjoittaa kunta.

Toimijan määritelmää olisi tulkittava oikeussubjektikohtaisesti. Oikeushenkilön kohdalla kriteerien täyttymistä olisi tarkasteltava sen toimintaa kokonaisuutena arvioiden. Oikeushenkilö täyttäisi pykälässä tarkoitetun toimijan määritelmän, vaikka vain osa sen harjoittamasta toiminnasta olisi liitteessä I tai II tarkoitettua tai osa siitä olisi liitteessä I tai II tarkoitettua

toimijatyyppiä, jos oikeushenkilön toiminnassa täyttyisi tai ylittyisi 1 momentissa tarkoitettu kokokriteeri tai sitä koskisi 2 tai 3 momentissa säädetty poikkeus, jonka nojalla oikeushenkilö kuuluisi soveltamisalaan sen koosta riippumatta. Kriteerien täyttymistä tulisi kuitenkin tarkastella oikeushenkilökohtaisesti. Selvyyden vuoksi todetaan, että tämän johdosta esimerkiksi konsernirakenteessa, kun emo- ja tytäryhtiö ovat erillisiä oikeushenkilöitä, ovat ne myös erillisiä toimijoita. Näin ollen tässä tilanteessa tytäryhtiön kuuluminen soveltamisalaan ei tarkoittaisi automaattisesti myös emoyhtiön kuulumista soveltamisalaan, jos emoyhtiö ei itsenäisesti täyttäisi 1–3 momentin nojalla toimijan määritelmää.

Konsernirakenteeseen kuuluvien yhtiöiden osalta olisi sovellettaessa kiinnitettävä erityistä huomioita komission suosituksen mukaisen keskisuuren yrityksen edellytysten täyttymiseen tai ylittymiseen yhtiöiden välisten sidosten johdosta. Komission suosituksen liitteen 6 artiklassa säädetään yrityksen tietojen määräytymisestä silloin, kun yrityksellä on omistusyhteys- tai sidosyrityksiä. Komission suosituksen liitteen 3 artiklassa säädetään omistusyhteyksistä ja muista sidoksista yritysten välillä, jotka vaikuttavat keskisuuren toimijan kynnyksen ylittymisessä huomioon otettaviin tietoihin. Poikkeuksena tästä olisivat kuitenkin myöhemmin lain 4 §:ssä säädetyt rajoitukset lain soveltamisalaan. Konsernirakenteeseen kuuluvat soveltamisalaan kuuluvat yhtiöt voisivat tehdä yhteistyötä muiden samaan konserniin kuuluvien yhtiöiden kanssa riskienhallinta- ja raportointivelvoitteiden toteuttamisessa. Jos konsernirakenteessa tai muussa yhtiöiden keskinäisiä omistuksia koskevassa järjestelyssä osa yhtiöistä kuuluisi soveltamisalaan ja osa ei, olisi niiden otettava huomioon esimerkiksi riippuvuus toisten yhtiöiden tarjoamista palveluista osana 2 luvussa säädettyjen riskienhallinta- ja raportointivelvoitteiden noudattamista.

Selvyyden vuoksi todetaan, että silloin kun lain liitteessä I tai II tarkoitettua toimintaa harjoittaa oikeushenkilö, kattaisi tässä laissa tarkoitettu toimijan määritelmä silloin kyseisen oikeushenkilön kokonaisuutena. Edellä todetulla tavalla toimijan määritelmää olisi tulkittava oikeussubjektikohtaisesti. Lain ja siinä säädettyjen velvoitteiden soveltaminen ei siten olisi tarkoitus rajoittua ainoastaan liitteissä tarkoitettua toimintaa harjoittavaan yksikköön tai toimintoon oikeushenkilössä, vaan velvoitteet koskisivat kyseistä oikeushenkilöä sellaisenaan, eli toimijaa kokonaisuutena. Esimerkiksi oikeushenkilö joka toimii usealla toimialalla, joista vain osa on mainittu lain liitteissä, kuuluisi siten sääntelyn piiriin myös sellaisten toimintojen osalta, joita ei ole mainittu lain liitteissä. Poikkeuksena tästä olisi kuitenkin myöhemmin 4 §:ssä säädetyt rajoitukset lain soveltamisalaan.

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 liikenteen palveluista annetussa laissa tarkoitetut tieliikenteen ohjaus- ja hallintapalvelun tarjoajat 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 omistaman, hallinnoiman ja operoiman maassa sijaitsevan infrastruktuurin ylläpitäjät, lukuun ottamatta yleisten sähköisten viestintäverkkojen tarjoajia. Määritelmän on katsottu sisältävän maa-asemalain (96/2023) 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, aluetunnusrekisterin ylläpitäjät, pilvipalvelun tarjoajat, datakeskuspalvelun tarjoajat, sisällönjakeluverkon tarjoajat, luottamuspalvelun tarjoajat, yleisten sähköisten viestintäverkkojen tarjoajat sekä yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat. Toimijatyypit määriteltäisiin tarkemmin 2 §:ssä. 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 §:ssä. 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 sosiaali- ja terveydenhuollon valvonnasta annetussa laissa

(741/2023) tarkoitetut palveluntuottajat, jotka tuottavat terveyspalvelua. Lisäksi soveltamisalaan kuuluisivat, EU:n vertailulaboratoriot, lääkkeiden tutkimusta ja kehitystä harjoittavat toimijat, lääkeaineiden ja lääkkeiden valmistusta harjoittavat toimijat sekä eräiden lääkinnällisten laitteiden valmistajat. Lisäksi soveltamisalaan kuuluisivat veripalvelulain mukaiset veripalvelulaitokset, apteekit sekä potilaiden oikeuksien soveltamisesta rajat ylittävässä terveydenhuollossa annetun EU-direktiivin (2011/24/EU) mukaiset lääkkeitä ja lääkinnällisiä laitteita toimittavat ja tarjoavat toimijat. Apteekilla tarkoitettaisiin myös avohuollon apteekkeja sekä sairaala-apteekkeja ja lääkekeskuksia. 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. Postipalvelujen tarjoajilla tarkoitettaisiin postidirektiivin 2 artiklan 1 a alakohdassa tarkoitettuja postipalvelujen tarjoajia. Postidirektiivissä postipalveluilla tarkoitetaan palveluja, joihin kuuluu postilähetysten keräily, lajittelu, kuljetus ja jakelu. Kuljetuspalvelut, jotka eivät koske jotain mainituista vaiheista, jäisivät postipalvelujen määritelmän ulkopuolelle. Postidirektiivissä postilähetyksellä tarkoitetaan postipalvelun tarjoajan kuljetettavaa valmista lähetystä, joka on osoitettu jollekin vastaanottajalle. Tällaiset lähetykset voivat kirjelähetysten lisäksi olla esimerkiksi kirjoja, luetteloita, sanomalehtiä ja aikakausjulkaisuja sekä postipaketteja, jotka sisältävät joko kaupallista arvoa omaavaa tai sitä vailla olevaa tavaraa. Kuriiripalvelujen tarjoajia olisivat esimerkiksi sellaiset palveluntarjoajat, jotka tarjoavat vähintään yhden postiketjun vaiheista, erityisesti postilähetysten keräilyn, lajittelun, kuljetuksen tai jakelun, mukaan lukien noutopalvelut. 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 §:ssä. 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.

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

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.

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

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. Yliopistoa tai muuta korkeakoulua taikka opetus- ja koulutusalan laitosta ei olisi pidettävä kohdan tarkoittamana tutkimusorganisaationa, ellei sen toiminnan ensisijaisena tavoitteena olisi harjoittaa soveltavaa tutkimusta tai kokeellista kehitystyötä tutkimuksen tulosten hyödyntämiseksi kaupallisiin tarkoituksiin.

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 johdanto-osan perustelukappaletta

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.

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
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

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.

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

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.

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

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

Pykälän *2 momentissa* säädettäisiin eräiden toimijoiden kuulumisesta laissa tarkoitetun toimijan määritelmään niiden koosta riippumatta, eli myös silloin, kun toimija ei täytä 1 momentin b kohdassa tarkoitettua kokoedellytystä. Näitä toimijoita olisivat yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat, luottamuspalvelun tarjoajat, aluetunnusrekisterin ylläpitäjät ja DNS-palveluntarjoajat.

Momentilla pantaisiin täytäntöön NIS2-direktiivin NIS2-direktiivin 2 artiklan 2 kohdan a alakohta.

Pykälän *3 momentissa* säädettäisiin eräiden toimijoiden kuulumisesta laissa tarkoitetun toimijan määritelmän alaan niiden koosta riippumatta, eli myös silloin, kun toimija ei täytä 1 momentin b kohdassa tarkoitettua kokoedellytystä. Näitä toimijoita olisivat lain liitteessä I tai II tarkoitettua toimintaa harjoittavat tai toimijatyyppiä olevat toimijat, jotka täyttävät yhden tai useamman momentin 1–4 alakohdan kriteereistä.

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. Ehdotetut 1–4 kohdat vastaisivat NIS2-direktiivin 2 artiklan 2 kohdan b–e alakohtia ja luettelo olisi tyhjentävä. Luetteloa olisi tulkittava suppeasti.

Pykälän *4 momentin* nojalla valtioneuvoston asetuksella voitaisiin antaa tarkempia säännöksiä 3 momentin 1–4 alakohdissa tarkoitetuista kriteereistä. . Kriteerien täsmentäminen voisi olla lain soveltamisen kannalta lakiteknisesti tarpeellista. Toimijoissa, joita kriteerit koskevat on kyse erityislaatuista toimintaa harjoittavista toimijoista, jotka kuuluisivat toiminnan erityisen laadun vuoksi poikkeuksellisesti lain velvoitteiden soveltamisalaan niiden koosta riippumatta. Ottaen huomioon 3 momentin 1–4 kohdassa tarkoitettujen kriteerien ja NIS2-direktiivin 2 artiklan 2 kohdan b-e alakohtien laatu, yksittäisen yrityksen käytettävissä olevien tietojen perusteella voi osoittautua epävarmaksi, täyttääkö yritys 1–4 kohdassa tarkoitettuja kriteereitä. Näin ollen kriteerien täsmentäminen valtioneuvoston asetuksella olisi tarpeen oikeustilan

tarkentamiseksi siitä, milloin yksittäinen toimija täyttää 3 momentin 1–4 kohdassa tarkoitetun kriteerin EU-säädöksen velvoittavan soveltamisalan täsmentämiseksi.

Valtioneuvoston asetuksella 3 momentissa tarkoitettujen kriteerien täsmentäminen myös selkeyttäisi oikeustilaa niille yrityksille, jotka harjoittavat liitteessä I tai II tarkoitettua toimintaa tai ovat niissä tarkoitettua toimijatyyppiä, mutta alittavat keskisuuren yrityksen määritelmän. Tällaisten yritysten osalta voisi olla oikeudellisesti haastavaa arvioida yrityksen näkökulmasta sitä, onko toiminnassa kyse 3 momentin 1-4 kohdissa tarkoitetusta tilanteesta, niillä tiedoilla, joita yrityksellä on käytettävissään, kriteerien laatu huomioon ottaen. Lisäksi tulkinnallisuus koskisi hyvin laajaa joukkoa suomalaisia pien- ja mikroyrityksiä. Tulkinnallisuus aiheuttaisi tarpeetonta hallinnollista taakkaa pien- ja mikroyrityksille, mikäli 3 momentissa tarkoitettuja kriteerejä ei täsmennettäisi valtioneuvoston asetuksella.

Valtioneuvoston asetuksella voitaisiin säätää vain täsmennyksestä 3 momentissa tarkoitettuihin kriteereihin. Valtioneuvoston asetuksella ei siten voitaisi laajentaa kriteereitä. Ehdotetussa 3 momentissa olisi lain tasolla perussäännökset sille, milloin toimija, jota kriteerit koskevat, kuuluisi lain soveltamisalaan. Jotta kriteerit täyttävä toimija kuuluisi lain soveltamisalaan, tulisi sen harjoittaa myös lain liitteessä I tai II tarkoitettua toimintaa tai olla liitteessä I tai II tarkoitettua toimijatyyppiä 3 momentin edellyttämällä tavalla. Asetuksenantovaltuuden perusteesta säädettäisiin laissa ja valtuutus olisi selkeä sekä täsmällisyyden ja tarkkarajaisuuden vaatimukset täyttävä.

NIS2 –direktiivin johdanto-osan perustelukappaleen 20 nojalla komission olisi annettava ohjeita mikroyrityksiin ja pieniin yrityksiin sovellettavien kriteerien käytöstä sen arvioimisessa, kuuluvatko ne NIS2-direktiivin soveltamisalaan. Milloin mainittua ohjeistusta olisi annettu, olisi se huomioitava sovellettaessa 4 momenttia.

Ehdotetulla 3 ja 4 momentilla pantaisiin täytäntöön NIS2-direktiivin 2 artiklan 2 kohdan b–e alakohdat soveltamisalasta.

Pykälän *5* momentin nojalla toimijaan ei sovelleta komission suosituksen liitteessä olevan 3 artiklan 4 kohtaa. Rajaus vastaisi NIS2-direktiivin 2 artiklan 1 kohtaa. Koska mainittua kohtaa ei sovellettaisi, myös julkisomisteista yritystä voitaisiin pitää yrityksenä, joka ei täytä tai ylitä 1 momentin 2 kohdassa tarkoitettua kynnystä. Momentin nojalla toimijaan ei sovellettaisi komission suosituksen liitteessä olevan 3 artiklan 4 kohtaa myöskään silloin, kun arvioitaisiin sen 27 §:n 2 momentissa tarkoitettua keskeisyyttä.

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 41 §: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 poikkeus lain soveltamisesta silloin, kun liitteessä I tai II tarkoitettu toiminta on satunnaista ja vähäistä. Toiminnan satunnaisuutta ja vähäisyyttä tulisi arvioida suhteessa toiminnan ajalliseen kestoon, toiminnan pääasialliseen tarkoitukseen, toiminnan laajuuteen ja toiminnasta riippuvien henkilöiden tai asiakkaiden määrään. Satunnaisena ja vähäisenä toimintana olisi pidettävä esimerkiksi pääasiassa omaa käyttöä varten tapahtuvaa sähkön tuottamista aurinkopaneelin tai tuuligeneraattorin avulla, jossa sähköverkkoon syötetään ajoittain sähkön ylituotantoa, joka on määrällisesti vähäistä. Poikkeus olisi tarpeen, jotta lain soveltamisala ei laajenisi sen tarkoituksen vastaisesti kattamaan vähäisen tai satunnaisen liitteessä I tai II tarkoitetun toiminnan johdosta kokonaisuudessaan sellaista oikeushenkilöä tai luonnollista henkilöä, jonka harjoittama toiminta muutoin täyttäisi tai ylittäisi keskisuuren toimijan määritelmän mutta ei muutoin kuuluisi lain soveltamisalaan.

Pykälän *6 momentissa* säädettäisiin poikkeus lain soveltamisesta kuntalaissa tarkoitettuun kuntaan. Momentin nojalla, jos lain liitteessä I tai II tarkoitettua toimintaa harjoittaa kunta, olisi kunnan osalta lakia sovellettava vain lain liitteessä I tai II tarkoitettuun toimintaan. Kun arvioidaan kunnan harjoittaman toiminnan kuulumista soveltamisalaan, tulisi kokokriteerin määrittämisessä ottaa huomioon vain liitteessä I tai II tarkoitettu toiminta, mutta ei kunnan henkilöstöä, tasetta tai liikevaihtoa muilta osin. Vastaavasti toimijaa koskevia riskienhallinta-, raportointi- ja ilmoittautumisvelvoitetta ei tulisi tulkita kuntaa velvoittavaksi muun kuin liitteessä I tai II tarkoitetun toiminnan osalta.

NIS2-direktiivin 2 artiklan 5 kohdan a-alakohdan nojalla ja jaksossa 2.10 kuvatulla tavalla julkishallinnon osalta paikallistason julkishallinnon toimijat, eli Suomessa kunnat, kuuluvat jäsenvaltion kansallisen liikkumavaran alaan. Kansallisen liikkumavaran nojalla kuntia ei ole tarkoitus saattaa esityksellä NIS2-direktiivin velvoitteiden soveltamisalaan kokonaisuutena. Kunnat voivat kuitenkin nykyisellään huolehtia joistakin tehtävistä, joita lain liitteessä I tai II tarkoitetaan. Näitä tehtäviä voivat olla esimerkiksi jätehuoltoon tai vesihuoltoon liittyvät tehtävät siten kuin jätelaissa (646/2011) ja vesihuoltolaissa (119/2001) säädetään. Pykälän 6 momentin tarkoituksena olisi rajata lain soveltamisalaa siten, että kunnan harjoittama pienimuotoinen liitteessä I tai II tarkoitettu toiminta ei johtaisi siihen, että lain velvoitteita sovellettaisiin kuntaan kokonaisuutena. Jos kunta harjoittaisi liitteessä I tai II tarkoitettua toimintaa siinä laajuudessa, joka täyttää tai ylittää keskisuuren toimijan määritelmän, olisi lakia sovellettava tähän toimintaan 5 momentin mukaisesti.

Pykälän *7 momentissa* säädettäisiin lain soveltamisen rajaamisesta tiedon luovuttamiseen silloin, jos tiedon luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin siihen liittyvää tärkeää etua. Lakia ei olisi tulkittava siten, että se velvoittaisi luovuttamaan tietoa, jos tiedon antamisessa olisi kyse 7 momentissa tarkoitetusta tilanteesta. Momentti voisi tulla sovellettavaksi tietojen luovuttamiseen toimijan ja viranomaisen välillä, kansallisten viranomaisten välillä sekä kansallisen viranomaisen Euroopan unionille luovuttamien tietojen osalta. Säännöksellä ei rajattaisi tahoja, joiden välillä tällainen tiedon luovuttaminen voisi tulla kyseeseen, vaan merkityksellistä olisi luovutettavan tiedon laatu ja luovuttamisen aiheuttama vaarantaminen. Säännös vastaisi NIS2-direktiivin 2 artiklan 11 kohdan rajausta tietojen luovuttamisesta.

5 §. *Suhde muuhun lainsäädäntöön*. Pykälässä säädettäisiin lain suhteesta muuhun kyberturvallisuuden riskienhallinta- ja raportointivelvoitteita koskevaan lainsäädäntöön. Lain soveltamisala olisi laaja, toimialarajat ylittävä ja velvoitteita sovellettaisiin horisontaalisesti. Tämän johdosta olisi tarpeen selkeyttää lain suhdetta muuhun kyberturvallisuuden riskienhallinta- ja raportointivelvoitteita koskevaan sääntelyyn. Pykälän tarkoituksena olisi selventää lain merkitys yleislakina suhteessa toimialakohtaisiin erityissäännöksiin, joilla varmistetaan korkeampi kyberturvallisuuden taso. Jos toimialakohtaisia erityissäännöksiä olisi muussa laissa, niitä olisi sovellettava tämän lain vastaavien säännösten sijasta.

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, täsmentää tai tarkentaa toimialakohtaisesti kynnystä poikkeamalle, josta viranomaiselle on raportoitava taikka edellyttää tiiviimpää tai nopeampaa raportointia valvovalle viranomaiselle. Sektorikohtaista sääntelyä tulisi soveltaa tämän lain asemasta siltä osin kuin sillä pyrittäisiin kyberturvallisuuden korkeamman tason turvaamiseen.

Lain suhteesta julkisen hallinnon tiedonhallinnasta annettuun lakiin säädettäisiin 1 §:n 3 momentissa.

Pykälän *1 momentissa* säädettäisiin lain suhteesta muussa kansallisessa laissa oleviin säännöksiin, jotka koskevat vaatimuksia kyberturvallisuusriskien hallintatoimenpiteistä tai merkittävistä poikkeamista ilmoittamisesta. Säännös olisi tarpeen lain suhteen selkeyttämiseksi mahdollisiin toimiala- tai toimijakohtaisiin erityissäännöksiin kyberturvallisuuden riskienhallinnasta ja poikkeamien ilmoittamisesta. Säännös ilmentäisi lain suhdetta sekä nykyisiin että tuleviin erityissäännöksiin, ellei laissa toisin säädettäisi. Lain tarkoituksena olisi olla yleislaki suhteessa toimiala- tai toimijakohtaisiin erityissäännöksiin muualla laissa. 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. Toimialakohtaista erityissääntelyä on esimerkiksi sähköisen viestinnän palveluista annetussa laissa.

Jos kansallisessa laissa tai sen nojalla annetuissa säännöksissä tai määräyksissä olisi toimialakohtaisia vaatimuksia, ja vaatimukset ovat vaikutuksiltaan vähintään tässä laissa säädettyjä velvoitteita vastaavia, niitä sovelletaan tämän lain vastaavien säännösten asemasta. Siltä osin kuin toimialakohtaisesti ei olisi säädetty muusta, toimijaan sovellettaisiin edelleen, mitä tässä laissa säädetään.

Pykälän *2 momentissa* säädettäisiin lain suhteesta toimialakohtaisissa unionin säädöksissä asetettaviin edellytyksiin toimijalle. Euroopan unionin asetuksia ovat esimerkiksi Euroopan parlamentin ja neuvoston asetukset sekä Euroopan komission täytäntöönpano- ja delegoidut asetukset. Ehdotuksella pantaisiin täytäntöön NIS2-direktiivin 4 artikla.

Jos Euroopan unionin asetuksessa tai NIS2-direktiivin nojalla säädetyssä komission asetuksessa edellytetään, että toimija ottaa käyttöön kyberturvallisuusriskien hallintatoimenpiteitä tai ilmoittaa merkittävistä poikkeamista, ja vaatimukset ovat vaikutuksiltaan vähintään tässä laissa säädettyjä vastaavia velvoitteita vastaavia, säännöksiä sovellettaisiin tämän lain 2, 4 ja 5 luvun

sekä 41 §:n asemasta. Siltä osin, kun toimialakohtaisesti ei olisi säädetty muusta, toimijaan sovellettaisiin edelleen, mitä tässä laissa säädetään.

Säännös tulisi sovellettavaksi NIS2-direktiivin 4 artiklan mukaisissa tilanteissa sekä silloin, kun NIS2-direktiivin nojalla säädetyssä komission täytäntöönpanoasetuksessa edellytettäisiin tätä lakia korkeampaa tasoa riskienhallinta- tai raportointivelvoitteilta.

Sektorikohtaisia vaatimuksia kyberturvallisuudesta on unionin alakohtaisissa säädöksissä ainakin finanssimarkkinoihin ja ilmaliikenteeseen liittyen. Lisäksi valmisteilla on sektorikohtaisia vaatimuksia energia-alalle. Mikäli EU:n asetuksessa tai suoraan sovellettavassa komission täytäntöönpanoasetuksessa tai delegoidussa asetuksessa taikka NIS2-direktiivin nojalla annetussa suoraan sovellettavassa täytäntöönpanosäädöksessä säädetään sektorikohtaisesta tarkennuksesta NIS2-direktiivin velvoitteiden soveltamiseen, olisi sitä tulkittava yhdenmukaisesti myös tämän lain soveltamisen kannalta.

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, sitä sovellettaisiin toimijaan tämän lain 2 luvun tai 41 §:n velvoitteiden sekä 4 ja 5 luvun säännöksien asemasta.

Sektorikohtaisesta sääntelystä huolimatta kaikki lain liitteissä I ja II tarkoitetut toimialat ja toimijatyypit sekä tiedonhallintalaissa tarkoitettu julkishallinnon toimiala tulisi huomioida kansallisten kyberturvallisuusstrategian ja laajamittaisten kyberturvallisuuspoikkeamien ja –kriisien hallintasuunnitelman valmistelussa ja CSIRT-yksikön toiminnassa.

NIS2-direktiivin 4 artiklan 3 kohdan nojalla komissio antaa ohjeita, joissa selvennetään NIS2-direktiivin 4 artiklan 1 ja 2 kohtien soveltamista. 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. Säännöstä olisi tulkittava yhdenmukaisesti sen ohjeistuksen mukaisesti, jota komissio antaa NIS2-direktiivin 4 artiklan 3 kohdan nojalla.

NIS2-direktiivin johdanto-osan perustelukappaleen 23 mukaan, jos alakohtaisessa unionin säädöksessä on säännöksiä, joissa keskeisiä tai tärkeitä toimijoita vaaditaan ottamaan käyttöön kyberturvallisuusriskien hallintatoimenpiteitä tai ilmoittamaan merkittävistä poikkeamista, ja jos kyseiset vaatimukset ovat vaikutukseltaan vähintään tässä direktiivissä säädettyjä velvoitteita vastaavia, tällaisiin toimijoihin olisi sovellettava kyseisiä säännöksiä, mukaan lukien valvontaa ja täytäntöönpanoa koskevat säännökset. Jos alakohtainen unionin säädös ei kata tämän direktiivin soveltamisalaan kuuluvan tietyn toimialan kaikkia toimijoita, tämän direktiivin asiaankuuluvia säännöksiä olisi edelleen sovellettava niihin toimijoihin, joita mainittu säädös ei kata.

Pykälän *3 momentti* olisi informatiivinen viittaus yleiseen tietosuoja-asetukseen ja tietosuojalakiin, joissa säädetään henkilötietojen käsittelyn tietoturvallisuudesta.

Pykälän *4 momentti* olisi informatiivinen viittaus niihin sektorikohtaisiin lakeihin, joissa säädetään eräiden lupien peruuttamisesta sillä perusteella, että luvanhaltija on rikkonut tämän lain mukaisia velvollisuuksiaan.

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. Suomen lain soveltamisalaan kuuluisi Suomeen sijoittautunut toimija kokonaisuudessaan, eli myös kyseisen toimijan sellaiset toiminnot, jotka sijaitsevat esimerkiksi toisessa jäsenvaltiossa tai kolmansissa maissa. 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. Jos päätoimipaikka sijaitsee Suomessa, toimija kuuluisi tämän lain soveltamisalaan. 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. Pykälän 4 momentin nojalla valvova viranomainen voi kieltäytyä pyynnöstä, jos sillä ei ole lain nojalla toimivaltaa antaa pyydettyä apua, pyydetty apu ei ole oikeassa suhteessa valvontatehtäviin tai pyyntö koskee sellaisia tietoja tai käsittää sellaisia toimintoja, joiden paljastaminen tai toteuttaminen olisi vastoin Suomen maapuolustukseen tai kansalliseen turvallisuuteen liittyviä etuja. Ennen pyynnöstä kieltäytymistä valvovan viranomaisen on kuultava muita asianomaisia toimivaltaisia viranomaisia sekä, jos jokin jäsenvaltio sitä pyytää, Euroopan unionin komissiota ja Euroopan unionin kyberturvallisuusvirastoa.

7 §. *Riskienhallinta*. 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 toimijan olisi tunnistettava, arvioitava ja hallittava riskejä, joita kohdistuu sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Toimijoiden velvollisuutena olisi siten 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. 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. Kyberturvallisuutta koskevien riskien hallinta olisi osa organisaation riskienhallintaa. Riskienhallinnassa lähtökohtana olisi sekä riskien tunnistaminen että tulokset, joilla organisaatio haluaa vähentää riskiä.

NIS2-direktiivin johdanto-osan perustelukappaleen 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 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.

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 tai korkeampia kustannuksia aiheuttavia hallintatoimenpiteitä edellytettäisiin oikeasuhtaiselta riskienhallinnalta.

Riskienhallintavelvoite kohdistuisi toimijan toimintaan, toiminnan jatkuvuuteen ja palveluntarjontaan. Riskienhallintavelvoitetta ei olisi tarkoitettu kohdentumaan toimijan valmistaman tai markkinoille tarjottavan tuotteen ominaisuuksiin.

Riskin määritelmästä säädettäisiin 2 §:n 13 kohdassa.

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

8 §. *Kyberturvallisuutta koskeva riskienhallinnan toimintamalli*. Pykälässä säädettäisiin toimijan velvoitteesta pitää käytössään ajantasainen kyberturvallisuutta koskeva riskienhallinnan toimintamalli säädetyn riskienhallintavelvoitteen toteuttamiseksi. Riskienhallinnan toimintamallissa tulisi tunnistaa toimijan käytössä oleviin tai palveluntarjontaan vaikuttaviin viestintäverkkoihin ja tietojärjestelmiin sekä niiden fyysiseen ympäristöön kohdistuvat riskit sekä tunnistaa ja kuvata riskienhallinnan tavoitteet, menettelyt ja vastuut sekä 9 §:n mukaiset toimenpiteet, joilla viestintäverkkoja ja tietojärjestelmiä sekä niiden fyysistä ympäristöä suojataan kyberuhkien ja poikkeamien toteutumiselta sekä niiden haitallisilta vaikutuksilta. Toimija voisi luoda riskienhallinnan toimintamallin itse tai hankkia sen ulkoistetusti. Kyberturvallisuutta koskeva riskienhallinnan toimintamalli voisi olla myös osa toimijan laajempaa riskienhallintasuunnitelmaa, jossa huomioidaan myös muita toimintaan kohdistuvia riskejä tai osa muuta turvallisuusvarautumista.

Kyberturvallisuutta koskeva 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 tieto- ja kyberturvallisuusriskit 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.

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

9 §. *Toimenpiteet kyberturvallisuutta koskevien riskien hallinnassa*. Pykälän *1 momentin* nojalla lain soveltamisalaan kuuluvat toimijat velvoitettaisiin toteuttamaan riskienhallinnan toimintamallin mukaiset hallintatoimenpiteet 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. Riskienhallinnassa olisi siten otettava huomioon toisaalta riskin toteutumisen todennäköisyys ja riskin toteutumisesta aiheutuvat kustannukset sekä toisaalta käytettävissä olevista riskinhallintatoimenpiteistä aiheutuva kustannus ja vaikuttavuus.

Pykälän *2 momentissa* säädettäisiin NIS2-direktiivin 21 artiklan 2 kohtaa vastaavasti osa-alueista, jotka olisi otettava huomioon kyberturvallisuuden riskienhallinnan toimintamallin luomisessa ja tarpeellisten riskienhallintatoimenpiteiden määrittelyssä. Osa-alueiden listaus olisi vähimmäistason listaus. Toimija voisi toteuttaa myös laaja-alaisempaa riskienhallintaa arvioidessaan sen tarpeelliseksi.

Riskienhallintatoimenpiteiden osalta olisi huomioitava, että ne elävät ajassa, kehittyvät ja ovat myös teknologiasidonnaisia. Lisäksi kyberturvallisuusympäristö muuttuu jatkuvasti sekä teknologioiden että kyberturvallisuuteen liittyvien parhaiden käytäntöjen kehittyessä. Toimijoille olisi jätettävä liikkumavaraa siihen, miten ne huolehtivat riskienhallinnan käytännön toteutuksesta. Riskienhallintatoimenpiteissä tulisi huomioida myös, että menetelmät ja käytetty tekniikka ovat keskenään sidoksissa – esimerkiksi vanhempien verkkoteknologioiden osalta riskienhallintatoimenpiteet eivät teknologisista syistä voi olla yhtä kattavia tai sofistikoituneita verrattuna uudempiin verkkoteknologioihin. Toimijoiden olisi kuitenkin huomioitava riskienhallinnassa ja riskienhallintatoimenpiteissä vähintään pykälän 2 momentissa tarkoitetut osa-alueet sekä kyettävä dokumentoimaan ja osoittamaan, miten riskienhallintaa osa-alueisiin liittyen toteutetaan. Osa-alueiden yksilöinti siten osoittaa toimijoille riskienhallintavaatimuksen edellyttämän vähimmäisalan.

Momentissa käytettävät termit on pyritty sovittamaan yhteen teknisen toimialan terminologian kanssa siten, että toimintaperiaatteilla tarkoitetaan toimijan yleisen tason periaatteita ja päämäärien määrittelyä eli politiikkoja (policy); menettelyillä tarkoitetaan erilaisia prosesseja ja teknisiä menettelytapoja (procedures, processes); ja käytännöillä tarkoitetaan toimintatapoja (practises). Termien merkityssisältö ja suomennokset ovat osin täsmentymättömiä, ja momentin tulkinnassa olisi otettava huomioon, että teknisissä lähteissä kuten standardeissa termejä voidaan käyttää erilaisissa merkityksissä.

Kohdassa 1 tarkoitettaisiin kyberturvallisuutta koskevan 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 tarkoitettaisiin esimerkiksi organisaation ylimmän tason suunnittelua, jonka tarkoituksena olisi tunnistaa, arvioida ja käsitellä järjestelmällisesti organisaatioon tai sen toimintaan kohdistuvia riskejä sekä asettaa tarpeelliset päämäärät ja seurata niiden toteutumista. Toimijalla tulisi olla käytössään kyberturvallisuuden riskienhallinnan toimintamalli, jolla tunnistetaan, analysoidaan, arvioidaan ja käsitellään viestintäverkkoihin ja tietojärjestelmiin sekä niiden fyysiseen ympäristöön kohdistuvia riskejä säännöllisesti. Toimintaperiaatteiden ja toimenpiteiden vaikuttavuuden arvioinnissa tulisi ottaa huomioon riskienhallinnan luonne jatkuvana osana organisaation toimintaa, minkä toteutuminen edellyttäisi 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 tieto- ja kyberturvallisuusriskit. Riskienhallinnan lähtökohtana tulisi olla tunnistaa luottamuksellisuuteen, eheyteen, saatavuuteen ja aitouteen liittyvät tarpeet sekä sen kohteena toimintojen kannalta keskeiset palvelut, järjestelmät, prosessit ja henkilöt. Tunnistaminen liittyy omaisuudenhallintaa koskevaan kohtaan 5. Riskienhallinta edellyttäisi, että tunnistetaan toimijaan kohdistuvat uhat ja arvioidaan näiden todennäköisyydet sekä vaikutukset. Riskienhallinnalla tulisi pyrkiä riskien käsittelyyn niin, että niiden todennäköisyys tai vaikutus olisi minimoitu, poistettu tai ulkoistettu ja riskien käsittelyn lopputuloksena muodostuneet jäännösriskit hyväksyttäisiin 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. Riskienhallinnassa tulisi arvioida riskienhallintatoimenpiteiden vaikuttavuutta suhteessa toimijaan kohdistuviin uhkiin ja niiden ennakoitavissa oleviin vaikutuksiin.

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 laitteen tai järjestelmän 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 esimerkiksi olla kirjalliset viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet ja menettelyt. Mikäli tällaisia on, tulisi niiden olla oikeasuhtaisia toimijan tarpeisiin nähden ja ajantasaisesti ylläpidettyjä. Lisäksi riskienhallinnassa voitaisiin pyrkiä siihen, että toimijan henkilöstön tulisi tuntea käytössä olevat turvallisuusmenettelyt ja sitoutua niiden noudattamiseen. Sopivien menettelyiden valinnassa voitaisiin huomioida esimerkiksi 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 pyrkiä ylläpitämään viestintäverkkojen ja tietojärjestelmien riittävää turvallisuuden tasoa koko niiden elinkaaren ajan. Esimerkiksi hankittavien järjestelmien olisi oltava toiminnan tarpeiden perusteella riittävän turvallisia muun muassa eheyden, saatavuuden ja luottamuksellisuuden suhteen. Järjestelmien hankinnassa voitaisiin kiinnittää huomiota esimerkiksi niiden kykyyn suojautua tavallisimpia hyökkäyksiä vastaan. Järjestelmien turvallinen konfiguraatio eli asetukset voitaisiin määritellä, dokumentoida ja ylläpitää koko elinkaaren ajan, ja erityistä huomiota voitaisiin kiinnittää tähän erityisesti päivitysten aikana. Konfiguraatio- ja ohjelmistopäivitysten osalta voitaisiin esimerkiksi pyrkiä siihen, että ne olisivat dokumentoituja, muutoshallintaprosessien mukaisesti suunniteltuja, kattavia sekä kohteen ominaispiirteiden ja päivitysten kriittisyyden kannalta oikea-aikaisia. Luvattomien tai haitallisten muutosten tekeminen voitaisiin esimerkiksi estää. Turvallisuuden kannalta kriittisimmät kohteet voitaisiin tunnistaa erikseen ja näiden turvallisuudesta voitaisiin huolehtia esimerkiksi tarkastelemalla säännöllisesti prosesseja tai teknisillä testauksilla. Toimijan voisi esimerkiksi varmistaa, että näiden viestintäverkkojen ja tietojärjestelmien turvallinen konfiguraatio ylipäätään on mahdollista ja että niille tuotetaan asianmukaisia turvallisuuspäivityksiä. Toimija voisi esimerkiksi kiinnittää huomiota siihen, että löydettyjä haavoittuvuuksia varten olisi olemassa raportointikanava sekä ennalta määritellyt

menettelytavat ja käytännöt ilmoitusten käsittelyä varten. Viestintäverkkojen osalta olisi huolehdittava verkon turvallisesta rakenteesta. Esimerkiksi toiminnoille kriittiset kohteet tulisi tunnistaa ja tarvittaessa suojata ajantasaisin teknisin keinoin, kuten esimerkiksi vyöhykkeistämällä. Mahdollinen haitallinen tekninen liikenne tulisi kyetä havaitsemaan ja estämään.

Kohdassa 4 tarkoitettaisiin välittömän toimitusketjun, toimittajien tuotteiden ja palveluntarjoajien palvelujen yleisestä laatua ja häiriönsietokykyä, tuotteisiin ja palveluihin sisällytettyjä kyberturvallisuusriskien hallintatoimenpiteitä sekä välittömien 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 esimerkiksi välittömälle toimittajalle ja palveluntarjoajalle ominaiset haavoittuvuudet, toimijan käyttämien tuotteiden ja palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt. Nämä voisivat sisältää esimerkiksi erilaisia turvallisuuteen liittyviä vaatimuksia esimerkiksi saatavuuden, ylläpidettävyyden ja sopimusten osalta. Tässä laissa säädettyjen vaatimusten kannalta toimija vastaisi itse siitä, että se käyttäisi toiminnassaan sellaisia tuotteita ja palveluita, jotka vastaisivat toimijan riskienhallinnan vaatimuksia. Selvyyden vuoksi todetaan, ettei lakiin perustuva riskienhallintavaatimus koskisi alihankkijaa, ellei se itsekin ole toimija, jonka toimintaa sääntely koskee. Toimijat voisivat tarvittaessa pyrkiä hallitsemaan toimitusketjujen kyberturvallisuusriskiä sopimusjärjestelyin, joita ne tekevät välittömien toimittajiensa ja palveluntarjoajiensa kanssa.

NIS2-direktiivin 85 johdanto-osan perustelukappaleen 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, valvova viranomainen voisi määräyksellä edellyttää toimijoiden ottavan huomioon riskiarvion tulokset.

Kohdassa 5 tarkoitettaisiin omaisuudenhallintaa ja sen turvallisuuden kannalta tärkeiden toimintojen tunnistamista. Kohdalla pantaisiin täytäntöön NIS2-direktiivin 21 artiklan 2 kohdan i alakohta osittain. Omaisuudenhallinnalla tarkoitettaisiin niitä menettelyjä ja toimenpiteitä, joilla toimija hallinnoi toiminnan ja kyberturvallisuuden 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 voisivat esimerkiksi sisältää 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 voitaisiin esimerkiksi tunnistaa ja luokitella suojaustarpeiden perusteella. Omaisuudesta voitaisiin esimerkiksi ylläpitää ajantasaista luetteloa. Omaisuudenhallinnan tulisi lähtökohtaisesti 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 esimerkiksi olla henkilöstöön liittyvät menettelytavat, joissa huomioidaan myös ulkoiset toimijat, kuten alihankkijat. Menettelytavoissa voitaisiin esimerkiksi huomioida myös työsuhteen päättymisen ja työtehtävien muutoksien jälkeiset vastuut ja velvollisuudet. Henkilöstöä ja ulkoisia toimijoita voitaisiin tarvittaessa esimerkiksi tiedottaa heidän työtehtäviensä ja tarjoamiensa palveluiden turvallisuuteen liittyvistä vastuista ja velvoitteista, kuten esimerkiksi salassapitoon liittyen. Jos työtehtävien ja vastuiden katsottaisiin vaativan erityistä luotettavuutta, henkilölle voitaisiin mahdollisuuksien mukaan tehdä esimerkiksi tarkoituksenmukainen taustatarkistus.

Toimijan olisi huolehdittava siitä, että henkilöstöllä on kyvykkyys toimia tavalla, joka vastaa kyberturvallisuuden hallintamallia ja hallintatoimenpiteitä. Tämän saavuttamiseksi henkilöstölle voitaisiin esimerkiksi 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 voisi esimerkiksi 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 voisi esimerkiksi olla menettelyt käyttäjätunnusten ja käyttöoikeuksien koko elinkaaren ajalle ja käyttöoikeuksia olisi hallittava niiden mukaisesti. Käyttöoikeuksia ja niiden käyttöä tulisi valvoa. Käyttöoikeuksista ja käyttöoikeusrooleista voitaisiin esimerkiksi pitää ajantasaista kirjaa ja käyttäjille voitaisiin antaa vain ne oikeudet, jotka ovat työtehtävien suorittamisen vuoksi välttämättömiä (vähimpien oikeuksien periaate). Toimijoilla tulisi olla menettelyt vahvojen oikeuksien käyttäjätilien ja pääkäyttäjätilien hallintaan, mitä voitaisiin toteuttaa esimerkiksi siten, että pääkäyttäjäoikeudet pyrittäisiin rajoittamaan mahdollisimman pienelle käyttäjäjoukolle ja tunnuksia olisi suojattava vahvoin menetelmin. Pääkäyttäjäoikeuksien käyttöä tulisi valvoa.

Valittavien todentamiskäytäntöjen ja -tekniikoiden olisi tavoiteltavaa 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 olisi 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 11 kohdan 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. Poikkeaman käsittelyn järjestäminen olisi toimijan itsensä vastuulla. Turvallisuuden palauttamisella tarkoitetaan järjestelmän palauttamista turvalliseen tilaan häiriötilan jälkeen. Toimintavarmuuden ylläpitämisellä tarkoitetaan menettelyjä, joilla parannetaan järjestelmän toimintavarmuutta sekä toimijan kykyä toimia poikkeamissa ja toipua häiriötilanteesta. 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 lähtökohtaisesti olla työkaluja ja prosesseja tapahtumien kirjaamiseen ja havainnointiin.

Havainnointi- ja analysointikyvyn kannalta olisi välttämätöntä, että toimijalla olisi kerättynä ja käytettävissä riittävät lokitiedot esimerkiksi ylläpidosta, muutoksista, käytöstä ja virheistä. Toimijan tulisi esimerkiksi arvioida relevantit 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 pyrkiä arvioimaan poikkeamaan johtaneet syyt ja oppia sen kokemuksista, jotta vastaavan poikkeaman uhkaan voidaan varautua jatkossa paremmin. Merkittäviin poikkeamiin tulisi olla olemassa menettelyt, vastuut ja viestintäkanavat 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 voitaisiin varmistaa 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 tai toimijan tulisi suunnitella muuten myös kriisinhallintamenettelyt vähintään erittäin vakavien poikkeamien varalta. Muun riskienhallinnan mukaisesti suunnitelmia tulisi ylläpitää ja kehittää säännöllisesti sekä niiden mukaista toimintaa harjoitella.

Varmuuskopioinnin osalta toimija voisi esimerkiksi määrittää riskienhallinnan perusteella tarvittavat varmuuskopiot tiedoista, järjestelmistä sekä varajärjestelmistä. Toimijalla tulisi lähtökohtaisesti olla käytännöt esimerkiksi varmuuskopioinnin tiheydestä, varmuuskopioiden säilytysajasta, varmuuskopioiden suojauksesta ja palautuksen testaamisesta tilanteessa, jossa alkuperäinen järjestelmä ei olisi käytettävissä. Varmuuskopioiden säilytysaika olisi arvioitava suhteessa säilytyksen tarkoitukseen ja niitä olisi otettava tarpeeksi usein, jotta toiminnot voidaan palauttaa tarvittavalla nopeudella ja tarpeeseen nähden riittävän tuoreella tiedolla poikkeama- ja kriisitilanteissa. Palautuksen toimivuutta voitaisiin esimerkiksi testata säännöllisesti toimivuuden varmistamiseksi. Varmuuskopioita voitaisiin esimerkiksi suojata siten, että niitä eivät koske samat uhkat kuin varmistettavaa järjestelmää.

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. Jos tarvetta on, toimija voisi määrittää esimerkiksi käytettävät varaviestintäjärjestelmät ja niiden tarpeen sekä tavan käyttöönotolle.

Kohdassa 11 tarkoitettaisiin perustason tietoturva- eli 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 tietoturvakäytäntöjen avulla. Toimijan tulisi varmistaa, että tarpeelliset perustason tietoturvatoimenpiteet on toteutettu ja että työntekijät noudattavat niitä. Näiden tietoturva- eli kyberhygieniakäytäntöjen taso tulisi mitoittaa riittäväksi perustuen toimintojen kriittisyyteen. Valittujen toimenpiteiden tulisi perustua yleisiin hyviin käytäntöihin sekä riskienarviointiin.

Tietoturva- eli kyberhygieniakäytännöillä tarkoitetaan yleisiä hyviä perustason tietoturvatoimenpiteitä, joilla varmistetaan järjestelmien, ohjelmien ja palveluiden turvallisen käytön perustaso. Tällä 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 eli asetusten määrittämistä, ohjelmistojen päivityksiä, kattavaa ja luotettavaa tunnistamista sekä käyttäjien osaamisen parantamista ja tietoisuuden lisäämistä. Perustason tietoturva- eli kyberhygieniakäytäntöihin voitaisiin lukea esimerkiksi ajantasaiset ohjelmistopäivitykset, laitteiden ja ohjelmistojen turvallinen konfigurointi eli asetusten määrittäminen, 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 johdanto-osan perustelukappaleen 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 voitaisiin esimerkiksi 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 mahdollisuuksiin 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 riskienhallintavelvoitetta tarkentavia teknisiä määräyksiä toimialakohtaisista erityispiirteistä, jotka olisi otettava huomioon kyberturvallisuuden riskienhallinnan toimintamallissa ja riskienhallinnan huomioitavista osa-alueista alueissa sekä riskienhallinnan ja viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden hallinnan menettelyissä toimialalla. Lisäksi valvova viranomainen voisi antaa riskienhallintavelvoitetta tarkentavia teknisiä määräyksiä kriittisiä toimitusketjuja koskevien unionin tason koordinoitujen riskinarviointien tuloksien huomioimisesta toimialakohtaisessa riskienhallinnassa. Kriittisellä toimitusketjuja koskevalla unionin tason koordinoidulla riskiarvioinnilla tarkoitettaisiin NIS 2 –direktiivin 22 artiklassa tarkoitettua riskiarviointia, minkä ottaminen huomioon osana riskienhallintaa jäsenvaltion on varmistettava NIS 2 –direktiivin 21 artiklan 3 kohdan nojalla.

Viranomaisen määräyksenantovaltuus koskisi riskienhallintavelvoitteen tarkentamista ja täsmentämistä momentissa tarkoitettujen seikkojen osalta. Määräykset voisivat kuitenkin koskea vain teknisiä seikkoja, eli niillä ei saisi laajentaa 9 §:ssä säädettyjä velvoitteita. Määräyksenantovaltuuden tarkoituksena olisi täsmentää ja tarkentaa toimialakohtaisten erityispiirteiden huomioimista riskienhallintavelvoitteessa.

Määräyksenantovaltuuden ohella valvova viranomainen voisi luonnollisesti antaa myös muita ohjeita tai suosituksia esimerkiksi kyberturvallisuuden riskienhallinnasta, hallintatoimenpiteistä ja hyvistä käytännöistä. Lisäksi Liikenne- ja viestintäviraston Kyberturvallisuuskeskus voisi antaa toimialarajat ylittäviä ohjeita tai suosituksia esimerkiksi kyberturvallisuusriskien hallintatoimenpiteistä ja hyvistä käytännöistä sekä valvovien viranomaisten että velvoitteiden kohteiden hyödynnettäväksi. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus voisi myös 18 §:ssä tarkoitetussa tehtävässä edistää riskinhallintatoimenpiteitä koskevien ohjeiden ja suositusten koordinointia valvovien viranomaisten välillä.

Pykälän *5 momentin* nojalla riskienhallinnan toimintamallissa ja hallintatoimenpiteissä on noudatettava lisäksi NIS2-direktiivin 21 artiklan 5 kohdan nojalla annettavia Euroopan komission täytäntöönpanosäädöksiä.

NIS2-direktiivin 21 artiklan 5 kohdan nojalla komissio hyväksyy viimeistään 17 päivänä lokakuuta 2024 tarkempia vaatimuksia täytäntöönpanosäädöksellä, joilla vahvistetaan riskienhallintatoimenpiteiden tekniset ja menetelmiin liittyvät vaatimukset sekä tarvittaessa alakohtaiset vaatimukset, jotka koskevat DNS-palveluntarjoajia, aluetunnusrekistereitä eli tässä laissa tarkoitettuja aluetunnusrekisterin ylläpitäjiä, pilvipalvelujen tarjoajia, datakeskuspalvelujen tarjoajia, sisällönjakeluverkkojen tarjoajia, hallintapalvelun tarjoajia,

tietoturvapalveluntarjoajia, verkossa toimivien markkinapaikkojen tarjoajia, verkossa toimivien hakukoneiden tarjoajia, verkkoyhteisöalustojen tarjoajia ja luottamuspalvelun tarjoajia.

Lisäksi komissio voi hyväksyä NIS2-direktiivin 21 artiklan 5 kohdan nojalla sektorikohtaisempia yksityiskohtaisempia vaatimuksia koskevia täytäntöönpanosäädöksiä, joilla vahvistetaan riskienhallintatoimenpiteiden tekniset ja menetelmiin liittyvät vaatimukset sekä tarvittaessa alakohtaiset vaatimukset, jotka koskevat muita kuin edellä tarkoitettuja toimijoita.

Komission 21 artiklan 5 kohdan nojalla antamia täytäntöönpanosäädöksiä sovellettaisiin ensisijaisesti suhteessa valvovan viranomaisen määräyksiin ja Liikenne- ja viestintäviraston 5 momentin nojalla antamiin ohjeisiin. Siltä osin kuin komissio on käyttänyt sille annettua toimivaltaa ja antanut NIS2-direktiiviä tarkentavia täytäntöönpanosäädöksiä, olisi viranomaisten huomioitava ne määräys- tai ohjevalmistelussa ja huolehdittava antamiensa määräysten ja ohjeiden yhteensovittamisesta komission täytäntöönpanosäädösten kanssa.

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.

Johdon vastuulla tarkoitettaisiin johdon vastuuta kyberturvallisuuden riskienhallinnan toteuttamisen ja sen valvonnan järjestämisestä toimijassa. Johdon vastuun laiminlyönti voisi johtaa toimijaan kohdistuvaan tässä laissa tarkoitettuun hallinnolliseen seuraamukseen. Keskeisessä toimijassa johdon vastuun vakava ja toistuva laiminlyönti voisi johtaa myös lain 4 luvussa tarkoitettuun valvovan viranomaisen päätökseen, jolla kielletään määräajaksi henkilöä toimimasta 10 §:ssä tarkoitetussa tehtävässä. Selvyyden vuoksi todetaan, että yhtiön johtoon kohdistuvasta vahingonkorvausvastuusta säädetään erikseen.

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 vakavan palvelujen toimintahäiriön tai huomattavia taloudellisia tappioita asianomaiselle toimijalle. Lisäksi merkittävällä poikkeamalla tarkoitettaisiin poikkeamaa, jos poikkeama on vaikuttanut tai voisi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin

aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa. Merkittävän poikkeaman edellytyksenä olisi siten vakava toimintahäiriö palvelulle tai huomattava taloudellinen tappio asianomaiselle toimijalle taikka huomattava aineellinen tai aineeton vahinko, jonka poikkeama aiheuttaa tai voisi aiheuttaisi vaikuttamalla muihin luonnollisiin henkilöihin tai oikeushenkilöihin. Poikkeama määriteltäisiin 2 §:n 11 kohdassa, minkä nojalla poikkeamalla tarkoitettaisiin tapahtumaa, joka vaarantaa viestintäverkoissa ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden. Merkittävän poikkeaman kynnystä tulisi tulkita yhdenmukaisesti suhteessa NIS 2 -direktiivin 23 artiklan 3 kohtaan ja johdantokappaleeseen 101.

Mikäli toimija havaitsee merkittävän poikkeaman kynnyksen täyttävän tapahtuman jonkun muun toiminnassa kuin sen omassa toiminnassa, esimerkiksi välittömän alihankkijan, järjestelmän toimittajan tai sen käyttämän pilvipalvelun toiminnassa, olisi toimijan ilmoitettava tällaisesta poikkeamasta vain silloin, jos kyseinen poikkeama aiheuttaisi toimijalle itselleen merkittävän poikkeaman kynnyksen ylittävän tapahtuman. 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. Merkittävän poikkeaman kynnystä olisi tulkittava yhdenmukaisesti NIS2-direktiivin 23 artiklan 3 kohdan kanssa.

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. Määräaika alkaisi siitä, kun toimija on tullut tietoiseksi poikkeamasta eli havainnut sen. Määräajan alkamiseen ei siten vaikuttaisi se, milloin poikkeama tosiasiallisesti on alkanut, vaan toimijassa tehty havainto poikkeamasta. Määräaika voisi alkaa tavanomaisen työskentelyajan ulkopuolella, mikäli toimijalla on päivystystoimintaa tai muulla tavoin kyky havaita poikkeamia tavanomaisen työskentelyajan ulkopuolella. Määräajan alkamisessa merkityksellistä olisi poikkeamasta tehty havainto, mutta ei se, kuka, miten tai missä osassa toimijaa havainto tehdään. 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 tekniset vaarantumisindikaattorit eli vaarantumista kuvaavat indikaattorit (Indicator of Compromise) eli IoC-tieto, jos sellaisia on saatavilla. Vaarantumista kuvaaviin indikaattoreihin voisi sisältyä välitystietoa. 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, joilla tarkennetaan 11 – 15 §:n nojalla tehtävän ilmoituksen, tiedotuksen tai raportin tietosisältöä, teknistä muotoa tai menettelyä. Kysymys olisi toimialakohtaisesta, teknisestä ja tarkentavasta määräyksenantovaltuudesta. NIS 2 –direktiivin 23 artiklan 11 kohdan nojalla komissio voi hyväksyä täytäntöönpanosäädöksiä, joissa täsmennetään 11 – 13 ja 15 §:ssä tarkoitetun ilmoituksen tai raportin sekä 14 §:n nojalla annettavan tiedonannon tietosisältö, muoto ja ilmoitusmenettely.

Pykälän *6 momentin nojalla* luottamuspalvelun tarjoajien olisi tehtävä myös jatkoilmoitus viimeistään 24 tunnin kuluessa merkittävän poikkeaman havaitsemisesta 2 momentissa säädetystä määräajasta poiketen NIS 2 –direktiivin 23 artiklan 4 kohdan toisen kappaleen edellyttämällä tavalla.

Pykälän *7 momentin* nojalla merkittävällä poikkeamalla tarkoitettaisiin 1 momentissa säädetyn lisäksi NIS 2 –direktiivin 23 artiklan 11 kohdan nojalla annetussa Euroopan komission täytäntöön-panosäädöksessä täsmennettyä tapausta, jossa poikkeama katsotaan merkittäväksi.

NIS 2 –direktiivin 23 artiklan 11 kohdan nojalla komissio hyväksyy viimeistään 17 päivänä lokakuuta 2024 DNS-palveluntarjoajia, aluetunnusrekistereitä eli tässä laissa tarkoitettuja aluetunnusrekisterien ylläpitäjiä, pilvipalvelujen tarjoajia, datakeskuspalvelujen tarjoajia, sisällönjakeluverkkojen tarjoajia, hallintapalvelun tarjoajia, tietoturvapalveluntarjoajia sekä verkossa toimivien markkinapaikkojen tarjoajia, verkossa toimivien hakukoneiden tarjoajia ja verkkoyhteisöalustojen tarjoajia koskevia täytäntöönpanosäädöksiä, joissa täsmennetään tapaukset, joissa poikkeama katsotaan merkittäväksi.

Lisäksi NIS 2 –direktiivin 23 artiklan 11 kohdan nojalla komissio voi hyväksyä vastaavia täytäntöönpanosäädöksiä myös muitakin keskeisiä ja tärkeitä toimijoita koskien.

12 §. *Poikkeamaa koskeva väliraportti*. Pykälässä säädettäisiin toimijan velvollisuudesta antaa valvovalle viranomaiselle lisätietoja tai väliraportti merkittävää poikkeamaa koskevista tilannepäivityksistä. Ensi- ja jatkoilmoituksen lisäksi toimijan olisi annettava valvovan viranomaisen pyynnöstä lisätietoja tai väliraportti asian tilannepäivityksistä ja käsittelyn edistymisestä. Jos merkittävä poikkeama on pitkäkestoinen, eli poikkeamatilanne tai sen vaikutukset eivät ole päättyneet 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, mikäli poikkeaman käsittely ei olisi päättynyt ja loppuraporttia ei voitaisi toimittaa. Väliraportin tarkoituksena olisi kuvata poikkeaman käsittelyn etenemistä, poikkeaman vaikutuksia ja muita asian vaikutukseen liittyviä olennaisia tekijöitä sekä muutoksia niissä tiedoissa. Lisäksi väliraportilla voitaisiin antaa päivityksiä ensi- ja jatkoilmoituksen tietoihin. Toimijan olisi valvovan viranomaisen pyynnöstä annettava lisätietoja poikkeamasta ja sen käsittelystä tai uusi väliraportti poikkeaman tilannepäivityksistä ja käsittelyn etenemisestä.

13 §. *Poikkeamaa koskeva loppuraportti*. Pykälän *1 momentin* nojalla toimijan olisi annettava valvovalle viranomaiselle merkittävää poikkeamaa koskeva 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 tällöin 12 §:ssä tarkoitettu väliraportti asian tilannepäivityksistä ja käsittelyn etenemisestä. Pitkäkestoista poikkeamaa koskeva loppuraportti olisi toimitettava viimeistään kuukauden kuluessa poikkeaman käsittelyn päättymisestä. Loppuraportin toimittaminen ei rajoittaisi toimijan mahdollisuuksia täydentää tai korjata siinä annettuja tietoja myöhemmin, mikäli toimijan tiedot tai ymmärrys tilanteesta täydentyy vielä loppuraportin toimittamisen jälkeen.

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 selvittää syyllistä tai kohdistaa seuraamuksia tai muita sanktioita toimijalle, vaan edistää hyvää turvallisuuskulttuuria kyberturvallisuuden tason kohottamiseksi yhteiskunnassa.

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 §:ssä 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.

Edellä 1 ja 2 momentissa tarkoitetut ilmoitukset voitaisiin tehdä yleisellä tavalla tai muutoin tavalla, jota toimija yleisesti käyttää palvelujensa vastaanottajille viestimiseen. Palvelujen vastaanottajalla olisi oltava tosiasiallinen mahdollisuus saada tieto merkittävän poikkeaman aiheuttamasta haitasta palvelulle sekä mahdollisista toimenpiteistä, joilla uhkaa voidaan hallita palvelun vastaanottajan toimesta. Erityisesti milloin palvelujen vastaanottajia on huomattava määrä, kuten vesi- tai jätehuollossa, ilmoitukset voitaisiin tehdä esimerkiksi verkkosivuston tai yleisen tiedottamisen kautta.

Pykälän *3 momentin* nojalla, jos poikkeamasta tiedottaminen eli ilmoittaminen yleisölle on yleisen edun mukaista, valvova viranomainen voisi päätöksellä velvoittaa toimijan tiedottamaan asiasta tai tiedottaa asiasta itse. Ennen tiedottamista koskevan hallintopäätöksen tekemistä toimijaa olisi kuultava siten kuin hallintolain 34 §:ssä säädetään. Hallintolain 34 §:n 2 momentissa säädettäisiin asian ratkaisemisesta asianosaista kuulematta.

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.

Poikkeaman ja kyberuhkan määritelmästä säädettäisiin 2 §:ssä. Läheltä piti –tilanteella tarkoitettaisiin NIS2-direktiivin 6 artiklan 5 kohdan määritelmää vastaavasti 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.

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 tarkoitetun poikkeamailmoituksen. 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. Ilmoitukset olisi toimitettava välittömästi niiden saavuttua valvovalle viranomaiselle, jotta CSIRT-yksiköllä olisi mahdollisuus antaa toimijan pyynnöstä ohjeita tai operatiivisia teknisiä neuvoja. Käytännössä keskitetyn ilmoituskanavan kautta tehdyt ilmoitukset välittyisivät CSIRT-yksikölle automaattisesti, eli valvovan viranomaisen ei tarvitsisi välittää niitä erikseen CSIRT-yksikölle.

Pykälän *2 momentin* nojalla silloin, jos merkittävästä 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. Valvovan viranomaisen velvollisuus tiedottaa asiasta tietosuojavaltuutettua ei kuitenkaan vaikuttaisi toimijaan kohdistuviin velvoitteisiin, eikä se siten esimerkiksi täyttäisi rekisterinpitäjän velvollisuutta ilmoittaa henkilötietojen tietoturvaloukkauksesta.

Pykälän *3 momentin* nojalla valvovalla viranomaisella olisi velvollisuus ilmoittaa merkittävän poikkeaman havaitsemisesta poliisille, jos poikkeaman epäillään johtuvan rikoksesta, josta säädetty enimmäisrangaistus olisi vähintään kolme vuotta vankeutta. Lähtökohtaisesti toimijalla olisi vapaus päättää itse, ilmoittako se epäilemästään rikoksesta poliisille, ellei toimija epäilisi rikoslain 15 luvun 10 §:ssä tarkoitettua tekoa. Jos merkittävän poikkeaman kohdalla olisi syytä epäillä rikosta, valvovan viranomaisen tulisi ohjata toimijaa tekemään rikosilmoitus tarvittaessa. Siltä osin kuin kyse olisi rikoslain 15 luvun 10 §:ssä tarkoitetusta rikoksesta, ehdotettu momentti ei kuitenkaan vaikuttaisi velvollisuuteen ilmoittaa rikoksesta toimivaltaiselle viranomaiselle (poliisille). Kun kysymys olisi vakavasta, eli momentissa tarkoitetun kynnyksen täyttävää rikosta koskevasta epäilystä, valvovalla viranomaisella olisi kuitenkin velvollisuus ilmoittaa sitä koskevasta epäilystä poliisille.

Pykälässä tarkoitettuja rikoksia olisivat esimerkiksi rikoslain 35 luvun 3 b §:ssä tarkoitettu törkeä datavahingonteko, 38 luvun 4 §:ssä tarkoitettu törkeä viestintäsalaisuuden loukkaus, 38 luvun 6 §:ssä tarkoitettu törkeä tietoliikenteen häirintä, 38 luvun 7 b §:ssä tarkoitettu törkeä tietojärjestelmän häirintä ja 38 luvun 8 a §:ssä tarkoitettu törkeä tietomurto. Pykälässä tarkoitettuja rikoksia olisivat myös esimerkiksi rikoslain 12 luvun 1–7 §:ssä ja 9 §:ssä tarkoitetut maanpetosrikokset.

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.

Pykälän *5 momentin* nojalla 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 7 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 ja 8 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. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus voisi edistää esimerkiksi tämän lain 9 §:n riskinhallintatoimenpiteitä koskevien ohjeiden ja suositusten koordinointia valvovien viranomaisten välillä.

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.

Poikkeaman ja kyberuhkan määritelmästä säädettäisiin 2 §:ssä. Läheltä piti –tilanteella tarkoitettaisiin NIS2-direktiivin 6 artiklan 5 kohdan määritelmää vastaavasti 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.

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

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

Pykälän *1 momentin* nojalla Suomessa tietoturvaloukkauksiin reagoiva ja niitä tutkiva CSIRT-yksikkö toimisi Liikenne- ja viestintävirastossa. Toiminto olisi järjestettävä erilliseksi toimijoihin kohdistuvasta valvonnasta. CSIRT-yksikön tehtävistä säädettäisiin jäljempänä 20 §:ssä.

CSIRT-yksikön itsenäisyys ja erillisyys valvonnasta tarkoittaisi samalla, että valvovalla viranomaisella ei olisi tiedonsaantioikeutta suhteessa CSIRT-yksikköön, vaan CSIRT-yksiköllä olisi sen tehtävien hoitamisen edellyttämä itsenäinen asema suhteessa valvovaan viranomaiseen ja luottamuksellinen asema suhteessa valvonnan kohteisiin. CSIRT-yksikkö kuitenkin luovuttaa tämän lain nojalla saamiaan ja hankkimiaan tietoja siten kuin sähköisen viestinnän palveluista annetun lain 319 §:n 2 ja 3 momentissa säädetään. Itsenäisestä asemasta seuraava luottamus CSIRT-toiminnan riippumattomuuteen mahdollistavat sen, että CSIRT-yksikkö saa jatkossakin vapaaehtoisuuteen perustuvia ilmoituksia laajasti eri toimijoilta, joihin perustuvien tietojen avulla se voi tukea ja vahvistaa kyberturvallisuutta suomalaisessa yhteiskunnassa. CSIRT-yksikön toiminnan luottamuksellisuus on edellytys kyberturvallisuuden kansallisen tilannekuvan muodostamiselle, joka mahdollistaa sen, että CSIRT-yksikkö voi luovuttaa

relevantteja kyberturvallisuuteen liittyviä uhkatietoja suomalaisille organisaatioille kyberturvallisuustietojen vapaaehtoisten jakamisjärjestelyjen puitteissa.

Pykälän *2 momentissa* säädettäisiin vaatimuksista, jotka CSIRT-yksikön olisi täytettävä NIS2-direktiivin 11 artiklan 1 kohdan mukaisesti. CSIRT-yksikön olisi huolehdittava muun muassa viestintäkanaviensa saatavuudesta, toimitilojensa ja tietojärjestelmiensä sijoittamisesta suojattuihin paikkoihin sekä henkilöstönsä riittävyydestä ja asianmukaisesta koulutuksesta. Varautumisjärjestelyillä tarkoitettaisiin varajärjestelmiä ja –työtiloja. Momentti vastaisi NIS2-direktiivin 11 artiklan 1 kohtaa.

Pykälän *3 momentissa* säädettäisiin CSIRT-yksikön 11 artiklan 1 kohtaan sisältyvästä vaatimuksesta, jonka mukaisesti CSIRT-yksikön olisi määritettävä selkeästi 2 momentin 1 kohdassa tarkoitetut viestintäkanavat ja tiedotettava niistä kohderyhmilleen ja yhteistyökumppaneilleen asianmukaisella tavalla.

19 ja 20 §:llä täytäntöönpantaisiin NIS2-direktiivin 10 ja 11 artiklat sekä osin 29 artikla.

20 §. *CSIRT-yksikön tehtävät.* Pykälässä säädettäisiin CSIRT-yksikön tehtävistä. CSIRT-yksikön tehtävänä olisi seurata ja analysoida kyberuhkia, haavoittuvuuksia ja poikkeamia sekä kerätä tietoja niistä ja antaa ennakkovaroituksia toimijoille yhteiskunnassa sekä muista operatiivisen ja teknisen tason viranomaistehtävistä, 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 suhteessa toimijoihin kohdistuvaan valvontaan Liikenne- ja viestintävirastossa.

Pykälän *1 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 muihin kuin keskeisiin 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 1 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 1 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 muiden kuin keskeisten toimijoiden tekemiin ilmoituksiin ja tarvittaessa avustaisi niitä poikkeaman käsittelyssä. Vastuu poikkeaman käsittelystä ja tarvittavien toimenpiteiden suorittamisesta olisi pääasiallisesti kuitenkin ilmoituksen tehneellä taholla itsellään.

Pykälän 1 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 1 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 1 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 1 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 1 momentin *8 kohdan* mukaan CSIRT-yksikön tehtävänä olisi edistää tietoturvallisten tiedonjakovälineiden käyttöönottoa. CSIRT-yksiköllä tulisi olla käytössään asianmukainen, suojattu ja häiriönsietokykyinen viestintä- ja tietoinfrastruktuuri tietojen vaihtamiseen keskeisten ja muiden kuin keskeisten 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 1 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 *2 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 merkittäviä 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 *3 momentissa* säädettäisiin CSIRT-yksikön tehtävästä koordinoida kyberturvallisuustietojen vapaaehtoisia jakamisjärjestelyjä tämän lain soveltamisalaan kuuluvien toimijoiden, muiden tahojen ja CSIRT-yksikön kesken. Kyberturvallisuustietojen vapaaehtoisista jakamisjärjestelyistä säädetään 23 §:ssä.

Pykälän *4 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 24 §: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.

CSIRT-yksikön tietosuoja-asetuksen 6 artiklan 1 kohdan mukainen henkilötietojen käsittelyn oikeusperuste CSIRT-yksikön tehtävien hoitamiseksi on tehtävästä riippuen rinnakkain 6 artiklan 1 kohdan c alakohdan mukainen lakisääteisen velvoitteen noudattaminen ja 6 artiklan 1 kohdan e alakohdan mukainen yleinen etu tai julkisen vallan käyttö.

Pykälän *5 momentin* nojalla CSIRT-yksikkö voisi periä maksun 1 momentin 1 ja 2 kohdassa tarkoitetusta palvelusta, joka on tarjottu toimijan tai muun tahon pyynnöstä. Maksullista toimintaa voisi olla esimerkiksi pyynnöstä toteutettu 21 §:n 4 momentissa tarkoitettu kohdennettu haavoittuvuuskartoitus sekä tietoturvaloukkausten havainnointipalvelu ja muu 1 momentin 1 ja 2 kohdassa tarkoitettu palvelu, jota tarjotaan toimijan tai muun tahon pyynnöstä, eli muuten kuin CSIRT-yksikön omasta aloitteesta. Maksullisessa suoritteessa olisi kyse

korvauksesta toimijalle tai muulle taholle kohdennetusta viranomaisen tuottamasta palvelusta, joka on toimijalle tai muulle taholle vapaaehtoinen. Viranomaisten suoritteiden maksullisuudesta ja suoritteista perittävien maksujen suuruuden yleisistä perusteista sekä maksujen muista perusteista säädetään valtion maksuperustelaissa (150/1992).

21 §. *Yleisten viestintäverkkojen ja tietojärjestelmien verkkopohjainen haavoittuvuuskartoitus*. Pykälän säädettäisiin CSIRT-yksikön oikeudesta havainnoida yleiseen viestintäverkkoon liitettyjä viestintäverkkoja ja tietojärjestelmiä haavoittuvuuksien, kyberuhkien ja turvattomasti määritettyjen asetuksien eli turvattomasti konfiguroitujen viestintäverkkojen tai tietojärjestelmien 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.

Pykälän *1 momentissa* säädettäisiin haavoittuvuuskartoituksen tarkoituksesta. Haavoittuvuuskartoituksen tarkoituksena olisi haavoittuvuuksien, kyberuhkien ja turvattomasti määritettyjen viestintäverkkojen ja tietojärjestelmien asetuksien eli turvattomien konfigurointien havaitseminen sekä näistä havainnoista asianomaisille tahoille ilmoittaminen, mikä parantaisi asianomaisten tahojen mahdollisuuksia suojautua haavoittuvuuksien hyväksikäytöltä ja kyberuhilta.

Pykälän 1 ja *2 momentin* nojalla haavoittuvuuskartoitus olisi toteutettava ennakoivalla ja muulla kuin intrusiivisella tavalla. Ennakoivuudella tarkoitettaisiin haavoittuvuuskartoituksen yhteyttä tiedossa oleviin tai ennakoitavissa oleviin haavoittuvuuksiin tai kyberuhkiin. Muu kuin intrusiivinen tapa tarkoittaisi havainnointia viestintäverkon avulla saatavilla olevista viestintäverkoista ja tietojärjestelmistä tavalla, joka ei edellyttäisi intrusiivisuutta, eli tunkeutumista viestintäverkkoihin tai tietojärjestelmiin havaintojen tai tietojen saamiseksi. Muussa kuin 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. Muulla kuin intrusiivisella tavalla tarkoitettaisiin NIS2-direktiivissä tarkoitettua ”ei-intrusiivista” tapaa.

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 esimerkiksi 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 ei olisi sallittua käsitellä viestintäverkkoon tai tietojärjestelmään tallennettua henkilötietoa tällaisen käsittelyn intrusiivisuuden vuoksi.

Haavoittuvuuskartoituksessa voitaisiin havainnoida tai kartoittaa vain viestintäverkkoja ja tietojärjestelmiä. Haavoittuvuuskartoituksella ei olisi sallittua hankkia ja käsitellä luottamuksellisen viestinnän suojaamia tietoja, kuten välitystietoja tai viestien sisältöä, jossa CSIRT-yksikkö ei ole viestinnän osapuolena. Haavoittuvuuskartoituksessa CSIRT-yksikkö toimii viestinnän osapuolen roolissa. Yleisellä verkkopohjaisella haavoittuvuuskartoituksella ei ole teknisesti mahdollista käsitellä kolmannen osapuolen viestintää sivullisen roolissa. Haavoittuvuuskartoituksella ei siten saisi eikä teknisesti voisikaan käsitellä luottamuksellisen viestinnän suojan alaan kuuluvia viestintää koskevia tietoja. Mikäli erittäin poikkeuksellisessa tapauksessa haavoittuvuuskartoituksen kohteena oleva viestintäverkko tai muu tietojärjestelmä palauttaisi erittäin poikkeuksellisen teknisen häiriötilanteen tai vastaavan vakavan haavoittuvuuden takia kolmannen osapuolen viestintää koskevia tietoja esimerkiksi sähköpostipalvelimen välimuistista, olisi tiedot poistettava viipymättä.

Haavoittuvuuskartoituksessa ei olisi sallittua käsitellä viestintäverkkoon tai tietojärjestelmään tallennettua henkilötietoa. 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.

Pykälän *3 momentissa* säädettäisiin haavoittuvuuskartoituksessa havaittujen tietojen käyttötarkoituksesta. Haavoittuvuuskartoituksessa havaittuja tietoja saisi käyttää vain haavoittuvuuskartoituksen kohteena olevalle taholle viestintäverkkoon ja tietojärjestelmään kohdistuvista haavoittuvuuksista ja riskeistä ilmoittamiseksi. Lisäksi CSIRT-yksikkö voisi käyttää tietoja 20 §:n 1 momentin 1, 4 ja 5 kohdissa tarkoitettujen tehtävien hoitamiseksi. Näitä tehtäviä olisivat:

1) kyberuhkien, haavoittuvuuksien ja poikkeamien seuranta ja analysointi kansallisella tasolla sekä niitä koskevien tietojen kerääminen ja niitä koskevien ennakkovaroituksien, hälytyksien, ilmoituksien ja tietojen antaminen;
4) poikkeamailmoituksiin reagoiminen ja tarvittaessa poikkeamasta ilmoittaneen tahon avustaminen; sekä
5) riski- ja poikkeama-analyysien laatiminen ja kyberturvallisuuden tilannekuvan ylläpitämisen tukeminen.

Haavoittuvuuskartoitus voitaisiin siten toteuttaa vain 1 momentissa säädettyä tarkoitusta varten. Haavoittuvuuskartoituksella kertyvää tietoa voitaisiin kuitenkin käyttää 3 momentissa säädetyllä tavalla myös CSIRT-yksikön tehtäviä varten. Tarpeettomat tiedot olisi poistettava viipymättä.

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.

Ehdotetun *5 momentissa* selvennettäisiin, ettei haavoittuvuuskartoituksessa tai kohdennetussa haavoittuvuuskartoituksessa saisi käsitellä välitystietoja tietoja sähköisten viestien sisällöstä. Kuten edellä kuvataan, kun haavoittuvuuskartoitus suoritetaan ei-intrusiivisesti ja muutoinkin edellä kuvatulla tavalla, sähköisten viestien sisällön käsitteleminen ei ole teknisesti mahdollista. Teknologisen kehittymisen varalta ja kohdennetun haavoittuvuuskartoituksen reunaehtojen selventämiseksi pykälässä säädettäisiin yksiselitteinen kielto käsitellä haavoittuvuuskartoituksessa tai kohdennetussa haavoittuvuuskartoituksessa välitystietoja tai tietoja sähköisten viestien sisällöstä. Lisäksi CSIRT-yksikön olisi hävitettävä haavoittuvuuskartoituksessa saamansa tiedot, kun ne eivät ole enää tarpeen haavoittuvuudesta asianomaiselle toimijalle ilmoittamiseksi tai edellä 3 momentissa tarkoitettua tehtävää varten.

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

22 §. *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 yhteyden ottaminen asianomaisiin toimijoihin, 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-yksikkö voisi lisäksi säännöksen estämättä ohjata ja neuvoa asianomaisia tahoja siitä, miten muuhun tarpeelliseen haavoittuvuustietokantaan voisi ilmoittaa tietoja tai hakea tietoja tarvittaessa. 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.

23 §. *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. Ehdotuksella pantaisiin täytäntöön NIS2-direktiivin 29 artikla.

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. CSIRT-yksikön koordinoimiin vapaaehtoisiin jakamisjärjestelyihin voisi osallistua sekä tämän lain soveltamisalaan kuuluvia toimijoita että muita kuin tämän lain soveltamisalaan kuuluvia julkisia tai yksityisiä organisaatioita. Jakamisjärjestelyn tarkoituksena olisi niihin osallistuvien organisaatioiden sekä niiden asiakkaiden viestintäverkkoihin, tietojärjestelmiin tai palveluihin kohdistuvien kyberuhkien ehkäiseminen ja havaitseminen, poikkeamien hallitseminen ja niistä palautuminen tai niiden vaikutuksien lieventäminen. Jakamisjärjestelyyn voisi siten osallistua organisaation oman toiminnan suojaamisen ohella esimerkiksi tietoturvapalveluntarjoaja sen asiakkaidensa suojaamiseksi.

Kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn osallistuvien kesken voitaisiin jakaa 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 eli asetusten määrittämistä. Jakamisjärjestelyn osapuolilla tulisi olla mahdollisuus sopia menettelyistä ja toimintatavoista jaettujen tietojen käsittelemisessä tai tietojen luottamuksellisuuden osalta säännöksen estämättä.

Selvyyden vuoksi todetaan, että tietojen jakaminen perustuisi tiedon luovuttajan vapaaehtoisuuteen. Säännöksellä ei siten tarkoitettaisi aiheutuvan jakamisjärjestelyyn osallistuvalle lakiin perustuvaa velvollisuutta jakaa pykälän 2 momentissa tarkoitettuja tietoja tai muitakaan tietoja muille jakamisjärjestelyyn osallistuville. Luovutettaessa tietoa kyberturvallisuustietojen vapaaehtoisessa jakamisjärjestelyssä olisi otettava huomioon mahdolliset luovutettavaan tietoon kohdistuvat salassapitoa koskevat velvoitteet tai muut tiedon luovuttamista koskevat rajoitteet. Selvyyden vuoksi todetaan myös, että lain 4 §:n 7 momentin nojalla tässä laissa ei velvoiteta sellaisen tiedon antamiseen, jonka luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin siihen liittyvää tärkeää etua.

Tietoja voitaisiin vaihtaa erityisesti 2 momentissa tarkoitetuista seikoista.

Kyberuhkilla tarkoitetaan 2 §:n mukaisesti potentiaalisia tilanteita, tapahtumia tai toimintaa, joka voi vahingoittaa tai häiritä viestintäverkkoja ja tietojärjestelmiä, tällaisten järjestelmien käyttäjiä ja muita henkilöitä tai muulla tavoin vaikuttaa näihin haitallisesti. Kyse on uhkasta, joka toteutuessaan vaarantaa yhteiskunnan elintärkeän toiminnon tai muun

kybertoimintaympäristöstä riippuvaisen toiminnon. Kyberuhkat voivat aiheutua paitsi toteutuneista tietoturvauhkista myös digitaalisessa viestintäympäristössä toteutettavista tietoturvallisuutta vaarantavista teoista. Kyberuhkat voivat kohdistua esimerkiksi yhteiskunnan elintärkeisiin toimintoihin, kansalliseen kriittiseen infrastruktuuriin, kaikenkokoisiin yrityksiin, valtion- ja kunnallishallinnon organisaatioihin kuin myös yksittäisiin kansalaisiin. Kyberuhkilla voi olla sekä suoria että välillisiä vaikutuksia erilaisiin toimijoihin yhteiskunnassa ja ne voivat olla peräisin niin Suomen rajojen sisäpuolelta kuin ulkopuolelta.

Kyberuhka voi olla esimerkiksi uhkatoimijan toteuttama organisaatioon kohdistettu tunnuskalastelukampanja, jolla pyritään saamaan haltuun organisaation työntekijöiden käyttäjätunnuksia ja salasanoja varsinaisen tietomurron tai kyberhyökkäyksen toteuttamista varten. Lisäksi onnistunut tietomurto organisaation ympäristöön voi aiheuttaa monenlaisia kyberuhkia, jotka voivat vaikuttaa organisaation toiminnan kannalta kriittisten tietojen eheyteen, luottamuksellisuuteen ja saatavuuteen. Toinen esimerkki kyberuhasta ovat palvelunestohyökkäykset, jotka voivat aiheuttaa kyberuhan organisaation toiminnalle estämällä esimerkiksi organisaation toiminnan kannalta kriittisten järjestelmien ja palveluiden käytön tai heikentämällä niiden saatavuutta. Kyberuhka voi myös olla peräisin organisaation omista toimista: esimerkiksi verkko- ja tietojärjestelmien ylläpitotoimissa tahallisesti tai tahattomasti suoritettu virheellinen komento tai virheellisesti asetettu konfiguraatio voi muodostaa kyberuhan aiheuttamalla häiriötilanteen toimintaympäristössä tai altistamalla sen haavoittuvaksi. Lisäksi kyberuhkilla voi olla merkittäviä vaikutuksia organisaation palvelujen saatavuuteen. Esimerkiksi tuotantolaitoksen automaatioympäristön ohjausjärjestelmään tai prosessituotannon säätöjärjestelmään kohdistuneen tietomurron seurauksena uhkatoimija voi yrittää vaikuttaa tuotantolaitoksen toimintaan negatiivisella tavalla muodostaen tuotannolle vakavan kyberuhkan. Tällaisella kyberuhkalla saattaa olla vakavia vaikutuksia, jos kyseessä on esimerkiksi sähköntuotantoon, vedenjakeluun tai elintarviketuotantoon tai johonkin muuhun yhteiskunnan tärkeään toimintaan liittyvä ympäristö.

Poikkeamilla tarkoitetaan 2 §:n mukaan tapahtumaa, joka vaarantaa viestintäverkoissa ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden. Poikkeama voi olla esimerkiksi yksittäinen havaittu tietoturvatapahtuma tai joukko toisiinsa liittyviä palvelimilta kerättyihin lokitietoihin perustuvia tapahtumia, jotka viittaavat palvelun murtoyrityksiin tai onnistuneeseen tietomurtoon. Poikkeama voi siten olla myös laajempi kokonaisuus erilaisia verkossa havaittuja tietotapahtumia, jotka viittaavat esimerkiksi tunnistetun uhkatoimijan tekniikan tai menettelyn toteuttamiseen kohdeympäristössä, kuten kiristyshaittaohjelmahyökkäyksen toteuttamiseen tai sellaisen valmisteluun. Toisaalta poikkeama voi myös yksinkertaisesti olla järjestelmähäiriön tai laiterikon aiheuttama tilanne, joka aiheuttaa uhkan organisaation tietoturvalle.

Läheltä piti -tilanteilla tarkoitetaan NIS2-direktiivin 6 artiklan 5 kohdan määritelmää vastaavasti tapahtumaa, joka olisi voinut vaarantaa viestintäverkoissa ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltävien tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden mutta jonka toteutuminen onnistuttiin estämään tai joka ei toteutunut satunnaisesti syystä.

Esimerkkinä läheltä piti -tilanteesta voidaan pitää esimerkiksi organisaation tietoturvavalvomossa (Security Operations Centre, SOC) havaittua tietoturvatapahtumaa, joka aiheutti valvontajärjestelmässä (Security Incident and Event Management, SIEM) hälytyksen perustuen tunnettuun vaarantumisindikaattoriin (IoC), mutta jonka seurauksena nopeasti aloitetut reagointi ja -suojaustoimenpiteet estivät meneillään olevan kiristyshaittaohjelmahyökkäyksen viimeisen vaiheen, jossa uhkatoimija salaisi

uhriorganisaation tiedot ja pyrkisi kiristämään uhrilta varoja tietojen palauttamiseksi. Tällaisessa tilanteessa varsinainen hyökkäys onnistuttiin pysäyttämään vaiheeseen, jossa tapahtui kyberpoikkeama ja tietomurto, sillä hyökkääjä onnistui murtautumaan organisaation tietojärjestelmiin, mutta hyökkäyksen varsinainen tavoite, eli tietojen salaus ja kiristäminen onnistuttiin estämään. Läheltä piti -tilanne voi olla myös esimerkiksi tilanne, jossa organisaatio saa Liikenne- ja viestintäviraston Kyberturvallisuuskeskukselta ilmoituksen kyseisen organisaation ylläpitotunnusten kaupittelusta kyberrikollisten kauppapaikassa. Ilmoituksen johdosta organisaatio estää kyseisten ylläpitotunnusten käytön juuri ennen kun organisaation etäkäyttöpalvelun lokeissa havaitaan kyseisen tunnuksen hyödyntämistä organisaation verkkoympäristöön kohdistuvassa tietomurron yrityksessä.

Haavoittuvuuksilla tarkoitetaan 2 §:n mukaan tieto- ja viestintätekniikan tuotteiden tai -palvelujen heikkoutta, alttiutta tai vikaa, jota kyberuhka voi hyödyntää. Haavoittuvuus on esimerkiksi tietyssä kaupallisesti tarjottavassa tai avoimen lähdekoodin ohjelmistossa havaittu vika tai heikkous, joka voi mahdollistaa ohjelmistoon toteutetun tietoturvakontrollin ohittamisen. Monien organisaatioiden verkkoympäristöissä on toteutettu joidenkin organisaation käyttämien tietojärjestelmien etäkäytön mahdollistava tekninen ratkaisu (VPN-palvelu). Jos organisaation käyttämän etäkäyttöpalvelun käyttäjien tunnistautumiseen liittyvän toiminnallisuuden toteutuksessa havaitaan virhe, joka mahdollistaa hyökkääjälle tietyllä tavalla muotoiltuja tunnistautumispyyntöjä lähettämällä sen, että hyökkääjä pystyy ohittamaan palvelun tunnistautumisvaiheen ja näin pääsee kirjautumaan palveluun millä tahansa tunnuksella, on kyseisessä etäkäyttöpalvelussa haavoittuvuus.

Mikäli tietyn haavoittuvuuden julkitulemisen aikaan siihen ei ole vielä virallista haavoittuvuuden korjaavaa ohjelmistopäivitystä saatavilla, on kyseessä ns. nollapäivähaavoittuvuus. Tällaisessa tilanteessa organisaation ei ole vielä itse mahdollista korjata haavoittuvuutta ohjelmistopäivityksellä. Organisaation on tästä huolimatta yleensä mahdollista tehdä muita haavoittuvuuden hyväksikäyttöä koskevia rajoittamistoimia, kuten poistaa haavoittuva toiminnallisuus käytöstä, mikäli se on mahdollista, tai estää haavoittuvuuden hyväksikäyttö jollain toisella tietoturvakontrollilla esimerkiksi eri verkkokerroksella.

Taktiikoilla, tekniikoilla ja menettelyillä (Tactics, Techniques ja Procedures - TTP) viitataan yleisesti uhkatoimijan käyttämään toimintamalliin kyberhyökkäyksessä. Taktiikka on hyökkääjän toiminnan korkeimman tason kuvaus, kun taas tekniikat antavat yksityiskohtaisemman tason kuvauksen hyökkääjän käyttäytymisestä taktiikan kontekstissa. Menettelyt ovat taas vielä alemman tason erittäin yksityisiä kuvauksia hyökkääjän toimista tekniikan yhteydessä.

Taktiikat kertovat uhkatoimijan ylätason toimintatavoista ja strategiasta hyökkäyksen toteuttamisessa tietyn päämäärän saavuttamiseksi. Esimerkiksi hyökkäyksen kohteen ympäristön kartoittamista ja tiedustelua, murtautumista kohteen ympäristöön, käyttöoikeusvaltuuksien korottamista, hyökkäyksen laajentamista ja tietojen varastamista tai kiristämistä. Tekniikat sen sijaan kuvaavat tarkemmin toimia, joita hyökkääjä tekee kohteen ympäristöön murtautumisen valmistelemiseksi tai varsinaisen hyökkäyksen toteuttamiseksi kohteen ympäristössä. Käytettyjä tekniikoita ovat esimerkiksi kalasteluviestin lähettäminen käyttäjätunnusten haltuun saamiseksi, tunnettujen haavoittuvuuksien hyväksikäyttäminen, käyttäjätunnusten ja oikeuksien muokkaaminen, hyökkääjän työkalujen suorittaminen, havainnointimenetelmien ohittaminen, palvelinohjelmiston toimintaan vaikuttaminen ja aktiivinen kohteen ympäristön jatkokartoittaminen. Menettelyt taas yhdistävät sen, miten uhkatoimijan taktiikoita toteutetaan valittujen tekniikoiden avulla hyvin yksityiskohtaisella tasolla. Esimerkiksi menettely voi olla yksityiskohtainen tieto siitä, että uhkatoimija toteuttaa

hyökkäyksen ensimmäisen vaiheen sisäänpääsyyn hyväksikäyttämällä juuri tietyn etäkäyttöjärjestelmän haavoittuvuutta ja saa näin suoritettua omaa ohjelmakoodiaan kohdejärjestelmässä, jolloin hyökkääjän ohjelmakoodi mahdollistaa palvelun oikeudettoman käytön muuttamalla etäkäyttöpalvelun konfiguraatiota kohteen sisäverkkoon pääsyn avaamiseksi.

Vaarantumisindikaattorit ovat teknisiä tunnisteita tai mitattavissa olevia havaintoja, joiden perusteella voidaan päätellä, onko kyberhyökkäys mahdollinen, parhaillaan käynnissä tai tapahtunut jo aiemmin. Tavanomaisimmat vaarantumisindikaattorit ovat verkko-, laite-, tiedosto- ja käyttäytymispohjaisia. Esimerkiksi verkkopohjaisia vaarantumisindikaattoreita ovat hyökkääjän käyttämät IP-osoitteet, verkkotunnukset, URL-osoitteet sekä asiakas- ja palvelinohjelmistojen yksilöivät tunnisteet. Verkkopohjaisia vaarantumisindikaattoreita voidaan havainnoida tunkeutumisenhavainnointijärjestelmällä (IDS) suoraan verkkoliikenteestä tai verkkoliikenteestä kerättyjen lokitietojen pohjalta tätä tarkoitusta varten suunnitellussa lokienhallintajärjestelmässä. Verkkopohjainen indikaattori voi olla periaatteessa mikä tahansa verkkotasolla havaittavissa oleva tekninen tunnistetieto tai tapahtuma. Laitepohjaiset vaarantumisindikaattorit sen sijaan liittyvät tyypillisesti normaalista poikkeaviin muutoksiin esimerkiksi laitteen konfiguraatiotiedoissa tai muuhun normaalista poikkeavaan toimintaan laitteessa tai sen ohjelmistossa. Näiden indikaattoreiden havainnointiin tarvitaan yleensä erillinen ohjelmisto, joka seuraa laitteen toimintaa, havainnoi siinä tapahtuvat poikkeavuudet ja tekee niistä hälytyksiä. Laitetasolla voidaan myös havainnoida hyökkääjän haitallisten ohjelmien suoritukseen liittyviä vaarantumisindikaattoreita, kuten esimerkiksi ohjelmien ajonaikaiseen yksilöintiin liittyviä tunnisteita tai muita muistinvaraisia ohjelmistotunnisteita.

Tiedostopohjaisista vaarantumisindikaattoreista yleisimpiä ovat taas haitallisiksi tunnistetuista tiedostoista lasketut yksilöivät tunnisteet eli tiedostotiivisteet, joiden pohjalta voidaan tunnistaa esimerkiksi hyökkääjän käyttämiä haittaohjelmia tai muita työkaluja. Näitä vaarantumisindikaattoreita voidaan hyödyntää esimerkiksi tietomurtotutkintaa suorittaessa tai havainnoitaessa tietyn uhkatoimijan menettelyjä suojattavassa ympäristössä. Käyttäytymispohjaiset vaarantumisindikaattorit voivat sen sijaan perustua esimerkiksi tietojärjestelmien käyttäjien eli ihmisten poikkeavaan käyttäytymiseen verkkoympäristössä, kuten käyttäjän kirjautumiseen organisaation tietojärjestelmään normaalista poikkeavana ajankohtana tai normaalista poikkeavasta sijainnista.

Yleisiä käytännön esimerkkejä vaarantumisindikaattoreista ovat epätavalliset nimipalvelukyselyt, epäilyttävät tiedostot, sovellukset ja prosessit, botnet-verkkoihin tai haittaohjelmiin kuuluvat IP-osoitteet ja verkkotunnukset, epäilyttävä toiminta pääkäyttäjän oikeuksilla varustetuilla käyttäjätileillä, odottamattomat ohjelmistopäivitykset, tiedonsiirto harvoin käytettyjen tietoliikenneporttien kautta, ihmiselle epätyypillinen tietoliikenne verkkosivustolla, tunnetun haittaohjelman tiedostotiivisteet, kokoonpanotiedostojen, rekisterien ja laiteasetusten luvaton muuttaminen sekä suuri määrä epäonnistuneita sisäänkirjautumisyrityksiä.

Erilaisia uhkatoimijoita ovat esimerkiksi yksittäiset kyberrikolliset, rikollisryhmittymät, valtiolliset toimijat, haktivistit, pahantahtoiset hakkerit, sisäiset uhkat ja terroristiset ryhmittymät. Näillä kaikilla on erilaiset tavoitteet toiminnalleen ja motivaation taustalla on usein joko rahallinen hyöty, poliittinen tai muu aatteellinen intressi tai maineen tavoittelu. Toisin sanoen uhkatoimijoita on monenlaisia ja ne voivat vaihdella yksittäisistä itsenäisistä hyökkääjistä hyvin resursoituihin ryhmittymiin, jotka toimivat koordinoidusti osana laajempaa rikollisjärjestöä tai valtiollisen toimijan tukemana. Uhkatoimijat voivat olla pitkäjänteisiä, motivoituneita ja mukautumiskykyisiä, ne voivat käyttää erilaisia taktiikoita, tekniikoita ja

menettelyjä (TTP) murtautuakseen tietojärjestelmiin, häiritäkseen palveluita ja tavoitellakseen taloudellista hyötyä. Uhkatoimijat voivat myös varastaa tai paljastaa organisaation liikesalaisuuksia ja muita arkaluonteisia tietoja.

Kyberturvallisuushälytyksillä tarkoitetaan yleensä tilanteita, jotka aiheutuvat jonkin tietoturvatapahtuman seurauksena joko organisaation automaattisen valvontajärjestelmän tuottamana tai aktiivisen uhkametsästyksen löydösten perusteella. Hälytys voi aiheutua esimerkiksi tietoturvatapahtumien valvontaan tarkoitetun järjestelmän havaitessa sen keräämissä tiedoissa jonkin tunnetun vaarantumisindikaattorin tai jonkin muun etukäteen määritellyn tapahtuman, jonka seurauksena on määritelty kyberturvallisuushälytyksen tapahtuvan.

Pykälän *3 momentissa* säädettäisiin CSIRT-yksikön oikeudesta luovuttaa kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn osallistuvalle tieto kyberuhkaan tai poikkeamaan liittyvästä välitystiedosta tai haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä. Sen lisäksi, mitä tässä laissa säädetään, CSIRT-yksikkö voisi luovuttaa tämän lain mukaisia tehtäviä hoitaessaan saamiaan ja hankkimiaan tietoja siten kuin sähköisen viestinnän palveluista annetun lain 319 §:ssä säädetään.

Pykälän *4 momentissa* säädettäisiin kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn osallistuvan oikeudesta 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 ja toiselle samaan kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn osallistuvalle taholle.

Kyberuhkien ja poikkeamien hallitsemiseksi ja haitallisten vaikutusten ehkäisemiseksi olisi välttämätöntä, että CSIRT-yksiköllä ja jakamisjärjestelyihin osallistuvilla olisi mahdollisuus antaa muille jakamisjärjestelyyn osallistuville oma-aloitteisesti tietoa haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä ja sen välitystiedoista siltä osin kuin se liittyy haitalliseen tietokoneohjelmaan tai käskyn teknisiin ominaisuuksiin ja teknisiin jälkiin tai muuhun kyberuhkan tai poikkeaman toteuttamiseen liittyvään tekniseen tietoon. Säännös kattaisi esimerkiksi tiedon antamisen haitalliseen tietokoneohjelmaan liittyvistä lokitiedoista. Kyberturvallisuustietojen vapaaehtoisen jakamisjärjestelyn tarkoituksen toteuttamiseksi olisi välttämätöntä, että vapaaehtoiseen jakamisjärjestelyyn osallistuvat voisivat 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. Tiedonvaihdon tarve ei kohdistuisi sähköisen viestinnän semanttiseen eli ihmisen luomaan sisältöön viestinnässä, vaan viestin teknisiin ominaisuuksiin. Ehdotuksen suhdetta luottamuksellisen viestinnän suojaan käsitellään jäljempänä säätämisjärjestysperustelussa.

Pykälän *5 momentin* nojalla jakamisjärjestelyyn osallistuva voisi käsitellä edellä 3 tai 4 momentin nojalla kyberuhkaan tai poikkeamaan liittyvistä välitystiedoista ja haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä saamaansa tietoa vain 1 momentin mukaisiin käyttötarkoituksiin. Lisäksi CSIRT-yksikkö voisi käsitellä tietoja 20 §:n 1 momentissa säädettyä tehtävää varten. Tiedon luovuttamisella ei saisi rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä 1 momentissa säädetyn tarkoituksen vuoksi.

Tämän pykälän mukaisissa kyberturvallisuustietojen vapaaehtoisissa jakamisjärjestelyissä tietosuoja-asetuksen 6 artiklan mukainen henkilötietojen luovuttamisen oikeusperuste on

jakamisjärjestelyihin osallistuvien viranomaisten osalta tietosuoja-asetuksen 6 artiklan 1 kohdan e alakohdan mukainen yleinen etu tai julkisen vallan käyttö, ja jakamisjärjestelyihin osallistuvien yksityisten toimijoiden ja yhteisöjen osalta 6 artiklan 1 kohdan f alakohdan mukainen oikeutettu etu.

Ehdotetulla 23 §:llä täytäntöönpantaisiin NIS2-direktiivin 29 artikla.

24 §. *Tietoturvaloukkausten havainnointipalveluun liittyvä tiedonkäsittely.* Pykälässä säädettäisiin tiedonkäsittelystä 20 §:n 4 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 toimija tai muu kuin tämän lain soveltamisalaan kuuluva yhteisö, 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 toimijan tai muun yhteisön 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 tukeakseen kansallisen kyberturvallisuuden tilannekuvan ylläpitämistä.

Pykälän *3 momentissa* täsmennettäisiin, että CSIRT-yksikölle 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.

CSIRT-yksikön yleisen tietosuoja-asetuksen mukainen henkilötietojen käsittelyn oikeusperuste tietoturvaloukkausten havainnointipalvelun tuottamiseksi on 6 artiklan 1 kohdan e alakohdan mukainen yleinen etu tai julkisen vallan käyttö.

25 §. *CSIRT-yksikölle vapaaehtoisesti luovutettu tieto.* Pykälässä säädettäisiin CSIRT-yksikölle vapaaehtoisesti luovutetun tiedon käyttörajoituksesta tietojen vapaaehtoisen luovuttajan suojaksi. Rajoitus koskisi CSIRT-yksikölle sen tämän lain mukaisten tehtävien hoitamiseksi vapaaehtoisesti luovutettua tietoa. CSIRT-yksikölle vapaaehtoisesti luovutettua tietoa ei saisi käyttää tiedon luovuttajaan kohdistuvassa rikostutkinnassa eikä hallinnollisessa tai muussa tiedon luovuttajaan kohdistuvassa päätöksenteossa ilman tiedon luovuttaneen suostumusta. CSIRT-yksikön tehtävien hoitaminen ja kyberturvallisuuden parantamiseksi organisaatioiden välillä tehtävän yhteistyön mahdollistaminen edellyttäisi luottamuksellista suhdetta CSIRT-yksikön ja sille tietoa antavien toimijoiden välillä. Sen turvaamiseksi olisi välttämätöntä, ettei CSIRT-yksikölle sen tehtävien hoitamiseksi vapaaehtoisesti luovutettavaa tietoa voitaisi käyttää tiedon luovuttaneeseen kohdistuvan sanktion kohdentamiseksi ilman tiedon luovuttajan suostumusta. Itsenäisestä asemasta seuraava luottamus CSIRT-toiminnan riippumattomuuteen yhdessä ehdotetun säännöksen kanssa mahdollistavat sen, että CSIRT-yksikkö saa jatkossakin vapaaehtoisuuteen perustuvia ilmoituksia laajasti eri toimijoilta, joihin perustuvien tietojen avulla se voi tukea ja vahvistaa kyberturvallisuutta suomalaisessa yhteiskunnassa.

Pykälä vastaisi NIS2-direktiivin johdanto-osan perustelukappaletta 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 myös valvontatoiminnassa ja CSIRT-yksikön operatiivisessa toiminnassa käytettäviä tietoja ja edistettäisiin toimijan oikeussuojan toteutumista.

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

Pykälän *1 momentissa* säädettäisiin valvovan viranomaisen tehtävästä. Valvovan viranomaisen tehtävänä olisi valvoa toimialallaan tämän lain, sen nojalla annettujen määräysten sekä NIS2-direktiivin nojalla annettujen säädösten noudattamista. Momentissa osoitettaisiin valvovan viranomaisen tehtävä kunkin liitteessä I ja II tarkoitetun toimijan osalta.

NIS 2 –direktiivin nojalla annetuilla säädöksillä tarkoitettaisiin sen 21 artiklan 5 kohdan ja 23 artiklan 11 kohdan nojalla annettavia Euroopan komission täytäntöönpanosäädöksiä ja 24 artiklan 2 kohdan annettavia Euroopan komission delegoituja asetuksia.

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, maakaasun jakelu- tai siirtoverkonhaltijoiden sekä vedyn siirtoa harjoittavien toimijoiden osalta.

Turvallisuus- ja kemikaalivirasto olisi tässä laissa tarkoitettu valvova viranomainen muiden kaasualan toimijoiden, öljyalan toimijoiden, vedyn tuotantoa ja varastointia harjoittavien 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 terveyspalvelun tuottajien ja EU:n vertailulaboratorioiden 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. Lääkealan turvallisuus- ja kehittämiskeskus olisi tässä laissa tarkoitettu valvova viranomainen myös veripalveluiden, apteekkien sekä potilaiden oikeuksien soveltamisesta rajat ylittävässä terveydenhuollossa annetun EU-direktiivin (2011/24/EU) mukaisten lääkkeiden ja lääkinnällisten laitteiden tarjoajien osalta.

Pykälän *2 momentissa* säädettäisiin valvovien viranomaisten velvollisuudesta tehdä yhteistyötä valvonnan toteuttamisessa. Yhteistyövelvoite konkretisoituisi erityisesti tilanteessa, jossa yksi toimija harjoittaisi toimintaa laaja-alaisesti usealla toimialalla siten, että toimijaan kohdistuisi 1 momentin nojalla useamman kuin yhden viranomaisen valvontatoimivalta. 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 sekä pidättäytyä päällekkäisten valvontatoimenpiteiden toteuttamisesta erillisesti. Toimijaan ei tulisi kohdistaa saman asian vuoksi päällekkäisiä valvontatoimenpiteitä. Yhteistyövelvoite kattaisi myös valvovien viranomaisten välisen yhteistyön muissa kuin yksittäiseen toimijaan kohdistuvissa asioissa.

27 §. *Valvonnan kohdistaminen*. Pykälässä säädettäisiin valvonnan kohdentamisesta, keskeisestä toimijasta ja valvovan viranomaisen tehtävien asettamisesta tärkeysjärjestykseen.

Pykälän *1 momentin* nojalla toimijoihin kohdistuva valvonta kohdistettaisiin keskeisiin toimijoihin NIS2-direktiivin vähimmäisvaatimuksen mukaisesti. Keskeisen toimijan määritelmä vastaisi NIS2-direktiivin 3 artiklaa. Valvova viranomainen voisi kuitenkin kohdistaa valvontaa myös muuhun kuin keskeiseen toimijaan, jos on perusteltu syy epäillä, että kyseinen toimija ei ole noudattanut tätä lakia, sen nojalla annettuja määräyksiä tai NIS 2 -direktiivin nojalla annettuja säädöksiä. Muulla kuin keskeisellä toimijalla tarkoitettaisiin toimijaa, joka ei ole keskeinen, eli NIS2-direktiivin 3 artiklassa tarkoitettua tärkeää toimijaa.

NIS2-direktiivin vähimmäisvaatimuksen mukaisesti tämän lain, sen nojalla annettujen määräysten sekä NIS2-direktiivin nojalla annettujen säädösten ennakkovalvonta olisi kohdistettava 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 johdanto-osan perustelukappaleesta 122 ilmenee lähtökohta valvonnan jakamisesta 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.

Keskeisten toimijoiden lisäksi valvova viranomainen voisi kohdistaa valvontaa muuhun toimijaan, jos on perusteltu syy epäillä, että kyseinen toimija ei ole noudattanut tätä lakia, sen nojalla annettuja määräyksiä tai NIS2-direktiivin nojalla annettuja säädöksiä. Näin ollen valvova viranomainen ei voisi kohdistaa valvontatoimenpiteitä muihin kuin keskeisiin toimijoihin ennakkovalvontana ilman perusteltua syytä epäillä lain noudattamattomuutta. Muulla kuin keskeisellä toimijalla tarkoitettaisiin niitä lain velvoitteiden soveltamisalaan kuuluvia toimijoita, jotka eivät olisi 2 momentissa säädetyllä perusteella keskeisiä, eli NIS2-direktiivin 3 artiklassa tarkoitettuja 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. Perusteltu syy voisi olla esimerkiksi 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. Perusteltu syy olisi käsillä myös silloin, jos toimijaan olisi kohdistunut merkittävä poikkeama.

Pykälän *2 momentissa* määriteltäisiin keskeiset toimijat NIS2-direktiivin 3 artiklan mukaisesti. Keskeisiä toimijoita olisivat liitteessä I tarkoitetut toimijat, jotka ylittävät komission suosituksen 2003/361/EY liitteessä olevan 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset. Suosituksen liitteessä olevan 3 artiklan 4 kohtaa ei sovelleta toimijan määrittelyssä. 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, vastaavasti kuten toimijan määritelmän kynnysarvossa.

Lisäksi keskeisiä toimijoita olisivat koosta riippumatta hyväksytyt luottamuspalvelun tarjoajat, aluetunnusrekisterien ylläpitäjät ja DNS-palveluntarjoajat. Lisäksi keskeisiä toimijoita olisivat 3 §:n 3 momentissa tarkoitetut toimijat.

Keskeisiä toimijoita olisivat myös yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat, jotka täyttävät tai ylittävät komission suosituksen 2003/361/EY liitteessä olevan 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset. Suosituksen liitteessä olevan 3 artiklan 4 kohtaa ei sovelleta toimijan määrittelyssä. Keskeisiä toimijoita olisivat siten kokoperusteisesti näitä toimintoja harjoittavat yritykset, joiden palveluksessa on vähintään 50 työntekijää taikka joiden vuotuinen liikevaihto on yli 10 miljoonaa euroa ja tase on yli 10 miljoonaa euroa.

Jos sama toimija harjoittaisi toimintaa useammalla lain liitteessä tarkoitetulla toimialalla ja toiminta olisi osin keskeisen toimijan määritelmän mukaista toimintaa sekä osin muuta toimintaa, toimijaa olisi pidettävä kokonaan keskeisenä toimijana.

Pykälän *3 momentissa* säädettäisiin valvovan viranomaisen oikeudesta asettaa laissa säädetyt tehtävät tärkeysjärjestykseen riskiperusteisesti. Valvottavien toimijoiden määrä, toimijoiden merkitys yhteiskunnan kriittisille toiminnoille sekä niihin kohdistuvien kyberturvallisuusriskien määrä vaihtelee merkittävästi toimialoittain. 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. Erityisesti tilanteissa, joissa valvottava toimija toimii useilla eri toimialoilla, joista vain osa on liitteessä I tai II tarkoitettua toimintaa, olisi toiminta kokonaisuudessaan sääntelyn piirissä, mutta valvontaa olisi syytä kohdistaa erityisesti liitteissä tarkoitettuun toimintaan ja sen kannalta merkityksellisiin tietojärjestelmiin ja viestintäverkkoihin ja niihin kohdistuvien riskien tai uhkien mahdollisiin vaikutuksiin liitteessä I tai II tarkoitetulle toiminnalle. 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 tarkoitetut eli jäljempänä lain 37 §:ssä 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.

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

28 §. *Tiedonsaantioikeus*. Pykälässä säädettäisiin valvovan viranomaisen tiedonsaantioikeudesta. Pykälässä säädettäisiin lisäksi oikeudesta luovuttaa tieto toiselle valvovalle viranomaiselle ja CSIRT-yksikölle.

Pykälän *1 momentissa* säädettäisiin valvovan viranomaisen oikeudesta saada salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä tässä laissa säädettyjen tehtäviensä suorittamiseksi toimijalta tarpeelliset tiedot, jotka koskevat kyberturvallisuuden riskienhallintaa toimijassa, riskienhallinnan toimintamallia, hallintatoimenpiteitä ja niiden toteutusta, sekä merkittävää poikkeamaa. Lisäksi valvovalla viranomaisella olisi oikeus saada muut edellä mainittuihin tietoihin liittyvät tiedot, jotka ovat välttämättömiä riskienhallintavelvoitteiden valvomista ja merkittävien poikkeamien ilmoittamisen ja raportoinnin valvomista varten.

Tiedonsaantioikeuden käyttäminen olisi ensisijainen ja pääasiallinen toimijoihin kohdistuva valvovan viranomaisen toimenpide, jonka tarkoituksena on mahdollistaa riskienhallinta- ja raportointivelvoitteiden noudattamisen valvonta. Viranomaisella olisi oikeus saada pääsy kyberturvallisuuden riskienhallintaa ja riskiarviointeja koskeviin asiakirjoihin ja tietoihin sekä riskienhallinnan toimintamalliin. Lisäksi viranomaisella olisi oikeus saada tietoa hallintatoimenpiteiden toteuttamisesta ja kyberturvallisuusperiaatteiden täytäntöönpanosta, kuten mahdolliset turvallisuusauditointien tulokset ja niiden perustana oleva näyttö, toimijan itse tekemät riskiarvioinnit tai lokitiedot kyberuhkatapahtumista, jotka eivät sisällä 2 momentissa tarkoitettuja tietoja. Tiedonsaantioikeuden avulla viranomainen voisi esimerkiksi arvioida tietoja toimijassa käytettävästä riskienhallinnan toimintamallista sekä riskienhallinnan asianmukaisuudesta, kyberturvallisuutta koskevista koulutuksista ja niiden toteuttamisesta, havaintoja poikkeamista, kyberuhkista ja läheltä piti -tilanteista, tietoja tietoturvan toteutuksesta, poikkeamien hallinnan toteutuksesta sekä toiminnan ja palveluiden jatkuvuuden varmistamisesta. Edellytyksenä olisi, että tiedot olisivat tarpeen riskienhallintavelvoitteiden ja merkittävistä poikkeamista ilmoittamisen ja raportoinnin valvomista varten. Lisäksi viranomaisella olisi oikeus saada muut tiedot, jotka ovat välttämättömiä riskienhallintavelvoitteiden valvomista ja merkittävistä poikkeamista ilmoittamisen ja raportoinnin valvontaa varten.

Kyberturvallisuuden riskienhallintavelvoitteesta säädettäisiin 7–9 §:ssä sekä eräiden toimijoiden osalta niistä voitaisiin säätää myös NIS2-direktiivin nojalla annetuissa komission täytäntöönpanoasetuksissa. Lisäksi kyberturvallisuuden riskienhallintavelvoitteiden sisältöä voitaisiin tarkentaa valvovien viranomaisten määräyksillä. Tiedonsaantioikeus koskisi lisäksi merkittävien poikkeamien ilmoittamisen ja raportoinnin valvontaa siten kuin siitä säädetään 11–14 §:ssä. Merkittävällä poikkeamalla tarkoitettaisiin 11 §:n 1 momentissa tarkoitettua merkittävää poikkeamaa. Lisäksi komission täytäntöönpanoasetuksella voitaisiin tarkentaa merkittävän poikkeaman kynnystä eräille toimijoille.

Pykälän *2 momentissa* säädettäisiin 1 momenttia täydentävä erityissäännös 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. Laissa säädetty erillinen ja täsmällinen tiedonsaantioikeus näitä tietoja koskien olisi tarpeen viestinnän luottamuksellisuuden suojan edellyttämistä syistä. Momentissa säädettäisiin viestinnän luottamuksellisuuden suojan turvaamiseksi myös erityisestä salassapitovelvoitteesta momentin nojalla saatuihin tietoihin. Salassapitovelvollisuus olisi tarpeen sen johdosta, että julkisuuslain salassapitoperusteet eivät riittävästi suojaa viestinnän luottamuksellisuuden alaan kuuluvien tietojen salassapitoa. Lisäksi tiedot tyypillisesti kuuluisivat tiedon luovuttajalla sähköisen viestinnän palveluista annetun lain 136 §:n 4 momentin mukaisen vaitiolovelvollisuuden alaan, jolloin olisi perusteltua, että salassapito jatkuisi myös viranomaisessa viestinnän luottamuksellisuuden turvaamiseksi. Salassapitovelvollisuus ei koskisi sellaisia tietoja haitallisesta tietokoneohjelmasta tai IP-osoitteesta, joihin ei kohdistu laissa säädettyä salassapitovelvollisuutta tai muuta tiedon luovuttamista koskevaa rajoitusta ja jotka toimija voisi muutoinkin luovuttaa salassapitosäännösten tai tiedon luovuttamista koskevien rajoitusten estämättä. Muiden kuin 2 momentissa tarkoitettujen erityisen salassapitovelvoitteen piirissä olevien tietojen salassapito määräytyisi julkisuuslain mukaan.

Pykälän *3 momentin* nojalla 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. Tietojen toimittamisesta ei saisi aiheutua toimijalle kohtuuttomia kustannuksia esimerkiksi pyydetyn muodon teknisistä ominaisuuksista johtuen. Milloin teknisistä syistä tietojen toimittaminen olisi mahdotonta, toimija voisi täyttää velvoitteen antamalla valvovalle viranomaiselle pääsyn tietoihin muulla tavalla.

Jos tietopyyntö kohdistuisi sellaiseen osaan toimijan riskienhallinnasta, jonka toimija on ulkoistanut, toimija olisi velvollinen toimittamaan tiedon riippumatta siitä, onko tieto toimijan vai ulkoistetun tahon hallussa. Toimija olisi siten tarvittaessa velvollinen hankkimaan pyydetyt tiedot toimittajaltaan ja toimittamaan ne valvovalle viranomaiselle.

Pykälän *4 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. Edellytyksenä on lisäksi, että tiedon saaminen on laissa säädetyn tehtävän hoitamiseksi välttämätöntä. Lisäksi tiedonsaantioikeuden käyttämisellä tai tietojen luovuttamisella viranomaisten välillä ei saisi rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä. Muusta kuin välttämättömästä tietojen pyytämisestä tai luovuttamisesta olisi pidättäydyttävä ja tarpeettomat tiedot poistettava.

Pykälän *5 momentin* nojalla valvovan viranomaisen tiedonsaantioikeus ei kuitenkaan ulottuisi CSIRT-yksikön tämän lain nojalla tuottamiin palveluihin tai tietoihin toimijassa. Valvovan viranomaisen tiedonsaantioikeus ei siten ulottuisi esimerkiksi sellaisiin CSIRT-yksikön tuottamiin palveluihin eikä niissä kertyneisiin tietoihin tai muihin tietoihin, joita toimijasta olisi kertynyt 20 §:n 1 momentin 2 kohdassa tarkoitetussa avustamisessa, tietoturvaloukkausten havainnointipalvelussa tai muussa CSIRT-yksikön toiminnassa CSIRT-yksikölle tai tietoturvaloukkausten havainnointipalvelua toteuttavalle palvelukeskukselle. Säännös olisi välttämätön erityissäännös CSIRT-yksikön luottamuksellisen aseman turvaamiseksi ja sen toimijoille antaman tuen mahdollistamiseksi.

Pykälän *6 momentissa* säädettäisiin julkisen hallinnon tiedonhallinnasta annetun lain 18 i §:ksi ehdotettua 3 momenttia vastaavasta valvovan viranomaisen tiedonsaantioikeuden rajoituksista. Säännöksen mukaan pykälässä säädetty tiedonsaantioikeus ei velvoittaisi luovuttamaan valvovalle viranomaiselle salassa pidettäviä tietoja turvallisuusverkkolaissa tarkoitetusta turvallisuusverkon palvelutuotannosta tai palvelujen käytöstä eikä tietoja, joiden luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin niihin liittyvää tärkeää etua.

Säännös olisi merkityksellinen erityisesti tilanteessa, jossa pykälässä säädetty tiedonsaantioikeus kohdistuisi toiseen viranomaiseen. Säännöksen estämättä viranomainen voisi kuitenkin (vapaaehtoisesti ja harkintansa mukaan) luovuttaa julkisuuslain julkisuus- tai salassapito-olettaman sisältävän salassapitosäännöksen osoittamissa rajoissa valvovalle viranomaiselle tietoja myös turvallisuusverkon palvelutuotannosta ja palvelujen käytöstä sekä maanpuolustukseen ja kansalliseen turvallisuuteen liittyviä tietoja, jotka ovat yleisöltä salassa pidettäviä. Vaikka mainitut tiedot on lähtökohtaisesti rajattu valvovan viranomaisen tiedonsaantioikeuden ulkopuolelle, niitä voitaisiin viranomaisen harkinnan mukaan, kuten tähänkin asti, luovuttaa julkisuuslaissa sallitulla tavalla. Tämä mahdollisuus voisi tulla sovellettavaksi esimerkiksi silloin kun viranomainen haluaisi vapaaehtoisesti ilmoittaa 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. Tietojen luovuttamisella ei saa vaarantaa niitä etuja, joita salassapitosäännöksellä tai -säännöksillä suojataan. Tietojen luovuttamisessa on otettava huomioon myös turvallisuusluokiteltua tietoa koskeva lähtökohta, jonka mukaan turvallisuusluokitellun asiakirjan antamisesta päättää asiakirjan laatinut viranomainen (julkisuuslaki 15 § 3 mom). Näin ollen, jos viranomainen olisi luovuttamassa Liikenne- ja viestintävirastolle sen 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 edelleen 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.

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.

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.

Pykälän *2 momentissa* säädettäisiin valvovan viranomaisen mahdollisuudesta päätöksellä pyytää tarkastuksen suorittajaksi toinen viranomainen tai käyttää tarkastuksessa apuna muita asiantuntijoita, jos se on tarkastuksen laadun tai siihen liittyvien teknisten syiden vuoksi tarpeen. Muiden viranomaisten tai ulkopuolisten asiantuntijoiden käyttäminen voisi olla tarpeen esimerkiksi tilanteessa, jossa tarkastus edellyttäisi sellaista teknistä erityisosaamista tai laajoja teknologisia kyvykkyyksiä, mitä valvovalla viranomaisella ei itsellään olisi. Valvova viranomainen voisi pyytää tarkastuksen suorittajaksi vain toisen valvovan viranomaisen. Toisella valvovalla viranomaisella ei kuitenkaan olisi velvollisuutta antaa virka-apua tähän tarkoitukseen, vaan kyse olisi hallintolain 10 §:ssä tarkoitetusta viranomaisten yhteistyöstä. Lisäksi valvova viranomainen voisi käyttää tarkastuksessa apuna toista valvovaa viranomaista, tietoturvallisuuden arviointilaitosta tai ulkopuolista tietotekniikan asiantuntijaa. Valvova viranomainen ei kuitenkaan voisi siirtää tarkastustehtävää kokonaisuudessaan tietoturvallisuuden arviointilaitoksen tai ulkopuolisen asiantuntijan suoritettavaksi.

Tarkastuksen suorittajalla ja siihen osallistuvalla olisi oltava sellainen koulutus ja kokemus, kuin tarkastuksen suorittamiseksi on tarpeen. Viranomainen voisi tietoturvallisuuden arviointilaitokselle tai ulkopuoliselle asiantuntijalle osoitetussa toimeksiannossa määritellä, millaista pätevyyttä arviointilaitokselta tai asiantuntijalta edellytetään ja mitä kriteeristöä arviointilaitoksen tai asiantuntijan tulee käyttää. Tarkastuksen kohdistuessa yhteiskunnan

toiminnan kannalta kriittiseen infrastruktuuriin olisi harkittava turvallisuusselvityslaissa tarkoitetun henkilöturvallisuusselvityksen edellyttämistä tarkastuksen suorittajalta tai siihen osallistuvalta. Tietoturvallisuuden arviointilaitoksen tai muun ulkopuolisen asiantuntijan käyttämisessä olisi kyse tältä osin julkisen hallintotehtävän siirtämisestä yksityiselle ja tehtävää suorittavaan asiantuntijaan tulisi soveltaa rikoslain virkavastuuta koskevia säännöksiä. 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 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. Tietojen julkistamista koskeva määräys ei kuitenkaan saisi aiheuttaa toimijan turvallisuusjärjestelyille lisähaittaa, vaan julkaistavat tiedot olisi rajattava siten, että ne eivät vaaranna toimijan kriittisiä turvallisuusjärjestelyjä. Tietojen julkistamista koskevassa päätöksessä olisi tarkennettava, millä tavalla toimijan tulisi julkistaa kyseiset tiedot. Tietojen julkistaminen voisi tapahtua esimerkiksi tiedottamalla asiasta toimijan verkkosivuilla tai muissa viestintäkanavissa.

Pykälän *2 momentissa* säädettäisiin varoituksen antamisesta. Valvova viranomainen voisi antaa keskeiselle toimijalle varoituksen, jos kyseinen toimija ei ole noudattanut tätä lakia, sen nojalla annettuja määräyksiä tai NIS 2 –direktiivin nojalla annettuja säädöksiä. Varoitus voitaisiin antaa, ellei asia kokonaisuutena arvioiden antaisi aihetta ankarampiin toimenpiteisiin. Kyse olisi siten lähtökohtaisesti vähäisistä rikkomuksista. Valvova viranomainen antaisi varoituksen toimijalle. Varoituksen julkisuus valvovassa viranomaisessa määräytyisi julkisuuslain mukaan. 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 §. *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. Kiellon perusteena olisi toistuva ja vakava 10 §:ssä säädetyn velvoitteen rikkominen, mikä ilmenee toimijan puutteena tai laiminlyöntinä lain noudattamisessa. Kielto voisi kohdistua 10 §:ssä tarkoitettuihin henkilöihin, joita olisivat hallituksen jäsenet ja varajäsenet, hallintoneuvoston jäsenet ja varajäsenet sekä toimitusjohtaja tai muu siihen rinnastettava tehtävä. Kiellon määräämisen tulisi olla poikkeuksellinen ja viimesijainen toimenpide lainvastaiseen toimintaan puuttumiseksi. Ennen kiellon määräämistä valvovan viranomaisen olisi annettava toimijalle varoitus, jossa yksilöidään puute tai laiminlyönti, jonka korjaamatta jättäminen voi johtaa päätökseen johdon toiminnan rajoittamisesta. Lisäksi valvovan viranomaisen olisi varattava kohtuullinen määräaika lain vastaisen toiminnan korjaamiseksi ennen päätöstä johdon toiminnan rajoittamisesta. Kiellon 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 lainvastainen menettely toimijassa. Valvovan viranomaisen olisi kussakin yksittäistapauksessa arvioitava, onko toimintakielto tarkoituksenmukaisin valvontatoimenpide.

Johdon toiminnan rajoittamista koskeva päätös olisi aina määräaikainen. Päätös voisi olla voimassa enintään niin kauan, kuin sen perusteena oleva lainvastainen toiminta eli puute tai laiminlyönti toimijaan kohdistuvien velvoitteiden noudattamisessa on korjaamatta. Johdon toiminnan rajoittamista koskeva päätös voisi olla voimassa kuitenkin enintään viisi vuotta.

Johdon toiminnan rajoittaminen ehdotetun pykälän nojalla ei kuitenkaan olisi mahdollista, jos keskeinen toimija on yksityinen elinkeinonharjoittaja, henkilöyhtiö tai julkishallinnon toimija. Rajauksella käytettäisiin NIS2-direktiivin 32 artiklan 5 kohdan 3 alakohdan mukaista kansallista liikkumavaraa. Lain soveltamisalassa ei mainita julkishallinnon toimijoita, eivätkä nämä toimijat pääsääntöisesti kuuluisi lain soveltamisalaan, mutta eräissä tilanteissa on mahdollista, että laki soveltuisi myös julkishallinnon toimijaan. Myös julkishallinnon toimija voisi kuulua lain soveltamisalaan, mikäli tämä harjoittaa lain liitteissä tarkoitettua toimintaa. Esimerkiksi hyvinvointialueet ja –yhtymät sekä kunnat ja kuntayhtymät voisivat kuulua lain soveltamisalaan harjoittamansa terveyspalvelun tai vesi- ja jätehuollon palvelun myötä. Johdon toiminnan rajoittaminen ei olisi mahdollista, jos kyse olisi esimerkiksi terveyspalvelua tarjoavasta hyvinvointialueesta tai –yhtymästä taikka vesi- tai jätehuoltopalvelua tarjoavasta kunnallisesta viranomaisesta. Kunnallisella viranomaisella tarkoitettaisiin kunnan tai kuntayhtymän toimielimiä, kunnan liikelaitosta sekä kunnan taseyksikköä. Rajoitus koskisi kuitenkin vain julkishallinnon toimijoita, eli esimerkiksi vesihuoltopalvelua tarjoavan, kunnan omistaman osakeyhtiön johdon toimintaa voisi rajoittaa samalla tavalla, kuin muidenkin lain soveltamisalaan kuuluvien osakeyhtiöiden osalta. 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.

33 §. *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 tietosuoja-asetuksen 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.

34 §. *Uhkasakko, teettämisuhka ja keskeyttämisuhka.* Pykälässä säädettäisiin valvovan viranomaisen mahdollisuudesta asettaa antamansa päätöksen tehosteeksi uhkasakko, teettämisuhka tai keskeyttämisuhka. Hallinnollisen tehosteen asettamisesta ja täytäntöönpanosta säädetään uhkasakkolaissa.

35 §. *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. NIS2-direktiivin 34 artiklan 4 ja 5 kohdat edellyttävät, että toimijoille voidaan määrätä enimmäismäärältään vähintään 38 §:n mukainen seuraamusmaksu direktiivin 21 artiklassa tarkoitetun riskienhallintavelvoitteen tai 23 artiklassa tarkoitetun raportointivelvoitteen rikkomisesta. Jäsenvaltio voi kansallisen liikkumavaran piirissä säätää seuraamusmaksun perusteeksi myös muita tekoja tai seuraamusmaksun korkeammasta enimmäismäärästä.

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.

NIS 2 –direktiivin mukaisista velvoitteista julkishallinnolle säädettäisiin tiedonhallintalaissa eivätkä julkishallinnon toimijat pääsääntöisesti kuuluisi lain soveltamisalaan. Eräissä tilanteissa on mahdollista, että laki soveltuisi myös julkishallinnon toimijaan. Myös julkishallinnon toimija voisi kuulua lain soveltamisalaan, mikäli tämä harjoittaa lain liitteissä tarkoitettua toimintaa. Esimerkiksi hyvinvointialueet ja –yhtymät sekä kunnat ja kuntayhtymät voisivat kuulua lain soveltamisalaan harjoittamansa terveyspalvelun tai vesi- ja jätehuollon palvelun myötä. Hallinnollista seuraamusmaksua ei kuitenkaan voisi määrätä, lain soveltamisalaan kuuluvalle keskeiselle toimijalle, jos tämä on esimerkiksi terveyspalvelua tarjoava hyvinvointialue tai –yhtymä taikka vesi- tai jätehuoltopalvelua tarjoava kunnallinen viranomainen. Kunnallisella viranomaisella tarkoitettaisiin kunnan tai kuntayhtymän toimielimiä, kunnan liikelaitosta sekä kunnan taseyksikköä. Rajoitus koskisi kuitenkin vain julkishallinnon toimijoita, eli esimerkiksi vesihuoltopalvelua tarjoavan, kunnan omistamalle osakeyhtiölle hallinnollisen seuraamusmaksun voisi määrätä samalla tavalla, kuin muillekin lain soveltamisalaan kuuluville osakeyhtiöille.

Momentin tarkoituksena olisi rajata selkeästi seuraamusmaksun ulkopuolelle momentissa tarkoitetut julkisoikeudelliset toimijat. Mikäli momentissa tarkoitettuun julkisoikeudelliseen toimijaan sovellettaisiin muilta osin kyberturvallisuuslakia, sille ei kuitenkaan voitaisi määrätä pykälässä tarkoitettua seuraamusmaksua. Viranomaiseen kohdistettava hallinnollinen seuraamusmaksu ei aiheuta samanlaista vaikutusta kuin yksityisellä sektorilla, koska viranomaisen toiminta on budjettisidonnaista, ja viranomaisen on kaikissa tehtävissä hoidettava lakisääteiset tehtävänsä ja noudatettava lakia. Viranomaisia sitoo hallinnon lainmukaisuusperiaate ja viranomaisten on noudatettava hallinnon yleislakeja. Virkamiehen asemaan kuuluu myös virkavastuu työssä tehdyistä virheistä ja viranomaisen toiminnasta voidaan tehdä myös hallintokantelu ylemmälle viranomaiselle.

36 §. *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 Liikenne- ja viestintäviraston yhteydessä toimii seuraamusmaksulautakunta, joka määrää hallinnollisen seuraamusmaksun 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 liittäen esitykseen selvityksen 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 seuraamusmaksun määräämiseksi välttämättömät tiedot. Seuraamusmaksun määräämiseksi välttämättömiä tietoja voisivat tapauskohtaisesti esimerkiksi riskienhallintaa ja –raportointia koskevat tiedot, jotka valvovalla viranomaisella olisi oikeus saada 28 §:n nojalla, sekä muut tiedot, jotka olisivat välttämättömiä seuraamusmaksun perusteen ja määrän arvioimiseksi. Jäljempänä 37 §:ssä säädettäisiin seuraamusmaksun määrää koskevassa kokonaisarvioinnissa huomioon otettavista tiedoista. Lautakunnalla olisi voitava hankkia tieto seuraamusmaksun määräämistä koskevaan asiaan vaikuttavista seikoista seuraamusmaksun määräämiseksi tai määräämättä jättämiseksi.

37 §. *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 sen 34 artiklan 3 kohta edellyttää vähintään otettavan huomioon seuraamusmaksua määrättäessä.

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 oma-

aloitteisesti 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.

38 §. *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 27 §:n 2 momentin mukaisesti.

39 §. *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 säilyttämisestä 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.

40 §. *Seuraamusmaksun täytäntöönpano.* Pykälässä 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, lainvoiman saanut päätös on annettu. Seuraamusmaksusta ei tulisi periä viivästyskorkoa.

41 §. *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 23 §:ssä tarkoitettuun kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn.

Ehdotetussa *1 momentissa* säädettäisiin valvovan viranomaisen velvollisuudesta ylläpitää toimijaluetteloa valvontatoimialansa osalta.

Ehdotetussa *2 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 27 §:ssä tarkoitettu keskeinen toimija. Valvovalle viranomaiselle olisi ilmoitettava myös NIS2-direktiivin 29 artiklan 4 kohdan johdosta osallistumisesta 23 §: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. Mikäli toimijalla olisi käytössä sekä staattisia että dynaamisia IP-osoitteita, tulisi toimijan toimittaa valvovalle viranomaiselle tiedot vähintään staattisista IP-osoitteista, sekä pyrkiä toimittamaan dynaamisia IP-osoitteita koskevat tarkoituksenmukaiset tiedot, joita voivat olla esimerkiksi listaus verkkoblokeista tai –lohkoista, joista toimijan IP-osoite on varattu, sekä kyseisten osoitteiden lukumäärä, tai muu vastaava tarkoituksenmukainen tieto.

Ehdotetussa *3 momentissa* säädettäisiin DNS-palveluntarjoajien, aluetunnusrekisterin ylläpitäjien, 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 *4 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 *5 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 ja CSIRT-yksikön oikeudesta saada tietoja toimijaluettelosta. Siltä osin kuin muusta ei olisi säädetty, toimijaluettelon tietojen julkisuus määräytyisi julkisuuslain mukaan.

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 – pois lukien 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 pois lukien.

CSIRT-yksiköllä olisi oikeus saada valvovalta viranomaiselta tietoja toimijaluettelosta. CSIRT-yksikön tehtävien kannalta merkityksellisiä tietoja ovat erityisesti toimijoiden yhteystiedot ja IP-osoitealueita koskevat tiedot. Valvovia viranomainen voisi antaa CSIRT-yksikölle tietoja esimerkiksi avaamalla katseluyhteyden toimijaluetteloon tai toimittamalla tietoja teknisen rajapinnan välityksellä, mikäli se on teknisesti mahdollista käytettävässä järjestelmässä ja siten kuin julkisen hallinnon tiedonhallinnasta annetussa laissa säädetään.

NIS 2 -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 toimijoiden ohjeistamisessa ja neuvonnassa.

42 §. *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.

43 §. *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 26 §: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 artiklan 3 ja 4 kohdassa tarkoitetut tiedot, jotka koskevat varautumista ja viranomaisten toimintaa laajamittaisen kyberturvallisuuspoikkeaman tai –kriisin hallitsemiseksi. Säännöksellä säädettäisiin suunnitelman vähimmäissisällöstä eikä sen tarkoituksena olisi rajata, mitä tietoja suunnitelmaan voidaan sisällyttää. Säännöksen rajaamatta suunnitelma voisi olla itsenäinen ja erillinen taikka osa myös muuta viranomaisten valmius- ja varautumissuunnittelua. Suunnitelma olisi laadittava 1 momentissa tarkoitettujen viranomaisten yhteistyössä.

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.

44 §. *Kyberkriisinhallintaviranomainen.* Pykälässä säädettäisiin NIS2-direktiivin 9 artiklassa tarkoitetusta kyberkriisinhallintaviranomaisesta. Suomessa NIS2-direktiivin 9 artiklan 1 kohdan tarkoittamana kyberkriisinhallintaviranomaisena toimisi kukin 43 §:n 1 momentissa tarkoitettu viranomainen sille erikseen laissa säädettyjen tehtävien mukaisesti, eli laajamittaisten kyberturvallisuuspoikkeamien ja –kriisien hallintasuunnitelman laatimiseen osallistuvat viranomaiset. Näitä viranomaisia olisivat tässä laissa tarkoitetut valvovat viranomaiset, poliisi, suojelupoliisi, Puolustusvoimat, huoltovarmuuskeskus ja Liikenne- ja viestintävirasto. Kyberkriisinhallintaviranomaisten välisenä koordinaattorina toimisi Liikenne- ja viestintäviraston Kyberturvallisuuskeskus. Kyberkriisinhallintaviranomaisten tehtäviä, vastuita ja yhteistoimintaa täsmennettäisiin suunnitelmassa.

45 §. *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 valvovien 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 ja teledirektiivin mukaisen kansallisen sääntelyviranomaisen 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* 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 *4 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. Suomessa nämä tehtävät olisi osoitettu momentissa tarkoitetuille viranomaisille. Momentilla täytäntöönpantaisiin NIS2-direktiivin 13 artiklan 5 kohta osin.

46 §. *Muutoksenhaku.* Valvovan viranomaisen ja seuraamusmaksulautakunnan tämän lain nojalla antamaan päätökseen saisi hakea muutosta siten kuin oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019) säädetään.

Valvovan viranomaisen päätöstä olisi noudatettava muutoksenhausta huolimatta, ellei muutoksenhakuviranomainen toisin määrää. Valitusta käsittelevä tuomioistuin voisi kieltää tai

keskeyttää täytäntöönpanon tai antaa muun täytäntöönpanoa koskevan väliaikaisen määräyksen (HOL 123 §).

Muutoksenhaussa uhkasakon asettamista ja maksettavaksi tuomitsemista sekä teettämis- tai keskeyttämisuhan asettamista ja täytäntöönpantavaksi määräämistä koskevaan päätökseen olisi kuitenkin sovellettava myös muutoksenhaun osalta, mitä uhkasakkolaissa (1113/1990) säädetään.

47 §. *Voimaantulo.* Lain voimaantulo esitetään NIS2-direktiivin 41 artiklassa säädetyn kansallisen täytäntöönpanon määräaikaa vastaavasti 18. päiväksi lokakuuta 2024.

Lain 41 §:ssä tarkoitettujen ilmoitusten tekemiseen ehdotetaan kuitenkin siirtymäaikaa siten, että ensimmäinen ilmoitus tiedoista olisi tehtävä 31.12.2024 mennessä. Tarkoituksena olisi antaa 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 ja julkishallinnon toimiala, jolla tarkoitettaisiin direktiivin liitteen I kohdassa 10 tarkoitettua julkishallinnon toimialaa. Direktiivissä säädetyistä kyberturvallisuuteen liittyvistä velvoitteista ja niiden noudattamisen valvonnasta, mukaan lukien valvontatoimista, ja seuraamuksista julkishallinnon toimialalla säädettäisiin uudessa 4 a luvussa. Lisäksi ehdotettuun 2 momenttiin sisältyisi informatiivinen viittaus ehdotettuun kyberturvallisuuslakiin eli NIS2-direktiivin täytäntöönpanon yleislakiin. Aineellinen viittaus mainittuun lakiin sisältyisi ehdotettuun tiedonhallintalain 18 h §:ään, jossa säädettäisiin Liikenne- ja viestintäviraston tehtävistä julkishallinnon toimialan valvovana viranomaisena.

Viranomainen voi harjoittaa toimintaa myös muulla NIS2-direktiivin liitteen toimialalla, esimerkiksi kunnallinen viranomainen vesi- tai jätehuollon toimialalla. Tällöin viranomainen voi olla vain kyberturvallisuuslaissa tarkoitettu toimija, jos viranomaiseen ei tiedonhallintalain 3 §:n mukaan sovelleta tiedonhallintalain 4 a lukua. Viranomainen voi myös kuulua kummankin lain soveltamisalaan, esimerkiksi hyvinvointialue tai -yhtymä, joka harjoittaa toimintaa kyberturvallisuuslain liitteessä tarkoitetulla Terveys-toimialalla ja johon sovellettaisiin tiedonhallintalain 3 §:n mukaisesti myös tiedonhallintalain 4 a lukua. Mikäli julkishallinnon organisaatio kuuluisi samanaikaisesti sekä tiedonhallintalain että kyberturvallisuuslain soveltamisalaan, tulisi sen noudattaa sekä tiedonhallintalain 4 a lukua että kyberturvallisuuslaissa toimijalle asetettavia velvoitteita, jotka ovat keskeiseltä osin vastaavia. Kyberturvallisuuslaissa tarkoitettua hallinnollista seuraamusmaksua ei voitaisi määrätä lain 35 §:ssä tarkoitetulle julkishallinnon organisaatiolle, vaikka se kuuluisi muutoin lain soveltamisalaan.

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 ja kriittisen toimijan määritelmä sisältyvät direktiivin 6 artiklaan. Merkittävä poikkeama on määritelty direktiivin 23 artiklan 3 kohdassa. Kriittisen toimijan määritelmä perustuu NIS2-direktiivin 2 artiklan 3 kohtaan, jonka mukaan direktiiviä sovelletaan CER-direktiivin nojalla kriittisiksi toimijoiksi määritettyihin toimijoihin niiden koosta riippumatta.

Tiedonhallintalakiin ehdotetut uudet määritelmät vastaavat sisällöltään ehdotetun kyberturvallisuuslain 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 kyberturvallisuuslain säännöksissä, mutta on kuvattu lain 14 §:n säännöskohtaisissa perusteluissa. Merkittävällä kyberuhkalla tarkoitettaisiin direktiivin 6 artiklan 11 kohdan mukaisesti 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 *22 kohdassa* määriteltäisiin kyberriski. NIS2-direktiivissä ja kyberturvallisuuslaissa riski määritellään vastaavan sisältöisesti. Tiedonhallintalaissa kuitenkin käytetään käsitettä riski myös 13, 13 a, 28 c ja 28 f §:ssä, joiden asiayhteyteen NIS2-direktiivin mukainen riskin määritelmä ei sellaisenaan sovellu. Tästä syystä tiedonhallintalaissa määriteltäisiin sen 4 a luvussa hyödynnettäväksi riskin sijaan käsite kyberriski.

Ehdotetussa *24 kohdassa* määritelty merkittävä poikkeama on määritelty ehdotetun kyberturvallisuuslain 11 §:n 1 momentissa.

Ehdotetussa *26 kohdassa* määriteltäisiin kriittinen toimija, jolla tarkoitettaisiin viranomaista tai muuta julkista hallintotehtävää hoitavaa, joka on CER-direktiivin 2 artiklan 1 kohdassa tarkoitettu kriittinen toimija julkishallinnon toimialalla.

NIS2-direktiivin 2 artiklan 3 kohdan mukaan direktiiviä sovelletaan direktiivin CER-direktiivin nojalla kriittisiksi toimijoiksi määritettyihin toimijoihin niiden koosta riippumatta. NIS2-direktiivin 3 artiklan 1 kohdan f alakohdan mukaan kriittisiä toimijoita olisi pidettävä keskeisinä toimijoina.

Kriittisen toimijan käsitettä käytettäisiin tiedonhallintalain 3 §:ssä, jonka ehdotetun uuden 3 momentin kohdassa tarkoitettuun viranomaiseen ei sovellettaisi 4 a luvun NIS2-säännöksiä, ellei se olisi kriittinen toimija. Ehdotetulla 3 §:n 3 momentin (ehdotettujen muutosten jälkeen 4 momentin) muutoksella säädettäisiin valvovan viranomaisen toimivallan rajauksista, koskien myös eräitä muita perustuslain kannalta merkityksellisiä tahoja, siinä tapauksessa, että niihin sovellettaisiin 4 a lukua sen vuoksi, että ne olisivat kriittisiä toimijoita. Lisäksi 3 §:n 4 momentissa (ehdotettujen muutosten jälkeen 5 momentissa) säädettäisiin 4 a luvun soveltumisesta myös julkista hallintotehtävää hoitavaan yksityiseen henkilöön ja yhteisöön sekä muuna kuin viranomaisena toimivaan julkisoikeudelliseen yhteisöön, jos se on kriittinen toimija.

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 rajaukset.* Pykälän otsikkoon ehdotetaan kielellistä täsmennystä. Pykälää ehdotetaan muutettavan siten, että siihen lisättäisiin uusi *3 momentti*, jossa säädettäisiin niistä viranomaisista, jotka eivät olisi ehdotetun uuden 4 a luvun soveltamisalassa, ellei viranomainen olisi kriittinen toimija. Voimassa olevan 3 §:n 3 – 5 momentti siirtyisivät 4 – 6 momentiksi. Myös voimassa olevia 3 ja 4 momenttia (3 momentin lisäämisen jälkeen 4 ja 5 momentti) ehdotetaan muutettavaksi, samoin kuin Ahvenanmaata koskevaa pykälän 5 momenttia (3 momentin lisäämisen jälkeen 6 momenttia).

Pykälän *2 momenttiin* korjataan uuden kirkkolain säädöskokoelmanumero.

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.

Lakiin ehdotetun 4 a luvun soveltamisalan lähtökohtana on pykälän 1 momentin mukaisesti, että lain sääntelyä sovelletaan viranomaisiin, joilla tiedonhallintalaissa tarkoitetaan viranomaisten toiminnan julkisuudesta annetun lain (621/1999, jäljempänä *julkisuuslaki*) 4 §:n 1 momentissa tarkoitettuja viranomaisia. Lisäksi 1 momentin mukaan lain viranomaista koskevaa sääntelyä sovelletaan myös yliopistolaissa (558/2009) tarkoitettuihin yliopistoihin ja ammattikorkeakoululaissa (932/2014) tarkoitettuihin ammattikorkeakouluihin.

Ehdotetun 3 momentin sääntelyn perusteella 4 a lukua sovellettaisiin pykälän 1 momentin nojalla niihin tiedonhallintalain soveltamisalaan kuuluviin viranomaisiin, joita ei ole 3 momentissa erikseen rajattu pois luvun soveltamisalasta.

Ehdotettu sääntely kattaisi direktiivissä säädetyn vähimmäissoveltamisalan julkishallinnon toimijoiden osalta. Soveltamisalaan lukeutuisivat valtion virastoina myös valtion aluehallintoviranomaiset kuten aluehallintovirastot ja elinkeino-, liikenne- ja ympäristökeskukset, joita voidaan pitää kansallisen lainsäädäntömme mukaisesti direktiivissä tarkoitettuina keskustason julkishallinnon toimijoina. Soveltamisalaan kuuluisivat myös valtion liikelaitokset poislukien Puolustuskiinteistöt (ehdotettu 3 §:n 3 kohta).

Hyvinvointialueiden ja hyvinvointiyhtymien viranomaiset kuuluisivat myös 4 a luvun soveltamisalaan. Kunnalliset viranomaiset eivät kuuluisi lain soveltamisalaan lukuun ottamatta Helsingin kaupunkia sen hoitaessa hyvinvointialueiden järjestämisvastuulle lailla säädettyjä tehtäviä.

Vastaavasti soveltamisalaan kuuluisivat Suomen Pankkia lukuun ottamatta itsenäiset julkisoikeudelliset laitokset, joita ovat muun muassa Kansaneläkelaitos, Työterveyslaitos, Suomen riistakeskus, Suomen metsäkeskus, Keva ja Kuntien takauskeskus. 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 kansallisen lainsäädännön mukaisesti keskustason julkishallinnon toimijoiksi määritettyihin, joihin pääsääntöisesti on sovellettava direktiiviä.

Suomen itsenäisyyden juhlarahaston (Sitra) toimintaan sovelletaan Suomen itsenäisyyden juhlarahastosta annetun lain (717/1990) 19 §:n mukaan mm. mitä julkisuuslaissa säädetään.

Sitraa ei tiedonhallintalain yhteydessä pidetä julkisuuslain 4 §:n 1 momentissa tarkoitettuna viranomaisena ja Sitraan sovelletaan tiedonhallintalakia siten kuin 3 §:n 4 momentissa (esitettyjen muutosten jälkeen 5 momentissa) säädetään. Näin ollen myöskään tiedonhallintalain 4 a luku ei koskisi Sitraa.

Direktiivin 6 artiklan 35 kohdan mukaan julkishallinnon toimijan käsitteen ulkopuolelle jäävät kansalliset parlamentit. Lain 4 a lukua sovellettaisiin kuitenkin eduskunnan virastoihin julkisuuslain 4 §:n 1 momentin 6 kohdasta ja sen perusteluista ilmenevällä tavalla, sillä direktiivissä käytetyllä käsitteellä ”parlamentti” viitataan kansanedustuslaitoksen toimintaan, Suomessa eduskunnan valtiopäivätoimintaan. Julkisuuslaissa eduskunnan virastoilla ja laitoksilla on tarkoitettu samaa kuin eduskunnan virkamiehistä annetussa laissa (1197/2003). Lain 2 §:n 2 momentin mukaan eduskunnan virastoja ovat eduskunnan kanslia ja eduskunnan oikeusasiamiehen kanslia sekä eduskunnan yhteydessä olevat valtiontalouden tarkastusvirasto ja kansainvälisten suhteiden ja Euroopan unionin asioiden tutkimuslaitos, joka käyttää nimeä Ulkopoliittinen instituutti. Eduskunnan kirjasto on kuulunut vuodesta 2001 alkaen eduskunnan kansliaan. Pohjoismaiden neuvoston Suomen valtuuskunnalla on sihteeristö eduskunnan kanslian kansainvälisellä osastolla.

Julkisuuslakia ei sovelleta eduskunnan eikä sen toimielimien toimintaan, vaan niissä julkisuus määräytyy perustuslain ja eduskunnan työjärjestyksen mukaan. Julkisuuslaki ei siten koske eduskunnan täysistunnon ja valiokuntien toimintaa. (Olli Mäenpää: Julkisuusperiaate, Helsinki 2020, s. 135) Näin ollen myöskään tiedonhallintalaki tai sen 4 a luku ei koskisi eduskunnan valtiopäivätoimintaa. Perustuslakivaliokunnan lausunnossa PeVL 14/2018 vp hallituksen esityksestä esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi edellytettiin, että eduskunnan valtiopäivätoiminta tulee kokonaisuudessaan rajata sääntelyn soveltamisalan ulkopuolelle. Eduskunnan virastot kuuluvat muutoin tietosuojalain soveltamisalaan.

Ehdotetun uuden 3 momentin mukaan 4 a lukua ei siis sovellettaisi momentissa lueteltuihin viranomaisiin, ellei momentissa tarkoitettu viranomainen ole kriittinen toimija. Kriittisellä toimijalla tarkoitettaisiin viranomaista tai muuta julkista hallintotehtävää hoitavaa, joka yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain nojalla on määritetty julkishallinnon toimialan kriittiseksi toimijaksi. Ehdotetulla 3 momentilla lain 4 a luvun soveltamisalasta poissuljettuun toimijaan sovellettaisiin 4 a lukua, jos se on kriittinen toimija.

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-yksikön palveluja, joista - ja joihin liittyvästä tietojen käsittelystä - säädettäisiin kyberturvallisuuslaissa. 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.

Momentin *1 kohdan* mukaan lukua ei sovellettaisi tasavallan presidentin kansliaan, Puolustusvoimiin, poliisin hallinnosta annetussa laissa (110/1992) tarkoitettuihin poliisiyksikköihin, Rajavartiolaitokseen, Syyttäjälaitokseen eikä Tullin rikostorjuntaan. Poliisiyksikköjä ovat poliisin hallinnosta annetun lain 1 §:n mukaan Poliisihallitus ja sen alaiset yksiköt sekä suojelupoliisi.

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 perustelukappaleen 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”.

Perustuslain 110 §:n 1 momentin mukaan valtioneuvoston oikeuskanslerin ja eduskunnan oikeusasiamiehen toimivaltaan kuuluu myös mahdollisuus nostaa syyte laillisuusvalvonta-asioissaan. Lisäksi ylimmät laillisuusvalvojat ovat saman perustuslain kohdan perusteella perustuslaissa säädettyjä erityissyyttäjiä, jotka ovat yksinomaan toimivaltaisia tuomaria koskevissa virkarikosasioissa ja lisäksi syyttäjälaitoksesta annetun lain (32/2019) 27 §:n perusteella yksinomaan toimivaltaisia erityissyyttäjiä kaikissa syyttäjiä koskevissa virkarikosasioissa. Syyttäjälaitoksesta annetun lain 8 §:ssä todetaan myös valtioneuvoston oikeuskansleri ja eduskunnan oikeusasiamies erityissyyttäjinä. Kuten edellä todetaan, NIS-direktiivin johdanto-osan perustelukappaleen 8 mukaan direktiivin on tarkoitus kattaa laajasti julkishallinnon toimijat ja direktiivin soveltamisalan ulkopuolelle jätettäviä julkishallinnon aloja tulkitaan suppeasti. Tästä syystä ylimpien laillisuusvalvojien toimintaa syyttäjinä ei ole erikseen huomioitu 3 §:n soveltamisalarajauksissa. On myös huomioitava, että tällaisen rajauksen merkitys jäisi osin vähäiseksi ja epätarkoituksenmukaiseksi, kun yksinomaan toimenpiteitä erityissyyttäjän koskevien toimien erottaminen yleisestä koko viranomaisen kyberturvallisuutta koskevasta riskienhallinnasta ei ole direktiivin johdannon valossa perusteltua eikä tarkoituksenmukaista. Lisäksi on huomioitava, että ylimpien laillisuusvalvojien toimintaan ei sovellettaisi miltään osin valvontaa tai valvovan viranomaisen toimivaltuuksia. Näin ollen valvova viranomainen ei valvoisi näiden viranomaisten toimintaa erityissyyttäjänäkään miltään osin eikä ylimmillä laillisuusvalvojilla myöskään olisi velvollisuutta luovuttaa valvovalle viranomaiselle tietoja erityissyyttäjän tehtävässä.

Momentin *2 kohdan* mukaan lukua ei sovellettaisi tuomioistuimiin eikä valitusasioita käsittelemään perustettuihin lautakuntiin. Direktiivin 6 artiklan 35 kohdan mukaan julkishallinnon toimijan käsitteen ulkopuolelle jäävät kansalliset oikeuslaitokset.

Momentin *3 kohdan* nojalla luvun soveltamisalan ulkopuolelle jäisi Puolustuskiinteistöt, jonka toiminta lukeutuu direktiivin 2 artiklan 7 kohdassa tarkoitetulla tavalla pääosin maanpuolustukseen ja kansalliseen turvallisuuteen.

Ehdotetun *4 kohdan* perusteella lukua ei sovellettaisi kunnallisiin viranomaisiin lukuun ottamatta Helsingin kaupunkia, johon sovellettaisiin 4 a lukua sen hoitaessa hyvinvointialueiden järjestämisvastuulle lailla säädettyjä tehtäviä. Paikallishallinnon viranomaiset eli kunnat eivät ole direktiivin vähimmäissoveltamisalassa. Kuntien osalta on katsottu tarkoituksenmukaiseksi rajata ne soveltamisalan ulkopuolelle edellä kohdassa 5.1.3 tarkemmin selostetuin perustein. Tiedonhallintalain 4 a luvun soveltamisalaan kuuluisivat hyvinvointialueet ja hyvinvointiyhtymät, jotka olisi katsottava kansallisen lainsäädännön mukaisesti direktiivissä tarkoitetuiksi aluetason julkishallinnon toimijoiksi. Tämän vuoksi myös Helsingin kaupunki kuuluisi lain soveltamisalaan sen hoitaessa hyvinvointialueiden järjestämisvastuulle lailla 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 kyberturvallisuuslaissa. Lisäksi tiedonhallintalain 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.

Momentin *5 kohdan* mukaan 4 a lukua ei sovellettaisi Suomen Pankkiin, koska direktiivin 6 artiklan 35 kohdan mukaan julkishallinnon toimijan käsitteen ulkopuolelle jäävät keskuspankit.

Ehdotetun *6 kohdan* mukaan 4 a luvun sääntelyä ei sovellettaisi yliopistolaissa tarkoitettuihin yliopistoihin, ammattikorkeakoululaissa tarkoitettuihin ammattikorkeakouluihin eikä Pelastusopistoon, koska nämä eivät NIS2-direktiivin 2 artiklan 5 kohdan b alakohdan mukaan kuulu direktiivin vähimmäissoveltamisalaan.

Ehdotetun *7 kohdan* mukaan 4 a lukua ei sovellettaisi julkisen hallinnon turvallisuusverkkotoiminnasta annetussa laissa (10/2015), jäljempänä turvallisuusverkkolaki, tarkoitettuun turvallisuusverkon palvelutuotantoon eikä turvallisuusverkon palvelujen käyttöön. Rajaus perustuisi 1 kohdan perusteluissa mainitun direktiivin 2 artiklan 7 kohtaan. 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 1 momentin pääsäännön mukaan sovellettaisiin. Turvallisuusverkon palvelujen käytön osalta rajaus tarkoittaisi sitä, että ne turvallisuusverkon palvelujen käyttäjät (esimerkiksi 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. CER-direktiivin täytäntöönpanon yhteydessä on arvioitava, missä määrin turvallisuusverkon palvelutuotantoon tai palvelujen käyttöön on tarkoituksenmukaista soveltaa CER-sääntelyä ja sitä myötä myös tiedonhallintalain 4 a lukua. Valvovan viranomaisen tiedonsaantioikeutta koskevassa ehdotetussa 18 i §:ssä ehdotetaan kuitenkin, että säännöksessä tarkoitettu tiedonsaantioikeus ei koskisi turvallisuusverkkotoimintaan liittyviä salassa pidettäviä tietoja.

Ehdotetun *8 kohdan* nojalla 4 a lukua ei sovellettaisi viranomaisiin, jotka on perustettu yhdessä Euroopan talousalueen ulkopuolisen maan kanssa kansainvälisen sopimuksen mukaisesti eikä näissä maissa sijaitseviin diplomaattisiin edustustoihin tai konsuliedustustoihin taikka näiden verkko- ja tietojärjestelmiin, siltä osin kuin tällaiset järjestelmät sijaitsevat edustuston tiloissa tai niitä ylläpidetään kolmannessa maassa olevia käyttäjiä varten. NIS2-direktiivin perusteluosan johdantokappaleen 8 mukaan: ”Julkishallinnon toimijat, jotka on perustettu yhdessä kolmannen maan kanssa kansainvälisen sopimuksen mukaisesti, eivät kuulu tämän direktiivin soveltamisalaan. Tätä direktiiviä ei sovelleta jäsenvaltioiden kolmansissa maissa sijaitseviin diplomaattisiin edustustoihin ja konsuliedustustoihin tai näiden verkko- ja tietojärjestelmiin, siltä osin kuin tällaiset järjestelmät sijaitsevat edustuston tiloissa tai niitä ylläpidetään kolmannessa näissä maissa olevia käyttäjiä varten.”

Pykälän 3 momenttia (uuden 3 momentin lisäämisen jälkeen *4 momentti*) ehdotetaan muutettavan siten, että sen toiseksi viimeisen virkkeen mukaan valvovan viranomaisen valvontatoimivaltuuksia tai tiedonsaanti- ja tarkastusoikeutta ei sovellettaisi eduskunnan oikeusasiamiehen eikä valtioneuvoston oikeuskanslerin toimintaan. Sääntelystä kävisi selkeästi ilmi, ettei Liikenne- ja viestintävirastolle syntyisi valvontatoimivaltaa suhteessa ylimpiin laillisuusvalvojiin, Lisäksi valvovan viranomaisen valvontatoimivaltuuksia tai tiedonsaanti- ja tarkastusoikeutta ei sovellettaisi myöskään tasavallan presidentin kansliaan taikka tuomioistuinten tai valitusasioita käsittelemään perustettujen lautakuntien lainkäyttöön edes siinä tapauksessa, että mainittuun sovellettaisiin 4 a lukua kriittisenä toimijana. 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 tai lainkäyttöön (esim. PeVL 46/2010 vp ja PeVL 14/2028 vp). Perustuslakivaliokunnan lausunnossa PeVL 14/2018 vp hallituksen esityksestä esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi todetaan, että perustuslakivaliokunnan mielestä ylimpien laillisuusvalvojien valtiosääntöinen asema ja tehtävät sekä laillisuusvalvonnan valtiosääntöinen kokonaisuus eivät mahdollista asteellisesti alemman tietosuojavaltuutetun ylimpiin laillisuusvalvojiin kohdistuvaa valvontaa ja että tällaisen rajauksen on ilmettävä myös tietosuojalain säännöksistä nimenomaisesti.

Pykälän voimassa oleva 4 momentin sääntely siirtyisi *5 momentiksi*, jonka loppuun lisättäisiin maininta siitä, että 4 a lukua sovellettaisiin julkista hallintotehtävää hoitavaan yksityiseen henkilöön ja yhteisöön sekä muuna kuin viranomaisena toimivaan julkisoikeudelliseen yhteisöön, jos se on kriittinen toimija. Lisäksi momenttiin ehdotetaan vähäisiä kieliopillisia täsmennyksiä.

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, ellei 3 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 3 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.

4 a luku Kyberturvallisuutta koskevat velvollisuudet 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 kyberturvallisuuslaissa sisältyisivät lain 41 §: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. Näistä ilmoituksista komissiolle ja yhteistyöryhmälle säädettäisiin kyberturvallisuuslaissa. 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 toimialan 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 valvovalle viranomaiselle. Liikenne- ja viestintävirasto voisi esimerkiksi perustaa verkkosivuilleen digitaalisen palvelun tietojen ilmoittamiseksi.

Tiedonhallintayksikön olisi ilmoitettava tiedonhallintayksikön nimi, osoite, sähköpostiosoite, puhelinnumero ja muut ajantasaiset yhteystiedot sekä 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 kyberturvallisuuslain 23 §:ssä tarkoitettuun kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn.

Pykälän *3 momentin* mukaan tiedonhallintayksikön olisi viipymättä, viimeistään kahden viikon kuluttua muutoksesta, ilmoitettava kaikista muutoksista 2 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 §. *Velvollisuus hallita kyberturvallisuusriskejä 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 kyberturvallisuuslaissa tiedonhallintalakiin ehdotettua 18 b §:ää vastaavista NIS 2 –direktiivin riskienhallintavelvoitteista säädettäisiin lain 7 ja 8 ja 10 §:ssä, joiden säännöskohtaisissa perusteluissa on esitetty muun muassa direktiivin johdanto-osan perustelukappaleissa riskienhallinnasta todettua sekä muita soveltuvia esimerkkejä riskienhallinnan toteuttamiseen.

Pykälän *1 momentin* ensimmäisen virkkeen mukaan tiedonhallintayksikön olisi tunnistettava, arvioitava ja hallittava kyberriskejä, joita kohdistuu sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen 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 1 momentin toisen virkkeen mukaan kyberturvallisuuden riskienhallinnalla tulisi estää tai minimoida poikkeamien vaikutus toimintaan, toiminnan jatkuvuuteen, palvelujen vastaanottajiin ja muihin palveluihin. Ehdotetun 1 momentin kolmannessa virkkeessä todettaisiin, että tiedonhallintayksikön on toteutettava 18 c §:ssä tarkoitetut kyberturvallisuuden riskienhallintatoimenpiteet. Näiden toimenpiteiden oikeasuhtaisuudesta säädettäisiin edotetun 18 c §:n 2 momentissa.

Ehdotetun *2 momentin* mukaan tiedonhallintayksiköllä olisi oltava käytössä ajantasainen kyberturvallisuutta koskeva riskienhallinnan toimintamalli viestintäverkkojen ja tietojärjestelmien ja niiden fyysisen ympäristön suojaamiseksi poikkeamilta ja niiden vaikutuksilta. Toimintamallissa tulisi tunnistaa tiedonhallintayksikön viestintäverkkoihin ja tietojärjestelmiin sekä niiden fyysiseen ympäristöön kohdistuvat riskit kaikki vaaratekijät huomioivan lähestymistavan mukaisesti. Kyberturvallisuuden riskienhallinnan toimintamallissa olisi lisäksi määritettävä ja 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 1 momentin 1 kohdassa tarkoitetuissa 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.

Kyberturvallisuutta koskeva riskienhallinnan toimintamalli voisi olla myös osa toimijan laajempaa riskienhallintasuunnitelmaa, jossa huomioidaan myös muita toimintaan kohdistuvia riskejä tai osa muuta turvallisuusvarautumista.

Kyberturvallisuutta koskevien 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. Kyberturvallisuuden riskienhallinnan toimintamallin suhdetta tiedonhallintamalliin on käsitelty tarkemmin jaksossa 4.4.2. Tiedonhallinnan muutosvaikutukset.

Pykälän *3 momentin* mukaan tiedonhallintayksikön johto vastaisi kyberturvallisuutta koskevan 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 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 pormestarille. Itsenäisissä julkisoikeudellisissa laitoksissa johdolla tarkoitettaisiin kutakin laitosta koskevien säännösten perusteella määriteltyä johtoa, joka voi delegoida vastuitaan muulle johdolle.

Käytännössä johto vastaisi siitä, että kyberturvallisuutta koskeva riskienhallinnan toimintamalli on hyväksytty, ajantasainen ja sen toteuttamista valvotaan. Johto vastaisi siten siitä, että tiedonhallintayksikössä on järjestetty kyberturvallisuutta koskevan riskienhallinnan toteuttaminen ja valvonta. Lisäksi johto hyväksyisi riskienhallinnan toimintamallin ja sen tulisi järjestää sen toteuttamisen 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. Johdon vastuun ala täyttäisi rikosoikeudellisen laillisuusperiaatteen edellytyksen tarkkarajaisuudesta ja täsmällisyydestä.

18 c §. *Toimenpiteet kyberturvallisuutta koskevien riskien hallinnassa.* Pykälässä säädettäisiin direktiivin 21 artiklassa tarkoitetuista riskienhallintatoimenpiteistä. Pykälän *1 momentissa* säädettäisiin tiedonhallintayksikön velvollisuudeksi toteuttaa oikeasuhtaiset tekniset, operatiiviset ja organisatoriset kyberturvallisuuden riskienhallintatoimenpiteet sen käyttämien viestintäverkkojen ja tietojärjestelmien turvallisuuteen kohdistuvien kyberriskien hallitsemiseksi ja haitallisten vaikutusten estämiseksi tai minimoimiseksi.

Lisäksi 1 momentissa säädettäisiin vähimmäistoimenpiteistä, jotka on ainakin huomioitava ja pidettävä ajantasaisina kyberturvallisuuden riskienhallinnan toimintamallissa ja siihen perustuvissa kyberturvallisuuden riskienhallintatoimenpiteissä.

Direktiivin johdanto-osan perustelukappaleen 83 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 tiedonhallintayksiköitä, mukaan lukien 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 riskienhallinnan ja riskienhallintatoimenpiteiden asianmukaisuuden ja oikeasuhtaisuuden arviointia varten. Kuvaukset voitaisiin tallentaa esimerkiksi asiakastyötilaan, jossa pidetään saatavilla muitakin palvelujen kuvauksia kuten yleisen tietosuoja-asetuksen mukaisia vaikutusarviointeja.

Pykälän 1 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 kyberturvallisuutta koskevan 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 välittömien toimitusketjujen turvallisuudesta huolehtimista yhtenä riskienhallinnan toimenpidekokonaisuutena. Muun ohessa toimitusketjujen turvallisuudesta huolehdittaessa tulisi ottaa huomioon NIS2 –direktiivin 22 artiklan 1 kohdan mukaisesti tehtyjen kriittisiä toimitusketjuja koskevien koordinoitujen riskinarviointien tulokset. 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 NIS2-direktiivin 21 artiklan 3 kohdan mukaisesti ottaa huomioon koordinoitujen turvallisuusriskiarviointien tulokset soveltuvin osin.

Momentin *5 kohdan* mukaan riskienhallintatoimenpiteisiin kuuluisi omaisuudenhallinta ja sen 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 tietoturvakäytäntöjä toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi. Tietoturvakäytäntöjä ei vastaavalla tavalla yksityiskohtaisella tasolla luetella 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 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.

Ehdotetun 18 c §:n *2 momentissa* määriteltäisiin yleisellä tasolla, mitä on otettava huomioon riskienhallintatoimenpiteitä valittaessa, toteutettaessa ja kuvattaessa kyberturvallisuuden riskienhallinnan toimintamalliin. Säännöksen mukaan kyberturvallisuuden riskienhallintatoimenpiteiden tulisi olla ajantasaiset, asianmukaiset ja oikeasuhtaiset suhteessa tiedonhallintayksikön käyttämien viestintäverkkojen ja tietojärjestelmien riskialttiuteen, viestintäverkon tai tietojärjestelmän merkitykseen tiedonhallintayksikön toiminnalle sekä niissä ilmenevän poikkeaman kohtuudella ennakoitavissa oleviin välittömiin vaikutuksiin.

Lisäksi toimenpiteiden mitoittamisessa tulisi ottaa huomioon tiedonhallintayksikön koko, sen toiminnan laatu, poikkeaman todennäköisyys ja vakavuus, toimenpiteistä aiheutuvat kustannukset sekä ajantasainen kehitys huomioiden käytettävissä olevat tekniset mahdollisuudet torjua kyberuhka.

Pykälän *3 momentin* mukaan kyberturvallisuuden riskienhallinnassa, riskienhallinnan toimintamallissa ja riskienhallintatoimenpiteitä toteutettaessa olisi lisäksi noudatettava NIS 2 -direktiivin 21 artiklan 5 kohdan nojalla annettavia Euroopan komission täytäntöönpanosäädöksiä. Mainitun direktiivin kohdan mukaan komissio voi hyväksyä täytäntöönpanosäädöksiä, joilla vahvistetaan direktiivin 21 artiklan 2 kohdassa tarkoitettujen toimenpiteiden tekniset ja menetelmiin liittyvät vaatimukset sekä tarvittaessa alakohtaiset vaatimukset. Valvovan viranomaisen tehtävänä olisi tiedottaa tiedonhallintayksiköitä mahdollisten täytäntöönpanosäännösten valmistelusta ja olemassaolosta sekä ohjeistaa niiden noudattamisessa.

NIS2-direktiivin 24 artiklan 2 kohdan mukaan komissiolla on valta antaa direktiivin 38 artiklan mukaisesti delegoituja säädöksiä, joilla täydennetään tätä direktiiviä täsmentämällä, mitä keskeisten ja tärkeiden toimijoiden luokkia on vaadittava käyttämään tiettyjä kyberturvallisuuden sertifiointijärjestelmän mukaisesti sertifioituja TVT-tuotteita, TVT-palveluja ja TVT-prosesseja tai hankkimaan sertifiointi kyberturvallisuusasetuksen 49 artiklan nojalla hyväksytyn eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti. Tällaisia delegoituja säädöksiä annetaan, kun on havaittu, että kyberturvallisuus ei ole riittävän korkealla tasolla, ja niissä säädetään täytäntöönpanokaudesta. Ennen tällaisten delegoitujen säädösten hyväksymistä komissio tekee vaikutustenarvioinnin ja toteuttaa kuulemisia kyberturvallisuusasetuksen 56 artiklan mukaisesti. Mikäli komissio antaisi edellä kuvattuja delegoituja säädöksiä, olisi valvovan viranomaisen tiedotettava tiedonhallintayksiköitä

mahdollisten täytäntöönpanosäännösten valmistelusta ja olemassaolosta sekä velvoitettava delegoiduissa säädöksissä tarkoitetulla tavalla käyttämään tiettyjä sertifioituja TVT-tuotteita, TVT-palveluja ja TVT-prosesseja tai hankkimaan sertifiointi kyberturvallisuusasetuksen 49 artiklan nojalla hyväksytyn eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti.

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. Merkittäviä poikkeamia koskevasta ilmoitusvelvollisuudesta direktiivin liitteiden muiden toimialojen osalta säädettäisiin kyberturvallisuuslain 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 viipymättä, viimeistään 24 tunnin kuluttua siitä, kun se on tullut tietoiseksi merkittävästä poikkeamasta. Ensi-ilmoituksessa olisi ilmoitettava poikkeamasta, epäilläänkö merkittävän poikkeaman johtuvan rikoksesta taikka muusta 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 viipymättä, viimeistään 72 tunnin kuluttua siitä, kun viranomainen on tullut tietoiseksi merkittävästä poikkeamasta. Jatkoilmoituksessa olisi ajantasaistettava ensi-ilmoituksessa annetut tiedot ja esitettävä ensimmäinen arvio merkittävän poikkeaman laadusta, 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 edelleen jatkuu, 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. Valvova viranomainen voisi poikkeaman kestäessä pyytää viranomaiselta lisätietoja tai väliraportin asiaan liittyvistä tilannepäivityksistä ja käsittelyn etenemisestä.

Ehdotetun *5 momentin* mukaan merkittävän poikkeaman ilmoittamisessa olisi noudatettava lisäksi NIS 2 -direktiivin 23 artiklan 11 kohdan nojalla mahdollisesti annettavia Euroopan komission täytäntöönpanosäädöksiä ilmoituksen tietosisällöstä, muodosta ja ilmoitusmenettelystä sekä merkittävän poikkeaman tarkemmasta määrittelystä. Valvovan viranomaisen tulisi ohjeistuksessaan ja toiminnassaan ottaa huomioon mainitut täytäntöönpanosäädökset.

18 e §. *Poikkeamailmoituksen vastaanottaminen.* Pykälässä säädettäisiin valvovan viranomaisen eli Liikenne- ja viestintäviraston vastauksesta poikkeamailmoitukseen. Pykälä perustuu direktiivin 23 artiklan 5 kohtaan.

Valvovan viranomaisen olisi pykälän *1 momentin* mukaan viipymättä ja mahdollisuuksien mukaan 24 tunnin kuluessa 18 d §:n 1 momentissa tarkoitetun ensi-ilmoituksen vastaanottamisesta annettava viranomaiselle vastaus. Tämä ei kuitenkaan edellyttäisi valvovalta viranomaiselta 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. Pykälän *2 momentin* mukaan valvova viranomainen tekisi 1 momentissa tarkoitettujen ohjeiden ja operatiivisten neuvojen

antamisessa yhteistyötä kyberturvallisuuslaissa tarkoitetun CSIRT-yksikön kanssa. Ohjeet ja operatiiviset neuvot voisi valvovan viranomaisen sijaan antaa CSIRT-yksikkö. Ehdotetun kyberturvallisuuslain 17 §:n 1 momentin mukaan valvovan viranomaisen olisi toimitettava poikkeamailmoitukset ja raportit CSIRT-yksikölle välittömästi. CSIRT-yksikkö antaisi toimijan pyynnöstä ohjeita tai operatiivisia neuvoja vaikutuksia lieventävien toimenpiteiden osalta. Myös yleislain perustelujen perusteella valvova viranomainen ja CSIRT-yksikkö tekisivät yhteistyötä.

18 f §. *Vapaaehtoinen ilmoittaminen.* Pykälässä säädettäisiin viranomaisten ja muiden julkishallinnon toimijoiden mahdollisuudesta ilmoittaa valvovalle viranomaiselle myös vapaaehtoisesti poikkeamista, kyberuhkista ja läheltä piti-tilanteista. Pykälä perustuu direktiivin 30 artiklaan. Ehdotetussa kyberturvallisuuslaissa vapaaehtoisesta ilmoittamisesta säädettäisiin lain 15 §:ssä.

Direktiivin johdanto-osan perustelukappaleen 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 valvovalle viranomaiselle 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 valvovalle viranomaiselle.

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 kyberturvallisuuslain 17 ja 18 §:ssä ja näihin velvoitteisiin viitattaisiin ehdotetussa tiedonhallintalain 18 h §:n 3 momentissa.

Pykälän *2 momentin* mukaan valvovan viranomaisen olisi käsiteltävä vapaaehtoiset ilmoitukset 18 e §:ssä säädettyä menettelyä noudattaen, mutta se voisi asettaa etusijalle 18 d §:n ilmoitusvelvollisuuden perusteella tehtyjen 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 valvovalle viranomaiselle tietoja, jotka valvovalla viranomaisella on oikeus saada 18 i §:n nojalla.

Pykälän *4 momentin* mukaan vapaaehtoisessa ilmoittamisessa olisi noudatettava lisäksi NIS 2 -direktiivin 23 artiklan 11 kohdan nojalla mahdollisesti annettavia Euroopan komission täytäntöönpanosäädöksiä ilmoituksen tietosisällöstä, muodosta ja ilmoitusmenettelystä.

Valvovan viranomaisen tulisi ohjeistaa julkishallinnon toimijoita mahdollisten täytäntöönpanosäädösten sisällöstä.

18 g §. *Tiedotusvelvollisuus merkittävästä kyberuhkasta ja poikkeamasta.* Pykälässä säädettäisiin viranomaisen 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. Kyberturvallisuuslaissa 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 tiedottaminen yleisölle olisi yleisen edun mukaista, Liikenne- ja viestintävirasto voisi velvoittaa viranomaisen tiedottamaan merkittävästä poikkeamasta tai 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. Hallintolain 34 §:ssä säädetään asianosaisen kuulemisvelvoitteesta sekä edellytyksistä asian ratkaisemiselle asianosaista kuulematta.

Ehdotettuun 18 g §:n velvoitteet sisältyvät osin tiedonhallintalain 13 a §:n 1 momentissa säädettyyn tiedotusvelvollisuuteen. Lain 13 a §:n 1 momentin mukaan viranomaisen on viipymättä tiedotettava sen tietoaineistoja hyödyntäville, jos sen tiedonhallintaan kohdistuu häiriö, joka estää tai uhkaa estää viranomaisen tietoaineistojen saatavuuden. Viranomaisen on tiedotettava häiriön tai sen uhkan arvioidusta kestosta, mahdollisuuksien mukaan korvaavista tavoista hyödyntää viranomaisen tietoaineistoja sekä häiriön tai uhkan päättymisestä.

Koska NIS2-direktiivistä johtuvaa sääntelyä ei sovellettaisi kaikkiin niihin, joihin tiedonhallintalain 4 lukua ja sen 13 a §:ää sovelletaan, lisättäisiin NIS2-direktiivistä johtuva velvoite kuitenkin sellaisenaan 4 a lukuun. Tämä on myös tarpeen valvovan viranomaisen toimivallan kohdentamiseksi NIS2-direktiivin täytäntöön panemiseksi annetun sääntelyn noudattamisen valvontaan ja vain niihin joilla on velvollisuus sitä noudattaa.

Pykälän *4 momentin* mukaan 1 ja 2 momentissa tarkoitetussa tiedottamisessa olisi noudatettava lisäksi NIS 2 -direktiivin 23 artiklan 11 kohdan nojalla mahdollisesti annettavia Euroopan komission täytäntöönpanosäädöksiä ilmoituksen tietosisällöstä, muodosta ja ilmoitusmenettelystä sekä merkittävän poikkeaman tarkemmasta määrittelystä. Valvovan viranomaisen tulisi ohjeistaa viranomaisia mahdollisista täytäntöönpanosäädöksistä.

18 h §. *Valvova 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 eli ehdotetussa 4 a luvussa tarkoitettuna valvovana viranomaisena julkishallinnon toimialalla. Julkishallinnon toimiala määriteltäisiin 1 §:n 2 momentissa.

Ehdotetun 1 momentin toisen virkkeen mukaan valvovan viranomaisen tehtävänä olisi sen lisäksi mitä muualla 4 a luvussa säädetään (muun muassa poikkeamailmoitusten käsittelystä), valvoa 4 a luvussa ja NIS 2 – direktiivin nojalla annetuissa säädöksissä säädettyjen velvollisuuksien noudattamista julkishallinnon toimialalla sekä ylläpitää julkishallinnon toimialan toimijaluetteloa 18 a §:n nojalla toimitetuista tiedoista.

Lisäksi 1 momentissa säädettäisiin, että Liikenne ja viestintävirasto olisi valvovan viranomaisen toiminnassaan itsenäinen ja riippumaton. Valvova viranomainen olisi ratkaisu- ja muussa toiminnassaan riippumaton muiden tahojen kuten viranomaisten tai eri intressiryhmien samoin kuin ratkaistavana olevan asian osapuolten vaikutuksesta. Julkihallinnon toimialan valvovan viranomaisen riippumattomuudesta säädetään NIS2-drektiivin 31 artiklan 4 kohdassa.

Liikenne- ja viestintävirastolla ei, toisin kuin ehdotetun kyberturvallisuuslain mukaisella valvovalla viranomaisella, olisi määräyksenantovaltuutta. Sen sijaan Liikenne- ja viestintävirasto voi luonnollisesti laatia ohjeita ja suosituksia esimerkiksi 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.

NIS 2 –direktiivin nojalla annetuilla säädöksillä tarkoitettaisiin sen 21 artiklan 5 kohdan ja 23 artiklan 11 kohdan nojalla annettavia Euroopan komission täytäntöönpanosäädöksiä ja 24 artiklan 2 kohdan annettavia Euroopan komission delegoituja asetuksia.

Pykälän *2 momentin* mukaan valvova viranomainen voisi asettaa valvontatehtävänsä tärkeysjärjestykseen soveltaen riskiperusteista lähestymistapaa. Valvovan viranomaisen olisi valvontatoimiaan kohdentaessaan ja suorittaessaan sekä 18 l §:ssä tarkoitettua valvontapäätöstä tehdessään otettava huomioon kyberturvallisuuslain 27 §:n 3 momentissa ja 37 §:ssä säädetyt seikat eli NIS2 – direktiivin 32 artiklan 7 kohdassa säädetyt seikat, kuten mainitussa direktiivin kohdassa edellytetään. Viranomaisen valvonnan, eli toimijoihin kohdistettavien toimenpiteiden ja niiden määrän tulisi olla tällöin suhteellista ja perustua kyberturvallisuusriskien arviointiin. Direktiivin johdanto-osan perustelukappaleen 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, mikä tässä yhteydessä tarkoittaa lähinnä sitä, että tietyt julkishallinnon toimialan toimijat on näiden perustuslaissa säädetystä asemasta johtuen 3 §:ssä rajattu valvonnan ulkopuolelle. Direktiivissä sallitaan myös se, ettei tiettyjä seuraamuksia, kuten johdon toiminnan rajoittaminen ja hallinnollinen seuraamusmaksu, sovelleta julkishallinnon toimijoihin. Näin ollen näistä seuraamuksista ei säädettäisi tiedonhallintalaissa, jossa säädettäisiin valvonnasta ja seuraamuksista julkishallinnon toimialalla. Kyberturvallisuus lain seuraamussääntely soveltuu vain mainitun lain soveltamisalaan kuuluviin toimijoihin ja tiettyjä seuraamuksia ei sovellettaisi

viranomaisiin, mikäli ne harjoittavat lain soveltamisalaan kuuluvaa toimintaa eli toimivat jollain muulla direktiivin liitteissä tarkoitetulla toimialalla kuin julkishallinnon toimialalla.

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 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 kyberturvallisuuslakiin. Tiedonhallintalaissa säädettäisiin ainoastaan toimijoiden velvoitteista ja niiden noudattamisen valvonnasta mukaan lukien valvontatoimista sekä seuraamuksista NIS2 – direktiivin liitteen I 10 kohdassa tarkoitetulla julkishallinnon toimialalla. Muilta osin direktiivin sääntely pantaisiin täytäntöön ehdotetulla kyberturvallisuuslailla.

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 sekä Euroopan unionin toimielinten, erillisvirastojen ja yhteistyöelinten kanssa sekä tietojen luovuttamisessa niille noudatettava mitä kyberturvallisuuslain 6 §:n 4 momentissa, 15 §:n 3 momentissa, 17 §:ssä, 18 §:n 3 momentissa, 26 §:n 2 momentissa, 28 §:n 4 ja 5 momentissa, 33 §:ssä, 41 §:n 5 momentissa ja 45 §:ssä säädetään tietojen käsittelystä valvovassa viranomaisessa sekä valvovan viranomaisen yhteistyöstä NIS 2 – direktiivissä tarkoitettujen muiden viranomaisten sekä Euroopan unionin toimielinten, erillisvirastojen ja yhteistyöelinten kanssa sekä tietojen luovuttamisesta niille.

Ehdotetussa *4 momentissa* todettaisiin informatiivisesti, että Liikenne- ja viestintäviraston tehtävistä NIS 2 -direktiivissä tarkoitettuna keskistettynä yhteyspisteenä ja CSIRT yksikkönä säädettäisiin kyberturvallisuuslaissa. NIS 2 – direktiivissä tarkoitetusta keskistetystä yhteyspisteestä ja CSIRT-yksiköstä ja niiden tehtävistä, mukaan lukien tietojen käsittelystä sekä yhteistyöstä NIS 2 – direktiivissä tarkoitettujen muiden viranomaisten sekä Euroopan unionin toimielinten, erillisvirastojen ja yhteistyöelinten kanssa, säädettäisiin siis ainoastaan kyberturvallisuuslaissa.

18 i §. *Valvovan viranomaisen tiedonsaantioikeus*. Pykälässä säädettäisiin Liikenne- ja viestintäviraston tiedonsaantioikeuksista valvovana viranomaisena. 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 valvovassa viranomaisessa.

Pykälän *1 momentin* mukaan valvovalla viranomaisella olisi 4 a luvun mukaisia tehtäviä suorittaessaan oikeus saada salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä kyberturvallisuutta koskevien riskien hallintaa, riskienhallinnan toimintamallia, hallintatoimenpiteitä ja merkittävää poikkeamaa koskevat tiedot sekä muut edellä mainittuihin tietoihin välittömästi liittyvät tiedot, jotka ovat välttämättömiä kyberturvallisuutta koskevan riskienhallintavelvoitteen noudattamisen ja merkittävistä poikkeamista ilmoittamisen ja raportoinnin valvontaa varten. Viranomaisen olisi luovutettava tiedot viipymättä ja maksutta. Säännös ei koskisi välitystietoja, sijaintitietoja eikä tietoa haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä, joiden osalta tiedonsaantioikeudesta säädettäisiin 2 momentissa.

Valvovalla viranomaisella olisi oikeus saada näyttöä esimerkiksi kyberturvallisuuden riskienhallintaan liittyvien velvoitteiden noudattamisesta ja toteuttamisesta, sekä 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 pyrittävä hankkimaan pyydetyt tiedot toimittajaltaan. Valvovalla viranomaisella 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 valvovalla viranomaisella olisi salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada viranomaiselta välitystieto, sijaintitieto sekä tieto haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä, jos se on välttämätöntä kyberturvallisuutta koskevan riskienhallintavelvoitteen noudattamisen tai merkittävistä poikkeamista ilmoittamisen ja raportoinnin valvomista varten. Momentissa säädettäisiin viestinnän luottamuksellisuuden suojan turvaamiseksi myös erityisestä salassapitovelvoitteesta, joka koskisi 2 momentin nojalla saatuja tietoja. Salassapitovelvollisuus olisi tarpeen sen johdosta, että julkisuuslain salassapitoperusteet eivät riittävästi suojaa viestinnän luottamuksellisuuden alaan kuuluvien tietojen salassapitoa. Lisäksi tiedot tyypillisesti kuuluisivat tiedon luovuttajalla sähköisen viestinnän palveluista annetun lain 136 §:n 4 momentin mukaisen vaitiolovelvollisuuden alaan, jolloin olisi perusteltua, että salassapito jatkuisi myös viranomaisessa viestinnän luottamuksellisuuden turvaamiseksi. Salassapitovelvollisuus ei koskisi sellaisia tietoja haitallisesta tietokoneohjelmasta tai IP-osoitteesta, joihin ei kohdistu laissa säädettyä salassapitovelvollisuutta tai muuta tiedon luovuttamista koskevaa rajoitusta ja jotka toimija voisi muutoinkin luovuttaa salassapitosäännösten tai tiedon luovuttamista koskevien rajoitusten estämättä. Muiden kuin 2 momentissa tarkoitettujen tietojen salassapito määräytyisi julkisuuslain mukaan.

Pykälän *3 momentissa* säädettäisiin valvovan viranomaisen tiedonsaantioikeuden rajoituksista. Säännöksen ensimmäisen virkkeen mukaan pykälässä säädetty tiedonsaantioikeus ei velvoittaisi luovuttamaan valvovalle viranomaiselle salassa pidettäviä 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 estämättä viranomainen voisi kuitenkin (vapaaehtoisesti ja harkintansa mukaan) luovuttaa julkisuuslain julkisuus- tai salassapito-olettaman sisältävän salassapitosäännöksen osoittamissa rajoissa valvovalle viranomaiselle tietoja myös turvallisuusverkon

palvelutuotannosta ja palvelujen käytöstä sekä maanpuolustukseen ja kansalliseen turvallisuuteen liittyviä tietoja, jotka ovat yleisöltä salassa pidettäviä. Vaikka mainitut tiedot on lähtökohtaisesti rajattu valvovan viranomaisen tiedonsaantioikeuden ulkopuolelle, niin niitä voitaisiin viranomaisen harkinnan mukaan, kuten tähänkin asti, luovuttaa julkisuuslaissa sallitulla tavalla. Mahdollisuus voisi tulla sovellettavaksi esimerkiksi silloin kun viranomainen, johon 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. Tietojen luovuttamisella ei saa vaarantaa niitä etuja, joita salassapitosäännöksellä tai -säännöksillä suojataan. Tietojen luovuttamisessa on otettava huomioon myös turvallisuusluokiteltua tietoa koskeva lähtökohta, jonka mukaan turvallisuusluokitellun asiakirjan antamisesta päättää asiakirjan laatinut viranomainen (julkisuuslaki 15 § 3 mom). Näin ollen, jos viranomainen olisi luovuttamassa Liikenne- ja viestintävirastolle sen 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 edelleen 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.

Ehdotettu *4 momentti* sisältäisi informatiivisen viittauksen kansainvälisistä tietoturvallisuusvelvoitteista annettuun lakiin (588/2004). Erityissuojattavan tietoaineiston luovuttamisen edellytyksiä olisi siis arvioitava mainitun lain ja tietoaineistoon soveltuvan kansainvälisen tietotuvallisuusvelvoitteen perusteella.

18 j §. *Valvovan viranomaisen oikeus tehdä tarkastuksia.* Pykälässä säädettäisiin valvovan viranomaisen 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 valvovalla viranomaisella olisi siinä laajuudessa kuin se on tarpeen, oikeus tehdä 4 a luvussa tai NIS 2 – direktiivin nojalla annetuissa säännöksissä säädettyjen velvollisuuksien noudattamisen valvomiseksi viranomaiseen kohdistuva tarkastus. Tarkastus voitaisiin tehdä viranomaisen tiloissa tai tietojärjestelmässä. Tietojärjestelmässä tehtävä tarkastus voisi olla esimerkiksi teknisten riskienhallintakeinojen havainnointia taikka tietokantojen, laitteistojen, palomuurien, salauksen ja verkkojen heikkouksien tunnistamista. Viranomaisen tiloissa tapahtuva tarkastus voisi kohdistua esimerkiksi pääsynhallintaan ja tilaturvallisuutta koskeviin seikkoihin. Muuta viranomaisen 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. Kyberturvallisuuslaissa säädettäisiin erikseen CSIRT-yksikön haavoittuvuuskartoituksista ja niissä saatujen tietojen sallituista käyttötarkoituksista. valvovan viranomaisen tarkastukset voisivat olla säännöllisiä, satunnaistarkastuksia tai tapauskohtaisia (esimerkiksi merkittävän poikkeaman jälkeen). Tarkastukset voisivat olla suppeampia, tiettyyn aihealueeseen keskittyviä tai laajempia, toiminnan kokonaisvaltaisia tarkastuksia. Viranomaisen tulisi toimitusketjujensa osalta pyrkiä hankintasopimuksessa ottamaan huomioon valvovan viranomaisen tarkastusoikeus niin, että se on tarkoituksenmukaisella tavalla toteutettavissa myös alihankintatilanteissa.

Pykälän *2 momentin* mukaan tarkastuksen suorittajalla olisi oltava tarkastuksen laatuun ja laajuuteen nähden riittävä koulutus ja kokemus. Valvovan viranomaisen olisi varmistettava, että tarkastuksen suorittajalla on kyseisten tehtävien suorittamiseen vaadittavat taidot ja että tarkastus toteutetaan objektiivisesti.

Pykälän *3 momentin* mukaan viranomaisen olisi tarkastusta varten päästettävä tarkastusta suorittava tarkastuksen edellyttämässä laajuudessa tarkastuksen kohteena olevaan viestintäverkkoon tai tietojärjestelmään ja muihin kuin pysyväisluonteiseen asumiseen tarkoitettuihin tiloihin. Tarkastuksen suorittamiseksi tarkastuksen suorittajalla olisi 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 viranomaisen toteuttamat turvallisuusjärjestelyt. Valvovalla viranomaisella 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.

Pykälän 3 momentin loppuun sisältyisi viittaus 18 i §:n 3 momentin ehdotettuihin tiedonsaantioikeuden rajoituksiin, jotka soveltuisivat myös tarkastuksen suorittajan tarkastus- ja tiedonsaantioikeuteen.

Ehdotettu *4 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 perustelukappaleen 123 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.

18 k §. *Avustavan tehtävän antaminen tietoturvallisuuden arviointilaitokselle ja arvioinnin teettäminen.* Pykälässä säädettäisiin tietoturvallisuuden arviointilaitoksista annetussa laissa (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 tarkastustehtävässä avustavan tehtävän antaminen ja arvioinnin suorittaminen hyväksyttyihin tietoturvallisuuden arviointilaitoksiin.

Pykälän *1 momentin* mukaan valvova viranomainen voisi antaa 18 j §:ssä tarkoitettuun tarkastustehtävään liittyvän avustavan tehtävän arviointilaitoslaissa tarkoitetulle hyväksytylle tietoturvallisuuden arviointilaitokselle. Valvova viranomainen voisi antaa avustavan tehtävän tietoturvallisuuden arviointilaitokselle, jonka pätevyysalue olisi soveltuva avustavan tehtävän suorittamiseen.

Pykälän *2 momentin* mukaan valvova viranomainen voisi velvoittaa viranomaisen teettämään tietoturvallisuuden arviointilaitoksen suorittaman kyberturvallisuuden riskienhallintaan kohdistuvan arvioinnin, jos viranomaiseen on kohdistunut merkittävä poikkeama, joka on aiheuttanut palvelujen vakavan toimintahäiriön tai huomattavaa aineellista tai aineetonta vahinkoa taikka, jos viranomainen on olennaisesti ja vakavasti laiminlyönyt 18 b tai c §:ssä tarkoitettujen kyberturvallisuuteen kohdistuvien riskienhallintavelvoitteiden noudattamisen. Arvioinnin tilaisi arvioinnin kohteena oleva viranomainen, joka myös vastaisi arvioinnin kustannuksista. Mikäli arviointilaitosten palvelujen saannissa olisi viivettä, valvovan viranomaisen tulisi ottaa huomioon tämä arviointiin velvoittaessaan, esimerkiksi mikäli se asettaa arvioinnin teettämiselle jonkin määräajan.

Pykälän *3 momentin* mukaan tietoturvallisuuden arviointilaitoksen palveluksessa olevaan tarkastuksessa avustavaan henkilöön ja arvioinnin suorittajaan sovellettaisiin, mitä 18 j §:n 2–4 momentissa säädetään tarkastuksen suorittajan kokemuksesta ja koulutuksesta sekä tarkastuksen suorittajan oikeuksista. Tietoturvallisuuden arviointilaitoksen henkilöstön pätevyys varmistetaan lähtökohtaisesti silloin kun arviointilaitos hyväksytään arviointilaitoslain mukaisessa menettelyssä. Tietoturvallisuuden arviointilaitoksen palveluksessa olevalla tarkastuksessa avustavalla henkilöllä ja arvioinnin suorittajalla olisivat samat tarkastustoimivaltuudet ja tiedonsaantioikeudet kuin valvovan viranomaisen palveluksessa olevalla tarkastuksen suorittajalla.

Liikenne- ja viestintävirastolla valvovana viranomaisena 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 tai NIS 2 – direktiivin nojalla annetuissa säädöksissä säädettyjä velvoitteita.

Ehdotetussa 3 momentissa säädettäisiin myös ehdotetun 18 k §:n ja arviointilaitoslain välisen suhteen selkeyttämiseksi, että tietoturvallisuuden arviointilaitokseen sovellettaisiin muilta osin arviointilaitoslakia, esimerkiksi arviointilaitoslain 13 §:ää, jonka mukaan hyväksytyn tietoturvallisuuden arviointilaitoksen on arvioitilaitoslaissa tarkoitettuja tehtäviä hoitaessaan noudatettava hallintolakia, julkisuuslakia sekä kielilakia (423/2003). Lisäksi 3 momentissa säädettäisiin tietoturvallisuuden arviointilaitoksen palveluksessa olevan henkilön

rikosoikeudellisesta virkavastuusta ja momenttiin sisältyisi myös informatiivinen viittaus vahingonkorvauslakiin.

18 l §. *Seuraamukset.* Pykälässä säädettäisiin valvovan viranomaisen valvontapäätöksestä eli oikeudesta velvoittaa viranomainen toteuttamaan 4 a luvussa tai NIS 2 –direktiivin nojalla säädetyt velvoitteet. Pykälä perustuu NIS2 – direktiivin 32 artiklan 1, 4 ja 7 kohtaan.

Pykälän *1 momentin* mukaan valvova viranomainen voisi velvoittaa viranomaisen määräajassa korjaamaan puutteet tässä luvussa tai NIS2-direktiivin nojalla annetuissa säännöksissä säädettyjen velvollisuuksien noudattamisessa. Liikenne- ja viestintävirasto voisi myös velvoittaa viranomaisen julkistamaan kyseiset puutteet tai muut seikat, jotka liittyvät mainittujen velvollisuuksien rikkomiseen. Julkistamisella ei luonnollisesti tarkoitettaisi salassa pidettävien tietojen julkistamista, esimerkiksi niin että viranomaisen kyberturvallisuuden hallinta vaarantuisi julkistamisen johdosta. Liikenne- ja viestintävirasto voisi päätöksessään yksilöidä ne toimenpiteet, jotka on suoritettava poikkeaman ehkäisemiseksi tai korjaamiseksi 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 valvova viranomainen voisi antaa viranomaiselle varoituksen, jos viranomainen ei ole noudattanut 4 a luvussa tai NIS 2 -direktiivin nojalla annetuissa säännöksissä säädettyjä velvollisuuksia. Varoituksessa olisi yksilöitävä puute tai laiminlyönti, jota varoitus koskee. Varoitus olisi annettava kirjallisena.

Pykälän *3 momentissa* säädettäisiin Liikenne- ja viestintäviraston mahdollisuudesta asettaa uhkasakko valvontapäätöksen noudattamisen 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 luvan tai sertifioinnin 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, koska keskeyttämis- ja teettämisuhka eivät ole tarkoituksenmukaisia täytäntöönpanon tehosteita viranomaistoimintaan kohdistettuina. Uhkasakon määräämisessä noudatettaisiin uhkasakkolakia.

18 m §. *Muutoksenhaku.* Pykälän *1 momenttiin* sisältyisi informatiivinen viittaus muutoksenhakua koskevaan yleislakiin, lakiin oikeudenkäynnistä hallintoasioista.

Oikeudenkäynnistä hallintoasioissa annetun lain 122 §:n 1 ja 2 momentin mukaan päätöstä ei saa panna täytäntöön ennen kuin se on saanut lainvoiman. Valitus korkeimpaan hallinto-oikeuteen ei kuitenkaan estä päätöksen täytäntöönpanoa asiassa, jossa tarvitaan valituslupa. Täytäntöönpanoon ei tällöinkään kuitenkaan saa ryhtyä, jos valitus käy täytäntöönpanon johdosta hyödyttömäksi. Lain 122 §:n 3 momentin mukaan päätös voidaan panna täytäntöön lainvoimaa vailla olevana, jos laissa niin säädetään tai päätös on luonteeltaan sellainen, että se on pantava täytäntöön heti taikka päätöksen täytäntöönpanoa ei yleisen edun vuoksi voida

lykätä. Valvova viranomainen voisi tapauskohtaisesti harkita, onko syytä ja perusteita määrätä päätös pantavaksi täytäntöön heti. Oikeudenkäynnistä hallintoasioissa annetun lain 123 §:ssä säädetään muun muassa hallintotuomioistuimen oikeudesta kieltää päätöksen täytäntöönpano, määrätä täytäntöönpano keskeytettäväksi sekä oikeudesta antaa päätöksen täytäntöönpanoa koskevan muu määräys.

Pykälän *2 momentti* sisältäisi informatiivisen viittauksen uhkasakkolakiin, jonka 24 § sisältää erityisiä säännöksiä muutoksenhausta uhkasakon asettamista ja maksettavaksi tuomitsemista koskevaan päätökseen.

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 6 §:ään.

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 kyberturvallisuuslain 18 §: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 rekisteröity verkkotunnus sekä rekisteröintipäivä.

Säännökseen ehdotetaan lisättävän *uusi 2 momentti*, jonka nojalla 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. Mikäli tietojen epäiltäisiin olevan puutteellisia tai virheellisiä eikä verkkotunnusvälittäjä vastaisi kehotukseen todentaa tietoja oikeellisiksi, olisi tiedot jätettävä merkitsemättä rekisteriin. Liikenne- ja viestintäviraston olisi julkaistava käytössään olevat, käyttäjätietojen oikeellisuuden varmistamista koskevat toimintaperiaatteet ja menettelyt. Verkkotunnuksen rekisteröinnin estämistä täydentäisi voimassa olevan 169 §:n mukainen Liikenne- ja viestintäviraston toimivaltuus verkkotunnuksen poistamisesta rekisteröinnin

jälkeen, jos tiedot ovat puutteellisia tai virheellisiä ja tietoja ei kehotuksesta huolimatta korjata määräajassa.

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. Henkilötietojen osalta olisi otettava huomioon, mitä henkilötietojen luovuttamiseen viranomaisen ylläpitämästä rekisteristä säädetään erikseen julkisuuslain 16 §:n 3 momentissa. Julkisuuslaista poiketen Liikenne- ja viestintäviraston olisi vastattava verkkotunnusten rekisteritietoihin pääsyä koskevaan pyyntöön ilman aiheetonta viivytystä ja viimeistään 72 tunnin kuluessa pyynnön vastaanottamisesta. Mikäli Liikenne- ja viestintävirastolle toimitettu tietopyyntö olisi puutteellinen tai epäselvä siten, että sen perusteella ei voida arvioida, onko tietojen luovuttaminen tietosuojalainsäädännön mukaista tai muusta syystä epäselvä tavalla, joka estää asian ratkaisemisen, Liikenne- ja viestintäviraston olisi vastattava tietopyynnön esittäjälle ilman aiheetonta viivytystä ja viimeistään 72 tunnin kuluessa ja pyydettävä täydentämään tietopyyntöä puutteellisuuden tai epäselvyyden osalta. Liikenne- ja viestintäviraston olisi vastattava edelleen täydennettyyn pääsyä koskevaan pyyntöön ilman aiheetonta viivytystä ja viimeistään 72 tunnin kuluessa täydennyksen vastaanottamisesta. 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 teknisiä määräyksiä myös verkkotunnuksen käyttäjää koskevien tietojen varmistamisesta. Tällä tarkoitettaisiin esimerkiksi teknisiä toimintaperiaatteita ja menettelyjä, joilla verkkotunnusvälittäjät 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 oikeat, 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 kyberturvallisuuslakiin. NIS2-direktiivin soveltamisalaan kuuluvien DNS-palveluntarjoajien osalta velvollisuudesta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja poikkeamien ilmoittamisesta säädettäisiin jatkossa kyberturvallisuuslaissa. 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 kyberturvallisuuslakia.

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 kyberturvallisuuslaissa. 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 kyberturvallisuuslaissa. 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 kyberturvallisuuslain 18 §: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.

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.

342 §. *Oikaisuvaatimus.* Pykälän 2 momenttiin ehdotetaan lisättäväksi 167 §:n 2 momentissa tarkoitettu verkkotunnuksen rekisteröinnin estäminen sekä 169 §:n 1 momentissa tarkoitettu verkkotunnuksen poistaminen päätöksiksi, joista vaaditaan oikaisua siten kuin hallintolaissa säädetään. Verkkotunnuksien rekisteröintien suuren määrän johdosta olisi perusteltua noudattaa oikaisuvaatimusmenettelyä myös näissä momenteissa tarkoitettujen päätöksien osalta.

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 kyberturvallisuuslakiin 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), koska esitykseen sisältyy ehdotus myös turvatoimilain 7 e ja 7 f §:n kumoamisesta. 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 kyberturvallisuuslakiin 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 kyberturvallisuuslakiin 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 kyberturvallisuuslakiin 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 kyberturvallisuuslakiin 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 kyberturvallisuuslakiin sisältyisi jatkossa satamanpitäjiä koskevat vastaavat velvollisuudet.

Ehdotuksella kumoutuisi myös yhteiskunnan toiminnan kannalta merkittävistä lentoasemista ja satamista annettu valtioneuvoston asetus (361/2018), koska esitykseen sisältyy ehdotus myös ilmailulain 128 a ja 128 b §:n kumoamisesta. 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) 2022/2555 ja sen täytäntöönpanemiseksi ehdotettua kyberturvallisuuslakia 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 NIS 2 -direktiiviä.

NIS 2 -direktiiviä ja kyberturvallisuuslakia 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. Lisäksi lain 90 § sisältää sääntelyn tietojärjestelmän ja hyvinvointisovelluksen olennaisten vaatimusten poikkeamista sekä tietoverkkoihin ja käyttöympäristöihin kohdistuvista tietoturvallisuuden häiriöistä. Pykälän mukaan sekä tietojärjestelmien että tietoverkkojen ja käyttöympäristöjen poikkeamista tulee ilmoittaa valvontaviranomaiselle, jos poikkeama voi aiheuttaa merkittävän riskin tietoturvalle, tietojärjestelmien käytölle tai palveluiden toteuttamiselle.

Sosiaali- ja terveydenhuollon asiakastietojen käsittelyä koskeva sääntely koskee kaikkia sosiaali- ja terveydenhuollon palvelunantajia ja apteekkeja, ja lisäksi se koskee laajasti tietojärjestelmiä sekä käyttöympäristöjen ja tietoverkkojen tietoturvallisuutta eli sen soveltamisala on laajempi kuin kyberturvallisuuslaissa. Sosiaali- ja terveydenhuollon asiakastiedot ovat valtiosääntöisesti arkaluonteisia, yksityisyyden suojan piiriin kuuluvia tietoja, joten on välttämätöntä varmistaa mahdollisuus valvonnan keinoin puuttua niiden käsittelyssä käytettävien tietojärjestelmien, käyttöympäristöjen ja tietoverkkojen turvallisuuteen siten, että ilmoitusvelvollisuudet ja valvonta muodostavat eheän ja aukottoman kokonaisuuden. Asiakastietojen käsittelystä annetun lain ehdotetut muutokset ovat jatkumoa voimassa olevalle sosiaali- ja terveydenhuollon asiakastietojen käsittelyä koskevalle sääntelylle, jota NIS 2 –direktiivi ja kyberturvallisuuslaki täydentävät julkisten palvelunantajien sekä vähintään keskisuurten yksityisten toimijoiden osalta mahdollistaen tehokkaammat puuttumisen keinot kyseisten säädösten tarkoittamien merkittävien riskien osalta. Asiakastietolaki taas mahdollistaa häiriötilanteisiin puuttumisen mahdollisesti myös matalammalla kynnyksellä. Asiakastietojen käsittelystä annettu laki, NIS 2-direktiivi ja kyberturvallisuuslaki muodostavat kokonaisuuden, joka mahdollistaa asianmukaiset ja tarkoituksenmukaiset menettelyt eritasoisiin tietoturvallisuuden riskeihin puuttumiseen sosiaali- ja terveydenhuollon asiakastietojen osalta.

90 §. *Ilmoittaminen tietojärjestelmän ja hyvinvointisovelluksen olennaisten vaatimusten poikkeamista sekä tietoverkkoihin kohdistuvista tietoturvallisuuden häiriöistä.*

Pykälän *1 momenttia* muutettaisiin niin, että apteekkien tulisi ilmoittaa Sosiaali- ja terveysalan lupa- ja valvontaviraston lisäksi Lääkealan turvallisuus- ja kehittämiskeskukselle, jos tietojärjestelmän poikkeama voi aiheuttaa merkittävän riskin apteekin toiminnalle. Muutos

vastaisi muun lainsäädännön mukaisia kyseisten virastojen valvontatehtävien vastuita, ja olisi yhdenmukainen myös kyberturvallisuuslain mukaisten valvontavastuiden kanssa. Apteekkien valvonta kuuluu Lääkealan turvallisuus- ja kehittämiskeskuksen vastuulle, ja Sosiaali- ja terveysalan lupa- ja valvontavirasto vastaa tietojärjestelmien valvonnasta. Lääkealan turvallisuus- ja kehittämiskeskuksen on tärkeää saada tieto apteekkien toimintaan vaikuttavista häiriöistä, joilla voi olla esimerkiksi vaikutusta alueen lääkehuoltoon.

Pykälän *2 momenttiin* tehtäisiin muutokset siten, että määräyksenantovaltuus tietoturvallisuuden häiriön merkittävyydestä ja häiriötä koskevan ilmoituksen sisällöstä, muodosta ja toimittamisesta olisi Terveyden ja hyvinvoinnin laitoksen sijasta Sosiaali- ja terveysalan lupa- ja valvontavirastolla, joka myös vastaanottaa kyseiset ilmoitukset.

Pykälän *3 momentissa* säädettäisiin siitä, että apteekin olisi Sosiaali- ja terveysalan lupa- ja valvontaviraston lisäksi ilmoitettava Lääkealan turvallisuus- ja kehittämiskeskukselle viipymättä sellaisesta sen käyttämiin käyttöympäristöihin ja tietoverkkoihin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena apteekin toiminta voi merkittävästi vaarantua. Lääkealan turvallisuus- ja kehittämiskeskus voisi antaa tarkempia määräyksiä siitä, milloin apteekkeja koskeva häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta. Ilmoitus tulisi tehdä molemmille virastoille, koska käyttöympäristöjen ja tietoverkkojen häiriöt voivat tiiviisti liittyä tietojärjestelmiin, eikä häiriön alkuvaiheessa ole aina selvää, johtuuko häiriö tietojärjestelmästä, sen käyttöympäristöstä vai tietoverkoista.

Pykälän *3 momentti* siirtyisi uudeksi 4 momentiksi ja vanha *4 momentti* kumottaisiin tarpeettomana kyberturvallisuuslain ja tiedonhallintalain uuden 4 a luvun johdosta. Momenttia ehdotetaan täydennettäväksi siten, että apteekkien häiriötilanteiden osalta Lääkealan turvallisuus- ja kehittämiskeskus voi velvoittaa apteekin tiedottamaan yleisölle asiasta taikka kuultuaan ilmoitusvelvollista tiedottaa asiasta itse. Jos kyseessä on paikallinen häiriö, apteekki voi tiedottaa asiasta itse mutta Lääkealan turvallisuus- ja kehittämiskeskus voisi tiedottaa suuremmista, valtakunnallisista häiriöistä. Lisäksi vastaava velvoittamismahdollisuus olisi edelleen Sosiaali- ja terveysalan lupa- ja valvontaviranomaisella, joka voisi osana tietojärjestelmiin liittyvää valvontatehtäväänsä velvoittaa apteekin tiedottamaan tietojärjestelmään liittyvästä häiriöstä tai tiedottaa siitä itse.

7.10 Laki sähkömarkkinalain muuttamisesta

29 a §. *Verkonhaltijan velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen.* Pykälä ehdotetaan kumottavaksi, sillä verkonhaltijan velvollisuudesta huolehtia käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta säädettäisiin jatkossa ehdotetussa kyberturvallisuuslaissa.

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 kyberturvallisuuslakiin 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 20 kohta, jonka mukaan Energiavirasto hoitaisi tehtävät, jotka sille on säädetty kyberturvallisuuslaissa. Energiavirasto olisi yksi kyberturvallisuuslain 26 §:ssä tarkoitetuista valvovista viranomaisista.

7.13 Laki sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain muuttamisesta

2 §. *Soveltamisala.* Pykälään ehdotetaan lisättäväksi uusi 2 momentti, jonka nojalla lain 23 ja 24 §:ää sovellettaisiin lisäksi niiden tehtävien hoitamiseen, jotka Energiaviraston tehtäviksi säädetään kyberturvallisuuslaissa. Lisäys olisi tarpeen lain soveltamisalan selkeyttämiseksi uuden 23 §:ään lisättäväksi ehdotettavan 6 kohdan johdosta.

9 §. *Energiamarkkinaviraston toimivalta valvonta-asioissa.* Pykälään tehtäisiin lainsäädäntötekninen tarkennus 2 §:ään lisättävän uuden 2 momentin johdosta. Pykälän viittaus 2 §:ään muutettaisiin viittaukseksi 2 §:n 1 momenttiin. Muutos olisi lainsäädäntötekninen ja säännöksen asiasisältöä ei tarkoitettaisi muutettavan.

23 §. *Sähkö- ja maakaasuverkkoluvan peruuttaminen*. Pykälään ehdotetaan lisättäväksi uusi 6 kohta, jonka nojalla Energiavirasto voisi peruuttaa sähkö- tai maakaasuverkkoluvan silloin, jos luvanhaltija toistuvasti ja oleellisesti rikkoo kyberturvallisuuslaissa säädettyjä velvoitteita. Luvan peruuttaminen voisi tulla kyseeseen, jos kyberturvallisuuslain soveltamisalaan kuuluva toimija ei esimerkiksi ole laatinut kyberturvallisuuslain 8 §:ssä tarkoitettua kyberturvallisuuden riskienhallinnan toimintamallia ja lisäksi toimija on laiminlyönyt viranomaisen kehotuksen korjaavien toimenpiteiden toteuttamisesta. Ennen luvan peruuttamista Energiaviraston olisi annettava luvanhaltijalle varoitus luvan peruuttamisesta. Pykälällä täytäntöönpantaisiin osin NIS2-direktiivin 32 artiklan 5 kohdan ensimmäisen alakohdan a-alakohta.

Samalla pykälän 4 ja 5 kohtiin tehtäisiin tarvittavat lakitekniset muutokset.

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 kyberturvallisuuslain 28 §:ään 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 kyberturvallisuuslain 28 §:än sisältyisi jatkossa vastaava mahdollisuus luovuttaa salassa pidettävää tietoa toiselle viranomaiselle. Muutos olisi lainsäädäntötekninen, eikä säännöstä muutettaisi muilta osin.

7.15 Laki sakon täytäntöönpanosta annetun lain 1 §:n muuttamisesta.

1 §. *Lain soveltamisala.* Pykälän 2 momentin listaan lisättäisiin uusi 31 kohta, jonka nojalla kyberturvallisuuslaissa tarkoitetun hallinnollisen seuraamusmaksun pantaisiin täytäntöön siten kuin sakon täytäntöönpanosta annetussa laissa säädetään. Lisäys olisi lainsäädäntötekninen ja vastaisi kyberturvallisuuslaissa hallinnollisen seuraamusmaksun täytäntöönpanosta säädettyä.

Sakon täytäntöönpanosta annetun lain nojalla täytäntöönpantavat uudet hallinnolliset seuraamusmaksut on viime vuosina säännönmukaisesti lisätty 1 §:n 2 momentin listaan.

7.16 Laki maa-asemista ja eräistä tutkista annetun lain 8 §:n muuttamisesta

8 §. *Luvan muuttaminen ja peruuttaminen.* Pykälän 1 momentin 3 kohtaan lisättäisiin maininta kyberturvallisuuslaista. Kyberturvallisuus laissa on asetettu eräille maa-asemalaissa tarkoitetuille toiminnanharjoittajille velvoitteita, joiden olennainen laiminlyönti voisi johtaa luvan muuttamiseen tai peruuttamiseen. Kyberturvallisuuslaissa säädetyn velvollisuuden olennainen laiminlyönti voisi olla kyseessä esimerkiksi silloin, jos kyberturvallisuuslain soveltamisalaan kuuluva toimija ei ole laatinut kyberturvallisuuslain 8 §:ssä tarkoitettua kyberturvallisuuden riskienhallinnan toimintamallia ja lisäksi toimija on laiminlyönyt viranomaisen kehotuksen korjaavien toimenpiteiden toteuttamisesta.

Pykälällä täytäntöönpantaisiin osin NIS2-direktiivin 32 artiklan 5 kohdan ensimmäisen alakohdan a-alakohta

7.17 Laki vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annetun lain muuttamisesta

5 §. *Suhde muuhun lainsäädäntöön*. Pykälään lisättäisiin selvyyden vuoksi informatiivinen viittaus kyberturvallisuuslakiin.

109 a §. *Kyberturvallisuutta koskevien velvoitteiden laiminlyömisestä johtuva luvan peruuttaminen.* Pykälässä säädettäisiin valvontaviranomaisen toimivaltuudesta peruuttaa myöntämänsä toiminnanharjoittamista koskeva lupa osittain tai kokonaan, jos toiminnanharjoittaja olennaisesti ja vakavasti laiminlyö sille kyberturvallisuuslaissa säädettyjä velvollisuuksia. Kyberturvallisuuslaissa on asetettu eräille kemikaaliturvallisuuslaissa tarkoitetuille toiminnanharjoittajille velvoitteita toiminnan kyberturvallisuuteen liittyen. Kyberturvallisuuslaissa säädetyn velvollisuuden olennainen laiminlyönti voisi olla kyseessä esimerkiksi silloin, jos kyberturvallisuuslain soveltamisalaan kuuluva toimija ei ole laatinut kyberturvallisuuslain 8 §:ssä tarkoitettua kyberturvallisuuden riskienhallinnan toimintamallia. Ennen luvan peruuttamista valvontaviranomaisen olisi annettava toiminnanharjoittajalle riittävä määräaika asian korjaamiseksi. Pykälä koskisi vain toimintaa, jossa turvallisuus- ja kemikaalivirasto on valvova viranomainen 115 § mukaisesti.

Pykälällä täytäntöönpantaisiin osin NIS2-direktiivin 32 artiklan 5 kohdan ensimmäisen alakohdan a-alakohta

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 ja valvovan viranomaisen teknisellä määräyksellä. Lisäksi esitykseen sisältyy ehdotuksia lakia alemman asteisen sääntelyn ja sen antamisvaltuuden kumoamisesta.

Asetuksenantovaltuus

Esitykseen sisältyy ehdotus asetuksenantovaltuudesta, jonka nojalla valtioneuvoston asetuksella voitaisiin tarkentaa kyberturvallisuuslain 3 §:n 3 momentissa tarkoitettuja kriteerejä. Kriteereissä on kyse poikkeuksesta kyberturvallisuuslain soveltamisalaan kuuluvan toimijan yleiseen kokorajaan eräiden erityistilanteiden osalta. Tämä toteutettaisiin kyberturvallisuuslakiin ehdotetun 3 § 4 momentin valtuussäännöksellä nojalla, jonka mukaan valtioneuvoston asetuksella voitaisiin antaa tarkempia säännöksiä 3 §:n 3 momentissa tarkoitetuista kriteereistä.

Valtioneuvoston asetuksella voitaisiin siten täsmentää kriteerejä, jotka määrittävät lain soveltamiseen kuuluvia toimijoita. Edellytyksenä toimijan määritelmän täyttymiselle olisi siten, 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, jota valtioneuvoston asetuksella voitaisiin täsmentää, mikäli se säännöksen soveltamiseksi olisi tarpeellista.

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:

> 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;

Kyberturvallisuuslaissa säädettäisiin NIS2-direktiivin velvoitteista sen vähimmäissoveltamisalaan kuuluville toimijoille, joita näissä kohdissa tarkoitetut toimijat myös ovat. Nämä toimijat kuuluisivat poikkeuksellisesti toiminnan erityisen laadun vuoksi lain ja NIS2-direktiivin velvoitteiden soveltamisalaan koosta riippumatta. Ottaen huomioon kriteerien laatu, ilman kriteerien täsmentämistä yksittäisen pien- tai mikroyrityksen käytettävissä olevien tietojen varassa voi olla haasteellista arvioida riittävällä oikeudellisella varmuudella, koskeeko yritystä edellä tarkoitettu kriteeri. Lisäksi kriteerien täsmentäminen parantaisi oikeusvarmuutta niiden liitteissä I tai II tarkoitettua toimintaa harjoittavien yritysten osalta, joita kriteerit eivät koske. Näiden syiden johdosta lainsäädäntövallan siirto olisi lakiteknisesti tarpeellista. Lähtökohtaisesti soveltamisalan ulottaminen kuvattuihin toimijoihin olisi poikkeuksellista, toimijoiden joukko olisi harvalukuinen ja erityislaatuinen.

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 asetetaan laissa. Laissa säädettäisiin kriteereistä, joiden nojalla toimija kuuluisi sen soveltamisalaan. Asetuksenantovaltuutta koskeva säännös on arvioitu asianmukaiseksi ja tarkkarajaiseksi.

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.

Kyberturvallisuus lain 9 § 4 momentissa säädettäisiin toimialallaan valvovalle viranomaiselle valtuus antaa valvontatoimialallaan tarkempia teknisiä määräyksiä momentissa tarkoitetuista seikoista riskienhallinnan osalta. Valvova viranomainen voisi antaa toimialallaan riskienhallintavelvoitetta tarkentavia teknisiä määräyksiä toimialakohtaisista erityispiirteistä, jotka olisi otettava huomioon kyberturvallisuutta koskevassa riskienhallinnassa sekä kriittisiä toimitusketjuja koskevien unionin tason koordinoitujen riskinarviointien tuloksien huomioimisesta toimialakohtaisessa riskienhallinnassa. Tarkemmat määräykset voisivat kuitenkin koskea vain teknisiä seikkoja, eli niillä ei saisi laajentaa 9 §:ssä säädettyjä tai NIS 2 –direktiivin nojalla säädettyyn komission täytäntöönpanoasetukseen perustuvia velvoitteita tai asiallisesti muuttaa velvoitteiden sisältöä. Määräysten olisi oltava teknologianeutraaleja. Määräyksenantovaltuus olisi tarpeen, sillä mainituista riskienhallinnan toimialakohtaisista seikoista olisi 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.

Kyberturvallisuuslain 11 § 5 momentissa säädettäisiin valvovalle viranomaiselle valtuus antaa omalla toimialallaan tarvittaessa tarkentavia teknisiä määräyksiä, joilla tarkennetaan 11–15 §:n nojalla tehtävän ilmoituksen, tiedotuksen tai raportin tietosisältöä, teknistä muotoa tai menettelyä. Määräyksenantovaltuus on tarpeen, sillä määräyksillä voitaisiin säätää sektorikohtaisisesti merkityksellisistä seikoista yksityiskohtaisemmin ja sektoreiden erityispiirteet huomioiden sekä täsmentää velvoitetta NIS 2 –direktiivin nojalla säädetyn komission täytäntöönpanoasetuksen edellyttämällä tavalla.

Kyberturvallisuuslain 41 §:n 3 momentissa säädettäisiin valvovan viranomaisen oikeudesta antaa tarkempia teknisiä määräyksiä tietojen ilmoittamisesta toimijaluetteloa varten.

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 vastaavat säännökset sisältyisivät jatkossa kyberturvallisuuslakiin. NIS 1 –direktiivin sääntelyn johdosta viranomaisille annetut määräyksenantovaltuudet edellä luetelluissa laeissa kumottaisiin, koska poikkeaman merkittävyydestä ja ilmoituksen sisällöstä, muodosta ja toimittamisesta säänneltäisiin jatkossa kyberturvallisuuslaissa. Valvovan viranomaien määräyksenantovaltuus poikkeaman loppuraportin sisällöstä sekä merkittävien poikkeamien ja poikkeaman väliraportin ja loppuraportin mukaisten tietojen ilmoitusmenettelystä sisältyisi jatkossa kyberturvallisuuslain 11 §:n 5 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 kyberturvallisuuslakiin.

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 kyberturvallisuuslakiin.

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 kyberturvallisuuslakiin.

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 kyberturvallisuuslakiin.

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 kyberturvallisuuslakiin.

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 kyberturvallisuuslakiin.

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 kyberturvallisuuslakiin.

9 Voimaantulo

Ehdotetaan, että lait tulevat voimaan 18.10.2024.

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.

Ensimmäisen lakiehdotuksen 41 §:ssä tarkoitettujen ilmoitusten ja toisen lakiehdotuksen 18 a §:n 2 momentissa tarkoitettujen ilmoitusten tekeminen ehdotetaan kuitenkin tulevaksi voimaan siten, että ensimmäinen ilmoitus tiedoista olisi tehtävä viimeistään 31.12.2024. Tämä antaisi valvoville viranomaisille ja toimijoille lisää siirtymäaikaa toimijaluetteloon ilmoittautumista varten. NIS2-direktiivi ei edellytä viranomaisilta näiden ilmoituksien tietoihin perustuvien ilmoituksien tekemistä Euroopan komissiolle ja NIS-yhteistyöryhmälle 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. Kyberturvallisuuslaista toteutetaan jälkiarviointi vuosien 2026–2027 aikana.

Valtiovarainministeriö seuraa tiedonhallintalakiin ehdotetun julkishallinnon toimialan NIS2-sääntelyn vaikutuksia ja arvioi velvoitteiden soveltamisalan tarkoituksenmukaisuutta sekä velvoitteiden ja niiden noudattamisen valvonnan toteutumista.

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.

Kyberturvallisuusstrategia uudistettaisiin vuoden 2024 aikana. Kyberturvallisuusstrategia olisi päivitettävä viiden vuoden kuluessa sen hyväksymisestä. Laajamittaisten kyberturvallisuuspoikkeamien ja –kriisien hallintasuunnitelma olisi laadittava ensimmäisen kerran vuoden 2025 aikana.

11 Suhde muihin esityksiin

Esityksellä on yhteys kriittisten toimijoiden häiriönsietokyvystä annettuun Euroopan parlamentin ja neuvoston direktiiviin (CER-direktiivi, (EU) 2022/2557) ja sen kansallista täytäntöönpanoa koskevaan säädöshankkeeseen (SM047:00/2022). Hankkeen tiedot löytyvät Valtioneuvoston hankeikkunasta: https://valtioneuvosto.fi/hanke?tunnus=SM047:00/2022. CER-direktiivin kansallista täytäntöönpanoa koskeva hallituksen esitys on suunniteltu annettavaksi eduskunnalle keväällä 2024.

CER-direktiivin nojalla yhteiskunnan kriittisiksi toimijoiksi tunnistettaviin toimijoihin on sovellettava NIS2-direktiivin velvoitteita. Lisäksi CER-direktiivin ja NIS2-direktiivin nojalla säädetään direktiivissä tarkoitettujen toimivaltaisten viranomaisten yhteistyöstä ja tiedonvaihdosta näiden toimijoiden valvonnassa. CER-direktiivin kansallista toimeenpanoa koskevaan hallituksen esitykseen sisältyisi näiden syiden johdosta myös kyberturvallisuuslakia koskevia ehdotuksia, jotka liittyvät CER-direktiivin nojalla yhteiskunnan kriittisiksi toimijoiksi tunnistettaviin toimijoihin sovellettaviin velvoitteisiin ja viranomaisten yhteistyöhön.

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 keväällä 2024. 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. Näin ollen NIS2-direktiivin liitteessä I tarkoitetut pankkitoiminnan ja finanssimarkkinoiden infrastruktuurin toimijat eivät kuuluisi esitetyn kyberturvallisuuslain soveltamisalaan, sillä niitä koskisi vastaavien velvoitteiden osalta DORA-asetus ja sitä täydentävä kansallinen sääntely.

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 15 §:ssä turvattuun omaisuudensuojaan, perustuslain 18 §:ssä turvattuun elinkeinovapauteen, perustuslain 21 §:ssä turvattuun oikeusturvaan, perustuslain 80 §:ssä asetuksen antamisesta ja lainsäädäntövallan siirtämisestä säädettyyn sekä perustuslain 124 §:ssä hallintotehtävän antamisesta muulle kuin viranomaiselle säädettyyn.

12.1 Luottamuksellisen viestinnän suoja

Ehdotukseen sisältyy säännöksiä, jotka ovat merkityksellisiä perustuslain 10 §:ssä turvatun luottamuksellisen viestinnän suojan kannalta. Näitä ovat erityisesti 1. lakiehdotuksen 23 §:ään sisältyvä ehdotus CSIRT-yksikön koordinoimista kyberturvallisuustietojen vapaaehtoisista jakamisjärjestelyistä sekä 1. lakiehdotuksen 28 §:ään ja 2. lakiehdotuksen 18 i §:ään sisältyvät ehdotukset valvovan viranomaisen tiedonsaantioikeudesta. Ehdotuksissa on kyse muun ohella oikeudesta käsitellä sähköiseen viestintään liittyvää välitystietoa ja haitallisen tietokoneohjelman tai käskyn sisältävään viestiin liittyvää tietoa. Luottamuksellisen viestin suojan kannalta merkityksellinen on myös esityksen 21 §:ssä säädetty toimivaltuus yleiseen

viestintäverkkoon liitettyjen viestintäverkkojen ja tietojärjestelmien haavoittuvuuksien havainnoinnista.

Luottamuksellisen viestin suoja

Perustuslain 10 §:n mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu, ja henkilötietojen suojasta säädetään tarkemmin lailla Pykälän 2 momentin nojalla 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. Nämä mahdollisuudet rajoittaa luottamuksellisen viestinnän suojaa on tarkoitettu tyhjentäväksi luetteloksi (HE 309/1993 vp, s. 54, PeVM 25/1994 vp, s. 6 ja PeVL 33/2013 vp, s. 3). 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.

Perustuslain 10 §:n 2 momentin esitöiden mukaan säännöksen on suojata luottamuksellisena pidettävän viestin sisältö ulkopuolisilta puuttumisilta. Suojan kohteena on oikeus viestiä ja kommunikoida muiden kanssa ilman, että ulkopuoliset voivat saada oikeudettomasti tietoa lähetettyjen tai vastaanotettujen luottamuksellisten viestien sisällöstä sekä oikeus viestiä ulkopuolisten puuttumatta siihen rajoittavasti. Luottamuksellisen viestinnän suoja käsittää perinteisen kirjeenvaihdon lisäksi puhelinliikenteen sekä tiedonvälityksen tietoliikenneyhteyksiä ja sähköisiä viestintävälineitä käyttämällä. Perusteluissa todetaan myös säännöksen edellyttävän lainsäädäntöä, joka käytännössä tehokkaasti turvaa luottamuksellista viestintää sekä viranomaisten että muiden ulkopuolisten loukkauksilta (HE 309/1993 vp, s. 53-54). 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) 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.

Sähköisen viestin välitystiedot

Sähköisen viestin välitystietojen osalta perustuslakivaliokunta on vakiintuneessa käytännössään arvioinut viestien tunnistamistietojen, joista sittemmin on alettu käyttää termiä välitystieto, jäävän luottamuksellisen viestin salaisuuden ydinalueen ulkopuolelle. Tämän myötä perustuslakivaliokunta 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 ja PeVL 33/2013).

Perustuslakivaliokunta on kuitenkin sittemmin arvioinut, että EU:n tuomioistuimen oikeuskäytäntö on antanut perusteita jossain määrin arvioida uudelleen sähköisessä viestinnässä saatavien tunnistamistietojen suojaa luottamuksellisen viestin salaisuuden näkökulmasta. Sähköisen viestinnän käyttöön liittyvät tunnistamistiedot sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen voivat 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 36/2018 vp, s. 22 ja PeVL 18/2014 vp, s. 5–9).

Edellä esitetyt seikat ovat merkinneet, ettei perustuslain 10 §:n aikaisemmassa 3 momentissa ja nykyisessä 4 momentissa olevaa erityistä lakivarausta ole sellaisenaan sovellettu tunnistamistietojen salaisuuden rajoittamiseen. Tunnistamistietojen salaisuuden suojaan puuttuvan sääntelyn on kuitenkin täytettävä perusoikeuksien rajoittamisen yleiset rajoitusedellytykset (PeVL 62/2010 vp, s.4-5 ja PeVL 23/2006 vp, s. 3).

Haitallisen tietokoneohjelman tai käskyn sisältävä viesti

Esitykseen sisältyvien haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelyä koskevien ehdotuksien perustuslainmukaisuuden arvioinnin kannalta ratkaisevaa on tulkinta siitä, nauttiiko haitallisen tietokoneohjelman tai käskyn sisältävä viesti luottamuksellisen viestinnän suojaa perustuslain 10 §:n 2 momentin mukaisena luottamuksellisena viestintänä siten, että perustuslain 10 § momentissa olevaa erityistä lakivarausta on sellaisenaan sovellettava, vai onko kysymys suojan ydinalueen ulkopuolelle sijoittuvasta toiminnasta, jota on arvioitava perusoikeuksien yleisten rajoitusedellytysten mukaisesti. Kysymyksestä on niukasti lainvalmisteluasiakirjoja, perustuslakivaliokunnan aineistoa tai muuta tulkinta-aineistoa.

Luottamuksellisen viestin tai luottamuksellisen viestinnän sisällön tai soveltamisalan tarkempaa määritelmää ei sisälly perustuslain 10 §:n 2 momenttiin eikä tavalliseen lakiin. Viestin sisältö on sellaisenaan nauttinut perinteisesti vahvasti perusoikeussuojaa ja yksityisen viestin sisällön on tulkittu olevan viestinnän luottamuksellisuuden suojan ydinalueella (PeVL 36/2018 vp, s. 23). On kuitenkin arvioitavissa, että kaikki sähköinen viestien lähettäminen ja vastaanottaminen ei ilman muuta ole perusoikeussuojan kohteena olevaa luottamuksellista viestintää.

Luottamuksellisen viestin suojan kohteena on erityisesti viestin lähettäjän ja sen vastaanottajan välisen viestin semanttisen eli viestinnän osapuolien luoman sisällön pysyminen luottamuksellisena ja suojattuna ulkopuolisten puuttumiselta. Luottamuksellisen viestin suojan voidaan katsoa siten kohdistuvan edes jollain tavoin merkitykselliseen viestintään ja kommunikointiin luonnollisten henkilöiden välillä.

Luottamuksellisen viestin salaisuuden suojan ulkopuolelle perustuslakivaliokunnan käytännössä on rajattu viestinnän pääasiallisen luonteen vuoksi liikenteenohjauksessa syntyvä puhe- ja viestiliikenne (PeVL 62/2010 vp, s. 5). Lisäksi perustuslakivaliokunta on arvioinut, ettei esimerkiksi vieraan valtion sotilas- tai muu viranomaisorganisaation viestintä nauti luottamuksellisen viestinnän suojaa (PeVM 4/2018 vp, s. 7). Postinkulun varmistamiseksi eli viestin lähettäjän ja vastaanottajan viestinnällisten oikeuksien toteutumiseksi on lailla voitu säätää suljetun kirjeen avaamisesta (PeVL 56/2010 vp, s. 3-4 ja PeVL 30/2001 vp, s. 2-3).

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 sisältävässä viestissä kysymys on usein teknisestä käskystä, ohjelmasta tai komennosta, jolla pyritään aiheuttamaan haittaa viestintäverkon tai tietojärjestelmän toiminnalle. Kysymys voi olla tietokonejärjestelmien välisestä automatisoidusta ja teknisestä toimesta, jonka osapuolina ei ole luonnollisia henkilöitä tai jossa ei ole teknisten ominaisuuksien ohella lainkaan semanttista sisältöä. Kysymys voi olla myös automatisoidusti luodusta kalasteluviestistä, jonka tarkoituksena on saada kohde erehdytettyä suorittamaan toimi, joka mahdollistaa haitallisen tietokoneohjelman suorittamisen viestintäverkossa ja tietojärjestelmässä taikka viestintäverkon ja tietojärjestelmän suojauksen murtamisen. Haitallisen tietokoneohjelman tai käskyn sisältävä viesti on pääasiallisesti semanttista sisältöä vailla oleva tekninen koneiden välinen viesti taikka haitallisen tietokoneohjelman automaattisesti luoma tai kyberhyökkäystä suorittavan tahon ennalta tuntemattomalle ja hyvin laajalle vastaanottajajoukolle lähettämä kalasteluviesti. Haitallisen tietokoneohjelman tai käskyn sisältävässä viestissä ei ole kysymys viestinnän osapuolten välisestä luottamuksellisen viestinnän suojan ydinalaan perinteisesti kuuluvasta viestistä, jolla on yksilöityä semanttista tai kommunikatiivista merkitystä osapuolille. Haitallisen tietokoneohjelman tai käskyn sisältävän viestin lähettäjänä on taho, jonka pyrkimyksenä on toteuttaa kyberhyökkäys tai aiheuttaa haittaa viestintäverkon ja tietojärjestelmän toiminnalle tai järjestelmässä olevien henkilö- ja muiden tietojen luottamuksellisuudelle. Haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsitteleminen on usein välttämätöntä sen teknisten ominaisuuksien selvittämiseksi sekä yleisön varoittamiseksi vastaavasta toimesta. Haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelytarpeen tarkoituksena ei ole saada selkoa viestin semanttisesta sisällöstä, eikä tämänkaltaisen viestin sisällössä pääasiallisesti ole luottamuksellisen viestinnän suojan ydinalueeseen kuuluvaa henkilökohtaista, vain toisen osapuolen vastaanotettavaksi tarkoitettua viestintää.

Haitallisen tietokoneohjelman tai käskyn sisältävässä viestissä semanttinen tai kommunikatiivinen sisältö jää edellä todetulla tavalla hyvin vähäiseksi tai puuttuu kokonaan. Haitallisen tietokoneohjelman tai käskyn sisältävässä viestissä on kysymys yksipuolisesta toimesta, jonka tarkoituksena on pyrkiä toteuttamaan kyberhyökkäys tai teknistä haittaa viestintäverkolle tai tietojärjestelmälle. Vaikka kyberhyökkäyksen tai –häiriön toteuttamisen aiheuttamiseksi tähtäävää toimintaa voitaisiin sellaisenaan pitää viestinä, sen kuuluminen luottamuksellisen viestinnän perusoikeussuojan piiriin ei ole ilmeistä. Koska viestinnällinen ja kommunikatiivinen sisältö, tarkoitus ja merkitys joko puuttuvat kokonaan tai jäävät hyvin vähäiseksi, viestin ei voida katsoa kuuluvan ainakaan luottamuksellisen viestin suojan ydinalueelle, sikäli kun jaottelulle perusoikeussuojan reuna- ja ydinalueeseen on valtiosääntöoikeudellisia perusteita. Viesti voi jäädä kokonaan myös suoja-alueen ulkopuolelle. Luottamuksellisen viestinnän perusoikeussuojan soveltamisalan arvioinnille on perusteita erityisesti sähköisessä viestinnässä, sillä teknologian kehittyessä sähköisten viestien alaan luettavissa olevien erilaisten teknisten sisältöjen, komentojen, käskyjen ja viestien tekninen monipuolistuminen, käyttömahdollisuuksien laajentuminen, ja sähköisen viestinnän teknisten toteutumismuotojen ja –tapojen muutokset luovat tilanteita, joissa sähköisten viestien alaan luettavien toimien merkityksellisyys luottamuksellisen viestinnän perinteisesti suojaamien oikeushyvien kannalta eroavat toisistaan merkittävällä, olennaisella ja painavalla tavalla.

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 on 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, viestien 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.

Lisäksi oikeusjärjestelmässä yleisesti omaksutun shikaanikiellon ja oikeuksien väärinkäytön kiellon näkökulmasta voidaan argumentoida, että luottamuksellisen viestinnän suojaa ei tulisi tulkita tavalla, joka estäisi haittaohjelmaviestin teknisten tietojen käsittelemistä haittaohjelman ehkäisemiseksi, milloin luottamuksellisen viestinnän suojalla suojattaisiin toimintaa, jonka tarkoituksena on 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 ja siten pyrkiä ehkäisemään esimerkiksi tietomurtoja tai muita luottamuksellisen viestinnän suojaa vaarantavia kyberhyökkäyksiä. Kyberhyökkäykset voisivat toteutuessaan johtaa merkittäviin luottamuksellisen viestinnän suojan tai henkilötietojen suojan loukkauksiin. Oikeuksien väärinkäytön kiellosta säädetään esimerkiksi Euroopan unionin perusoikeuskirjan (2016/C 202/02) 54 artiklassa, jonka nojalla perusoikeuskirjan määräysten ei saa tulkita antavan oikeutta ryhtyä sellaiseen toimintaan tai tehdä sellaista tekoa, jonka tarkoituksena on tehdä tyhjäksi jokin tässä perusoikeuskirjassa tunnustettu oikeus tai vapaus tai rajoittaa sitä laajemmalti kuin tässä perusoikeuskirjassa on sallittu.

Edellä esitetyt seikat huomioon ottaen esityksen valmistelussa on päädytty arvioon, jossa kyberhyökkäyksen toteuttamiseksi luotu haitallisen tietokoneohjelman tai käskyn sisältävä viesti ei kuuluisi viestinnän luottamuksellisuuden suojan ydinalueelle, etenkään sen teknisten haittaohjelmaan liittyvien ominaisuuksien taikka automatisoidusti luodun sisällön osalta, viestinnän osapuoliksi luettavien luonnollisten henkilöiden välisen sisällön puutteen vuoksi. Näin ollen kysymys ei olisi perustuslain 10 §:n 2 momentissa tarkoitetusta luottamuksellisesta viestinnästä, eli sen käsittelystä voitaisiin säätää perustuslain 10 §:n 4 momentista riippumatta. Haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelyä koskevan sääntelyn perustuslainmukaisuutta olisi arvioitava perustuslain yleisten rajoitusedellytysten kautta siten, että sääntely on välttämätöntä, asianmukaista ja oikeasuhtaista sillä tavoiteltavien hyväksyttävien ja painavan yhteiskunnallisen tarpeen mukaisten tavoitteiden toteuttamiseksi.

Vapaaehtoiset kyberturvallisuustietojen jakamisjärjestelyt

Kyberturvallisuustietojen vapaaehtoisissa jakamisjärjestelyissä olisi kyse CSIRT-yksikön koordioimasta tiedonvaihtoyhteisöstä, jonka tarkoituksena olisi parantaa siihen osallistuvien yhteisöjen kykyä ehkäistä ja havaita kyberuhkia, hallita poikkeamia ja palautua niistä sekä lieventää niiden vaikutuksia. Jakamisjärjestelyyn osallistuminen perustuisi vapaaehtoisuuteen ja sitä koordinoisi viranomainen, eli CSIRT-yksikkö.

Tiedonvaihtoon osallistuva yhteisö sekä CSIRT-yksikkö saisivat luovuttaa muille jakamisjärjestelyyn osallistuvalle haitalliseen tietokoneohjelmaan tai käskyyn liittyvän välitystiedon taikka haitallisen tietokoneohjelman tai käskyn sisältävään viestiin liittyvää tietoa siltä osin kuin se liittyy haitallisen tietokoneohjelman tai käskyn teknisiin ominaisuuksiin ja

teknisiin jälkiin tai muuhun kyberuhkan tai poikkeaman toteuttamiseen liittyvään tekniseen tietoon. Jakamisjärjestelyyn osallistuva voisi käsitellä tällaista tietoa vain, mikäli se on tarpeen kyberuhkien ehkäisemiseksi, havaitsemiseksi, poikkeamien hallitsemiseksi ja niistä palautumiseksi sekä vaikutusten lieventämiseksi. Lisäksi CSIRT-yksikkö saisi käsitellä tietoja sille laissa säädettyä tehtävää varten. Edellytyksenä olisi, että tiedon luovuttaminen olisi välttämätöntä 23 §:n 1 momentissa säädettyä tarkoitusta varten, sillä tiedon luovuttamisella ei saisi rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä 1 momentissa säädettyä tarkoitusta varten.

Ehdotuksen tarkoituksena on tietoturvan parantaminen siten, että mahdollistetaan tiedon jakaminen haitallisista teknologioista ja siten edistetään yhteiskunnan mahdollisuuksia ehkäistä kyberturvallisuushäiriöitä, joilla voisi toteutuessaan olla laajoja ja vakavia haitallisia seurauksia. Aiemmin havaitun haitallisen tietokoneohjelman tai käskyn tietoja ja välitystietoja voitaisiin käyttää tietoturvan vaarantumista aiheuttavan toiminnan tunnistamiseen, vastaavalta haitallisen tietokoneohjelman tai käskyn sisältävältä viestiltä suojautumiseen ja sen teknisten ominaisuuksien selvittämiseen sekä poikkeaman vaikutusten lieventämiseen. Haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsitteleminen tässä tarkoituksessa on usein välttämätöntä.

Ehdotuksella pantaisiin täytäntöön NIS 2 –direktiivin 29 artikla, joka edellyttää jäsenvaltioita mahdollistamaan vapaaehtoisen tiedonvaihdon direktiivin soveltamisalaan kuuluvien toimijoiden välillä. Muiden kuin direktiivin soveltamisalaan kuuluvien toimijoiden osalta ehdotuksessa on kansallista liikkumavaraa.

Ehdotuksen tarkoittamassa käsittelytarkoituksessa voidaan todeta, että kyse ei ole sellaisesta tietojen kokoamisesta tai yhdistämisestä, jolla olisi merkittävä vaikutus yksityiselämän suojan kannalta. Kyse on välitystiedon käyttämisestä teknisenä tunnisteena yksittäiseltä kyberuhkalta, -poikkeamalta, haavoittuvuudelta tai uhkatoimijalta suojautumiseksi taikka häiriötä aiheuttavan viestinnän torjumista varten.

Ehdotuksen arvioidaan täyttävän perusoikeuksien yleiset rajoitusedellytykset, kun haitallisen tietokoneohjelman tai käskyn sisältävä viesti ei edellä kuvatulla tavalla nauti luottamuksellisen viestinnän suojaa sen ydinalueella. Ehdotuksessa on kyse täsmällisestä, tarkkarajaisesta ja oikeasuhtaisesta lain tasoisesta säännöksestä hyväksyttävää tarkoitusta, eli viestintäverkkoihin ja tietojärjestelmiin kohdistuvien kyberhyökkäysten, -uhkien ja merkittävien poikkeamien sekä niistä aiheutuvien haitallisten vaikutusten torjumiseksi yhteiskunnassa. Näin ollen ehdotuksen arvioidaan olevan siten perustuslain mukainen, että ehdotus voidaan käsitellä tavanomaisessa lainsäädäntöjärjestyksessä. Haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelyä koskevan ehdotuksen johdosta esityksestä olisi kuitenkin tarpeen pyytää perustuslakivaliokunnan lausunto.

Valvovan viranomaisen tiedonsaantioikeus

Ehdotuksen 28 §:n ja ehdotetun tiedonhallintalain 18 i §:n nojalla 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 riskienhallintaa koskevien velvoitteiden valvomista varten tai merkittävistä poikkeamista ilmoittamisen ja raportoinnin valvomista varten. Edellytyksenä olisi siten välttämättömyys viranomaiselle säädettyä valvontatehtävää varten. Välttämättömyys edellyttäisi, että tarkoitusta, jota varten näitä tietoja pyydettäisiin, ei

olisi saavutettavissa luottamuksellisen viestin ja yksityisyyden suojaan vähemmän puuttuvalla tavalla.

Valvovan viranomaisen olisi tietopyynnössä ilmoitettava pyynnön tarkoitus sekä täsmennettävä pyydetyt tiedot. Lisäksi tiedot olisivat erillisen salassapitovelvoitteen alassa. Valvovalla viranomaisella olisi kuitenkin salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa laissa säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto rajatulle viranomaisjoukolle. Asiakirjan tai tiedon voisi luovuttaa toiselle valvovalle viranomaiselle ja CSIRT-yksikölle, jos se on välttämätöntä viranomaiselle tässä laissa säädettyä tehtävää varten. Tiedonsaantioikeuden käyttämisellä tai tietojen luovuttamisella ei saisi rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.

Yleisesti arvioituna ehdotuksilla on ensisijaisesti luottamuksellisen viestin suojaa rajoittava vaikutus tiedonsaantioikeus- ja 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. Lisäksi sillä edistettäisiin osaltaan niiden oikeushyvien toteutumista yhteiskunnassa, joiden kannalta kulloisenkin viestintäverkon ja tietojärjestelmän häiriötön toiminta on merkityksellistä. Luottamuksellisen viestin suojaamista koskeva perusoikeusvaikutus olisi siten välillinen seuraus niistä toimenpiteistä, joita viranomaiset tietoturvaloukkauksen selvittämisen, ennaltaehkäisemisen ja vaikutusten poistamisen yhteydessä tekevät.

Tiedonsaantioikeuden käyttämisellä tai tietojen luovuttamisella ei saisi rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä. Tämä edellyttäisi, että haitallisen tietokoneohjelman tai käskyn sisältävät viestit kyetään yksilöimään ja erottamaan tehokkaasti, jolloin perustellusti luottamuksellisen viestin salaisuutta nauttivaan viestintään ei tahattomasti kohdistettaisi viranomaistoimenpiteitä, eikä luottamuksellisen viestin salaisuuden suojaa niin ollen myöskään rajoitettaisi perusteettomasti.

Ehdotuksen tarkoittamassa käsittelytarkoituksessa voidaan todeta, että kyse ei ole sellaisesta tietojen kokoamisesta tai yhdistämisestä, jolla olisi merkittävä vaikutus yksityiselämän suojan kannalta. Viranomaisen ei olisi valvontatehtävänsä suorittamiseksi välttämätöntä pyytää tai luovuttaa välitystietoja, sijaintitietoja tai haitallisen tietokoneohjelman tai käskyn sisältäviä viestejä yleisesti, kohdentamattomasti tai säännönmukaisesti, vaan kyse olisi pääosin yksittäisiin kyberuhkiin, -poikkeamiin, haavoittuvuuksiin tai uhkatoimijoihin liittyvistä tiedoista.

Edellä esitetyin perustein haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelyn arvioidaan jäävän viestinnän luottamuksellisuuden suojan ydinalueen ulkopuolelle, kun otetaan huomioon siitä ja välitystiedoista edellä esitetty. Käsittelyn arvioidaan täyttävän perusoikeuksien yleiset rajoitusedellytykset, kun huomioidaan käsittelyn tarkoitus ja tavoite suhteessa rajoituksen laatuun ja merkittävyyteen. Lisäksi NIS 2 –direktiivin täytäntöönpano edellyttää näiden tietojen käsittelemisen mahdollisuutta valvovassa viranomaisessa valvontatehtävän suorittamiseksi. Ehdotus täyttäisi myös muilta osin perusoikeuksien yleiset rajoitusedellytykset. Näin ollen tiedonsaantioikeutta ja tietojen vaihtoa viranomaisten välillä 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.

Haavoittuvuuskartoitus

Ehdotuksen 21 §:ään sisältyy ehdotus CSIRT-yksikön toimivaltuudesta suorittaa yleiseen viestintäverkkoon liitettyjen viestintäverkkojen ja tietojärjestelmien verkkopohjaista haavoittuvuuksien havainnointia. Havainnoinnin tarkoituksena olisi haavoittuvien tai turvattomasti määritettyjen viestintäverkkojen ja tietojärjestelmien asetuksien havaitseminen ja havainnoista asianomaisille tahoille ilmoittaminen. Havainnot perustuisivat yleisessä viestintäverkossa olevien tietojen havainnointiin. Toimivaltuuden taustalla on painava peruste kyberuhkiin varautumiseksi ja kyberhyökkäyksistä aiheutuvien haitallisten vaikutuksien torjumiseksi yhteiskunnassa. CSIRT-yksikön kyky havaita yleisesti saatavilla oleva 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, edistäisi merkittävästi vakavilta tietoturvaloukkauksilta suojautumista haavoittuvuuksilta.

Haavoittuvuuskartoitus olisi sallittua toteuttaa vain ei-intrusiivisella tavalla. Ehdotuksen säännöskohtaisissa perusteluissa kuvatulla tavalla se tarkoittaisi, ettei haavoittuvuuskartoituksessa saisi aiheuttaa haittaa kartoituksen kohteena olevan järjestelmän tai palvelun toiminnalle eikä tunkeutua viestintäverkkoon tai tietojärjestelmään tai hankkia pääsyä niissä käsiteltäviin tietoihin. Haavoittuvuuskartoituksen teknistä toteuttamistapaa on käsitelty tarkemmin pykälää koskevissa säännöskohtaisissa perusteluissa. Ehdotus ei mahdollistaisi tunkeutumista viestintäverkkoihin tai tietojärjestelmiin vaan kyse on yleiseen viestintäverkkoon avoinna olevien laitteiden ja tietojärjestelmien teknisten tietojen havainnoinnista. Haavoittuvuuskartoituksessa ei saisi aiheuttaa sen kohteena olevan tietojärjestelmän tai palvelun toiminnalle haittaa eikä haavoittuvuuskartoituksella saisi hankkia tietoa yleisessä viestintäverkossa tai yleisesti saatavilla olevassa viestintäpalvelussa välitettävänä olevasta viestinnästä. Haavoittuvuuskartoituksessa voitaisiin havainnoida tai kartoittaa vain viestintäverkkoja ja tietojärjestelmiä. Haavoittuvuuskartoituksella ei siten olisi sallittua hankkia ja käsitellä luottamuksellisen viestinnän suojaamia tietoja, kuten välitystietoja tai viestin sisältöä, ellei CSIRT-yksikkö käsittelisi viestinnän osapuolen roolissa omaa viestintäänsä. Haavoittuvuuskartoituksessa tai kohdennetussa haavoittuvuuskartoituksessa ei saisi käsitellä sähköisten viestien sisältöä ja pykälän 5 momentin nojalla CSIRT-yksikön olisi hävitettävä saamansa tiedot, kun ne eivät ole enää tarpeen laissa säädettyjen tehtävien hoitamiseksi.

Perusoikeuksien yleisten rajoitusedellytysten kannalta ehdotus täyttää täsmällisyyden ja tarkkarajaisuuden vaatimuksen. Ehdotus sisältää useita toimintaa rajaavia tekijöitä. Ensinnäkin toiminta on rajattu yleisesti saatavilla oleviin viestintäverkkoihin ja tietojärjestelmiin eli ehdotus rajaa toiminnan ulkopuolelle muun muassa yksityiset verkot. Toiminnan tarkoitus on rajattu haavoittuvien tai turvattomasti määritettyjen viestintäverkkojen ja tietojärjestelmien asetusten 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 rajattu edellä kuvatulla tavalla siten, että se täyttää kokonaisuudessaan oikeasuhtaisuuden vaatimuksen.

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, miten haavoittuvuuskartoituksella havaittua tietoa voidaan käyttää. 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 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.

Haavoittuvuuskartoituksessa ei saisi käsitellä tai hankkia tietoja yleisessä viestintäverkossa tai yleisesti saatavilla olevassa viestintäpalvelussa välitettävänä olevasta viestinnästä. Selvyyden vuoksi todetaan, että sen ohella, että vaikka haavoittuvuuskartoituksessa ei säännöksen nojalla saisi käsitellä sähköisten viestien sisältöä tai välitystietoa, ei sähköisten viestien tai välitystiedon käsitteleminen olisi teknisesti mahdollista, jos haavoittuvuuskartoitus toteutetaan teknisesti säännöksen edellyttämällä tavalla. Lisäksi ehdotuksessa säädettäisiin täsmällisesti ja tarkkarajaisesti haavoittuvuuskartoituksella hankittavien tietojen käyttötarkoituksesta ja tarpeettomien tietojen poistamisesta. Ehdotus täyttäisi perusoikeuksien yleiset rajoitusedellytykset. Edellä esitetyin perustein haavoittuvuuskartoitusta koskevan ehdotuksen arvioidaan olevan perustuslain asettamien edellytysten mukainen.

12.2 Julkisen hallintotehtävän antaminen muulle kuin viranomaiselle ja viranomaisen suoritteen maksullisuus

Ulkopuolisen asiantuntijan käyttäminen apuna tarkastuksessa

Kyberturvallisuuslain 29 §:n nojalla valvova viranomainen voisi tehdä toimijaa koskevan tarkastuksen käyttäen apunaan tarkastuksen suorittamisessa tietoturvallisuuden arviointilaitosta tai ulkopuolista tietotekniikan asiantuntijaa, jos se on tarkastuksen laadun tai siihen liittyvien teknisten syiden vuoksi tarpeellista. Myös 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. Valvova viranomainen ei myöskään voisi siirtää tehtävää kokonaisuudessaan tietoturvallisuuden arviointilaitoksen tai ulkopuolisen asiantuntijan suoritettavaksi, vaan vastuu tarkastustehtävän suorittamisesta säilyisi valvovalla viranomaisella myös silloin, kun se olisi päättänyt käyttää tarkastuksessa apuna tietoturvallisuuden arviointilaitosta tai ulkopuolista asiantuntijaa. 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 tietoturvallisuuden arviointilaitoksen tai ulkopuolisen asiantuntijan käyttäminen olisi mahdollista vain, jos tarkastuksen laatu tai siihen liittyvät tekniset syyt sitä edellyttävät. Käytännössä ehdotus koskisi siis tilannetta, jossa tarkastuksen tarkoitus kohdistuisi sellaisiin seikkoihin, joiden tarkastaminen vaatisi sellaista teknistä erityisosaamista tai poikkeuksellista osaamista, jota viranomaisella itsellään ole hallussa. Lisäksi ehdotus koskisi sellaisia tilanteita, joissa tarkastuksen suorittaminen edellyttäisi merkittäviä resursseja, joita valvovalla viranomaisella ei ole jatkuvasti käytettävissään.

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 kyberturvallisuuslain 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/I, PeVL 67/2002 vp, s. 5/I ja PeVL 2/2002 vp, s. 2/II). 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 kyberturvallisuuslain 29 §:n 2 momentissa ja tiedonhallintalain 18 j §:n 2 momentissa säädetään, että tarkastajalla tulee olla tarkastustehtävään nähden sellainen koulutus ja kokemus, joka on tarpeen tarkastuksen suorittamiseksi. Tämä pätevyysvaatimus koskee myös sellaista tietoturvallisuuden arviointilaitosta ja ulkopuolista asiantuntijaa, jota voitaisiin käyttää tarkastuksessa apuna 29 §: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 kyberturvallisuuslain 29 §:n 1 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 julkisuuslain 4 §:n 2 momentin mukaisesta toimijasta.

Perustuslain 124 §:n mukaan merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan antaa vain viranomaiselle. Ehdotetuissa kyberturvallisuuslain 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.

12.3 Elinkeinonvapaus

Toimijoiden ilmoittautumisvelvollisuus valvovalle viranomaiselle

Esitykseen sisältyy ehdotus soveltamisalaan kuuluvien toimijoiden velvollisuudesta ilmoittaa valvovalle viranomaiselle kyberturvallisuuslain 45 §: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 kyberturvallisuuslain soveltamisalaan kuuluvat toimijat ja mahdollistaisi valvonnan kohdentamisen näihin toimijoihin.

Kyberturvallisuuslain 41 §:n mukaan toimijoiden olisi ilmoitettava valvovalle viranomaiselle 41 §:n 2 momentin a-g kohdissa listatut tiedot toimijaluettelon ylläpitämiseksi. Näiden tietojen lisäksi DNS-palveluntarjoajien, aluetunnusrekisterin ylläpitäjien, 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 41 §:n 3 momentin a-c kohdan tiedot. Pykälän 3 momentissa 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 54/2002 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 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. Ilmoituksen tekemättä jättäminen ei sinänsä merkitse kieltoa tarjota palvelua tai harjoittaa toimintaa. Ilmoitusvelvollisuuden laiminlyönti olisi kuitenkin sanktioitu hallinnollisella seuraamusmaksulla 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, eli muun ohella ilmoituksen tekemättä jättämisen, oikaisemiseksi. 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). Ehdotuksessa on kyse NIS 2 –direktiivin toimeenpanosta velvoittavalta osin, mihin ei liity kansallista liikkumavaraa. Esityksen tavoitteena on vahvistaa kyberturvallisuuden tasoa yhteiskunnan toiminnan kannalta keskeisten ja tärkeiden toimijatyyppien osalta. Ehdotuksen tavoitteena on parantaa soveltamisalaan kuuluvien toimijoiden kyberturvallisuuden riskienhallintaa ja siten turvata yhteiskunnan toiminnan kannalta kriittisten palvelujen jatkuvuutta. Ehdotuksella arvioidaan olevan ilmoitusvelvollisuuden asettamiseksi painava ja hyväksyttävä syy.

Toimijoiden velvollisuus ilmoittautua valvovalle viranomaiselle ja toimijaluettelon ylläpitäminen mahdollistaa toimijoille asetettujen velvoitteiden valvonnan sekä laajassa kyberhäiriötilanteessa sen vaikuttavuuden 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*. 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 41 §:stä ilmenisi, että valvova viranomainen ylläpitää valvontatoimialansa osalta toimijaluetteloa ilmoitettujen tietojen perusteella.

Kyberturvallisuuslain 41 § 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 toiminnan rajoittaminen

Esitykseen sisältyy luvanvaraisen toiminnan rajoittamista tai luvan peruuttamista koskevia ehdotuksia. Luvan peruuttamista koskevia ehdotuksia olisivat sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain 23 §:n, maa-asemista ja eräistä tutkista annetun lain 8 §:n ja

vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annetun lain 109 §:n muutokset. Ehdotuksilla pantaisiin osin täytäntöön NIS2-direktiivin 32 artiklan 5 kohta, joka ei sisällä kansallista liikkumavaraa. Ehdotukset ovat merkityksellisiä perustuslain 18 §:ssä turvatun elinkeinovapauden kannalta.

Luvanvaraisen toiminnan rajoittamista tai luvan peruuttamista koskevat ehdotukset kohdistuisivat vain sellaiseen toimintaan, joka on jo aiemmin säädetty luvanvaraiseksi. Muutokset eivät myöskään vaikuttaisi kyseisten lupien myöntämisen edellytyksiin, vaan niissä on kyse jo myönnetyn toimiluvan muuttamisesta tai peruuttamisesta tilanteessa, jossa luvanhaltija ei ole noudattanut siihen kohdistuvia velvoitteita.

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 tällaisten 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). Esitykseen sisältyvät, luvan peruuttamista koskevat ehdotukset on sidottu kyberturvallisuuslaissa säädettyjen velvoitteiden olennaiseen laiminlyöntiin, eli esimerkiksi siihen, että toimija ei ole ollenkaan laatinut kyberturvallisuuslain 8 §:ssä tarkoitettua kyberturvallisuuden riskienhallinnan toimintamallia. Lisäksi edellytyksenä on, että laiminlyönti on siten toistuvaa, että viranomaisen antama huomautus tai varoitus ei ole johtanut korjaaviin toimenpiteisiin. Luvan peruuttaminen olisi viimesijainen keino suhteessa muihin valvontatoimivaltuuksiin, eli ennen sitä viranomaisen olisi pyrittävä puuttumaan laiminlyöntiin lievemmillä keinoilla.

Luvanvaraisen toiminnan rajoittamista koskevan ehdotuksen ei edellä esitetyin perustein katsota olevan ristiriidassa suhteessa perustuslakiin.

Johdon toiminnan rajoittaminen

Hallituksen esityksen 32 §:n mukaan valvova viranomainen voisi kieltää henkilöä toimimasta keskeisen toimijan hallituksen jäsenenä ja varajäsenenä, hallintoneuvoston jäsenenä ja varajäsenenä, toimitusjohtajana tai muussa siihen rinnastettavassa asemassa, jos tämä on toistuvasti ja vakavasti rikkonut 10 §:ssä säädettyjä velvoitteita. Päätös voisi olla voimassa enintään niin kauan, kuin sen perusteena oleva puute tai laiminlyönti on korjaamatta ja kuitenkin enintään viisi vuotta. 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. Esityksen 1. lakiehdotukseen sisältyvän ehdotuksen perusteena on sellaisen Suomea velvoittavan EU-säännöksen täytäntöönpano, jolla tavoitellaan yhteiskunnan toiminnan kannalta kriittisten 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 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 tietyissä johtotehtävissä. 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 32 §: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 varoitus sekä varattava kohtuullinen määräaika 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, eli yhteiskunnan toiminnan kannalta erittäin kriittiseksi määriteltyyn toimijaan.

12.4 Omaisuudensuoja

Kyberturvallisuuslain 30 §:ssä säädettäisiin valvovan viranomaisen oikeudesta velvoittaa toimija päätöksellä toteuttamaan kyberturvallisuuden riskienhallintaan kohdistuva turvallisuusauditointi. Lisäksi valvovalla viranomaisella olisi säännöksen nojalla oikeus saada tieto auditoinnin tuloksista ja velvoittaa toimija toteuttamaan turvallisuusauditoinnin suosittelemat kohtuulliset ja oikeasuhtaiset toimenpiteet kyberturvallisuuden riskienhallinnan kehittämiseksi. Ehdotus on merkityksellinen perustuslain 15 §:ssä turvatun omaisuudensuojan kannalta, sillä velvoitteen täyttämisestä aiheutuisi toimijalle lähtökohtaisesti kustannuksia ja rajoituksia omaisuuden käyttöön kohdistuen. Lisäksi 2 luvun 7–9 §:ssä säädettävä velvoite kyberturvallisuuden riskienhallinnasta voi aiheuttaa toimijoille kustannuksia tai velvoittaa toimijaa tekemään toimenpiteitä, joilla voi olla merkitystä omaisuudensuojan kannalta.

Perustuslain 15 §:n 1 momentin nojalla jokaisen omaisuus on turvattu. Omaisuudensuoja sisältää paitsi omistajalle lähtökohtaisesti kuuluvan vallan hallita, käyttää ja hyödyntää omaisuuttaan haluamallaan tavalla myös vallan määrätä siitä (PeVL 41/2006 vp, s. 2, PeVL 49/2005 vp, s. 2, PeVL 15/2005 vp, s. 2). Perustuslakivaliokunnan käytännön mukaan omistajan oikeuksia voidaan rajoittaa lailla, kunhan sääntely täyttää perusoikeuksien yleiset rajoitusedellytykset.

Perustuslakivaliokunta on pitänyt perusoikeusjärjestelmän kannalta hyväksyttävänä rajoitusperusteena pyrkimystä radioviestinnän häiriöttömyyden turvaamiseen (PeVL 26/2001 vp, s. 4).

Viranomaisen toimivaltuus teettää turvallisuusauditointi ja määrätä toimenpiteitä toteutettavaksi sekä toimijoihin kohdistuvasta riskienhallintavelvoitteesta säätäminen ovat NIS 2 –direktiivin velvoittavan soveltamisalan toimeenpanon edellyttämiä ehdotuksia, joihin ei liity kansallista liikkumavaraa velvoitteiden vähimmäistason osalta. Ehdotuksen tavoitteena on vahvistaa kyberturvallisuuden tasoa yhteiskunnan toiminnan kannalta keskeisissä toimijoissa.

Ehdotetussa 30 §:ssä säädettäisiin tyhjentävästi perusteista, joilla turvallisuusauditointi voitaisiin määrätä toteutettavaksi. Näitä olisivat toimijaan kohdistunut merkittävä poikkeama, joka on aiheuttanut vakavan toimintahäiriön tai huomattavaa vahinkoa; tai olennainen ja vakava riskienhallintavelvoitteen laiminlyönti. Valvova viranomainen voisi velvoittaa toimijan toteuttamaan vain sellaisia auditoinnin suosittelemia toimenpiteitä, jotka ovat kohtuullisia ja oikeasuhtaisia toimijan kyberturvallisuuden riskienhallinnan kehittämiseksi. Valvovalla viranomaisella olisi käytössään muita toimivaltuuksia varmistaa lain noudattaminen ennen turvallisuusauditoinnin määräämistä. Turvallisuusauditoinnin teettäminen tai toimenpiteisiin velvoittaminen olisi muutoksenhakukelpoinen hallintopäätös, joka valvovan viranomaisen on perusteltava.

Ehdotuksien arvioidaan olevan perusoikeuksien yleisten rajoitusedellytysten kannalta täsmällisiä ja tarkkarajaisia sekä riittävän oikeasuhtaisia suhteessa niihin tavoitteisiin, joita esityksen taustalla on. Ehdotuksista säädetään laintasoisesti eikä niillä puututa omaisuudensuojan ydinalueelle. Lisäksi päätöksiin sisältyy muutoksenhakumahdollisuus. Ehdotuksien katsotaan olevan perustuslaissa turvatun omaisuudensuojan kannalta hyväksyttäviä.

12.5 Hallinnollinen seuraamusmaksu

Kyberturvallisuuslain 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 17/2012 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 yleistä 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).

Kyberturvallisuuslaissa 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.

Perustuslakivaliokunta on lausuntokäytännössään pitänyt ongelmallisena sitä, että asia voitaisiin yksittäistapauksessa ratkaista ilman esittelyä (PeVL 14/2018 vp, s.19). Seuraamusmaksulautakunta 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 säädettävän näistä seikoista 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 37 §:n mukaan kokonaisarviointiin, jossa olisi huomioitava pykälässä säädetyt seikat. Maksun enimmäismäärä on määritelty esityksen 38 §: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 harkinta 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 39 §: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). Esityksen 1. lakiehdotuksessa periaate on huomioitu 39 §:n 3 momentissa, jonka mukaan 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 saisi myöskään määrätä sille, jolle on samasta teosta määrätty yleisen tietosuoja-asetuksen nojalla seuraamusmaksu.

Hallinnollista seuraamusmaksua ei voitaisi määrätä viranomaiselle. Perustuslakivaliokunta on katsonut lausuntokäytännössään vieraaksi sen, että hallinnollinen seuraamusmaksu voitaisiin määrätä viranomaiselle (PeVL 13/2023 vp, PeVL 37/2021 vp ja PeVL 14/2018 vp).

Hallinnollista seuraamusmaksua koskevan ehdotuksen arvioidaan vastaavan edellä kuvattuja perustuslain reunaehtoja.

12.6 Valtion toimielinten yleiset perusteet

Kyberturvallisuuslain 19 §:ssä säädettäisiin tietoturvaloukkauksiin reagoivasta ja niitä tutkivasta CSIRT-yksiköstä. Lisäksi lain 36 §:ssä säädettäisiin Liikenne- ja viestintäviraston yhteyteen perustettavasta seuraamusmaksulautakunnasta, jonka tehtävänä olisi määrätä hallinnollinen seuraamusmaksu siten kuin lain 5 luvussa säädetään. Ehdotukset ovat merkityksellisiä perustuslain 119 §:n 2 momentin mukaan valtionhallinnon toimielinten yleisistä perusteista on säädettävä lailla, jos niiden tehtäviin kuuluu julkisen vallan käyttöä.

Perustuslain esitöiden mukaan valtionhallinnon toimielinten yleisillä perusteilla tarkoitetaan lähinnä yksikön nimeä, toimialaa sekä pääasiallisia tehtäviä ja toimivaltuuksia (HE 1/1998 vp, s. 174/II). Myös toimielimen toimikauden mahdollisen määräaikaisuuden on katsottu kuuluvan yleisiin perusteisiin (PeVL 12/2004 vp, s. 2-3).

CSIRT-yksikköä koskevat 19 ja 20 §:t sisältäisivät säännökset yksikön vaatimuksista, tehtävistä ja sijoittumisesta Liikenne- ja viestintävirastoon. CSIRT-yksikön toiminta olisi järjestettävä erilliseksi Liikenne- ja viestintävirastossa tehtävästä valvontatoiminnosta.

Seuraamusmaksulautakuntaa koskeva säännös sisältäisi yleiset perusteet, jotka koskevat seuraamusmaksulautakunnan tehtäviä, jäsenten nimeämistä, päätöksentekomenettelyä ja toimikauden määräaikaisuutta.

Ehdotettujen säännösten katsotaan täyttävän perustuslain 119 §:n 2 momentin asettamat edellytykset valtionhallinnon toimielinten yleisistä perusteista säätämisestä lain tasolla.

12.7 Lainsäädäntövallan siirtäminen

Valtioneuvoston asetus soveltamisalaan kuuluvien toimijoiden määrittämisestä.

Kyberturvallisuuslain 3 §;n 4 momenttiin sisältyy ehdotus, jonka nojalla valtioneuvoston asetuksella voitaisiin tarkentaa lain 3 §:n 3 momentissa tarkoitettuja kriteerejä, joiden perusteella liitteessä I tai II tarkoitettua toimintaa harjoittava toimija voisi poikkeuksellisesti kuulua lain soveltamisalaan, vaikka se olisi kooltaan keskisuurta yritystä pienempi. Ehdotus on merkityksellinen perustuslain 80 §:n kannalta.

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 laissa säädettyjen kriteerien täsmentämisestä EU-säädöksen velvoittavan soveltamisalan tarkentamiseksi. Lain tasolla säädettäisiin oikeuksien ja velvollisuuksien perusteista, eli yksilöivistä ja tyhjentävistä kriteereistä, joiden täyttyessä liitteessä I tai II määriteltyä toimintaa harjoittava tai toimijatyyppiä oleva toimija kuuluisi soveltamisalaan sen koosta riippumatta. Asetuksenantovaltuudella ei voitaisi laajentaa kriteerejä laissa säädetystä. Asetuksella voitaisiin kuitenkin selventää ja täsmentää kriteerejä, sillä yksittäisen toimijan osalta kriteerien täyttymisen arvioiminen voisi muodostua haastavaksi niiden tietojen perusteella, joita yksittäisellä yrityksellä on käytettävissään. Valtioneuvoston asetuksella 3 momentissa tarkoitetuista kriteereistä säätäminen selkeyttäisi siten oikeustilaa myös muille kuin soveltamisalaan kuuluville yrityksille, jotka harjoittavat liitteessä I tai II tarkoitettua toimintaa tai ovat niissä tarkoitettua toimijatyyppiä, mutta alittavat keskisuuren yrityksen määritelmän. Tällaisten yritysten osalta voisi muodostua oikeudellisesti haastavaksi arvioida yrityksen käytettävissä olevien tietojen perusteella sitä, onko toiminnassa kyse 3 momentin 1-4 kohdissa tarkoitetusta tilanteesta, ilman kohtien täsmentämistä, niillä tiedoilla, joita yrityksellä on käytettävissään, kriteerien laatu huomioon ottaen. Lisäksi tulkinnallisuus koskisi hyvin laajaa joukkoa suomalaisia pien- ja mikroyrityksiä. Tulkinnallisuus aiheuttaisi tarpeetonta hallinnollista taakkaa pien- ja mikroyrityksille, mikäli 3 momentissa tarkoitettuja kriteerejä ei täsmennettäisi valtioneuvoston asetuksella. Lisäksi kriteerien laatu huomioon ottaen olisi

todennäköistä, että niiden alaan kuuluvissa toimijoissa tapahtuisi muutoksia toiminnan laadun tai laajuuden muuttuessa tai toiminnan päättyessä.

Valtioneuvoston asetuksella ei voitaisi säätää lain osittaisesta soveltamisesta tai laissa säädettyjen oikeuksien ja velvollisuuksien sisällöstä. Kriteerit säädettäisiin tyhjentävästi lain tasolla. Jotta toimija kuuluisi lain soveltamisalaan 3 momentin nojalla, tulisi sen ensinnäkin harjoittaa lain liitteessä I tai II tarkoitettua toimintaa tai olla liitteessä I tai II tarkoitettua toimijatyyppiä. Edellytyksenä olisi lisäksi, että toimijassa olisi kyse vähintään yhdestä 1–4 kohdassa tarkoitetusta tilanteesta. Ehdotetut 1–4 kohdat vastaisivat NIS2-direktiivin 2 artiklan 2 kohdan b–e alakohtia ja luettelo olisi tyhjentävä. Asetuksenantovaltuuden soveltamisessa olisi myös otettava huomioon komission antama ohjeistus mikroyrityksiin ja pieniin yrityksiin sovellettavien kriteerien käytöstä sen arvioimiseksi, kuuluvatko ne NIS2-direktiivin soveltamisalaan, mikäli tällainen ohjeistus on annettu.

Perustuslakivaliokunta on todennut, että asetuksella voidaan säätää esimerkiksi lain soveltamisen kannalta vähäisen teletoiminnan rajaamisesta lain soveltamisalan ulkopuolelle, kun asetuksenantajan toimivalta on riittävästi rajattu (PeVL 8/2002 vp, s. 3; ks. myös PeVL 14/2005 vp, s. 3).

Asetuksenantovaltuuden perusteesta säädettäisiin laissa ja valtuutus olisi selkeä sekä täsmällisyyden ja tarkkarajaisuuden vaatimukset täyttävä. Näistä syistä arvioidaan, että ehdotus vastaa perustuslain 80 §:n 1 momentin edellytyksiä asetuksenantovaltuudelle siten, että lailla säädetään yksilön oikeuksien ja velvollisuuksien perusteista, ja yksityiskohtainen ja teknisluontoinen kriteerejä koskeva täsmentäminen voitaisiin tehdä valtioneuvoston asetuksella.

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).

Kyberturvallisuuslain 9 §:n 4 momentin nojalla valvova viranomainen valtuutettaisiin antamaan tarkempia teknisiä määräyksiä kyberturvallisuuden riskienhallinnassa huomioitavista toimialakohtaisista erityispiirteistä sekä kriittisiä toimitusketjuja koskevien unionin tason koordinoitujen riskinarviointien tuloksien huomioimisesta toimialakohtaisessa riskienhallinnassa. Lisäksi määräyksenantovaltuus valvovalle viranomaiselle sisältyisi kyberturvallisuuslain 11 §:n 5 momenttiin, jonka nojalla valvovalla viranomaisella olisi toimialallaan mahdollisuus antaa tarkempia teknisiä määräyksiä, joilla tarkennetaan 11–15 §:n nojalla tehtävän ilmoituksen, tiedotuksen tai raportin tietosisältöä, teknistä muotoa tai menettelyä., Kyse olisi yksilöidyistä ja laissa säädettyyn poikkeamaraportointiin liittyvistä teknisistä yksityiskohdista sekä niiden yhdenmukaistamisesta komission täytäntöönpanosäädösten kanssa. Kolmas valvovalle viranomaiselle kohdennettu määräyksenantovaltuus sisältyy kyberturvallisuuslain 41 §:n 4 momenttiin, jonka mukaan valvova viranomainen voisi antaa tarkempia teknisiä määräyksiä tietojen ilmoittamisesta

toimijaluetteloon, jota se ylläpitää. Ehdotukset ovat merkityksellisiä perustuslain 80 § 2 momentin kannalta.

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 5 momentissa yksilöimällä ja listaamalla tyhjentävästi ja täsmällisesti toimialakohtaiset tekniset seikat, joista valvova viranomainen voisi pykälän nojalla antaa tarkempia määräyksiä. Ehdotuksen 41 §:ssä määräyksenantovaltuus koskee 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 esimerkiksi Viestintävirastoa sellaisena viranomaisena, jolle määräyksenantovaltaa on mahdollista antaa (mm. PeVL 9/2004 vp, s. 8).

Perustuslakivaliokunnan mietinnön (PeVM 10/1998 vp, s.23/II) mukaan ministeriötä alemmalle viranomaistasolle 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 5 momentin ja 41 § 3 momentin sanamuodoista, joiden mukaan valvova viranomainen voi toimialallaan antaa tarkempia *teknisiä* määräyksiä. Ehdotuksien katsotaan 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 23 artiklan nojalla antamiin täytäntöönpanosäädöksiin. Käsillä ovat perustuslain 80 §:n 2 momentissa tarkoitetut erityiset syyt. Ehdotettujen määräyksenantovaltuuksien katsotaan olevan perustuslain 80 §:n 2 momentin mukaisia.

12.8 Julkisuusperiaate

Perustuslain 12 § 2 momentissa säädetään julkisuusperiaatteesta. Sen nojalla viranomaisen hallussa olevat asiakirjat ja muut tallenteet ovat julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi lailla erikseen rajoitettu. Jokaisella on oikeus saada tieto julkisesta asiakirjasta ja tallenteesta.

Perustuslain esitöissä (HE 309/1993 vp, s. 58/I) on korostettu julkisuusperiaatteen liittymistä poliittisiin vapausoikeuksiin ja erityisesti sananvapauteen siten, että riittävän julkisuuden takaaminen on edellytys yksilöiden mahdollisuudelle vaikuttaa ja osallistua yhteiskunnalliseen toimintaan. Julkisuus on myös vallankäytön ja viranomaistoiminnan kritiikin ja valvonnan edellytys. Esitöissä todetaan myös, että julkisuudesta joudutaan poikkeamaan erilaisten tärkeiden intressien vuoksi, joita voivat olla muun muassa liikesalaisuudet ja valtakunnan turvallisuuteen liittyvät intressit. Perustuslakivaliokunta on katsonut, että julkisuutta lähtökohtana tulisi voida rajoittaa vain lailla ja vain välttämättömästä syystä. Perustuslakivaliokunta on katsonut, että salassapitovelvoitteen on täytettävä kolme edellytystä: (1) salassapito perustuu välttämättömiin syihin ja (2) sen perusteet määritellään laintasoisella säännöksellä, jolla (3) julkisuutta rajoitetaan erikseen (PeVM 25/1994 vp, s. 9 ja PeVL 43/1998 vp, s. 2).

Kyberturvallisuuslain 28 :n 3 momenttiin ja ehdotettuun tiedonhallintalain 18 i §:n 2 momenttiin sisältyisi julkisuusperiaatteen kannalta merkityksellinen säännös, jonka nojalla valvovan viranomaisen toimijalta pyytämät eräät tiedot olisi pidettävä salassa. Salassapidon perusteena olisi tietoihin liittyvän yksityisyyden suojaan ja luottamuksellisen viestin suojaan liittyvän oikeushyvän suojaaminen. Salassapito ei kohdistuisi julkisuusperiaatteen ydinalueelle, sitä koskeva säännös olisi täsmällinen ja tarkkarajainen, ja se olisi välttämätöntä tärkeän intressin vuoksi. Ehdotettujen säännösten katsotaan olevan perustuslain 12 §:n 2 momentin kannalta hyväksyttävä.

12.9 Eräiden valtioelinten ja viranomaisten asema

NIS2-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.

Julkishallinnon toimijalla tarkoitetaan direktiivin 6 artiklan 35 kohdan mukaan ”jäsenvaltiossa kansallisen lainsäädännön mukaisesti julkishallinnon toimijaksi tunnustettua toimijaa, lukuun ottamatta oikeuslaitosta, parlamentteja ja keskuspankkeja, joka täyttää seuraavat kriteerit:

a) se on perustettu tyydyttämään yleisen edun mukaisia tarpeita, eikä sillä ole teollista tai kaupallista luonnetta;

b) se on oikeushenkilö tai sillä on lain nojalla oikeus toimia toisen sellaisen toimijan puolesta, joka on oikeushenkilö;

c) sitä rahoittavat pääosin valtio, alueviranomaiset tai muut julkisoikeudelliset laitokset, sen johto on näiden viranomaisten tai laitosten valvonnan alainen taikka valtio, alueviranomaiset tai muut julkisoikeudelliset laitokset nimittävät yli puolet sen hallinto-, johto- tai valvontaelimen jäsenistä;

d) sillä on valtuudet osoittaa luonnollisille henkilöille tai oikeushenkilöille hallinnollisia tai sääntelyyn liittyviä päätöksiä, jotka vaikuttavat näiden oikeuksiin henkilöiden, tavaroiden, palvelujen tai pääoman rajatylittävässä liikkuvuudessa.”

NIS2-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.

NIS2-direktiivin 31 artiklan 4 kohdan mukaan Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on valvoessaan julkishallinnon toimijoita tämän direktiivin noudattamisessa ja määrätessään tämän direktiivin rikkomista koskevia täytäntöönpanotoimenpiteitä asianmukaiset valtuudet tällaisten tehtävien suorittamiseksi ja että ne ovat toiminnallisesti riippumattomia valvomistaan julkishallinnon toimijoista, sanotun kuitenkaan rajoittamatta kansallisten lainsäädäntö- ja toimielinkehysten soveltamista. Jäsenvaltiot voivat päättää määrätä kyseisiä toimijoita koskevia asianmukaisia, oikeasuhteisia ja tehokkaita valvonta- ja täytäntöönpanotoimenpiteitä kansallisten lainsäädäntö- ja toimielinkehysten mukaisesti.

NIS2-direktiivin toimeenpanoa julkishallinnon toimialalla koskevan tiedonhallintalain 4 a luvun soveltamisalan sekä valvovan viranomaisen toimivallan rajaamisessa perustuslaillisista syistä on noudatettu pitkälti vastaavaa sääntelytapaa kuin, mihin yleisen tietosuoja-asetuksen ja tietosuojalain soveltamisen osalta päädyttiin perustuslakivaliokunnan lausunnossa (PeVL 14/2018 vp) esitetyn johdosta. NIS2-direktiivi sisältää jonkin verran yleistä tietosuoja-asetusta laajemmin liikkumavaraa kansallisessa soveltamisessa.

Ehdotetun tiedonhallintalain 3 §:n 1 momentin lähtökohdan mukaan lakia, mukaan lukien ehdotettua 4 a luvun NIS2-direktiiviin perustuvaa sääntelyä, sovellettaisiin julkisuuslain 4 §:n 1 momentissa tarkoitettuihin viranomaisiin eli myös eduskunnan virastoihin sekä valtioneuvoston oikeuskanslerin ja eduskunnan oikeusasiamiehen toimintaan. Tiedonhallintalain 4 a lukua sovellettaisiin eduskunnan virastoihin julkisuuslain 4 §:n 1 momentin 6 kohdasta ja sen perusteluista ilmenevällä tavalla, sillä direktiivin 6 artiklan 35 kohdassa käytetyllä käsitteellä ”parlamentti” viitataan kansanedustuslaitoksen toimintaan, eli Suomessa eduskunnan valtiopäivätoimintaan. Myös perustuslakivaliokunta on todennut tietosuojalain hallituksen esityksestä antamassaan lausunnossa PeVL 14/2018 vp, ettei lähtökohtaista estettä ole sille, että hallintoa koskevat yleislait ulotetaan koskemaan eduskunnan virastoja. Julkisuuslakia ei sovelleta eduskunnan eikä sen toimielimien toimintaan, vaan niissä julkisuus määräytyy perustuslain ja eduskunnan työjärjestyksen mukaan. Julkisuuslaki ei siten koske eduskunnan täysistunnon ja valiokuntien toimintaa. (Olli Mäenpää: Julkisuusperiaate, Helsinki 2020, s. 135) Näin ollen myöskään tiedonhallintalaki tai sen 4 a luku ei koske eduskunnan valtiopäivätoimintaa

Tasavallan presidentin kansliaan tai tuomioistuimiin taikka valitusasioita käsittelemään perustettuihin lautakuntiin ehdotettua 4 a lukua ei sovellettaisi ehdotettujen 3 §:n 3 momenttiin sisältyvien poikkeusten perusteella, ellei mainittua katsottaisi kriittiseksi toimijaksi. Tuomioistuinten ja valitusasioita käsittelemään perustettujen lautakuntien osalta rajaus perustuu NIS2-direktiivin 6 artiklan 35 kohtaan. Tasavallan presidentin kanslian osalta valmistelussa on katsottu, että se ei kuulu direktiivin pakolliseen soveltamisalaan, vaikka sen tyyppistä toimijaa ei ole nimenomaisesti mainittu direktiivin soveltamisalaa koskevissa poikkeuksissa. Direktiivin poikkeukset koskevat keskushallinnon viranomaisia ja lisäksi soveltamisessa on jätetty kansallista liikkumavaraa viittauksella jäsenvaltion kansallisen lainsäädännön mukaiseen keskustason julkishallinnon toimijan määrittelyyn. Tasavallan presidentin kanslian osalta nimenomainen poikkeus NIS2-sääntelyn osalta perustuu Tasavallan presidentin asemaan valtioelimenä ja Suomen puolustusvoimien ylipäällikkönä sekä tasavallan presidentin kanslian tehtäviin tasavallan presidentin avustamisessa (laki tasavallan presidentin kansliasta 2 §). Tasavallan presidentin kansliaa ei myöskään voida pitää perustuslain 119 §:ssä tarkoitettuna

valtion keskushallinnon viranomaisena eikä myöskään ole selvää, onko sillä NIS2-direktiivin 6 artiklan 35 kohdan d alakohdassa tarkoitettua toimivaltaa.

NIS2-direktiivin valvovan viranomaisen eli julkishallinnon toimialalla Liikenne- ja viestintäviraston valvontatoimivaltuuksia tai tiedonsaanti- ja tarkastusoikeutta ei ehdotetun tiedonhallintalain 3 §:n 4 momentin mukaan sovellettaisi eduskunnan oikeusasiamiehen eikä valtioneuvoston oikeuskanslerin toimintaan. Valvontatoimivaltuuksia ei sovellettaisi myöskään tasavallan presidentin kansliaan taikka tuomioistuinten tai valitusasioita käsittelemään perustettujen lautakuntien lainkäyttöön siinä tapauksessa, että mainittuihin sovellettaisiin 4 a lukua kriittisenä toimijana, joka yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain nojalla olisi määritetty julkishallinnon toimialan kriittiseksi toimijaksi. Valvontatoimivallan 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 tai lainkäyttöön (esim. PeVL 46/2010 vp ja PeVL 14/2028 vp).

Mainittujen viranomaisten osalta ei ehdotetussa tiedonhallintalain 3 §:n 4 momentissa ole suljettu pois velvoitetta ilmoittautua toimijaksi (tiedonhallintalain 18 a §) eikä velvoitetta ilmoittaa merkittävistä poikkeamista valvovalle viranomaiselle (18 d §). Näiden säännösten voidaan nähdä jossain suhteessa palvelevan valvonnallisia tarkoituksia, mutta tarkoituksena on myöskin toimijoiden ja niiden määrän tilastointi sekä tietojen kerääminen kriittisillä toimialoilla käytetyistä IP-osoitealueista sekä tilannekuvatiedon kerryttäminen merkittävistä poikkeamista. Valvonnallista tarkoitusta rajaa myös se, että valvovan viranomaisen tiedonsaantioikeus ei koskisi ylimpiä laillisuusvalvojia, eli niillä ei olisi velvoitetta luovuttaa valvovalle viranomaiselle salassa pidettäviä tietoja. Tiedonsaantioikeus ei koskisi myöskään tasavallan presidentin kansliaa tai tuomioistuimia taikka valitusasioita käsittelemään perustettujen valiokuntien lainkäyttöä, jos näihin sovellettaisiin 4 a lukua yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain johdosta. Tietojen luovuttamiseen liittyviä näkökulmia on esitetty tarkemmin valvovan viranomaisen tiedonsaantioikeutta koskevan tiedonhallintalain 18 i §:n ja vapaaehtoista ilmoittamista koskevan 18 f §:n säännöskohtaisissa perusteluissa.

Tiedonhallintalain voimassa olevan 3 §:n 3 momentin mukaan lain tiedonhallinnan yleistä ohjausta koskevaa 3 lukua ei sovelleta eduskunnan oikeusasiamiehen eikä valtioneuvoston oikeus-kanslerin 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. Lain 3 lukua sovelletaan hyvinvointialueisiin, hyvinvointiyhtymiin, kuntiin ja kuntayhtymiin vain niiden hoitaessa laissa säädettyjä tehtäviä.

Mainittuja tiedonhallinnan yleistä ohjausta koskevia rajauksia ei ole eduskunnan virastojen, itsenäisten julkisoikeudellisten laitosten, yliopistojen, ammattikorkeakoulujen (jos sääntelyä sovellettaisiin niihin kriittisinä toimijoina) taikka hyvinvointialueiden ja hyvinvointiyhtymien osalta sisällytetty NIS2-direktiivin valvontatoimivaltuuksien soveltamisen rajauksiin. Tämä johtuu siitä, että NIS2-direktiivissä lähtökohtana on julkishallinnon toimijoidenkin osalta valvonnan kohdistaminen kaikkiin toimijoihin, joskin NIS2-direktiivin 31artiklan 4 kohdan mukaan valvontaan velvoittamisella ei rajoiteta kansallisten lainsäädäntö- ja toimielinkehysten soveltamista. Tietosuojalain hallituksen esityksestä annetussa perustuslakivaliokunnan lausunnossa PeVL 14/2018 vp on arvioitu mahdollisuuksia poiketa EU-oikeuden täysimääräisestä soveltamisesta seuraavasti: ”Perustuslakivaliokunnan käsityksen mukaan on

kuitenkin selvää, että kansallista valtiosäännön rakenteisiin kiinnittyvää identiteettiä koskeva sopimusmääräys voi muodostaa vain kapeasti sovellettavissa olevan oikeasuhtaisen perusteen poiketa EU-oikeuden täysimääräisestä soveltamisesta. Unionin tuomioistuimen vakiintuneessa oikeuskäytännössä on katsottu, että unionin oikeuden ensisijaisuuden periaatteen, joka on unionin oikeusjärjestyksen olennainen ominaisuus, mukaan se, että jäsenvaltio vetoaa kansallisen oikeutensa säännöksiin, edes perustuslain tasoisiin säännöksiin, ei voi heikentää unionin oikeuden vaikutusta tämän jäsenvaltion alueella (ks. mm. asia 11/70, Internationale Handelsgesellschaft, tuomio 17.12.1970, 3 kohta ja asia C 409/06, Winner Wetten, tuomio 8.9.2010, 61 kohta ja erityisesti asia C-399/11, Melloni, tuomio 26.2.2013, k. 59).”

Kyberturvallisuuslakiin ei esitetä tiedonhallintalakia vastaavia soveltamisalaa taikka valvovan viranomaisen toimivaltaa koskevia yleisiä rajauksia, koska tässä jaksossa kuvatut perustuslaillisten näkökohtien nojalla merkitykselliset valtioelimet ja viranomaiset eivät tarjoa palveluja kyberturvallisuuslain liitteissä tarkoitetuilla toimialoilla eivätkä siten tulisi lain soveltamisalaan. NIS2-direktiivin liitteessä tarkoitetun julkishallinnon toimialan osalta toimijoiden velvoitteista ja niiden noudattamisen valvonnasta säädettäisiin tiedonhallintalaissa, vaikka harjoittaessaan muuta NIS2-direktiivin liitteessä tarkoitettua toimintaa, myös viranomainen voisi tulla eräissä tilanteissa kyberturvallisuuslain soveltamisalaan. Tämän johdosta eräiden seuraamusten osalta (johdon toiminnan rajoittaminen ja hallinnollinen seuraamusmaksu) kyberturvallisuuslaissa kuitenkin rajattaisiin julkishallinto kattavasti mainittujen seuraamusten soveltamisen ulkopuolelle, koska osa julkishallinnon toimialan toimijoista (esimerkiksi hyvinvointialueet ja hyvinvointiyhtymät) kuuluisivat tiedonhallintalain ohella kyberturvallisuuslainlain soveltamisalaan, koska ne harjoittavat lain liitteessä tarkoitettua toimintaa.

12.10 Ahvenanmaan asema ja suhde itsehallintoon

Esitys jakautuu osin valtakunnan ja osin maakunnan lainsäädäntövaltaan, kuten Ahvenanmaan maakuntahallitus on lausunnossaan arvioinut, koska NIS2-direktiivin soveltamisalan osalta lainsäädäntövalta jakautuu Ahvenanmaan itsehallintolain (1144/1991) nojalla maakunnan ja valtakunnan kesken. NIS1-direktiivi arvioitiin valtakunnan toimivaltaan kuuluvaksi, mutta NIS2-direktiivin soveltamisala on laajempi, kattaen osin myös Ahvenanmaan maakunnan lainsäädäntövaltaan kuuluvia asioita. Kyberturvallisuus ja tietoturvallisuus liittyvät siihen lainsäädäntövaltaan, mihin kutakin toimialaa koskeva lainsäädäntövalta kuuluu. Esitykseen sisältyvistä ehdotuksista valtakunnan lainsäädäntövaltaan kuuluvat osat tulisivat sovellettavaksi myös Ahvenanmaan maakunnassa. Esityksen niissä osissa, jotka Ahvenanmaan itsehallintolain nojalla kuuluvat maakunnan lainsäädäntövaltaan, kuulu lainsäädäntövalta kuuluu maakunnalle.

Ahvenanmaan itsehallintolain 18 §:n 1, 4, 6, 12, 20 ja 21 kohtien mukaan maakunnalla on lainsäädäntövalta asioissa, jotka koskevat maakuntapäivien järjestysmuotoa, maakunnan hallitusta sekä sen alaisia viranomaisia ja laitoksia, kuntien hallintoa, yleistä järjestystä ja turvallisuutta, terveyden- ja sairaanhoitoa, postilaitosta, teitä ja kanavia, tieliikennettä raideliikennettä, veneliikennettä sekä paikallisen meriliikenteen väyliä. Lisäksi 18 §:n 22 kohdan mukaan maakunnalla on eräin rajoituksin lainsäädäntövaltaa asioissa, jotka koskevat elinkeinotoimintaa. Myös tietosuoja ja henkilötietojen käsittely kuuluvat maakunnan toimivaltaan niillä aloilla, joilla maakunnalla on lainsäädäntövaltaa.

Ahvenanmaan itsehallintolain 27 §:n 3, 8, 13, 14, 18, 19, 30 ja 40 kohtien mukaan valtakunnalla on lainsäädäntövalta asioissa, jotka koskevat valtion viranomaisten järjestysmuotoa ja toimintaa, yhtiöitä ja muita yksityisoikeudellisia yhteisöjä, kauppamerenkulkua ja kauppamerenkulun väyliä, ilmailua, ydinvoimaa, standardisointia, apteekkeja, lääkkeitä ja lääkkeenomaisia tuotteita sekä teletoimintaa.

Ahvenanmaan maakunnan toimivalta sähkö- ja energia-asioissa on maakunnan sähkölain (Ellag för landskapet Åland, ÅFS 1982:38) lainsäädäntövalvonnan yhteydessä johdettu aikaisemman Ahvenanmaan itsehallintolain (670/1951) 13 §:n 1 momentin 9 kohdasta, joka vastasi voimassa olevan Ahvenanmaan itsehallintolain elinkeinotoiminnasta säädettyä 18 §:n 22 kohtaa (HE 73/1990 vp s. 71). Itsehallintolaissa säädetystä valtakunnan ja maakunnan välisestä toimivallanjaosta johtuu, että sähkömarkkinalakia ei sovelleta Ahvenanmaan maakunnassa siltä osin kuin maakunnalla on lainsäädäntövalta sähkömarkkinoihin liittyvissä asioissa. (NIS1-HE)

Avaruustoimialalla satelliittikaukokartoitus sekä maa-asema- ja tutkatoiminta kuuluvat valtakunnan lainsäädäntövaltaan itsehallintolain 27 §:n 40 ja 42 kohdan mukaisesti kuten avaruustoiminnan ja radiolupien osaltakin.

Ahvenanmaan maakunnassa on valmisteltu maakuntalainsäädäntöä julkisen hallinnon tiedonhallinnasta. Ahvenanmaan maakuntahallitus on lausunnossaan arvioinut, että tiedonhallintalain 4 a lukuun ehdotettavia säännöksiä vastaavat säännökset voitaisiin sisällyttää myös maakunnassa valmisteltavana olevaan lainsäädäntöön.

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 täytäntöönpano vähimmäistasolla edellyttää ja jonka on katsottava olevan sen taustalla olevien tavoitteiden toteutumisen kannalta välttämätöntä ja oikeasuhtaista.

Edellä mainituilla perusteilla lakiehdotukset voidaan käsitellä tavallisessa lainsäätämisjärjestyksessä. Esitys sisältää kuitenkin muun muassa ehdotuksen haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelystä ja arvion eräiden valtioelinten ja viranomaisten asemasta. Hallitus pitää suotavana, että perustuslakivaliokunta antaisi asiasta lausunnon.

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 annetussa Euroopan parlamentin ja neuvoston direktiivissä (EU) 2022/2555 on säännöksiä, jotka ehdotetaan pantaviksi täytäntöön lailla, annetaan eduskunnan hyväksyttäviksi seuraavat lakiehdotukset:

1.

Kyberturvallisuuslaki

Eduskunnan päätöksen mukaisesti säädetään:

1 luku

Yleiset säännökset

1 §

Soveltamisala

Tässä laissa säädetään kyberturvallisuutta koskevien riskien hallinnasta.

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*).

NIS 2 –direktiivin täytäntöönpanosta mainitun direktiivin liitteen I kohdassa 10 tarkoitetulla julkishallinnon toimialalla säädetään julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019).

2 §

Määritelmät

Tässä laissa tarkoitetaan:

1) *aluetunnusrekisterin ylläpitäjällä* tahoa, jolle on myönnetty oikeus hallinnoida tiettyä aluetunnusta ja joka sitä hallinnoidessaan vastaa verkkotunnusten rekisteröinnistä sen alle sekä sen teknisestä toiminnasta;

2) *datakeskuspalvelulla* palvelua, joka käsittää rakenteita tai rakenteiden ryhmiä, jotka on tarkoitettu datan tallennus-, käsittely- ja siirtopalveluja tarjoavien tietoteknisten laitteiden ja verkkolaitteiden keskitettyyn ylläpitoon, yhteenliittämiseen ja ohjaukseen yhdessä kaikkien tarvittavien sähkönjakeluun ja toimintaolosuhteiden säätelyyn tarkoitettujen laitteiden ja infrastruktuurin kanssa;

3) *DNS-palveluntarjoajalla* toimijaa, joka tarjoaa yleisesti saatavilla olevia rekursiivisia verkkotunnusten selvityspalveluja internetin loppukäyttäjille tai auktoritatiivisia verkkotunnusten selvityspalveluja kolmansille osapuolille, lukuun ottamatta juurinimipalvelimia;

4) *haavoittuvuudella* tieto- ja viestintätekniikan tuotteiden tai -palvelujen heikkoutta, alttiutta tai vikaa, joka voi aiheuttaa kyberuhkan tai poikkeaman;

5) *hallintapalvelun tarjoajalla* toimijaa, joka tarjoaa 17 kohdassa tarkoitettujen 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;

6) *hyväksytyllä luottamuspalvelun tarjoajalla* sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY

kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 (*eIDAS-asetus*) 3 artiklan 20 alakohdassa tarkoitettua hyväksyttyä luottamuspalvelun tarjoajaa;

7) *kyberturvallisuudella* toimia, joita tarvitaan viestintäverkkojen ja tietojärjestelmien, niiden käyttäjien ja muiden asianosaisten henkilöiden suojaamiseksi kyberuhilta;

8) *kyberuhkalla* tilannetta, tapahtumaa tai toimintaa, joka toteutuessaan voi vahingoittaa tai häiritä viestintäverkkoja tai tietojärjestelmiä, tällaisten järjestelmien käyttäjiä ja muita henkilöitä tai muulla tavoin vaikuttaa näihin haitallisesti;

9) *luottamuspalvelun tarjoajalla* eIDAS-asetuksen 3 artiklan 19 alakohdassa määriteltyä luottamuspalvelun tarjoajaa;

10) *pilvipalvelulla* digitaalista palvelua, joka tarjoaa laajaan etäkäyttöön skaalattavan ja joustavan joukon jaettavissa olevia ja tarveperusteisesti ohjattavia tietoteknisiä resursseja;

11) *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;

12) *poikkeaman käsittelyllä* toimia ja menettelyjä, joilla pyritään ehkäisemään ja havaitsemaan poikkeama, analysoimaan, rajoittamaan tai hallitsemaan sitä ja palautumaan siitä;

13) *riskillä* poikkeaman aiheuttamien menetysten tai häiriön mahdollisuutta, joka ilmaistaan menetyksen tai häiriön suuruuden ja poikkeaman toteutumisen todennäköisyyden yhdistelmänä;

14) *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;

15) *tietoturvapalveluntarjoajalla* hallintapalvelun tarjoajaa, joka toimii kyberturvallisuusriskien hallitsemiseksi tai antaa tukea sitä varten;

16) *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 (*kyberturvallisuusasetus*) 2 artiklan 13 kohdassa tarkoitettua tieto- ja viestintätekniikan palvelua;

17) *TVT-tuotteella* kyberturvallisuusasetuksen 2 artiklan 12 kohdassa tarkoitettua tieto- ja viestintätekniikan tuotetta;

18) *valvovalla viranomaisella* 26 §:ssä mainittuja viranomaisia;

19) *verkkoyhteisöalustalla* alustaa, jonka avulla loppukäyttäjät voivat olla yhteydessä toisiinsa, jakaa sisältöä, hakea tietoa ja viestiä keskenään monenlaisilla päätelaitteilla;

20) *verkossa toimivalla hakukoneella* oikeudenmukaisuuden ja avoimuuden edistämisestä verkossa toimivien välityspalvelujen yrityskäyttäjiä varten annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/1150 2 artiklan 5 kohdassa tarkoitettua verkossa toimivaa hakukonetta;

21) *verkossa toimivalla markkinapaikalla* kuluttajansuojalain (38/1978) 6 luvun 8 §:n 4 kohdassa tarkoitettua verkossa toimivaa markkinapaikkaa;

22) *viestintäverkolla ja tietojärjestelmällä*

a) eurooppalaisesta sähköisen viestinnän säännöstöstä annettua Euroopan parlamentin ja neuvoston direktiivin (EU) 2018/1972 (*teledirektiivi*) 2 artiklan 1 kohdassa tarkoitettua sähköistä viestintäverkkoa;

b) laitetta taikka yhteen kytkettyjen tai toisiinsa yhteydessä olevien laitteiden ryhmää, joista yksi tai useampi suorittaa ohjelman avulla digitaalisten tietojen automaattista käsittelyä; ja

c) digitaalisia tietoja, joita a ja b alakohdassa tarkoitetuissa järjestelmissä säilytetään, käsitellään, haetaan tai siirretään näiden järjestelmien toimintaa, käyttöä, suojausta tai ylläpitoa varten;

23) *viestintäverkon ja tietojärjestelmän turvallisuudella* viestintäverkon ja tietojärjestelmien kykyä suojautua tietyllä varmuudella tapahtumilta, jotka saattavat vaarantaa niissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden;

24) *yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajalla* sitä, joka tarjoaa sähköisen viestinnän palveluista annetun lain (917/2014) 3 §:n 37 kohdassa tarkoitettua viestintäpalvelua ennalta rajaamattomalle käyttäjäpiirille;

25) *yleisten sähköisten viestintäverkkojen tarjoajalla* sitä, joka tarjoaa sähköisen viestinnän palveluista annetun lain 3 §:n 34 kohdassa tarkoitettua verkkopalvelua;

3 §

Toimijat

Tätä lakia sovelletaan oikeushenkilöön ja luonnolliseen henkilöön (*toimija*), joka

1) harjoittaa liitteessä I tai II tarkoitettua toimintaa tai on mainituissa liitteissä tarkoitettu toimija; ja

2) täyttää tai ylittää mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä annetun komission suosituksen 2003/361/EY liitteen 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset ja tarjoaa palvelujaan tai harjoittaa toimintaansa jossakin Euroopan unionin jäsenvaltiossa.

Tätä lakia sovelletaan myös toimijaan, joka koostaan riippumatta on:

1) yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoaja;

2) luottamuspalvelun tarjoaja;

3) aluetunnusrekisterin ylläpitäjä; tai

4) DNS-palveluntarjoaja.

Lisäksi tätä lakia sovelletaan sellaiseen toimijaan sen koosta riippumatta, joka harjoittaa liitteessä I tai II tarkoitettua toimintaa tai on mainituissa liitteissä tarkoitettu toimijaa, jos:

1) se tarjoaa palvelua, joka on yhteiskunnan tai talouden kriittisten toimintojen ylläpitämisen kannalta keskeinen ja jota muut toimijat eivät tarjoa;

2) häiriö sen tarjoamassa palvelussa vaikuttaisi merkittävästi yleiseen järjestykseen, yleiseen turvallisuuteen tai kansanterveyteen;

3) häiriö sen tarjoamassa palvelussa voisi aiheuttaa merkittävän systeemisen riskin erityisesti aloilla, joilla tällaisella häiriöllä voisi olla rajat ylittäviä vaikutuksia; tai

4) se on kriittinen, koska sillä on erityisen suuri merkitys kansallisella tai alueellisella tasolla kyseisen toimialan tai palvelutyypin tai jonkin Euroopan unionin jäsenvaltion muiden keskinäisriippuvaisten toimialojen kannalta.

Edellä 3 momentissa tarkoitetuista kriteereistä voidaan antaa tarkempia säännöksiä valtioneuvoston asetuksella.

Toimijaan ei sovelleta 1 momentin 2 kohdassa mainitun suosituksen liitteen 3 artiklan 4 kohtaa.

4 §

Soveltamisalan rajaukset

Tämän lain 2 lukua ei sovelleta toimintaan eikä 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 momentista poiketen lakia sovelletaan toimijaan, joka on luottamuspalvelun tarjoaja.

Tätä lakia ei sovelleta toimijaan, johon 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 (*DORA*-asetus) ei sovelleta sen 2 artiklan 4 kohdan nojalla.

Tätä lakia ei sovelleta toimijaan, jonka harjoittama liitteessä I tai II tarkoitettu toiminta on satunnaista ja vähäistä.

Tätä lakia sovelletaan kuntalaissa (410/2015) tarkoitettuun kuntaan vain liitteessä I tai II tarkoitetun toiminnan osalta.

Tämän lain säännöksiä, jotka velvoittavat antamaan tietoa, ei sovelleta, jos tiedon luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin siihen liittyvää tärkeää etua.

5 §

Suhde muuhun lainsäädäntöön

Jos muussa laissa tai sen nojalla annetuissa säännöksissä tai määräyksissä on tästä laista poikkeavia vaatimuksia kyberturvallisuusriskien hallinnasta tai merkittävistä poikkeamista ilmoittamisesta ja vaatimukset ovat vaikutuksiltaan vähintään tässä laissa säädettyjä velvoitteita vastaavia, niitä sovelletaan tämän lain vastaavien säännösten asemasta.

Jos Euroopan unionin asetuksessa tai NIS 2 -direktiivin nojalla säädetyssä komission asetuksessa edellytetään, että toimija ottaa käyttöön kyberturvallisuutta koskevien riskien hallitsemiseksi toimenpiteitä tai ilmoittaa merkittävistä poikkeamista, ja vaatimukset ovat vaikutuksiltaan vähintään tässä laissa säädettyjä velvoitteita vastaavia, säännöksiä sovelletaan tämän lain 2, 4 ja 5 luvun sekä 41 §:n asemasta.

Henkilötietojen käsittelyn tietoturvallisuudesta säädetään luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksessa (EU) 2016/679 (*yleinen tietosuoja-asetus*) ja tietosuojalaissa (1050/2018).

Sen lisäksi mitä tässä laissa säädetään valvovan viranomaisen toimivaltuuksista, luvan peruuttamiseen sovelletaan sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain (590/2013) 23 §:n 6 kohdassa, vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annetun lain (390/2005) 109 a §:ssä ja maa-asemista ja eräistä tutkista annetun lain (96/2023) 8 §:n 1 momentin 3 kohdassa säädettyä.

6 §

Lainkäyttövalta ja alueellisuus

Tätä lakia sovelletaan toimijaan, joka on sijoittautunut Suomeen, jollei laissa toisin säädetä tai Euroopan unionin lainsäädännöstä tai Suomea sitovasta kansainvälisestä velvoitteesta muuta johdu.

Riippumatta valtiosta, johon toimija on sijoittautunut, tätä lakia sovelletaan yleisen sähköisen viestintäverkon tarjoajaan ja yleisesti saatavilla olevan sähköisen viestintäpalvelun tarjoajaan silloin kun se tarjoaa palvelujaan Suomessa.

DNS-palveluntarjoaja, aluetunnusrekisterin ylläpitäjä, pilvipalvelujen tarjoaja, datakeskuspalvelujen tarjoaja, sisällönjakeluverkkojen tarjoaja, hallintapalvelun tarjoaja, tietoturvapalveluntarjoaja, verkossa toimivien markkinapaikkojen tarjoaja, verkossa toimivien hakukoneiden tarjoaja ja verkkoyhteisöalustojen tarjoaja kuuluvat tämän lain soveltamisalaan, jos sen NIS 2 -direktiivin 26 artiklan 2 kohdassa tarkoitettu päätoimipaikka tai 3 kohdassa tarkoitettu Euroopan unioniin nimetty edustaja sijaitsee Suomessa. Jos tällainen toimija ei ole sijoittautunut Euroopan unionin jäsenvaltioon ja se tarjoaa palvelujaan Suomessa tai muun Euroopan unionin jäsenvaltion alueella, sen on nimettävä NIS 2 -direktiivin 26 artiklan 3 kohdassa tarkoitettu edustaja Euroopan unionin jäsenvaltioiden aluetta varten. Jos toimija ei ole

sijoittautunut Euroopan unionin jäsenvaltioon tai asettanut NIS 2 -direktiivin 26 artiklan 3 kohdassa tarkoitettua nimettyä edustajaa 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. Valvova viranomainen voi kieltäytyä pyynnöstä, jos sillä ei ole lain nojalla toimivaltaa antaa pyydettyä apua, pyydetty apu ei ole oikeassa suhteessa valvontatehtäviin tai pyyntö koskee sellaisia tietoja tai käsittää sellaisia toimintoja, joiden paljastaminen tai toteuttaminen olisi vastoin Suomen maapuolustukseen tai kansalliseen turvallisuuteen liittyviä etuja. Ennen pyynnöstä kieltäytymistä valvovan viranomaisen on kuultava muita asianomaisia toimivaltaisia viranomaisia sekä, jos jokin Euroopan unionin jäsenvaltio sitä pyytää, Euroopan komissiota ja Euroopan unionin kyberturvallisuusvirastoa.

2 luku

Riskienhallinta ja poikkeamista ilmoittaminen

7 §

Riskienhallinta

Toimijan on tunnistettava, arvioitava ja hallittava riskejä, joita kohdistuu sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Kyberturvallisuutta koskevalla riskienhallinnalla tulee estää tai minimoida poikkeamien vaikutus toimintaan, toiminnan jatkuvuuteen, palvelujen vastaanottajiin ja muihin palveluihin.

Toimijan on toteutettava riskienhallintatoimenpiteet, jotka ovat ajantasaisia, oikeasuhtaisia ja riittäviä suhteessa toiminnassa käytettäville viestintäverkoille ja tietojärjestelmille aiheutuviin riskeihin ja viestintäverkon tai tietojärjestelmän merkitykseen toimijan toiminnan ja palveluntarjonnan kannalta.

8 §

Kyberturvallisuutta koskeva riskienhallinnan toimintamalli

Toimijalla on oltava käytössä ajantasainen kyberturvallisuutta koskeva riskienhallinnan toimintamalli viestintäverkkojen ja tietojärjestelmien ja niiden fyysisen ympäristön suojaamiseksi poikkeamilta ja niiden vaikutuksilta.

Kyberturvallisuutta koskevassa riskienhallinnan toimintamallissa on tunnistettava viestintäverkkoihin ja tietojärjestelmiin ja niiden fyysiseen ympäristöön kohdistuvat riskit ottaen huomioon kaikki vaaratekijät huomioiva lähestymistapa. Toimintamallissa on määritettävä ja kuvattava kyberturvallisuutta koskevan riskienhallinnan tavoitteet, menettelyt ja vastuut sekä 9 §:n mukaiset toimenpiteet, joilla viestintäverkkoja ja tietojärjestelmiä ja niiden fyysistä ympäristöä suojataan kyberuhkilta ja poikkeamilta (*hallintatoimenpiteet*).

9 §

Toimenpiteet kyberturvallisuutta koskevien riskien hallinnassa

Toimijoiden on toteutettava kyberturvallisuutta koskevan riskienhallinnan toimintamallin mukaiset oikeasuhtaiset tekniset, operatiiviset tai organisatoriset hallintatoimenpiteet viestintäverkkojen ja tietojärjestelmien turvallisuuteen kohdistuvien riskien hallitsemiseksi ja haitallisten vaikutusten estämiseksi tai minimoimiseksi.

Toimintamallissa ja siihen perustuvissa hallintatoimenpiteissä on otettava huomioon ja pidettävä yllä ajantasaisesti ainakin:

1) kyberturvallisuutta koskevan riskienhallinnan toimintaperiaatteet ja hallintatoimenpiteiden vaikuttavuuden arviointi;

2) viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet;

3) viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus sekä tarvittavat menettelyt haavoittuvuuksien käsittelemiseksi ja julkistamiseksi;

4) toimitusketjun välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, niihin sisällytetyt hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt;

5) omaisuudenhallinta ja sen 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 käyttämiseksi;

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;

11) perustason tietoturvakäytännöt 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, poikkeamasta kohtuudella ennakoitavissa oleviin välittömiin vaikutuksiin, toimijan viestintäverkkojen ja tietojärjestelmien riskialttiuteen, poikkeamien todennäköisyyteen ja vakavuuteen, toimenpiteistä aiheutuviin kustannuksiin sekä ajantasainen kehitys huomioon ottaen käytettävissä oleviin teknisiin mahdollisuuksiin torjua uhka.

Valvova viranomainen voi toimialallaan antaa riskienhallintavelvollisuuksia tarkentavia teknisiä määräyksiä:

1) toimialakohtaisista erityispiirteistä, jotka on otettava huomioon kyberturvallisuutta koskevassa riskienhallinnan toimintamallissa ja 2 momentissa tarkoitetuissa osa-alueissa sekä riskienhallinnan ja viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden hallinnan menettelyissä;

2) kriittisiä toimitusketjuja koskevien unionin tason koordinoitujen riskinarviointien tuloksien huomioimisesta toimialakohtaisessa riskienhallinnassa.

Riskienhallinnassa, 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 kyberturvallisuutta koskevan riskienhallinnan toteuttamisen ja valvonnan järjestämisestä sekä hyväksyy kyberturvallisuutta koskevan riskienhallinnan toimintamallin ja valvoo sen toteuttamista. Toimijan johdolla tulee olla riittävä perehtyneisyys kyberturvallisuutta koskevaan riskienhallintaan.

Johdolla tarkoitetaan toimijan hallitusta, hallintoneuvostoa ja toimitusjohtajaa sekä muussa niihin rinnastettavassa asemassa olevaa, joka tosiasiallisesti johtaa sen toimintaa.

11 §

Poikkeamailmoitukset viranomaiselle

Toimijan on viipymättä ilmoitettava valvovalle viranomaiselle merkittävästä poikkeamasta. Merkittävällä poikkeamalla tarkoitetaan poikkeamaa, joka on aiheuttanut tai voi aiheuttaa vakavan palvelujen toimintahäiriön tai huomattavia taloudellisia tappioita asianomaiselle toimijalle, sekä poikkeamaa, joka 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;

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) tekniset vaarantumisindikaattorit, jos sellaisia on saatavilla;

3) mahdolliset päivitykset ensi-ilmoituksen tietoihin.

Valvova viranomainen voi toimialallaan antaa tarkempia teknisiä määräyksiä, joilla tarkennetaan 11–15 §:n nojalla tehtävän ilmoituksen, tiedotuksen tai raportin tietosisältöä, teknistä muotoa ja menettelyä.

Edellä 2 momentissa säädetystä poiketen luottamuspalvelun tarjoajan on tehtävä jatkoilmoitus 24 tunnin kuluessa merkittävän poikkeaman havaitsemisesta, jos merkittävä poikkeama vaikuttaa sen luottamuspalvelujen tarjontaan.

Edellä 1 momentissa tarkoitetun lisäksi merkittävällä poikkeamalla tarkoitetaan NIS 2 –direktiivin 23 artiklan 11 kohdan nojalla annetussa Euroopan komission täytäntöönpanosäädöksessä täsmennettyä tilannetta, jossa poikkeama katsotaan merkittäväksi.

12 §

Poikkeamaa koskeva väliraportti

Toimijan on annettava valvovan viranomaisen pyynnöstä lisätietoja tai väliraportti merkittävää poikkeamaa koskevista tilannepäivityksistä ja käsittelyn edistymisestä.

Jos merkittävä poikkeama on pitkäkestoinen, toimijan on annettava väliraportti viimeistään kuukauden kuluttua jatkoilmoituksen antamisesta.

13 §

Poikkeamaa koskeva loppuraportti

Toimijan on annettava valvovalle viranomaiselle merkittävää poikkeamaa koskeva loppuraportti kuukauden kuluessa jatkoilmoituksen toimittamisesta tai, jos kyseessä on pitkäkestoinen poikkeama, kuukauden kuluessa sen käsittelyn päättymisestä.

Loppuraportin on sisällettävä:

1) yksityiskohtainen kuvaus poikkeamasta, sen vakavuudesta ja vaikutuksista;

2) selvitys poikkeaman todennäköisesti aiheuttaneen uhkan tai juurisyyn tyypistä;
3) selvitys toteutetuista ja meneillään olevista toimenpiteistä poikkeaman vaikutusten lieventämiseksi; ja
4) selvitys mahdollisista rajat ylittävistä vaikutuksista.

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 tiedottaminen on yleisen edun mukaista, valvova viranomainen voi velvoittaa toimijan tiedottamaan asiasta tai tiedottaa asiasta itse.

15 §

Vapaaehtoinen ilmoittaminen

Toimijat voivat vapaaehtoisesti tehdä valvovalle viranomaiselle ilmoituksia muista kuin 11 §:ssä tarkoitetuista poikkeamista, kyberuhkista ja läheltä piti –tilanteista.

Valvovan viranomaisen on toimialallaan otettava vastaan vapaaehtoisia poikkeamailmoituksia merkittävistä poikkeamista, poikkeamista, kyberuhkista ja läheltä piti -tilanteista myös muilta kuin tässä laissa tarkoitetuilta toimijoilta.

Valvovan viranomaisen on toimitettava tieto tämän pykälän nojalla tehdyistä ilmoituksista 18 §:ssä tarkoitetulle keskitetylle yhteyspisteelle.

16 §

Poikkeamailmoituksen vastaanottaminen

Valvovan viranomaisen on vastattava poikkeamailmoituksen tehneelle taholle viivytyksettä. Vastauksessa on oltava alustava palaute merkittävästä poikkeamasta sekä ohjeet siitä 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 11 – 13 ja 15 §:ssä tarkoitetut ilmoitukset ja raportit CSIRT-yksikölle välittömästi. CSIRT-yksikkö antaa toimijan pyynnöstä ohjeita ja operatiivisia neuvoja vaikutuksia lieventävistä toimenpiteistä.

Jos merkittävästä poikkeamasta on aiheutunut yleisen tietosuoja-asetuksen 33 artiklassa tarkoitettu henkilötietojen tietoturvaloukkaus, josta on ilmoitettava, valvovan viranomaisen on ilmoitettava poikkeaman havaitsemisesta tietosuojavaltuutetulle.

Jos merkittävässä poikkeamassa on toimijan ilmoituksen perusteella syytä epäillä rikosta, josta säädetty enimmäisrangaistus on vähintään kolme vuotta vankeutta, valvovan viranomaisen on ilmoitettava merkittävän poikkeaman havaitsemisesta poliisille.

Jos merkittävällä poikkeamalla on vaikutuksia muihin Euroopan unionin jäsenvaltioihin tai muihin toimialoihin, valvovan viranomaisen on tiedotettava siitä 18 §:ssä tarkoitetulle keskitetylle yhteyspisteelle ja toimitettava sitä koskevat ilmoitukset, raportit ja muut tiedot yhteyspisteelle.

Jos poikkeama vaikuttaa toiseen Euroopan unionin jäsenvaltioon, keskitetyn yhteyspisteen on ilmoitettava siitä ilman aiheetonta viivytystä Euroopan unionin kyberturvallisuusvirastolle ja niille jäsenvaltioille, joihin poikkeama vaikuttaa. Keskitetyn yhteyspisteen on pyynnöstä toimitettava myös 11–13 §:ssä tarkoitetut ilmoitukset ja raportit sen Euroopan unionin jäsenvaltion, johon poikkeama vaikuttaa, keskitetylle yhteyspisteelle. Keskitetty yhteyspiste saa luovuttaa tässä tarkoituksessa Euroopan unionin kyberturvallisuusvirastolle ja muiden Euroopan unionin jäsenvaltioiden keskitetyille yhteyspisteille tietoja merkittävästä poikkeamasta.

18 §

Keskitetty yhteyspiste

Liikenne- ja viestintäviraston Kyberturvallisuuskeskus toimii NIS 2 -direktiivin 8 artiklan 3 kohdassa tarkoitettuna keskitettynä yhteyspisteenä.

Keskitetyn yhteyspisteen tehtävänä on edistää valvovien viranomaisten välistä yhteistyötä ja koordinaatiota tämän lain mukaisten tehtävien toteuttamisessa.

Keskitetyn yhteyspisteen on toimitettava Euroopan unionin kyberturvallisuusvirastolle kolmen kuukauden välein yhteenvetoraportti, joka sisältää anonymisoidut koontitiedot 11–13 ja 15 §:n nojalla ilmoitetuista merkittävistä poikkeamista, poikkeamista, kyberuhkista ja läheltä piti –tilanteista. Keskitetyllä yhteyspisteellä on oikeus saada tätä tarkoitusta varten anonymisoidut koontitiedot valvovalta viranomaiselta.

3 luku

CSIRT-yksikkö

19 §

CSIRT-yksikkö

Liikenne- ja viestintävirastossa toimii tietoturvaloukkauksiin reagoiva ja niitä tutkiva NIS 2 –direktiivin 1 artiklan 2 kohdan a alakohdassa tarkoitettu CSIRT-yksikkö. Sen toiminta on järjestettävä erilliseksi 26 §:n nojalla tehtävästä valvonnasta.

CSIRT-yksikön on täytettävä seuraavat vaatimukset:

1) sen on varmistettava viestintäkanaviensa kattava saatavuus välttäen viestinnän täysin katkaisevia yksittäisiä vikaantumispisteitä ja ylläpidettävä useita viestintäkeinoja, joilla muut voivat ottaa siihen ja se voi ottaa muihin yhteyttä milloin tahansa.;

2) sen toimitilat ja niiden toimia tukevat tietojärjestelmät on sijoitettava suojattuihin paikkoihin;

3) sillä on oltava tarkoituksenmukainen järjestelmä pyyntöjen hallintaa ja reititystä varten, erityisesti tapausten tuloksekkaan ja tehokkaan edelleen ohjauksen helpottamiseksi;

4) sen on varmistettava toimintojensa luottamuksellisuus ja luotettavuus;

5) sillä on oltava riittävä henkilöstö palvelujensa jatkuvan saatavuuden varmistamiseksi, ja sen on varmistettava henkilöstönsä asianmukainen koulutus;

6) sillä on oltava varautumisjärjestelyt palvelujensa jatkuvuuden varmistamiseksi.

CSIRT-yksikön on määritettävä selkeästi 2 momentin 1 kohdassa tarkoitetut viestintäkanavat ja tiedotettava niistä kohderyhmilleen ja yhteistyökumppaneilleen.

20 §

CSIRT-yksikön tehtävät

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 sen jäseniä niiden pyynnöstä;

7) nimetä asiantuntijoita NIS 2 -direktiivin 19 artiklassa tarkoitettuihin vertaisarviointeihin;

8) edistää tietoturvallisten tiedonjakovälineiden käyttöönottoa;

9) antaa ohjeita ja suosituksia poikkeamien käsittelemisestä, kyberturvallisuuden kriisinhallinnasta ja koordinoidusta haavoittuvuuksien julkistamisesta.

CSIRT-yksikkö voi asettaa tehtäviään riskiperusteisesti tärkeysjärjestykseen käytettävissään olevien voimavarojen mukaisesti.

CSIRT-yksikkö koordinoi 23 §:ssä tarkoitettuja kyberturvallisuustietojen vapaaehtoisia jakamisjärjestelyjä itsensä, tämän lain soveltamisalaan kuuluvien toimijoiden ja muiden yhteisöjen kesken.

CSIRT-yksikkö voi tuottaa 1 momentin 2 kohdassa tarkoitettua viestintäverkon ja tietojärjestelmien reaaliaikaista tai lähes reaaliaikaista tietoturvallisuuden seurantaa koskevaa palvelua viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden varmistamiseksi, poikkeamien havaitsemiseksi ja selvittämiseksi sekä kyberuhkien ennalta estämiseksi (*tietoturvaloukkausten havainnointipalvelu*). CSIRT-yksikkö voi tarjota tietoturvaloukkausten havainnointipalvelua suoraan sitä pyytäville toimijoille ja muille yhteisöille sekä sellaisille tietoturvapalveluntarjoajille, jotka tarjoavat tietoturvaloukkausten havainnointipalvelua toimijoille tai muille yhteisöille käytettäväksi (*palvelukeskus*).

CSIRT-yksikön 1 momentin 1 ja 2 kohdassa sekä 21 §:n 4 momentissa tarkoitetusta palvelusta voidaan periä maksu siltä, joka palvelua pyytää. Viranomaisten suoritteiden maksullisuudesta ja suoritteista perittävien maksujen suuruuden yleisistä perusteista sekä maksujen muista perusteista säädetään valtion maksuperustelaissa (150/1992).

21 §

Yleisten viestintäverkkojen ja tietojärjestelmien verkkopohjainen haavoittuvuuskartoitus

CSIRT-yksiköllä on oikeus ennakoivalla, muulla kuin intrusiivisella tavalla havainnoida ja kartoittaa tietoja yleiseen viestintäverkkoon liitetyistä viestintäverkoista ja tietojärjestelmistä haavoittuvuuksien, kyberuhkien ja turvattomasti määritettyjen viestintäverkkojen tai tietojärjestelmien asetuksien havaitsemiseksi (*haavoittuvuuskartoitus*). Haavoittuvuuskartoitus

tehdään haavoittuvien tai turvattomasti määritettyjen viestintäverkkojen ja tietojärjestelmien asetuksien havaitsemiseksi ja havainnoista asianomaisille tahoille ilmoittamiseksi.

Haavoittuvuuskartoituksen toteuttamisessa CSIRT-yksiköllä on oikeus yleisen viestintäverkon välityksellä hankkia tietoja siihen kytkettyjen viestintäverkkolaitteiden, telepäätelaitteiden, muiden tietojärjestelmien ja 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.

Haavoittuvuuskartoituksessa havaittuja, kartoituksen kohteeseen yhdistettävissä olevia tietoja saa käyttää vain viestintäverkkoon tai tietojärjestelmään kohdistuvista haavoittuvuuksista ja riskeistä ilmoittamiseksi kartoituksen kohteelle. CSIRT-yksikkö voi käyttää haavoittuvuuskartoituksella hankittuja tietoja lisäksi 20 §:n 1 momentin 1, 4 ja 5 kohdassa tarkoitettujen tehtävien hoitamiseksi. Tarpeettomat tiedot on poistettava viipymättä.

CSIRT-yksiköllä on oikeus tehdä kartoituksen kohteen pyynnöstä haavoittuvuuskartoitus kartoituksen kohteen viestintäverkossa tai tietojärjestelmissä 1–3 momentissa säädetystä poikkeavalla tavalla sellaisen haavoittuvuuden, kyberuhkan tai turvattomasti määritettyjen asetuksien havaitsemiseksi, jolla voi olla merkittävä vaikutus viestintäverkkoon tai tietojärjestelmään tai niiden avulla tarjottaviin palveluihin (*kohdennettu haavoittuvuuskartoitus*).

Haavoittuvuuskartoituksessa ja kohdennetussa haavoittuvuuskartoituksessa ei saa käsitellä sähköisten viestien sisältöä eikä välitystietoa. CSIRT-yksikön on hävitettävä haavoittuvuuskartoituksessa tai kohdennetussa haavoittuvuuskartoituksessa saamansa tiedot, kun ne eivät ole enää tarpeen tässä pykälässä tarkoitettujen tehtävien hoitamiseksi.

22 §

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 niistä johtuvista tarpeellisista jatkotoimista. Ilmoituksen saa antaa nimettömänä.

Koordinaattorina CSIRT-yksikkö ottaa yhteyttä ja toimii tarvittaessa välittäjänä haavoittuvuudesta ilmoittavan tahon ja TVT-tuotteen tai -palvelun valmistajan tai tarjoajan välillä, avustaa haavoittuvuudesta ilmoittavia tahoja ja neuvottelee haavoittuvuuden julkistamisen aikataulusta sekä koordinoi useisiin toimijoihin vaikuttavien haavoittuvuuksien hallintaa. Lisäksi CSIRT-yksikkö ohjaa ja neuvoo tietojen ilmoittamisessa Euroopan haavoittuvuustietokantaan ja tietojen hakemisessa siitä.

CSIRT-yksiköllä on oikeus ilmoittaa Euroopan haavoittuvuustietokantaan haavoittuvuuksista tiedot:

1)jotka sisältävät kuvauksen haavoittuvuudesta;

2) TVT-tuotteista tai -palveluista, joihin haavoittuvuus vaikuttaa, sekä haavoittuvuuden vakavuus niiden olosuhteiden perusteella, joissa haavoittuvuutta voidaan hyödyntää;

3) ohjelmistokorjausten saatavuudesta ja, jos niitä ei ole saatavilla, valvovan viranomaisen tai CSIRT-yksikön ohjeistuksesta 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 Euroopan unionin jäsenvaltioihin, sen on tehtävä yhteistyötä kyseisten valtioiden CSIRT-yksiköiden kanssa CSIRT-verkostossa.

23 §

Kyberturvallisuustietojen vapaaehtoiset jakamisjärjestelyt

CSIRT-yksikön, toimijoiden ja muiden kuin tämän lain soveltamisalaan kuuluvien yhteisöiden välillä voidaan muodostaa CSIRT-yksikön koordinoimia kyberturvallisuustietojen vapaaehtoisia jakamisjärjestelyitä niihin osallistuvien yhteisöjen sekä niiden asiakkaiden viestintäverkkoihin, tietojärjestelmiin tai palveluihin kohdistuvien kyberuhkien ehkäisemiseksi ja havaitsemiseksi, poikkeamien hallitsemiseksi ja niistä palautumiseksi ja niiden vaikutusten lieventämiseksi.

Kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn osallistuvien kesken voidaan luovuttaa tietoja:

1) kyberuhkista;
2) poikkeamista ja läheltä piti –tilanteista;
3) haavoittuvuuksista;
4) taktiikoista, tekniikoista ja menettelyistä;
5) vaarantumisindikaattoreista;
6) yksittäisistä uhkatoimijoista;
7) kyberturvallisuushälytyksistä;
8) muista kuin 1-7 kohdassa tarkoitetuista kyberuhkien ja poikkeamien torjumiseksi tarpeellisista seikoista.

Sen lisäksi, mitä sähköisen viestinnän palveluista annetun lain 319 §:ssä säädetään tietojen luovuttamisesta, CSIRT -yksikkö voi luovuttaa jakamisjärjestelyyn osallistuvalle tämän lain mukaisia tehtäviä suorittaessaan saamansa tiedon kyberuhkaan tai poikkeamaan liittyvästä välitystiedosta tai haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä.

Jakamisjärjestelyihin osallistuva toimija tai muu yhteisö saa sähköisen viestinnän palveluista annetun lain 136 §:n 4 momentin estämättä luovuttaa oma-aloitteisesti CSIRT-yksikölle ja toiselle tämän lain mukaiseen vapaaehtoiseen jakamisjärjestelyyn osallistuvalle tietoa kyberuhkaan tai poikkeamaan liittyvästä välitystiedosta tai haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä.

Jakamisjärjestelyihin osallistuva saa käsitellä tämän pykälän nojalla saamaansa kyberuhkaan tai poikkeamaan liittyvää välitystietoa tai haitallisen tietokoneohjelman tai käskyn sisältävää viestiä koskevaa tietoa vain 1 momentissa tarkoitettuihin tarkoituksiin. CSIRT-yksikkö voi lisäksi käsitellä tämän pykälän nojalla saamiaan tietoja 20 §:n 1 momentissa säädetyn tehtävänsä hoitamiseksi. Tiedon luovuttamisella ei saa rajoittaa luottamuksellisen viestin ja yksityiselämän suojaa enempää kuin on välttämätöntä 1 momentissa säädetyn tarkoituksen vuoksi.

24 §

Tietoturvaloukkausten havainnointipalveluun liittyvä tiedonkäsittely

Tietoturvaloukkausten havainnointipalvelua käyttävä toimija, muu yhteisö, palvelukeskus ja CSIRT-yksikkö saavat luovuttaa toisilleen viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden seurannan kannalta tarpeellisia tietoja kyberuhkien ehkäisemiseksi ja havaitsemiseksi sekä poikkeamien hallitsemiseksi, niistä palautumiseksi ja niiden vaikutusten lieventämiseksi. Siinä määrin kuin tietoturvaloukkausten havainnointipalvelun toteuttamiseksi on välttämätöntä, luovutettavat tiedot saavat sisältää palvelua käyttävän toimijan tai muun yhteisön palvelussa käsiteltäväksi pyytämiä sellaisia sähköisiä viestejä tai niihin liittyviä välitystietoja, joita sillä on oikeus käsitellä sähköisen viestinnän palveluista annetun lain 272 §:n nojalla.

Välitystietojen ja sähköisten viestien käsittelyyn tietoturvaloukkausten havainnointipalvelussa CSIRT-yksikössä ja palvelukeskuksessa sovelletaan, mitä sähköisen viestinnän palveluista annetun lain 136–138, 145 ja 272 §:ssä säädetään. CSIRT-yksikkö saa lisäksi käyttää palvelun tuottamisen yhteydessä saamiaan välitystietoja ja muita tietoja kansallisen kyberturvallisuuden tilannekuvan ylläpitämisen tukemiseksi.

Mitä sähköisen viestinnän palveluista annetun lain 316 §:n 4 momentissa säädetään merkittävien tietoturvaloukkausten tai -uhkien selvittämistä koskevien tietojen hävittämisestä ja 319 §:n 1 momentissa salassapitovelvollisuudesta, koskee myös CSIRT-yksikölle tietoturvaloukkausten havainnointipalvelun toteuttamiseksi luovutettuja viestejä ja välitystietoja.

25 §

CSIRT-yksikölle vapaaehtoisesti luovutettu tieto

Siitä riippumatta, mitä viranomaisten tiedonsaantioikeuksista muualla laissa säädetään, CSIRT-yksikölle tämän lain mukaisten tehtävien hoitamiseksi vapaaehtoisesti luovutettua tietoa ei saa ilman tiedon luovuttaneen suostumusta käyttää tiedon luovuttajaan kohdistuvassa rikostutkinnassa eikä hallinnollisessa tai muussa tiedon luovuttajaan kohdistuvassa päätöksenteossa.

4 luku

Valvonta

26 §

Valvovat viranomaiset

Tämän lain, sen nojalla annettujen määräysten ja NIS 2 –direktiivin nojalla annettujen säännösten noudattamista valvoo:

1) Liikenne- ja viestintävirasto siltä osin kuin kyse on liitteen I kohdissa 1-7 ja liitteen II kohdissa 1-5 tarkoitetuista toimijoista;

2) Energiavirasto siltä osin kuin kyse on liitteen I kohdissa 8 ja 9 sekä kohdan 10 alakohdissa a-c ja kohdan 12 alakohdassa b tarkoitetuista toimijoista;

3) Turvallisuus- ja kemikaalivirasto siltä osin kuin kyse on liitteen I kohdan 10 alakohdissa d-g, kohdassa 11, kohdan 12 alakohdassa a sekä liitteen II kohdissa 6 ja 11-13 tarkoitetuista toimijoista;

4) Sosiaali- ja terveysalan lupa- ja valvontavirasto siltä osin kuin kyse on liitteen I kohdan 13 alakohdissa a ja b tarkoitetuista toimijoista;

5) Etelä-Savon elinkeino-, liikenne- ja ympäristökeskus siltä osin kuin kyse on liitteen I kohdissa 14-15 sekä liitteen II kohdassa 8 tarkoitetuista toimijoista.

6) Ruokavirasto siltä osin kuin kyse on liitteen II kohdassa 7 tarkoitetuista toimijoista;

7) Lääkealan turvallisuus- ja kehittämiskeskus siltä osin kuin kyse on liitteen I kohdan 13 alakohdissa c-f ja liitteen II kohdissa 9 ja 10 tarkoitetuista toimijoista.

Valvovien viranomaisten on tehtävä yhteistyötä valvonnan toteuttamisessa.

27 §

Valvonnan kohdistaminen

Valvonta on kohdistettava keskeisiin toimijoihin. Valvova viranomainen voi kuitenkin kohdistaa valvontaa myös muuhun kuin keskeiseen toimijaan, jos on perusteltu syy epäillä, että tämä ei ole noudattanut tätä lakia, sen nojalla annettuja määräyksiä tai NIS 2 -direktiivin nojalla annettuja säännöksiä.

Keskeisellä toimijalla tarkoitetaan

1) liitteessä I tarkoitettua toimijaa, joka ylittää mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä annetun komission suosituksen 2003/361/EY liitteen 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset;

2) hyväksyttyjä luottamuspalvelun tarjoajia, aluetunnusrekisterin ylläpitäjiä sekä DNS-palveluntarjoajia;

3) yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajia, jotka täyttävät tai ylittävät mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä annetun komission suosituksen 2003/361/EY liitteen 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset; sekä

4) 3 §:n 3 momentissa tarkoitettua toimijaa.

Valvova viranomainen voi asettaa sille tässä laissa säädetyt tehtävät tärkeysjärjestykseen riskiperusteisesti. Valvovan viranomaisen on otettava valvonnan kohdistamisessa ja 29–34 §:ssä tarkoitettujen toimien käyttämisestä päättäessään huomioon:

1) liitteessä I tai II tarkoitetun toiminnan laatu ja laajuus;

2) tietojärjestelmän tai viestintäverkon merkitys liitteessä I tai II tarkoitetulle toiminnalle; ja

3) 37 §:ssä tarkoitetut seikat.

28 §

Tiedonsaantioikeus

Valvovalla viranomaisella on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada toimijalta kyberturvallisuutta koskevien riskien hallintaa, riskienhallinnan toimintamallia, hallintatoimenpiteitä ja merkittävää poikkeamaa koskevat tiedot sekä muut edellä mainittuihin tietoihin välittömästi liittyvät tiedot, jotka ovat välttämättömiä kyberturvallisuutta koskevan riskienhallintavelvoitteen noudattamisen ja merkittävistä poikkeamista ilmoittamisen ja raportoinnin valvontaa varten.

Valvovalla viranomaisella on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada toimijalta välitystieto, sijaintitieto sekä tieto haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä, jos se on välttämätöntä kyberturvallisuutta koskevan riskienhallintavelvoitteen noudattamisen tai merkittävistä poikkeamista ilmoittamisen ja raportoinnin valvomista varten. Valvovan viranomaisen tämän momentin nojalla saamat tiedot on pidettävä salassa.

Valvovan viranomaisen on tietopyynnössä ilmoitettava pyynnön tarkoitus sekä täsmennettävä pyydetyt tiedot. Tiedot on luovutettava viipymättä, viranomaisen pyytämässä muodossa ja maksutta.

Valvovalla viranomaisella on salassapitosäännösten, 2 momentissa säädetyn salassapitovelvollisuuden ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa tässä laissa säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto toiselle valvovalle viranomaiselle ja CSIRT-yksikölle, jos se on välttämätöntä viranomaiselle tässä laissa säädettyä tehtävää varten. Tiedonsaantioikeuden käyttämisellä tai tietojen luovuttamisella ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.

Valvovan viranomaisen tiedonsaantioikeus ei koske CSIRT-yksikön tämän lain nojalla tuottamia palveluita eikä tietoja toimijassa.

Tässä pykälässä tarkoitettu tiedonsaantioikeus ei koske salassa pidettäviä tietoja julkisen hallinnon turvallisuusverkkotoiminnasta annetussa laissa (10/2015) tarkoitetusta

turvallisuusverkon palvelutuotannosta tai palvelujen käytöstä eikä tietoja, joiden luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin niihin liittyvää tärkeää etua.

29 §

Tarkastusoikeus

Valvovalla viranomaisella on oikeus tehdä toimijaa koskeva tarkastus. Tarkastus tehdään tässä laissa tai sen nojalla annetussa määräyksessä taikka NIS 2-direktiivin nojalla annetuissa säännöksissä säädettyjen velvollisuuksien noudattamisen valvomiseksi siinä laajuudessa kuin se on tarpeen.

Jos se on tarkastuksen laadun tai siihen liittyvien teknisten syiden vuoksi tarpeellista, valvova viranomainen voi pyytää tarkastuksen suorittajaksi toisen valvovan viranomaisen tai käyttää tarkastuksessa apuna toista valvovaa viranomaista, tietoturvallisuuden arviointilaitosta ja ulkopuolista tietotekniikan asiantuntijaa. Tarkastuksen suorittajalla ja siihen osallistuvalla on oltava sellainen koulutus ja kokemus kuin tarkastuksen suorittamiseksi on tarpeen. 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, tietoturvallisuuden arviointilaitoksella 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. Tarkastuksen suorittajan tarkastus- ja tiedonsaantioikeuteen sovelletaan mitä 28 §:n 6 momentissa säädetään tiedonsaantioikeuden rajoituksista.

Tarkastuksessa noudatettavaan menettelyyn sovelletaan, mitä hallintolain (434/2003) 39 §:ssä säädetään tarkastuksesta.

30 §

Turvallisuusauditointi

Valvovalla viranomaisella on oikeus velvoittaa 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 tarkoitetun kyberturvallisuutta koskevan riskienhallinnan toimintamallin tai siinä edellytettyjä hallintatoimenpiteitä taikka muutoin olennaisesti ja vakavasti toiminut tässä laissa tai sen nojalla taikka NIS 2 –direktiivin nojalla säädetyn velvollisuuden vastaisesti.

Valvovalla viranomaisella on oikeus saada tieto teetetyn turvallisuusauditoinnin tuloksista sekä velvoittaa toimija toteuttamaan turvallisuusauditoinnin suosittelemat kohtuulliset ja oikeasuhtaiset toimenpiteet kyberturvallisuutta koskevan riskienhallinnan kehittämiseksi.

31 §

Valvontapäätös ja varoitus

Valvova viranomainen voi velvoittaa toimijan määräajassa korjaamaan puutteet tässä laissa tai sen nojalla annetuissa määräyksissä taikka NIS 2-direktiivin nojalla annetuissa säännöksissä säädettyjen velvollisuuksien noudattamisessa. Valvova viranomainen voi päätöksellä velvoittaa toimijan julkistamaan kyseiset puutteet tai muut seikat, jotka liittyvät tämän lain, sen nojalla annettujen määräysten tai NIS 2-direktiivin nojalla annettujen säännösten rikkomiseen.

Valvova viranomainen voi antaa toimijalle varoituksen, jos tämä ei ole noudattanut tätä lakia, sen nojalla annettuja määräyksiä tai NIS 2 -direktiivin nojalla annettuja säännöksiä. Varoituksessa on yksilöitävä puute tai laiminlyönti, jota se koskee. Varoitus on annettava kirjallisena.

32 §

Johdon toiminnan rajoittaminen

Valvova viranomainen voi kieltää määräajaksi henkilöä toimimasta keskeisen toimijan hallituksen jäsenenä tai varajäsenenä, hallintoneuvoston jäsenenä tai varajäsenenä, toimitusjohtajana tai muussa siihen rinnastettavassa asemassa, jos tämä on toistuvasti ja vakavasti rikkonut 10 §:ssä säädettyjä velvollisuuksia. Valvovan viranomaisen on ennen päätöksen tekemistä annettava keskeiselle toimijalle varoitus, jossa yksilöidään puute tai laiminlyönti, jonka korjaamatta jättäminen voi johtaa päätökseen johdon toiminnan rajoittamisesta, sekä varattava toimijalle kohtuullinen määräaika puutteen tai laiminlyönnin korjaamiseksi. Päätös saa olla voimassa enintään niin kauan, kuin sen perusteena oleva puute tai laiminlyönti on korjaamatta, kuitenkin enintään viisi vuotta.

Edellä 1 momentissa säädetystä poiketen johdon toimintaa ei saa rajoittaa, jos kyse on yksityisestä elinkeinonharjoittajasta, avoimesta yhtiöstä, kommandiittiyhtiöstä, valtion viranomaisesta, valtion liikelaitoksesta, hyvinvointialueesta tai –yhtymästä, kunnallisesta viranomaisesta, itsenäisestä julkisoikeudellisesta laitoksesta, eduskunnan virastosta, tasavallan presidentin kansliasta, Suomen evankelisluterilaisesta kirkosta, Suomen ortodoksisesta kirkosta tai niiden seurakunnista, seurakuntayhtymistä tai muista elimistä.

33 §

Ilmoitus tietosuojavaltuutetulle

Jos valvova viranomainen saa tässä laissa tarkoitettujen tehtävien hoitamisen yhteydessä tietoonsa, että 2 luvussa säädettyjen velvollisuuksien laiminlyönti voi johtaa tai on johtanut yleisessä tietosuoja-asetuksessa tarkoitettuun henkilötietojen tietoturvaloukkaukseen, josta on mainitun asetuksen 33 artiklan nojalla ilmoitettava asetuksessa tarkoitetulle valvontaviranomaiselle, valvovan viranomaisen on ilmoitettava asiasta tietosuojavaltuutetulle.

Valvovan viranomaisen on tehtävä 1 momentissa tarkoitettu ilmoitus tietosuojavaltuutetulle myös, jos yleisen tietosuoja-asetuksen nojalla toimivaltainen valvontaviranomainen on sijoittunut toiseen jäsenvaltioon.

34 §

Uhkasakko, teettämisuhka ja keskeyttämisuhka

Valvova viranomainen voi asettaa tämän lain nojalla antamansa päätöksen tehosteeksi uhkasakon, teettämisuhan tai keskeyttämisuhan.

5 luku

Seuraamusmaksu

35 §

Hallinnollinen seuraamusmaksu

Toimijalle voidaan määrätä hallinnollinen seuraamusmaksu, jos se tahallaan tai törkeästä huolimattomuudesta laiminlyö:

1) 7 §:ssä tarkoitetun velvollisuuden hallita riskejä, 8 §:ssä tarkoitetun kyberturvallisuutta koskevan riskienhallinnan toimintamallin laatimisen tai 9 §:n 1 momentissa tarkoitettujen osa-alueiden huomioimisen osana kyberturvallisuuden riskienhallinnan toimintamallia;

2) toteuttaa 9 §:n 2 momentissa tarkoitetut toimenpiteet;

3) antaa 11 §:ssä tarkoitetun poikkeamailmoituksen, 12 §:ssä tarkoitetun väliraportin tai 13 §:ssä tarkoitetun loppuraportin valvovalle viranomaiselle;

4) antaa 41 §:ssä tarkoitetut tiedot valvovalle viranomaiselle.

Seuraamusmaksua ei voi määrätä valtion viranomaisille, valtion liikelaitoksille, hyvinvointialueille eikä –yhtymille, 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.

36 §

Seuraamusmaksulautakunta

Liikenne- ja viestintäviraston yhteydessä toimii seuraamusmaksulautakunta. Lautakunta määrää hallinnollisen seuraamusmaksun valvovan viranomaisen esityksestä. Hallinnollinen seuraamusmaksu määrätään maksettavaksi valtiolle.

Liikenne- ja viestintävirasto nimeää lautakunnan puheenjohtajan ja varapuheenjohtajan. Kukin valvova viranomainen nimeää lautakuntaan jäsenen ja tälle henkilökohtaisen varajäsenen. Lautakunnan jäseneltä ja varajäseneltä edellytetään perehtyneisyyttä kyberturvallisuutta koskevien riskien hallintaan sekä NIS 2-direktiiviin ja sitä täytäntöönpanevassa sääntelyssä asetettuihin velvollisuuksiin 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 seuraamusmaksun määräämiseksi välttämättömät 28 §:ssä tarkoitetut tiedot sekä muut tiedot, jotka ovat välttämättömiä seuraamusmaksun määräämiseksi tai sen määrän arvioimiseksi.

37 §

Seuraamusmaksun määrääminen

Hallinnollisen seuraamusmaksun määrä perustuu kokonaisarviointiin, jossa otetaan huomioon tapauksen olosuhteet sekä ainakin 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) havaittujen puutteiden jättäminen korjaamatta valvovan viranomaisen päätöksistä 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.

38 §

Seuraamusmaksun enimmäismäärä

Keskeiselle toimijalle määrättävän hallinnollisen seuraamusmaksun enimmäismäärä on 10 000 000 euroa tai kaksi prosenttia toimijan edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

Muulle kuin keskeiselle toimijalle määrättävän hallinnollisen seuraamusmaksun enimmäismäärä on 7 000 000 euroa tai 1,4 prosenttia toimijan edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

39 §

Seuraamusmaksun määräämättä jättäminen

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.

40 §

Seuraamusmaksun täytäntöönpano

Seuraamusmaksun täytäntöönpanosta säädetään sakon täytäntöönpanosta annetussa laissa (672/2002). Seuraamusmaksu vanhenee viiden vuoden kuluttua lainvoiman saaneen päätöksen antamispäivästä.

6 luku

Muut säännökset

41 §

Toimijaluettelo

Valvova viranomainen ylläpitää valvontatoimialansa osalta toimijaluetteloa.

Toimijoiden on ilmoitettava valvovalle viranomaiselle:

1) toimijan nimi;

2) osoitteensa, sähköpostiosoitteensa, puhelinnumeronsa ja muut ajantasaiset yhteystietonsa;

3) IP-osoitealueensa;

4) NIS 2 -direktiivin liitteessä I tai II tarkoitettu asiaankuuluva toimialansa ja sen osa;

5) tieto siitä, onko se keskeinen toimija;

6) luettelo niistä Euroopan unionin jäsenvaltioista, joissa se tarjoaa NIS 2 -direktiivin soveltamisalaan kuuluvia palveluja; ja

7) osallistumisesta 23 §:ssä tarkoitettuun kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn.

DNS-palveluntarjoajien, aluetunnusrekisterin ylläpitäjien, pilvipalvelujen tarjoajien, datakeskuspalvelujen tarjoajien, sisällönjakeluverkkojen tarjoajien, hallintapalvelun tarjoajien, tietoturvapalveluntarjoajien, verkossa toimivien markkinapaikkojen tarjoajien, verkossa toimivien hakukoneiden tarjoajien ja verkkoyhteisöalustojen tarjoajien on ilmoitettava valvovalle viranomaiselle 2 momentissa tarkoitettujen tietojen lisäksi:

1) NIS 2 -direktiivin liitteessä I tai II tarkoitettu toimijatyyppinsä;

2) päätoimipaikkansa ja muiden Euroopan unionin jäsenvaltiossa sijaitsevien laillisten toimipaikkojensa osoite tai, jos toimija ei ole sijoittautunut Euroopan unioniin, sen Euroopan unioniin nimetyn edustajan osoite, sähköpostiosoite, puhelinnumero ja muut ajantasaiset yhteystiedot; ja

3) luettelo Euroopan unionin jäsenvaltioista, joissa toimija tarjoaa palveluita.

Toimijoiden on ilmoitettava muutoksista tässä pykälässä tarkoitettuihin tietoihin viipymättä. Muutoksesta 2 momentissa tarkoitettuihin tietoihin on ilmoitettava valvovalle viranomaiselle kahden viikon kuluessa ja 3 momentissa tarkoitettuihin tietoihin kolmen kuukauden kuluessa muutoshetkestä. Valvova viranomainen voi antaa tarkempia teknisiä määräyksiä tietojen ilmoittamisesta.

Valvovan viranomaisen on toimitettava keskitetylle yhteyspisteelle NIS 2 -direktiivin 3 artiklan 5 kohdassa ja 27 artiklan 4 kohdassa tarkoitettujen ilmoituksien tekemiseksi tarpeelliset tiedot toimijaluettelosta. Keskitetty yhteyspiste vastaa mainituissa kohdissa tarkoitettujen ilmoituksien tekemisestä Euroopan komissiolle, NIS-yhteistyöryhmälle ja Euroopan unionin kyberturvallisuusvirastolle. CSIRT-yksiköllä on oikeus saada valvovalta viranomaiselta tietoja toimijaluettelosta.

42 §

Kansallinen kyberturvallisuusstrategia

Valtioneuvosto hyväksyy kansallisen kyberturvallisuusstrategian ja vastaa sen päivittämisestä säännöllisesti vähintään viiden vuoden välein.

Kansalliseen kyberturvallisuusstrategiaan on sisällytettävä vähintään NIS 2 -direktiivin 7 artiklan 1 kohdassa tarkoitetut osa-alueet ja 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 niihin liittyvää tärkeää etua.

43 §

Laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintasuunnitelma

Kyberturvallisuutta koskevissa kriisitilanteissa käytettävissä olevien valmiuksien, voimavarojen ja menettelyiden yksilöimiseksi laaditaan laajamittaisten kyberturvallisuuspoikkeamien ja –kriisien hallintasuunnitelma. Liikenne- ja viestintävirasto vastaa suunnitelman laatimisesta yhteistoiminnassa 26 §:ssä tarkoitettujen valvovien viranomaisten, poliisin, suojelupoliisin, Puolustusvoimien ja Huoltovarmuuskeskuksen kanssa.

Suunnitelman tulee sisältää laajamittaisten kyberturvallisuuspoikkeamien ja –kriisien hallitsemiseksi tarpeelliset tiedot:

1) kansallisten varautumiskeinojen ja –toimien tavoitteista;

2) viranomaisten tehtävistä ja vastuista;

3) kriisinhallintaa koskevista toimintatavoista ja niiden sisällyttämisestä yleiseen kansalliseen kriisinhallintakehykseen sekä tiedonvaihtokanavista viranomaisten välillä;

4) kansallisista varautumiskeinoista, joihin kuuluvat myös harjoitukset ja koulutustoimenpiteet;

5) keskeisistä julkisista ja yksityisistä sidosryhmistä ja keskeisestä infrastruktuurista;

6) viranomaisten välisestä menettelystä osallistuttaessa laajamittaisten kyberturvallisuuspoikkeamien ja –kriisien koordinoituun hallintaan Euroopan unionin tasolla.

Edellä 2 momentissa tarkoitetut tiedot on annettava tiedoksi Euroopan komissiolle ja NIS 2 -direktiivin 16 artiklassa tarkoitetulle Euroopan kyberkriisien yhteysorganisaatioiden verkostolle kolmen kuukauden kuluessa suunnitelman hyväksymisestä. Tietoja voidaan jättää antamatta siltä osin, jos niiden luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin niihin liittyvää tärkeää etua.

44 §

Kyberkriisinhallintaviranomainen

NIS 2 -direktiivin 9 artiklan 1 kohdan kohdassa tarkoitettuna kyberkriisinhallintaviranomaisena toimii kukin 43 §:n 1 momentissa tarkoitettu viranomainen sille laissa säädettyjen tehtävien mukaisesti. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus toimii koordinaattorina laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallinnassa.

45 §

Viranomaisten yhteistyö

Valvovien viranomaisten, CSIRT-yksikön ja keskitetyn yhteyspisteen on toimittava yhteistyössä tässä laissa ja NIS 2 -direktiivin nojalla säädettyjen tehtävien hoitamiseksi.

Valvovien viranomaisten, CSIRT-yksikön ja keskitetyn yhteyspisteen on toimittava tarvittaessa yhteistyössä poliisin tai muun esitutkintaviranomaisen, tietosuojavaltuutetun, Liikenne- ja viestintäviraston sille ilmailulaissa, sähköisen viestinnän palveluista annetussa laissa ja eIDAS-asetuksessa säädettyjen tehtävien osalta ja Finanssivalvonnan kanssa.

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, Liikenne- ja viestintäviraston ja Finanssivalvonnan on vaihdettava keskenään säännöllisesti tietoja merkittävistä poikkeamista ja kyberuhkista.

46 §

Muutoksenhaku

Muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).

Valvovan viranomaisen tekemää päätöstä on noudatettava muutoksenhausta huolimatta, ellei muutoksenhakuviranomainen toisin määrää. Muutoksenhaussa uhkasakon asettamista ja maksettavaksi tuomitsemista sekä teettämis- tai keskeyttämisuhan asettamista ja täytäntöönpantavaksi määräämistä koskevaan päätökseen sovelletaan kuitenkin, mitä uhkasakkolaissa (1113/1990) säädetään.

47 §

Voimaantulo

Tämä laki tulee voimaan päivänä kuuta 20 .

Tämän lain 41 §:ssä tarkoitettu ilmoitus on tehtävä viimeistään 31 päivänä joulukuuta 2024.

Liite I

Toimijat, jotka harjoittavat seuraavaa toimintaa tai ovat seuraavaa toimijatyyppiä:

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) Liikenteen palveluista annetun lain (320/2017) 15 luvussa tarkoitetun tieliikenteen ohjaus- ja hallintapalvelun tarjoaja.
   b) Liikenteen palveluista annetun lain 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) Aluetunnusrekisterin ylläpitäjät
   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 (587/2017) 3 §:n 1 momentin 10 kohdassa tarkoitetut jakeluverkonhaltijat
    b) Maakaasumarkkinalain 3 §:n 1 momentin 9 kohdassa tarkoitetut siirtoverkonhaltijat
    c) Maakaasumarkkinalain 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. Vety:
    a) Vedyn tuotantoa ja varastointia harjoittavat toimijat
    b) Vedyn siirtoa harjoittavat toimijat
13. Terveys:
    a) Sosiaali- ja terveydenhuollon valvonnasta annetun lain (741/2023) 4 §:n 2 kohdassa tarkoitetut palveluntuottajat, jotka tuottavat 4 kohdassa tarkoitettua terveyspalvelua
    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

f) veripalvelulain (197/2005) mukaiset veripalvelulaitokset, apteekit ja potilaiden oikeuksien soveltamisesta rajat ylittävässä terveydenhuollossa annetun EU-direktiivin (2011/24/EU) mukaiset lääkkeitä ja lääkinnällisiä laitteita toimittavat ja tarjoavat 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

Toimijat, jotka harjoittavat seuraavaa toimintaa tai ovat seuraavaa toimijatyyppiä:

1. Kuriiripalvelun tarjoajat ja yhteisön postipalvelujen sisämarkkinoiden kehittämistä ja palvelun laadun parantamista koskevista yhteisistä säännöistä annetun Euroopan parlamentin ja Neuvoston direktiivin 97/67/EY 2 artiklan 1 a alakohdassa tarkoitetut 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 § ja 10 §:n 1 momentin 2 kohta, sellaisina kuin niistä ovat 2 §:n 16 kohta laissa 488/2023 ja 3 § osaksi laeissa 653/2021 ja 488/2023, sekä

lisätään 1 §:ään siitä lailla 710/2021 kumotun 2 momentin tilalle uusi 2 momentti ja 2 §:ään uusi 17 – 26 kohta sekä lakiin uusi 4 a luku seuraavasti:

1 §

Lain tarkoitus

— —

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 annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2022/2555 (*NIS 2 -direktiivi*) toimijaa koskevia velvoitteita, niiden noudattamisen valvontaa ja seuraamuksia koskevat säännökset NIS 2 -direktiivin liitteen I kohdassa 10 tarkoitetulla julkishallinnon toimialalla *(julkishallinnon toimiala)*. NIS 2 -direktiivin täytäntöönpanosta muilta osin säädetään kyberturvallisuuslaissa (/).

2 §

Määritelmät

Tässä laissa tarkoitetaan:

— —

16) *käsittelysäännöillä* luonnollisen henkilön ennalta laatimia automaattisen tietojenkäsittelyn ohjaamiseen tarkoitettuja sääntöjä;

17) *viestintäverkolla ja tietojärjestelmällä*

a) eurooppalaisesta sähköisen viestinnän säännöstöstä annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2018/1972 2 artiklan 1 kohdassa tarkoitettua sähköistä viestintäverkkoa;

b) laitetta taikka yhteen kytkettyjen tai toisiinsa yhteydessä olevien laitteiden ryhmää, joista yksi tai useampi suorittaa ohjelman avulla digitaalisten tietojen automaattista käsittelyä; ja

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 niissä 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* tilannetta, tapahtumaa tai toimintaa, joka toteutuessaan 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) *kyberriskillä* poikkeaman aiheuttamien menetysten tai häiriön mahdollisuutta, joka ilmaistaan menetyksen tai häiriön suuruuden ja poikkeaman toteutumisen todennäköisyyden yhdistelmänä;

23) *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;

24) *merkittävällä poikkeamalla* poikkeamaa, joka:

a) on aiheuttanut tai voi aiheuttaa vakavan palvelujen toimintahäiriön tai viranomaiselle huomattavia taloudellisia tappioita; tai

b) on vaikuttanut tai voi vaikuttaa luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa;

25) *poikkeaman käsittelyllä* toimia ja menettelyjä, joilla pyritään ehkäisemään ja havaitsemaan poikkeama, analysoimaan, rajoittamaan tai hallitsemaan sitä ja palautumaan siitä;

26) *kriittisellä toimijalla* viranomaista tai muuta julkista hallintotehtävää hoitavaa, joka on kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2022/2557 2 artiklan 1 kohdassa tarkoitettu kriittinen toimija julkishallinnon toimialalla.

3 §

Lain soveltamisala ja sen rajaukset

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.

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 (652/2023).

Tämän lain 4 a lukua sovelletaan seuraaviin viranomaisiin ja viranomaisen toimintaan vain, jos viranomainen on kriittinen toimija:

1) tasavallan presidentin kanslia, Puolustusvoimat, poliisin hallinnosta annetussa laissa (110/1992) tarkoitetut poliisiyksiköt, Rajavartiolaitos, Syyttäjälaitos ja Tullin rikostorjunta;

2) tuomioistuimet ja valitusasioita käsittelemään perustetut lautakunnat;

3) Puolustuskiinteistöt;

4) kunnalliset viranomaiset lukuun ottamatta Helsingin kaupunkia, johon sovelletaan 4 a lukua sen hoitaessa hyvinvointialueiden järjestämisvastuulle lailla säädettyjä tehtäviä, vaikka se ei olisi kriittinen toimija;

5) Suomen Pankki;

6) yliopistolaissa tarkoitetut yliopistot, ammattikorkeakoululaissa tarkoitetut ammattikorkeakoulut ja Pelastusopisto;

7) julkisen hallinnon turvallisuusverkkotoiminnasta annetussa laissa (10/2015) tarkoitettu turvallisuusverkon palvelutuotanto ja turvallisuusverkon palvelujen käyttö;

8) viranomaiset, jotka on perustettu yhdessä Euroopan talousalueeseen kuulumattoman maan kanssa kansainvälisen sopimuksen mukaisesti ja näissä maissa sijaitsevat diplomaattiset edustustot ja konsuliedustustot sekä näiden verkko- ja tietojärjestelmät, siltä osin kuin tällaiset järjestelmät sijaitsevat edustuston tiloissa tai niitä ylläpidetään näissä maissa olevia käyttäjiä varten.

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. Tämän lain 18 g §:n 3 momenttia ja 18 h–18 l §:ää ei sovelleta eduskunnan oikeusasiamiehen eikä valtioneuvoston oikeuskanslerin toimintaan. Tämän lain 18 g §:n 3 momenttia ja 18 h–18 l §:ää ei sovelleta myöskään tasavallan presidentin kansliaan eikä tuomioistuinten tai valitusasioita käsittelemään perustettujen lautakuntien lainkäyttöön, vaikka niihin muutoin sovellettaisiin 4 a lukua niiden toimiessa kriittisenä toimijana.

Mitä 4 luvussa, 22–24 ja 25–27 §:ssä sekä 6 a luvussa säädetään tiedonhallintayksiköstä ja viranomaisesta, sovelletaan yksityisiin henkilöihin ja yhteisöihin sekä 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 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. Mitä 4 a luvussa säädetään tiedonhallintayksiköstä ja viranomaisesta, sovelletaan yksityiseen henkilöön ja yhteisöön sekä muuna kuin viranomaisena toimivaan julkisoikeudelliseen yhteisöön siltä osin kuin se hoitaa julkista hallintotehtävää ja on kriittinen toimija.

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, jollei 3 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.

— —

4 a luku

Kyberturvallisuutta koskevat velvollisuudet ja niiden noudattamisen valvonta

18 a §

Toimijajaottelu ja toimintaa koskeva ilmoitus

Tämän luvun soveltamisalaan kuuluvat tiedonhallintayksiköt ovat julkishallinnon toimialan keskeisiä toimijoita. Hyvinvointialueet ja hyvinvointiyhtymät sekä Helsingin kaupunki ovat kuitenkin tärkeitä toimijoita.

Tiedonhallintayksikön on ilmoitettava valvovalle viranomaiselle:

1) nimensä;
2) osoitteensa, sähköpostiosoitteensa, puhelinnumeronsa ja muut ajantasaiset yhteystietonsa;
3) IP-osoitealueensa;
4) tieto siitä, onko se julkishallinnon toimialan keskeinen vai tärkeä toimija;
5) luettelo muista Euroopan unionin jäsenvaltioista, joissa se tarjoaa palvelujaan;
6) osallistumisestaan kyberturvallisuuslain 23 §:ssä tarkoitettuun kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn.

Tiedonhallintayksikön on ilmoitettava kaikista 2 momentissa tarkoitettujen tietojen muutoksista viipymättä, viimeistään kahden viikon kuluttua muutoksesta.

18 b §

Velvollisuus hallita kyberturvallisuusriskejä ja riskienhallinnan toimintamalli

Tiedonhallintayksikön on tunnistettava, arvioitava ja hallittava kyberriskejä, joita kohdistuu sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Kyberturvallisuutta koskevalla riskienhallinnalla tulee estää tai minimoida poikkeamien vaikutus toimintaan, toiminnan jatkuvuuteen, palvelujen vastaanottajiin ja muihin palveluihin. Tiedonhallintayksikön on toteutettava 18 c §:ssä tarkoitetut kyberturvallisuutta koskevat riskienhallintatoimenpiteet.

Tiedonhallintayksiköllä on oltava käytössä ajantasainen kyberturvallisuutta koskeva riskienhallinnan toimintamalli viestintäverkkojen ja tietojärjestelmien ja niiden fyysisen ympäristön suojaamiseksi poikkeamilta ja niiden vaikutuksilta. Kyberturvallisuutta koskevassa riskienhallinnan toimintamallissa on tunnistettava viestintäverkkoihin ja tietojärjestelmiin ja niiden fyysiseen ympäristöön kohdistuvat riskit ottaen huomioon kaikki vaaratekijät huomioiva lähestymistapa. Toimintamallissa on määritettävä ja kuvattava kyberturvallisuutta koskevan riskienhallinnan tavoitteet, menettelyt ja vastuut sekä 18 c §:n mukaiset toimenpiteet, joilla viestintäverkkoja ja tietojärjestelmiä ja niiden fyysistä ympäristöä suojataan kyberuhkilta ja poikkeamilta.

Tiedonhallintayksikön johto vastaa kyberturvallisuutta koskevan riskienhallinnan toteuttamisen ja valvonnan järjestämisestä sekä hyväksyy riskienhallinnan toimintamallin ja valvoo sen toteuttamista. Tiedonhallintayksikön johdolla tulee olla riittävä perehtyneisyys kyberturvallisuutta koskevaan riskienhallintaan.

18 c §

Toimenpiteet kyberturvallisuutta koskevien riskien hallinnassa

Tiedonhallintayksikön on toteuttava oikeasuhtaiset tekniset, operatiiviset ja organisatoriset kyberturvallisuutta koskevat riskienhallintatoimenpiteet käyttämiensä viestintäverkkojen ja tietojärjestelmien turvallisuuteen kohdistuvien kyberriskien hallitsemiseksi ja haitallisten vaikutusten estämiseksi tai minimoimiseksi. Kyberturvallisuutta koskevassa riskienhallinnan toimintamallissa ja siihen perustuvissa kyberturvallisuuden riskienhallintatoimenpiteissä on otettava huomioon ja pidettävä yllä ajantasaisesti ainakin:

1) kyberturvallisuutta koskevan 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 käsittelemiseksi ja julkistamiseksi;

4) toimitusketjun välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, niihin sisällytetyt kyberturvallisuutta koskevat riskienhallintatoimenpiteet ja välittömien toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt sekä NIS2 -direktiivin 22 artiklan 1 kohdassa tarkoitetut kriittisiä toimitusketjuja koskevien koordinoitujen riskinarviointien tulokset;

5) omaisuudenhallinta ja sen 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 käyttämiseksi;

9) poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden ylläpitämiseksi ja palauttamiseksi;

10) varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan jatkuvuuden hallinta sekä tarvittaessa suojattujen varaviestintäjärjestelmien käyttö;

11) perustason tietoturvakäytännöt toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi;

12) toimenpiteet viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön suojaamiseksi sekä tilaturvallisuuden ja välttämättömien resurssien varmistamiseksi.

Toimenpiteiden on oltava ajantasaiset, asianmukaiset ja oikeasuhtaiset suhteessa tiedonhallintayksikön käyttämien viestintäverkkojen ja tietojärjestelmien riskialttiuteen, viestintäverkon tai tietojärjestelmän merkitykseen tiedonhallintayksikön toiminnalle sekä niissä ilmenevän poikkeaman kohtuudella ennakoitavissa oleviin välittömiin vaikutuksiin. Lisäksi toimenpiteiden mitoittamisessa on otettava huomioon tiedonhallintayksikön koko, sen toiminnan laatu, poikkeaman todennäköisyys ja vakavuus, toimenpiteistä aiheutuvat kustannukset sekä ajantasainen kehitys huomioon ottaen käytettävissä olevat tekniset mahdollisuudet torjua kyberuhka.

Riskienhallinnassa, riskienhallinnan toimintamallissa ja riskienhallintatoimenpiteitä toteutettaessa on noudatettava lisäksi NIS 2 -direktiivin 21 artiklan 5 kohdan nojalla mahdollisesti annettavia Euroopan komission täytäntöönpanosäädöksiä.

18 d §

Ilmoitusvelvollisuus merkittävästä poikkeamasta

Viranomaisen on viipymättä, viimeistään 24 tunnin kuluttua poikkeaman havaitsemisesta, toimitettava valvovalle viranomaiselle poikkeamaa koskeva ensi-ilmoitus, jossa on ilmoitettava, epäilläänkö poikkeaman johtuvan rikoksesta taikka muusta lainvastaisesta tai vihamielisestä teosta ja voiko poikkeamalla olla rajat ylittäviä vaikutuksia sekä näiden vaikutusten todennäköisyys.

Viranomaisen on viipymättä, viimeistään 72 tunnin kuluttua poikkeaman havaitsemisesta, toimitettava valvovalle viranomaiselle poikkeamaa koskeva jatkoilmoitus, jossa on saatettava

ajan tasalle 1 momentissa tarkoitetut tiedot ja esitettävä ensimmäinen arvio merkittävän poikkeaman laadusta, vakavuudesta ja vaikutuksista sekä vaarantumisindikaattorit, jos sellaisia on saatavilla.

Viranomaisen on annettava valvovalle viranomaiselle merkittävää poikkeamaa koskeva loppuraportti kuukauden kuluessa jatkoilmoituksen toimittamisesta. Loppuraportin on sisällettävä:

1) yksityiskohtainen kuvaus poikkeamasta, sen vakavuudesta ja vaikutuksista;

2) selvitys poikkeaman todennäköisesti aiheuttaneen uhkan tai juurisyyn tyypistä;

3) selvitys toteutetuista ja meneillään olevista toimenpiteistä poikkeaman vaikutusten lieventämiseksi; ja

4) selvitys mahdollisista rajat ylittävistä vaikutuksista.

Jos poikkeama edelleen jatkuu, kun 3 momentissa tarkoitettu loppuraportti pitäisi toimittaa, on loppuraportin sijaan toimitettava väliraportti poikkeaman käsittelyn edistymisestä. Loppuraportti on tällöin toimitettava kuukauden kuluessa siitä, kun viranomainen on käsitellyt poikkeaman. Valvovalla viranomaisella on oikeus poikkeaman kestäessä saada viranomaiselta lisätietoja tai väliraportti.

Merkittävän poikkeaman ilmoittamisessa on noudatettava lisäksi NIS 2 -direktiivin 23 artiklan 11 kohdan nojalla mahdollisesti annettavia Euroopan komission täytäntöönpanosäädöksiä ilmoituksen tietosisällöstä, muodosta ja ilmoitusmenettelystä sekä merkittävän poikkeaman tarkemmasta määrittelystä.

18 e §

Poikkeamailmoituksen vastaanottaminen

Valvovan viranomaisen on viipymättä, 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 poikkeaman käsittelyä koskevia ohjeita tai operatiivisia neuvoja sekä ohjeet merkittävän poikkeaman ilmoittamisesta esitutkintaviranomaiselle, jos asiassa epäillään rikosta.

Valvova viranomainen tekee 1 momentissa tarkoitettujen ohjeiden ja operatiivisten neuvojen antamisessa yhteistyötä kyberturvallisuuslaissa tarkoitetun CSIRT-yksikön kanssa. Ohjeet ja operatiiviset neuvot voi valvovan viranomaisen sijaan antaa CSIRT-yksikkö.

18 f §

Vapaaehtoinen ilmoittaminen

Viranomainen voi ilmoittaa valvovalle viranomaiselle myös muista kuin merkittävistä poikkeamista sekä kyberuhkista ja läheltä piti –tilanteista. Myös ne 3 §:ssä tarkoitetut, joihin tätä lukua ei sovelleta, voivat tehdä tällaisen ilmoituksen.

Valvovan viranomaisen on käsiteltävä 1 momentissa tarkoitetut vapaaehtoiset ilmoitukset 18 e §:ssä säädettyä menettelyä noudattaen. Valvova viranomainen voi asettaa 18 d §:ssä tarkoitettujen ilmoitusten käsittelyn etusijalle vapaaehtoisten ilmoitusten käsittelyyn nähden.

Viranomainen ja muut 3 §:ssä tarkoitetut voivat vapaaehtoisen ilmoituksen yhteydessä luovuttaa valvovalle viranomaiselle tietoja, jotka valvovalla viranomaisella on oikeus saada 18 i §:n nojalla.

Vapaaehtoisessa ilmoittamisessa on noudatettava lisäksi NIS 2 -direktiivin 23 artiklan 11 kohdan nojalla mahdollisesti annettavia Euroopan komission täytäntöönpanosäädöksiä ilmoituksen tietosisällöstä, muodosta ja ilmoitusmenettelystä.

18 g §

Tiedotusvelvollisuus merkittävästä kyberuhkasta ja poikkeamasta

Viranomaisen on viipymättä ilmoitettava merkittävästä poikkeamasta palvelujensa vastaanottajille, jos merkittävä poikkeama todennäköisesti haittaa sen palvelujen tarjoamista.

Viranomaisen on viipymättä ilmoitettava merkittävästä kyberuhkasta sekä kyberuhkan hallitsemiseksi käytettävissä olevista toimenpiteistä niille palvelujensa vastaanottajille, joihin merkittävä kyberuhka saattaa vaikuttaa.

Jos merkittävästä poikkeamasta tiedottaminen on yleisen edun mukaista, valvova viranomainen voi velvoittaa viranomaisen tiedottamaan merkittävästä poikkeamasta tai tiedottaa asiasta itse.

Edellä 1 ja 2 momentissa tarkoitetussa tiedottamisessa on noudatettava lisäksi NIS 2 -direktiivin 23 artiklan 11 kohdan nojalla mahdollisesti annettavia Euroopan komission täytäntöönpanosäädöksiä ilmoituksen tietosisällöstä, muodosta ja ilmoitusmenettelystä sekä merkittävän poikkeaman tarkemmasta määrittelystä.

18 h §

Valvova viranomainen

Tässä luvussa tarkoitettu valvova viranomainen ja NIS 2 -direktiivin 8 artiklan 1 kohdassa tarkoitettu toimivaltainen viranomainen julkishallinnon toimialalla on Liikenne- ja viestintävirasto. Valvovan viranomaisen tehtävänä on sen lisäksi mitä tässä luvussa säädetään, valvoa tässä luvussa ja NIS 2 -direktiivin nojalla annetuissa säännöksissä säädettyjen velvollisuuksien noudattamista julkishallinnon toimialalla sekä ylläpitää julkishallinnon toimialan toimijaluetteloa 18 a §:n nojalla toimitetuista tiedoista. Liikenne ja viestintävirasto on valvovan viranomaisen toiminnassaan itsenäinen ja riippumaton.

Valvova viranomainen voi asettaa tässä laissa säädetyt valvontatehtävänsä tärkeysjärjestykseen riskiperusteisesti. Valvovan viranomaisen on valvonnan kohdistamisessa ja 18 l §:ssä tarkoitettua valvontapäätöstä tehdessään otettava huomioon kyberturvallisuuslain 27 §:n 3 momentissa ja 37 §:ssä tarkoitetut seikat. Valvova viranomainen voi kohdistaa valvontaa hyvinvointialueeseen, hyvinvointiyhtymään tai Helsingin kaupunkiin vain, jos on perusteltu syy epäillä, että mainittu ei ole noudattanut tässä luvussa tai NIS 2 -direktiivin nojalla annetuissa säädöksissä säädettyä.

Ellei tässä luvussa toisin säädetä, valvovan viranomaisen on 18 a §:ssä tarkoitettujen toimintaa koskevien ilmoitusten, 18 d ja 18 f §:ssä tarkoitettujen poikkeamailmoitusten ja muiden valvontatehtävässä saatujen tietojen käsittelyssä sekä yhteistyössä muiden viranomaisten, Euroopan unionin toimielinten, erillisvirastojen ja yhteistyöelinten kanssa sekä tietojen luovuttamisessa niille noudatettava mitä kyberturvallisuuslain 6 §:n 4 momentissa, 15 §:n 3 momentissa, 17 §:ssä, 18 §:n 3 momentissa, 26 §:n 2 momentissa, 28 §:n 4 ja 5 momentissa, 33 §:ssä, 41 §:n 5 momentissa sekä 45 §:ssä säädetään tietojen käsittelystä valvovassa viranomaisessa sekä valvovan viranomaisen yhteistyöstä muiden viranomaisten, Euroopan unionin toimielinten, erillisvirastojen ja yhteistyöelinten kanssa sekä tietojen luovuttamisesta niille.

Liikenne- ja viestintäviraston tehtävistä NIS 2 -direktiivissä tarkoitettuna keskistettynä yhteyspisteenä ja CSIRT-yksikkönä säädetään kyberturvallisuuslaissa.

18 i §

Valvovan viranomaisen tiedonsaantioikeus

Valvovalla viranomaisella on tämän luvun mukaisia tehtäviä suorittaessaan salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus

saada kyberturvallisuutta koskevien riskien hallintaa, riskienhallinnan toimintamallia, hallintatoimenpiteitä ja merkittävää poikkeamaa koskevat tiedot sekä muut edellä mainittuihin tietoihin välittömästi liittyvät tiedot, jotka ovat välttämättömiä kyberturvallisuutta koskevan riskienhallintavelvoitteen noudattamisen ja merkittävistä poikkeamista ilmoittamisen ja raportoinnin valvontaa varten. Viranomaisen on luovutettava tiedot viipymättä ja maksutta.

Valvovalla viranomaisella on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada viranomaiselta välitystieto, sijaintitieto sekä tieto haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä, jos se on välttämätöntä kyberturvallisuutta koskevan riskienhallintavelvoitteen noudattamisen tai merkittävistä poikkeamista ilmoittamisen ja raportoinnin valvomista varten. Valvovan viranomaisen tämän momentin nojalla saamat tiedot on pidettävä salassa.

Tässä pykälässä tarkoitettu tiedonsaantioikeus ei koske salassa pidettäviä tietoja julkisen hallinnon turvallisuusverkkotoiminnasta annetussa laissa tarkoitetusta turvallisuusverkon palvelutuotannosta tai palvelujen käytöstä eikä tietoja, joiden luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin niihin liittyvää tärkeää etua.

Erityissuojattavan tietoaineiston käsittelyä koskevista velvollisuuksista säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa.

18 j §

Valvovan viranomaisen oikeus tehdä tarkastuksia

Valvovalla viranomaisella on siinä laajuudessa kuin se on tarpeen, oikeus tehdä tässä luvussa tai NIS 2 -direktiivin nojalla annetuissa säännöksissä säädettyjen velvollisuuksien noudattamisen valvomiseksi viranomaiseen kohdistuva tarkastus.

Tarkastuksen suorittajalla on oltava tarkastuksen laatuun ja laajuuteen nähden riittävä koulutus ja kokemus.

Viranomaisen on tarkastusta varten päästettävä tarkastuksen suorittaja tarkastuksen edellyttämässä laajuudessa tarkastuksen kohteena olevaan viestintäverkkoon tai tietojärjestelmään ja muihin kuin pysyväisluonteiseen asumiseen tarkoitettuihin tiloihin. Tarkastuksen suorittamiseksi tarkastuksen suorittajalla 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 viranomaisen toteuttamat turvallisuusjärjestelyt. Tarkastuksen suorittajan tarkastus- ja tiedonsaantioikeuteen sovelletaan mitä 18 i §:n 3 momentissa säädetään tiedonsaantioikeuden rajoituksista.

Tarkastuksessa noudatettavaan menettelyyn sovelletaan, mitä hallintolain 39 §:ssä säädetään tarkastuksesta.

18 k §

Avustavan tehtävän antaminen tietoturvallisuuden arviointilaitokselle ja arvioinnin teettäminen

Valvova viranomainen voi antaa 18 j §:ssä tarkoitettuun tarkastustehtävään liittyvän avustavan tehtävän tietoturvallisuuden arviointilaitoksista annetussa laissa (1405/2011) tarkoitetulle hyväksytylle tietoturvallisuuden arviointilaitokselle.

Valvova viranomainen voi valvonnan toteuttamiseksi velvoittaa viranomaisen teettämään tietoturvallisuuden arviointilaitoksella kyberturvallisuuteen kohdistuvan riskienhallinnan 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 18 c §:ssä tarkoitettujen kyberturvallisuuteen kohdistuvien riskienhallintavelvollisuuksien noudattamisen.

Tietoturvallisuuden arviointilaitoksen palveluksessa olevaan tarkastuksessa avustavaan henkilöön ja arvioinnin suorittajaan sovelletaan, mitä 18 j §:n 2–4 momentissa säädetään tarkastuksen suorittajan kokemuksesta ja koulutuksesta sekä tarkastuksen suorittajan oikeuksista. Ellei tässä luvussa toisin säädetä, tietoturvallisuuden arviointilaitokseen sovelletaan tietoturvallisuuden arviointilaitoksista annettua lakia. Tietoturvallisuuden 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

Valvova viranomainen voi velvoittaa viranomaisen määräajassa korjaamaan puutteet tässä luvussa tai NIS 2 -direktiivin nojalla annetuissa säännöksissä säädettyjen velvollisuuksien noudattamisessa. Valvova viranomainen voi velvoittaa viranomaisen julkistamaan kyseiset puutteet tai muut seikat, jotka liittyvät mainittujen velvollisuuksien rikkomiseen.

Valvova viranomainen voi antaa viranomaiselle varoituksen, jos tämä ei ole noudattanut tässä luvussa tai NIS 2 -direktiivin nojalla annetuissa säännöksissä säädettyjä velvollisuuksia. Varoituksessa on yksilöitävä puute tai laiminlyönti, jota varoitus koskee. Varoitus on annettava kirjallisena.

Valvova viranomainen voi asettaa uhkasakon 1 momentissa tarkoitetun päätöksen noudattamisen tehosteeksi.

18 m §

Muutoksenhaku

Muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).

Muutoksenhausta uhkasakon asettamista ja maksettavaksi tuomitsemista koskevaan päätökseen säädetään uhkasakkolaissa (1113/1990).

Tämä laki tulee voimaan päivänä kuuta 20 .

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) 2 §:n 2 momentti ja 247 a §, sellaisina kuin ne ovat, ensin mainittu laissa 1207/2020 ja viimeksi mainittu laissa 281/2018,

muutetaan 165 §:n 1 momentti, 167, 170 ja 275 §, 308 §:n 3 momentti, 313 §:n 2 momentin 2 kohta, 318 §:n 4 momentti ja 342 §:n 2 momentti,

sellaisina kuin ne ovat, 165 §:n 1 momentti, 170 §, 308 §:n 3 momentti sekä 313 §:n 2 momentin 2 kohta laissa 1003/2018, 167 § laeissa 1003/2018 ja 1207/2020 sekä 275 § ja 318 §:n 4 momentti laissa 1207/2020 sekä 342 §:n 2 momentti laissa 1182/2023, ja

lisätään 165 §:ään, sellaisena kuin se on laissa 1003/2018, uusi 4 momentti ja 247 §:ään, sellaisena kuin se on laissa 1003/2018, uusi 5 momentti

seuraavasti:

165 §

Verkkotunnusvälittäjän ilmoitusvelvollisuudet

Verkkotunnusvälittäjän on ennen toimintansa aloittamista tehtävä ilmoitus verkkotunnusrekisteriä hallinnoivalle viranomaiselle. Ilmoituksessa on oltava seuraavat tiedot:

1) verkkotunnusvälittäjän nimi, y-tunnus tai sellaisen puuttuessa muu yksilöivä tieto sekä kuulemisiin ja tiedoksiantoihin käytettävä sähköpostiosoite;

2) verkkotunnusvälittäjän päätoimipaikan ja muiden Euroopan 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;

3) verkkotunnusvälittäjän IP-osoitealueet;

4) luettelo niistä Euroopan unionin jäsenvaltioista, joissa verkkotunnusvälittäjä tarjoaa palveluja; ja

5) muut kuin 1–4 kohdassa tarkoitetut valvonnan kannalta tarpeelliset tiedot.

— —

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 (*NIS 2 -direktiivi*) 27 artiklan 4 kohdassa tarkoitetun ilmoituksen tekemiseksi tarpeelliset tiedot verkkotunnusvälittäjien ilmoituksista kyberturvallisuuslain (/) 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 ja 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 teknisestä 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 momentissa säädetyn 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 1 momentin 8 ja 11 kohdassa tarkoitetuista toimintaperiaatteista ja menettelyistä, toiminnan tietoturvallisuudesta sekä siitä, milloin 1 momentin 7 kohdassa tarkoitettu häiriö on merkittävä sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

Kyberturvallisuuslain 2 §:n 3 kohdassa tarkoitetun DNS-palveluntarjoajan velvollisuudesta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja poikkeamien ilmoittamisesta säädetään kyberturvallisuuslaissa.

247 §

Viestinnän välittäjän ja lisäarvopalvelun tarjoajan velvollisuus huolehtia tietoturvasta

— —

Tietoturvasta huolehtimiseen sovelletaan lisäksi, mitä kyberturvallisuuslaissa 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 kyberturvallisuuslaissa 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

— —

Liikenne- ja viestintävirasto voi asettaa tässä laissa säädetyt valvontatehtävänsä tärkeysjärjestykseen. Liikenne- ja viestintävirasto voi jättää asian tutkimatta, jos:

— —

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 mainitun 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.

— —

342 §

Oikaisuvaatimus

— —

Liikenne- ja viestintäviraston päätökseen, joka koskee 39 §:ssä tarkoitettua radiolupaa, 44 §:ssä tarkoitettua radiotaajuuksien varausta koskevaa päätöstä, 100 §:ssä tarkoitettua numerointipäätöstä, 167 §:n 2 momentissa tarkoitettua verkkotunnuksen rekisteröinnin estämistä, 169 §:n 1 momentissa tarkoitettua verkkotunnuksen poistamista, 288 §:ssä tarkoitettua markkinaehtoista taajuusmaksua, 289 §:ssä tarkoitettua tietoyhteiskuntamaksua,

293 §:ssä tarkoitettua televisio- ja radiotoiminnan valvontamaksua tai datanhallinta-asetuksen 19 artiklan 5 kohdassa tarkoitettua rekisteröintiä, saa vaatia oikaisua.

Tämä laki tulee voimaan päivänä kuuta 20 .

4.

Laki

ilmailulain 128 a ja 128 b §:n kumoamisesta

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Tällä lailla kumotaan ilmailulain (864/2014) 128 a ja 128 b §, sellaisina kuin ne ovat laissa 965/2018.

2 §

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 §.

2 §

Tämä laki tulee voimaan päivänä kuuta 20 .

6.

Laki

liikenteen palveluista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan liikenteen palveluista annetun lain (320/2017) 161 §, sellaisena kuin se on laissa 1256/2020, sekä

muutetaan 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 kyberturvallisuuslaissa (/).

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 (623/2005) 18 a §, sellaisena kuin se on laissa 947/2018.

2 §

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 §, sellaisina kuin ne ovat laissa 955/2018.

2 §

Tämä laki tulee voimaan päivänä kuuta 20 .

9.

Laki

sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain 2 ja 90 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain (703/2023) 2 §:n 3 momentti ja 90 § seuraavasti:

2 §

Soveltamisala ja suhde muuhun lainsäädäntöön

— —

Tällä 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 kyberturvallisuuslakia (/) täydentävät ja täsmentävät säännökset käsiteltäessä sosiaali- ja terveydenhuollon asiakastietoja ja asiakkaan itsensä tuottamia hyvinvointitietoja sosiaali- ja terveyspalveluita järjestettäessä ja toteutettaessa.

90 §

Ilmoittaminen tietojärjestelmän ja hyvinvointisovelluksen olennaisten vaatimusten poikkeamista sekä tietoverkkoihin kohdistuvista tietoturvallisuuden häiriöistä

Jos palvelunantaja tai apteekki havaitsee, että tietojärjestelmän olennaisten vaatimusten täyttymisessä on merkittäviä poikkeamia, sen on ilmoitettava asiasta tietojärjestelmäpalvelun tuottajalle. Jos tietojärjestelmän tai hyvinvointisovelluksen poikkeama voi aiheuttaa merkittävän riskin asiakas- tai potilasturvallisuudelle tai tietoturvalle, on palvelunantajan, apteekin, tietojärjestelmäpalvelun tuottajan tai tietojärjestelmän valmistajan, hyvinvointisovelluksen valmistajan, Kansaneläkelaitoksen tai Terveyden ja hyvinvoinnin laitoksen ilmoitettava siitä Sosiaali- ja terveysalan lupa- ja valvontavirastolle. Myös muu taho voi ilmoittaa Sosiaali- ja terveysalan lupa- ja valvontavirastolle havaitsemistaan riskeistä. Jos tietojärjestelmän poikkeama voi aiheuttaa merkittävän riskin apteekin toiminnalle, on apteekin ilmoitettava siitä lisäksi Lääkealan turvallisuus- ja kehittämiskeskukselle. Henkilötietojen tietoturvaloukkauksista ilmoittamisesta tietosuojavaltuutetulle säädetään tietosuoja-asetuksen 33 artiklassa.

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 sosiaali- ja terveyspalveluiden toteuttaminen voi merkittävästi vaarantua. Sosiaali- ja terveysalan lupa- ja valvontavirasto voi antaa tarkempia määräyksiä siitä, milloin häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

Apteekin on lisäksi ilmoitettava viipymättä Lääkealan turvallisuus- ja kehittämiskeskukselle sellaisesta sen käyttämiin käyttöympäristöihin ja tietoverkkoihin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena apteekin toiminta voi merkittävästi

vaarantua. Lääkealan turvallisuus- ja kehittämiskeskus 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 palvelunantajan, apteekin, Kansaneläkelaitoksen, tietojärjestelmäpalvelun tuottajan tai tietojärjestelmän valmistajan taikka välittäjän tiedottamaan yleisölle asiasta taikka kuultuaan ilmoitusvelvollista tiedottaa asiasta itse. Lisäksi Lääkealan turvallisuus- ja kehittämiskeskus voi velvoittaa apteekin tiedottamaan yleisölle 3 momentissa tarkoitetusta häiriöstä taikka kuultuaan ilmoitusvelvollista tiedottaa häiriöstä 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, sellaisina 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, 23 a eikä 26 a §:ää, 27 §:n 3 momenttia, 28, 29, 29 b, 50–52, 52 a, 53, 53 a, 54–56, 56 a, 58 eikä 59 §:ää ja 61 a §:n 2 momenttia.

— —

_____

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 §, sellaisena kuin se on laeissa 288/2018 ja 327/2020.

2 §

Tämä laki tulee voimaan päivänä kuuta 20 .

12.

Laki

Energiavirastosta annetun lain 1 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan Energiavirastosta annetun lain (870/2013) 1 §:n 2 momentin 19 kohta, sellaisena kuin se on laissa 418/2019, sekä

lisätään 1 §:n 2 momenttiin, sellaisena kuin se on osaksi laeissa 634/2020, 804/2020, 606/2021 ja 500/2023, uusi 20 kohta

seuraavasti:

1 §

Tehtävät

— —

Energiavirasto hoitaa tehtävät, jotka sille on annettu:

— —

19) biopolttoöljyn käytön edistämisestä annetussa laissa (418/2019);

20) kyberturvallisuuslaissa (/).

— —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

13.

Laki

sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain (590/2013) 9 §, 23 §:n 4 ja 5 kohta sekä 28 §:n 1 momentin 1 kohta, sellaisina kuin niistä ovat 23 §:n 4 ja 5 kohta laissa 589/2017 ja 28 §:n 1 momentin 1 kohta laissa 1002/2018, sekä

lisätään 2 §:ään, sellaisena kuin se on laeissa 633/2020 ja 499/2023, uusi 2 momentti ja 23 §:ään, sellaisena kuin se on laissa 589/2017, uusi 6 kohta

seuraavasti:

2 §

Soveltamisala

— —

Tämän lain 23 ja 24 §:ää sovelletaan lisäksi niiden tehtävien hoitamiseen, jotka säädetään Energiaviraston tehtäviksi kyberturvallisuuslaissa (/).

9 §

Energiamarkkinaviraston toimivalta valvonta-asioissa

Jos joku rikkoo tai laiminlyö 2 §:n 1 momentissa tarkoitetussa kansallisessa tai Euroopan unionin lainsäädännössä säädettyjä velvoitteitaan, Energiamarkkinaviraston on velvoitettava hänet korjaamaan rikkomuksensa tai laiminlyöntinsä. Päätöksessä voidaan määrätä, millä tavoin rikkomus tai laiminlyönti tulee korjata. Päätöksessä voidaan myös määrätä palauttamaan asiakkaalle virheellisesti peritty maksu, jos palautukseen ei sovelleta 14 §:ssä säädettyä palautusmenettelyä.

23 §

Sähkö- ja maakaasuverkkoluvan peruuttaminen

Energiavirasto voi peruuttaa sähköverkkoluvan, maakaasuverkkoluvan sekä sähkömarkkinalain 12 §:ssä ja maakaasumarkkinalain 11 §:ssä säädetyn vapautuksen tai poikkeusluvan:

— —

4) jos luvanhaltija toistuvasti ja oleellisesti rikkoo maakaasuverkkoasetusta tai sen nojalla annettujen, suuntaviivoja koskevien komission asetusten tai päätösten säännöksiä, siltä osin kuin niitä sovelletaan Suomessa, eikä luvanhaltijalle etukäteen annettu varoitus luvan peruuttamisesta ole johtanut toiminnassa esiintyneiden puutteiden korjaamiseen;

5) jos luvanhaltija toistuvasti ja oleellisesti rikkoo maakaasun siirtoverkonhaltijan eriyttämisestä annetun lain säännöksiä eikä luvanhaltijalle etukäteen annettu varoitus luvan peruuttamisesta ole johtanut toiminnassa esiintyneiden puutteiden korjaamiseen; tai

6) jos luvanhaltija toistuvasti ja oleellisesti rikkoo kyberturvallisuuslakia (/), eikä luvanhaltijalle etukäteen annettu varoitus luvan peruuttamisesta ole johtanut toiminnassa esiintyneiden puutteiden korjaamiseen.

28 §

Energiaviraston oikeus luovuttaa tietoja toiselle viranomaiselle

Sen lisäksi, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetään, Energiavirastolla on oikeus luovuttaa salassapitosäännösten estämättä tietoja:

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

muutetaan vesihuoltolain (119/2001) 35 §:n 2 momentti, sellaisena kuin se on laissa 1013/2018, seuraavasti:

35 §

Salassapitovelvollisuus

— —

Viranomaisten toiminnan julkisuudesta annetussa laissa säädetyn salassapitovelvollisuuden estämättä saa tämän lain mukaisia tehtäviä suoritettaessa saatuja tietoja yksityisen ja yhteisön taloudellisesta asemasta, liikesalaisuudesta sekä yksityisen henkilökohtaisista oloista luovuttaa:

1) valvontaviranomaiselle tämän lain mukaisten tehtävien suorittamista varten; sekä

2) rikoksen selvittämiseksi syyttäjä- tai poliisiviranomaiselle.

Tämä laki tulee voimaan päivänä kuuta 20 .

15.

Laki

sakon täytäntöönpanosta annetun lain 1 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

lisätään sakon täytäntöönpanosta annetun lain (672/2002) 1 §:n 2 momenttiin, sellaisena kuin se on laeissa 1183/2023, 23/2024 ja 36/2024, uusi 31 kohta seuraavasti:

1 §

Lain soveltamisala

— —

Siten kuin tässä laissa säädetään, pannaan täytäntöön myös:

— —

31) kyberturvallisuuslain (/) 35 §:ssä tarkoitettu seuraamusmaksu.

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———————

16.

Laki

maa-asemista ja eräistä tutkista annetun lain 8 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan maa-asemista ja eräistä tutkista annetun lain (96/2023) 8 §:n 1 momentin 3 kohta seuraavasti:

8 §

Luvan muuttaminen ja peruuttaminen

Luvan myöntänyt viranomainen voi muuttaa maa-asema- tai tutkatoiminnan harjoittamiseen myönnettyä lupaa tai peruuttaa luvan, jos:

— —

3) toiminnanharjoittaja on olennaisella tavalla laiminlyönyt tai rikkonut tässä laissa tai kyberturvallisuuslaissa (/) säädettyä velvollisuutta tai rajoitusta taikka luvan ehtoja;

— —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

17.

Laki

vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

lisätään vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annetun lain (390/2005) 5 §:ään, sellaisena kuin se on laeissa 358/2015 ja 794/2020, uusi 10 momentti sekä lakiin uusi 109 a § seuraavasti:

5 §

Suhde muuhun lainsäädäntöön

— —

Kyberturvallisuuden riskienhallinta- ja raportointivelvoitteista sekä viranomaisten yhteistyöstä kyberturvallisuuspoikkeamien ja –riskien hallitsemiseksi säädetään kyberturvallisuuslaissa (/).

109 a §

Kyberturvallisuutta koskevien velvoitteiden laiminlyömisestä johtuva luvan peruuttaminen

Jos toiminnanharjoittaja olennaisesti ja vakavasti laiminlyö kyberturvallisuuslaissa säädettyjä velvollisuuksia, on valvontaviranomaisen asetettava toiminnanharjoittajalle riittävä määräaika asian korjaamiseksi. Jos toiminnanharjoittaja ei ole korjannut puutteita määräajan kuluessa, valvontaviranomainen voi peruuttaa myöntämänsä toiminnanharjoittamista koskevan luvan osittain tai kokonaan.

Tämä pykälä koskee toimintaa, jossa turvallisuus- ja kemikaalivirasto on valvova viranomainen 115 §:n mukaisesti.

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

Helsingissä 23.5.2024

Pääministeri

Petteri Orpo

Liikenne- ja viestintäministeri Lulu Ranne

2

Laki

julkisen hallinnon tiedonhallinnasta annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 2 §:n 16 kohta, 3 § ja 10 §:n 1 momentin 2 kohta, sellaisina kuin niistä ovat 2 §:n 16 kohta laissa 488/2023 ja 3 § osaksi laeissa 653/2021 ja 488/2023, sekä

lisätään 1 §:ään siitä lailla 710/2021 kumotun 2 momentin tilalle uusi 2 momentti ja 2 §:ään uusi 17 – 26 kohta sekä lakiin uusi 4 a luku seuraavasti:

Voimassa oleva laki	*Ehdotus*
1 §	1 §
Lain tarkoitus	*Lain tarkoitus*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
(lisätään)	*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 annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2022/2555 (NIS 2 -direktiivi) toimijaa koskevia velvoitteita, niiden noudattamisen valvontaa ja seuraamuksia koskevat säännökset NIS 2 -direktiivin liitteen I kohdassa 10 tarkoitetulla julkishallinnon toimialalla (julkishallinnon toimiala). NIS 2 -direktiivin täytäntöönpanosta muilta osin säädetään kyberturvallisuuslaissa (/).*
2 §	2 §
Määritelmät	*Määritelmät*
Tässä laissa tarkoitetaan:	Tässä laissa tarkoitetaan:
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
16) *käsittelysäännöillä* luonnollisen henkilön ennalta laatimia automaattisen tietojenkäsittelyn ohjaamiseen tarkoitettuja sääntöjä**.**	*16) käsittelysäännöillä* luonnollisen henkilön ennalta laatimia automaattisen

Voimassa oleva laki	*Ehdotus*
(lisätään)	tietojenkäsittelyn ohjaamiseen tarkoitettuja sääntöjä***;***
	17) viestintäverkolla ja tietojärjestelmällä
	a) eurooppalaisesta sähköisen viestinnän säännöstöstä annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2018/1972 2 artiklan 1 kohdassa tarkoitettua sähköistä viestintäverkkoa;
	b) laitetta taikka yhteen kytkettyjen tai toisiinsa yhteydessä olevien laitteiden ryhmää, joista yksi tai useampi suorittaa ohjelman avulla digitaalisten tietojen automaattista käsittelyä; ja
	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 niissä 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 tilannetta, tapahtumaa tai toimintaa, joka toteutuessaan 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) kyberriskillä poikkeaman aiheuttamien menetysten tai häiriön mahdollisuutta, joka ilmaistaan menetyksen tai häiriön suuruuden

Voimassa oleva laki

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.

Asiankäsittelyssä ja palvelujen tuottamisessa noudatettavista menettelyistä, salassapidosta ja tiedonsaantioikeudesta viranomaisten asiakirjoihin sekä asiakirjojen arkistoinnista säädetään erikseen. Tiedonhallinnasta ja tietojärjestelmien käytöstä Suomen evankelisluterilaisessa kirkossa säädetään kirkkolaissa *(1054/1993)*.

Ehdotus

ja poikkeaman toteutumisen todennäköisyyden yhdistelmänä;

23) 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;

24) merkittävällä poikkeamalla poikkeamaa, joka:

a) on aiheuttanut tai voi aiheuttaa vakavan palvelujen toimintahäiriön tai viranomaiselle huomattavia taloudellisia tappioita; tai

b) on vaikuttanut tai voi vaikuttaa luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa;

25) poikkeaman käsittelyllä toimia ja menettelyjä, joilla pyritään ehkäisemään ja havaitsemaan poikkeama, analysoimaan, rajoittamaan tai hallitsemaan sitä ja palautumaan siitä;

26) kriittisellä toimijalla viranomaista tai muuta julkista hallintotehtävää hoitavaa, joka on kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2022/2557 2 artiklan 1 kohdassa tarkoitettu kriittinen toimija julkishallinnon toimialalla.

3 §

Lain soveltamisala ja sen rajaukset

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.

Asiankäsittelyssä ja palvelujen tuottamisessa noudatettavista menettelyistä,

Voimassa oleva laki	*Ehdotus*
(lisätään)	salassapidosta ja tiedonsaantioikeudesta viranomaisten asiakirjoihin sekä asiakirjojen arkistoinnista säädetään erikseen. Tiedonhallinnasta ja tietojärjestelmien käytöstä Suomen evankelis-luterilaisessa kirkossa säädetään kirkkolaissa *(652/2023)*. *Tämän lain 4 a lukua sovelletaan seuraaviin viranomaisiin ja viranomaisen toimintaan vain, jos viranomainen on kriittinen toimija:* *1) tasavallan presidentin kanslia, Puolustusvoimat, poliisin hallinnosta annetussa laissa (110/1992) tarkoitetut poliisiyksiköt, Rajavartiolaitos, Syyttäjälaitos ja Tullin rikostorjunta;* *2) tuomioistuimet ja valitusasioita käsittelemään perustetut lautakunnat;* *3) Puolustuskiinteistöt;* *4) kunnalliset viranomaiset lukuun ottamatta Helsingin kaupunkia, johon sovelletaan 4 a lukua sen hoitaessa hyvinvointialueiden järjestämisvastuulle lailla säädettyjä tehtäviä, vaikka se ei olisi kriittinen toimija;* *5) Suomen Pankki;* *6) yliopistolaissa tarkoitetut yliopistot, ammattikorkeakoululaissa tarkoitetut ammattikorkeakoulut ja Pelastusopisto;* *7) julkisen hallinnon turvallisuusverkkotoiminnasta annetussa laissa (10/2015) tarkoitettu turvallisuusverkon palvelutuotanto ja turvallisuusverkon palvelujen käyttö;* *8) viranomaiset, jotka on perustettu yhdessä Euroopan talousalueeseen kuulumattoman maan kanssa kansainvälisen sopimuksen mukaisesti ja näissä maissa sijaitsevat diplomaattiset edustustot ja konsuliedustustot sekä näiden verkko- ja tietojärjestelmät, siltä osin kuin tällaiset järjestelmät sijaitsevat edustuston tiloissa tai niitä ylläpidetään näissä maissa olevia käyttäjiä varten.*
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	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

Voimassa oleva laki	*Ehdotus*
hyvinvointialueisiin, hyvinvointiyhtymiin, kuntiin ja kuntayhtymiin niiden hoitaessa laissa säädettyjä tehtäviä.	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. *Tämän lain 18 g §:n 3 momenttia ja 18 h–18 l §:ää ei sovelleta eduskunnan oikeusasiamiehen eikä valtioneuvoston oikeuskanslerin toimintaan. Tämän lain 18 g §:n 3 momenttia ja 18 h–18 l §:ää ei sovelleta myöskään tasavallan presidentin kansliaan eikä tuomioistuinten tai valitusasioita käsittelemään perustettujen lautakuntien lainkäyttöön, vaikka niihin muutoin sovellettaisiin 4 a lukua niiden toimiessa kriittisenä toimijana.*
(lisätään)	
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.	Mitä 4 luvussa, 22–24 ja 25–27 §:ssä sekä 6 a luvussa säädetään tiedonhallintayksiköstä ja viranomaisesta, sovelletaan yksityisiin henkilöihin *ja* yhteisöihin *sekä* 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 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. *Mitä 4 a luvussa säädetään tiedonhallintayksiköstä ja viranomaisesta, sovelletaan yksityiseen henkilöön ja yhteisöön sekä muuna kuin viranomaisena toimivaan julkisoikeudelliseen yhteisöön siltä osin kuin*
(lisätään)	
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	

Voimassa oleva laki

viranomaistehtäviä, joissa tehdään hallintolain 53 e §:ssä tarkoitettuja asian automaattisia ratkaisuja.

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.

— — — — — — — — — — — — — — —

(uusi)

Ehdotus

se hoitaa julkista hallintotehtävää ja on kriittinen toimija.

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, jollei 3 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.*

— — — — — — — — — — — — — — —

4 a luku

Kyberturvallisuutta koskevat velvollisuudet ja niiden noudattamisen valvonta

18 a §

Toimijajaottelu ja toimintaa koskeva ilmoitus

Tämän luvun soveltamisalaan kuuluvat tiedonhallintayksiköt ovat julkishallinnon toimialan keskeisiä toimijoita. Hyvinvointialueet ja hyvinvointiyhtymät sekä Helsingin kaupunki ovat kuitenkin tärkeitä toimijoita.

Tiedonhallintayksikön on ilmoitettava valvovalle viranomaiselle:

Voimassa oleva laki *Ehdotus*

1) nimensä;
2) osoitteensa, sähköpostiosoitteensa, puhelinnumeronsa ja muut ajantasaiset yhteystietonsa;
3) IP-osoitealueensa;
4) tieto siitä, onko se julkishallinnon toimialan keskeinen vai tärkeä toimija;
5) luettelo muista Euroopan unionin jäsenvaltioista, joissa se tarjoaa palvelujaan;
6) osallistumisestaan kyberturvallisuuslain 23 §:ssä tarkoitettuun kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn.
Tiedonhallintayksikön on ilmoitettava kaikista 2 momentissa tarkoitettujen tietojen muutoksista viipymättä, viimeistään kahden viikon kuluttua muutoksesta.

18 b §

Velvollisuus hallita kyberturvallisuusriskejä ja riskienhallinnan toimintamalli

Tiedonhallintayksikön on tunnistettava, arvioitava ja hallittava kyberriskejä, joita kohdistuu sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Kyberturvallisuutta koskevalla riskienhallinnalla tulee estää tai minimoida poikkeamien vaikutus toimintaan, toiminnan jatkuvuuteen, palvelujen vastaanottajiin ja muihin palveluihin. Tiedonhallintayksikön on toteutettava 18 c §:ssä tarkoitetut kyberturvallisuutta koskevat riskienhallintatoimenpiteet.
Tiedonhallintayksiköllä on oltava käytössä ajantasainen kyberturvallisuutta koskeva riskienhallinnan toimintamalli viestintäverkkojen ja tietojärjestelmien ja niiden fyysisen ympäristön suojaamiseksi poikkeamilta ja niiden vaikutuksilta. Kyberturvallisuutta koskevassa riskienhallinnan toimintamallissa on tunnistettava viestintäverkkoihin ja tietojärjestelmiin ja niiden fyysiseen ympäristöön kohdistuvat riskit ottaen huomioon kaikki vaaratekijät huomioiva lähestymistapa. Toimintamallissa on

määritettävä ja kuvattava kyberturvallisuutta koskevan riskienhallinnan tavoitteet, menettelyt ja vastuut sekä 18 c §:n mukaiset toimenpiteet, joilla viestintäverkkoja ja tietojärjestelmiä ja niiden fyysistä ympäristöä suojataan kyberuhkilta ja poikkeamilta.

Tiedonhallintayksikön johto vastaa kyberturvallisuutta koskevan riskienhallinnan toteuttamisen ja valvonnan järjestämisestä sekä hyväksyy riskienhallinnan toimintamallin ja valvoo sen toteuttamista. Tiedonhallintayksikön johdolla tulee olla riittävä perehtyneisyys kyberturvallisuutta koskevaan riskienhallintaan.

18 c §

Toimenpiteet kyberturvallisuutta koskevien riskien hallinnassa

Tiedonhallintayksikön on toteuttava oikeasuhtaiset tekniset, operatiiviset ja organisatoriset kyberturvallisuutta koskevat riskienhallintatoimenpiteet käyttämiensä viestintäverkkojen ja tietojärjestelmien turvallisuuteen kohdistuvien kyberriskien hallitsemiseksi ja haitallisten vaikutusten estämiseksi tai minimoimiseksi. Kyberturvallisuutta koskevassa riskienhallinnan toimintamallissa ja siihen perustuvissa kyberturvallisuuden riskienhallintatoimenpiteissä on otettava huomioon ja pidettävä yllä ajantasaisesti ainakin:

1) kyberturvallisuutta koskevan 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 käsittelemiseksi ja julkistamiseksi;

4) toimitusketjun välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, niihin

sisällytetyt kyberturvallisuutta koskevat riskienhallintatoimenpiteet ja välittömien toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt sekä NIS2 -direktiivin 22 artiklan 1 kohdassa tarkoitetut kriittisiä toimitusketjuja koskevien koordinoitujen riskinarviointien tulokset;

5) omaisuudenhallinta ja sen 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 käyttämiseksi;

9) poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden ylläpitämiseksi ja palauttamiseksi;

10) varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan jatkuvuuden hallinta sekä tarvittaessa suojattujen varaviestintäjärjestelmien käyttö;

11) perustason tietoturvakäytännöt toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi;

12) toimenpiteet viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön suojaamiseksi sekä tilaturvallisuuden ja välttämättömien resurssien varmistamiseksi.

Toimenpiteiden on oltava ajantasaiset, asianmukaiset ja oikeasuhtaiset suhteessa tiedonhallintayksikön käyttämien viestintäverkkojen ja tietojärjestelmien riskialttiuteen, viestintäverkon tai tietojärjestelmän merkitykseen tiedonhallintayksikön toiminnalle sekä niissä ilmenevän poikkeaman kohtuudella ennakoitavissa oleviin välittömiin vaikutuksiin. Lisäksi toimenpiteiden mitoittamisessa on otettava huomioon tiedonhallintayksikön koko, sen toiminnan laatu, poikkeaman todennäköisyys ja vakavuus, toimenpiteistä aiheutuvat kustannukset sekä ajantasainen kehitys

Voimassa oleva laki *Ehdotus*

huomioon ottaen käytettävissä olevat tekniset mahdollisuudet torjua kyberuhka.

Riskienhallinnassa, riskienhallinnan toimintamallissa ja riskienhallintatoimenpiteitä toteutettaessa on noudatettava lisäksi NIS 2 -direktiivin 21 artiklan 5 kohdan nojalla mahdollisesti annettavia Euroopan komission täytäntöönpanosäädöksiä.

18 d §

Ilmoitusvelvollisuus merkittävästä poikkeamasta

Viranomaisen on viipymättä, viimeistään 24 tunnin kuluttua poikkeaman havaitsemisesta, toimitettava valvovalle viranomaiselle poikkeamaa koskeva ensi-ilmoitus, jossa on ilmoitettava, epäilläänkö poikkeaman johtuvan rikoksesta taikka muusta lainvastaisesta tai vihamielisestä teosta ja voiko poikkeamalla olla rajat ylittäviä vaikutuksia sekä näiden vaikutusten todennäköisyys.

Viranomaisen on viipymättä, viimeistään 72 tunnin kuluttua poikkeaman havaitsemisesta, toimitettava valvovalle viranomaiselle poikkeamaa koskeva jatkoilmoitus, jossa on saatettava ajan tasalle 1 momentissa tarkoitetut tiedot ja esitettävä ensimmäinen arvio merkittävän poikkeaman laadusta, vakavuudesta ja vaikutuksista sekä vaarantumisindikaattorit, jos sellaisia on saatavilla.

Viranomaisen on annettava valvovalle viranomaiselle merkittävää poikkeamaa koskeva loppuraportti kuukauden kuluessa jatkoilmoituksen toimittamisesta. Loppuraportin on sisällettävä:

1) yksityiskohtainen kuvaus poikkeamasta, sen vakavuudesta ja vaikutuksista;

2) selvitys poikkeaman todennäköisesti aiheuttaneen uhkan tai juurisyyn tyypistä;

3) selvitys toteutetuista ja meneillään olevista toimenpiteistä poikkeaman vaikutusten lieventämiseksi; ja

4) selvitys mahdollisista rajat ylittävistä vaikutuksista.

Voimassa oleva laki *Ehdotus*

Jos poikkeama edelleen jatkuu, kun 3 momentissa tarkoitettu loppuraportti pitäisi toimittaa, on loppuraportin sijaan toimitettava väliraportti poikkeaman käsittelyn edistymisestä. Loppuraportti on tällöin toimitettava kuukauden kuluessa siitä, kun viranomainen on käsitellyt poikkeaman. Valvovalla viranomaisella on oikeus poikkeaman kestäessä saada viranomaiselta lisätietoja tai väliraportti.

Merkittävän poikkeaman ilmoittamisessa on noudatettava lisäksi NIS 2 -direktiivin 23 artiklan 11 kohdan nojalla mahdollisesti annettavia Euroopan komission täytäntöönpanosäädöksiä ilmoituksen tietosisällöstä, muodosta ja ilmoitusmenettelystä sekä merkittävän poikkeaman tarkemmasta määrittelystä.

18 e §

Poikkeamailmoituksen vastaanottaminen

Valvovan viranomaisen on viipymättä, 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 poikkeaman käsittelyä koskevia ohjeita tai operatiivisia neuvoja sekä ohjeet merkittävän poikkeaman ilmoittamisesta esitutkintaviranomaiselle, jos asiassa epäillään rikosta.

Valvova viranomainen tekee 1 momentissa tarkoitettujen ohjeiden ja operatiivisten neuvojen antamisessa yhteistyötä kyberturvallisuuslaissa tarkoitetun CSIRT-yksikön kanssa. Ohjeet ja operatiiviset neuvot voi valvovan viranomaisen sijaan antaa CSIRT-yksikkö.

18 f §

Vapaaehtoinen ilmoittaminen

Viranomainen voi ilmoittaa valvovalle viranomaiselle myös muista kuin

merkittävistä poikkeamista sekä kyberuhkista ja läheltä piti –tilanteista. Myös ne 3 §:ssä tarkoitetut, joihin tätä lukua ei sovelleta, voivat tehdä tällaisen ilmoituksen.

Valvovan viranomaisen on käsiteltävä 1 momentissa tarkoitetut vapaaehtoiset ilmoitukset 18 e §:ssä säädettyä menettelyä noudattaen. Valvova viranomainen voi asettaa 18 d §:ssä tarkoitettujen ilmoitusten käsittelyn etusijalle vapaaehtoisten ilmoitusten käsittelyyn nähden.

Viranomainen ja muut 3 §:ssä tarkoitetut voivat vapaaehtoisen ilmoituksen yhteydessä luovuttaa valvovalle viranomaiselle tietoja, jotka valvovalla viranomaisella on oikeus saada 18 i §:n nojalla.

Vapaaehtoisessa ilmoittamisessa on noudatettava lisäksi NIS 2 -direktiivin 23 artiklan 11 kohdan nojalla mahdollisesti annettavia Euroopan komission täytäntöönpanosäädöksiä ilmoituksen tietosisällöstä, muodosta ja ilmoitusmenettelystä.

18 g §

Tiedotusvelvollisuus merkittävästä kyberuhkasta ja poikkeamasta

Viranomaisen on viipymättä ilmoitettava merkittävästä poikkeamasta palvelujensa vastaanottajille, jos merkittävä poikkeama todennäköisesti haittaa sen palvelujen tarjoamista.

Viranomaisen on viipymättä ilmoitettava merkittävästä kyberuhkasta sekä kyberuhkan hallitsemiseksi käytettävissä olevista toimenpiteistä niille palvelujensa vastaanottajille, joihin merkittävä kyberuhka saattaa vaikuttaa.

Jos merkittävästä poikkeamasta tiedottaminen on yleisen edun mukaista, valvova viranomainen voi velvoittaa viranomaisen tiedottamaan merkittävästä poikkeamasta tai tiedottaa asiasta itse.

Edellä 1 ja 2 momentissa tarkoitetussa tiedottamisessa on noudatettava lisäksi NIS 2 -direktiivin 23 artiklan 11 kohdan nojalla mahdollisesti annettavia Euroopan komission

täytäntöönpanosäädöksiä ilmoituksen tietosisällöstä, muodosta ja ilmoitusmenettelystä sekä merkittävän poikkeaman tarkemmasta määrittelystä.

18 h §

Valvova viranomainen

Tässä luvussa tarkoitettu valvova viranomainen ja NIS 2 -direktiivin 8 artiklan 1 kohdassa tarkoitettu toimivaltainen viranomainen julkishallinnon toimialalla on Liikenne- ja viestintävirasto. Valvovan viranomaisen tehtävänä on sen lisäksi mitä tässä luvussa säädetään, valvoa tässä luvussa ja NIS 2 -direktiivin nojalla annetuissa säännöksissä säädettyjen velvollisuuksien noudattamista julkishallinnon toimialalla sekä ylläpitää julkishallinnon toimialan toimijaluetteloa 18 a §:n nojalla toimitetuista tiedoista. Liikenne ja viestintävirasto on valvovan viranomaisen toiminnassaan itsenäinen ja riippumaton.

Valvova viranomainen voi asettaa tässä laissa säädetyt valvontatehtävänsä tärkeysjärjestykseen riskiperusteisesti. Valvovan viranomaisen on valvonnan kohdistamisessa ja 18 l §:ssä tarkoitettua valvontapäätöstä tehdessään otettava huomioon kyberturvallisuuslain 27 §:n 3 momentissa ja 37 §:ssä tarkoitetut seikat. Valvova viranomainen voi kohdistaa valvontaa hyvinvointialueeseen, hyvinvointiyhtymään tai Helsingin kaupunkiin vain, jos on perusteltu syy epäillä, että mainittu ei ole noudattanut tässä luvussa tai NIS 2 -direktiivin nojalla annetuissa säädöksissä säädettyä.

Ellei tässä luvussa toisin säädetä, valvovan viranomaisen on 18 a §:ssä tarkoitettujen toimintaa koskevien ilmoitusten, 18 d ja 18 f §:ssä tarkoitettujen poikkeamailmoitusten ja muiden valvontatehtävässä saatujen tietojen käsittelyssä sekä yhteistyössä muiden viranomaisten, Euroopan unionin toimielinten, erillisvirastojen ja yhteistyöelinten kanssa sekä tietojen luovuttamisessa niille noudatettava mitä

kyberturvallisuuslain 6 §:n 4 momentissa, 15 §:n 3 momentissa, 17 §:ssä, 18 §:n 3 momentissa, 26 §:n 2 momentissa, 28 §:n 4 ja 5 momentissa, 33 §:ssä, 41 §:n 5 momentissa sekä 45 §:ssä säädetään tietojen käsittelystä valvovassa viranomaisessa sekä valvovan viranomaisen yhteistyöstä muiden viranomaisten, Euroopan unionin toimielinten, erillisvirastojen ja yhteistyöelinten kanssa sekä tietojen luovuttamisesta niille.

Liikenne- ja viestintäviraston tehtävistä NIS 2 -direktiivissä tarkoitettuna keskistettynä yhteyspisteenä ja CSIRT-yksikkönä säädetään kyberturvallisuuslaissa.

18 i §

Valvovan viranomaisen tiedonsaantioikeus

Valvovalla viranomaisella on tämän luvun mukaisia tehtäviä suorittaessaan salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada kyberturvallisuutta koskevien riskien hallintaa, riskienhallinnan toimintamallia, hallintatoimenpiteitä ja merkittävää poikkeamaa koskevat tiedot sekä muut edellä mainittuihin tietoihin välittömästi liittyvät tiedot, jotka ovat välttämättömiä kyberturvallisuutta koskevan riskienhallintavelvoitteen noudattamisen ja merkittävistä poikkeamista ilmoittamisen ja raportoinnin valvontaa varten. Viranomaisen on luovutettava tiedot viipymättä ja maksutta.

Valvovalla viranomaisella on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada viranomaiselta välitystieto, sijaintitieto sekä tieto haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä, jos se on välttämätöntä kyberturvallisuutta koskevan riskienhallintavelvoitteen noudattamisen tai merkittävistä poikkeamista ilmoittamisen ja raportoinnin valvomista varten. Valvovan viranomaisen tämän momentin nojalla saamat tiedot on pidettävä salassa.

Voimassa oleva laki *Ehdotus*

Tässä pykälässä tarkoitettu tiedonsaantioikeus ei koske salassa pidettäviä tietoja julkisen hallinnon turvallisuusverkkotoiminnasta annetussa laissa tarkoitetusta turvallisuusverkon palvelutuotannosta tai palvelujen käytöstä eikä tietoja, joiden luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin niihin liittyvää tärkeää etua.

Erityissuojattavan tietoaineiston käsittelyä koskevista velvollisuuksista säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa.

18 j §

Valvovan viranomaisen oikeus tehdä tarkastuksia

Valvovalla viranomaisella on siinä laajuudessa kuin se on tarpeen, oikeus tehdä tässä luvussa tai NIS 2 -direktiivin nojalla annetuissa säännöksissä säädettyjen velvollisuuksien noudattamisen valvomiseksi viranomaiseen kohdistuva tarkastus.

Tarkastuksen suorittajalla on oltava tarkastuksen laatuun ja laajuuteen nähden riittävä koulutus ja kokemus.

Viranomaisen on tarkastusta varten päästettävä tarkastuksen suorittaja tarkastuksen edellyttämässä laajuudessa tarkastuksen kohteena olevaan viestintäverkkoon tai tietojärjestelmään ja muihin kuin pysyväisluonteiseen asumiseen tarkoitettuihin tiloihin. Tarkastuksen suorittamiseksi tarkastuksen suorittajalla 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 viranomaisen toteuttamat turvallisuusjärjestelyt. Tarkastuksen suorittajan tarkastus- ja tiedonsaantioikeuteen sovelletaan mitä 18 i §:n 3 momentissa säädetään tiedonsaantioikeuden rajoituksista.

Voimassa oleva laki *Ehdotus*

Tarkastuksessa noudatettavaan menettelyyn sovelletaan, mitä hallintolain 39 §:ssä säädetään tarkastuksesta.

18 k §

Avustavan tehtävän antaminen tietoturvallisuuden arviointilaitokselle ja arvioinnin teettäminen

Valvova viranomainen voi antaa 18 j §:ssä tarkoitettuun tarkastustehtävään liittyvän avustavan tehtävän tietoturvallisuuden arviointilaitoksista annetussa laissa (1405/2011) tarkoitetulle hyväksytylle tietoturvallisuuden arviointilaitokselle.

Valvova viranomainen voi valvonnan toteuttamiseksi velvoittaa viranomaisen teettämään tietoturvallisuuden arviointilaitoksella kyberturvallisuuteen kohdistuvan riskienhallinnan 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 18 c §:ssä tarkoitettujen kyberturvallisuuteen kohdistuvien riskienhallintavelvollisuuksien noudattamisen.

Tietoturvallisuuden arviointilaitoksen palveluksessa olevaan tarkastuksessa avustavaan henkilöön ja arvioinnin suorittajaan sovelletaan, mitä 18 j §:n 2–4 momentissa säädetään tarkastuksen suorittajan kokemuksesta ja koulutuksesta sekä tarkastuksen suorittajan oikeuksista. Ellei tässä luvussa toisin säädetä, tietoturvallisuuden arviointilaitokseen sovelletaan tietoturvallisuuden arviointilaitoksista annettua lakia. Tietoturvallisuuden arviointilaitoksen palveluksessa olevaan henkilöön sovelletaan hänen tässä pykälässä tarkoitettuja tehtäviä hoitaessaan virkamiehen rikosoikeudellista virkavastuuta koskevia säännöksiä, viraltapanoseuraamusta lukuun ottamatta. Vahingonkorvausvastuusta säädetään vahingonkorvauslaissa.

Voimassa oleva laki	*Ehdotus*
	18 l §
	Seuraamukset
	Valvova viranomainen voi velvoittaa viranomaisen määräajassa korjaamaan puutteet tässä luvussa tai NIS 2 -direktiivin nojalla annetuissa säännöksissä säädettyjen velvollisuuksien noudattamisessa. Valvova viranomainen voi velvoittaa viranomaisen julkistamaan kyseiset puutteet tai muut seikat, jotka liittyvät mainittujen velvollisuuksien rikkomiseen.
	Valvova viranomainen voi antaa viranomaiselle varoituksen, jos tämä ei ole noudattanut tässä luvussa tai NIS 2 -direktiivin nojalla annetuissa säännöksissä säädettyjä velvollisuuksia. Varoituksessa on yksilöitävä puute tai laiminlyönti, jota varoitus koskee. Varoitus on annettava kirjallisena.
	Valvova viranomainen voi asettaa uhkasakon 1 momentissa tarkoitetun päätöksen noudattamisen tehosteeksi.
	18 m §
	Muutoksenhaku
	Muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).
	Muutoksenhausta uhkasakon asettamista ja maksettavaksi tuomitsemista koskevaan päätökseen säädetään uhkasakkolaissa (1113/1990).
	Tämä laki tulee voimaan päivänä kuuta 20 .
	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) 2 §:n 2 momentti ja 247 a §, sellaisina kuin ne ovat, ensin mainittu laissa 1207/2020 ja viimeksi mainittu laissa 281/2018,

muutetaan 165 §:n 1 momentti, 167, 170 ja 275 §, 308 §:n 3 momentti, 313 §:n 2 momentin 2 kohta, 318 §:n 4 momentti ja 342 §:n 2 momentti,

sellaisina kuin ne ovat, 165 §:n 1 momentti, 170 §, 308 §:n 3 momentti sekä 313 §:n 2 momentin 2 kohta laissa 1003/2018, 167 § laeissa 1003/2018 ja 1207/2020 sekä 275 § ja 318 §:n 4 momentti laissa 1207/2020 sekä 342 §:n 2 momentti laissa 1182/2023, ja

lisätään 165 §:ään, sellaisena kuin se on laissa 1003/2018, uusi 4 momentti ja 247 §:ään, sellaisena kuin se on laissa 1003/2018, uusi 5 momentti

seuraavasti:

Voimassa oleva laki	*Ehdotus*
2 §	2 §
Eräiden säännösten soveltaminen	*Eräiden säännösten soveltaminen*
— — — — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — — — —
Jäljempänä 247 a §:ssä tarkoitetun verkossa toimivan markkinapaikan, hakukonepalvelun ja pilvipalvelun tarjoajan katsotaan kuuluvan sen jäsenvaltion lainkäyttövallan piiriin, jossa sen tosiasiallinen toimipaikka sijaitsee. Mainitussa pykälässä tarkoitetun toimijan, joka ei ole sijoittautunut Euroopan unioniin, on nimettävä edustaja Euroopan unionin aluetta varten. Edustajan on oltava sijoittautunut johonkin niistä jäsenvaltioista, joissa palveluja tarjotaan. Toimijan katsotaan kuuluvan sen jäsenvaltion lainkäyttövallan piiriin, johon edustaja on sijoittautunut.	*(kumotaan)*
— — — — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — — — —
165 §	165 §
Verkkotunnusvälittäjän ilmoitusvelvollisuudet	*Verkkotunnusvälittäjän ilmoitusvelvollisuudet*
Verkkotunnusvälittäjän on ennen toimintansa aloittamista tehtävä ilmoitus verkkotunnusrekisteriä hallinnoivalle viranomaiselle. Ilmoituksessa on oltava	Verkkotunnusvälittäjän on ennen toimintansa aloittamista tehtävä ilmoitus verkkotunnusrekisteriä hallinnoivalle

Voimassa oleva laki	*Ehdotus*
verkkotunnusvälittäjän yksilöivät tiedot, kuulemisiin ja tiedoksiantoihin käytettävä sähköpostiosoite sekä muut valvonnan kannalta tarpeelliset tiedot.	viranomaiselle. Ilmoituksessa on oltava *seuraavat tiedot:*
(lisätään)	*1) verkkotunnusvälittäjän nimi, y-tunnus tai sellaisen puuttuessa muu yksilöivä tieto sekä kuulemisiin ja tiedoksiantoihin käytettävä sähköpostiosoite;* *2) verkkotunnusvälittäjän päätoimipaikan ja muiden Euroopan 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;* *3) verkkotunnusvälittäjän IP-osoitealueet;* *4) luettelo niistä Euroopan unionin jäsenvaltioista, joissa verkkotunnusvälittäjä tarjoaa palveluja; ja* *5) muut kuin 1–4 kohdassa tarkoitetut valvonnan kannalta tarpeelliset tiedot.*
— — — — — — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — — — — — —
(lisätään)	*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 (NIS 2-direktiivi) 27 artiklan 4 kohdassa tarkoitetun ilmoituksen tekemiseksi tarpeelliset tiedot verkkotunnusvälittäjien ilmoituksista kyberturvallisuuslain (/) 18 §:ssä tarkoitetulle keskitetylle yhteyspisteelle*.
167 § *Tietojen merkitseminen verkkotunnusrekisteriin ja tietojen julkaiseminen* Verkkotunnus on merkittävä verkkotunnuksen käyttäjän nimiin. Verkkotunnusvälittäjän on merkittävä verkkotunnusrekisteriin verkkotunnuksen	167 §

Voimassa oleva laki

käyttäjää koskevat oikeat, ajantasaiset ja yksilöivät tiedot sekä kuulemisiin ja tiedoksiantoihin käytettävä sähköpostiosoite.

(lisätään)

Liikenne- ja viestintävirasto *voi julkaista internet-sivuillaan ja sen lisäksi muussa sähköisessä palvelussa tietoja verkkotunnusrekisteristä.* 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. Rekisterin tietojen luovuttamiseen sovelletaan muutoin viranomaisten toiminnan julkisuudesta annetun lain 16 §:ää.

(lisätään)

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

Ehdotus

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 ja 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*

Voimassa oleva laki

teknisestä toteuttamistavasta ja merkitsemisen yhteydessä ilmoitettavista tiedoista sekä verkkotunnuksen käyttäjän tunnistamisesta.

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 viestintäviraston, 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.

(lisätään)

Ehdotus

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 teknisestä 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 viestintäviraston, 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*;*

Voimassa oleva laki

Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä verkkotunnuksen käyttäjälle annettavista tiedoista, toiminnan tietoturvallisuudesta, siitä milloin 1 momentin 7 kohdassa tarkoitettu häiriö on merkittävä sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

(lisätään)

247 §

Viestinnän välittäjän ja lisäarvopalvelun tarjoajan velvollisuus huolehtia tietoturvasta

— — — — — — — — — — — — — — —

(lisätään)

247 a §

Verkossa toimivan markkinapaikan, hakukonepalvelun ja pilvipalvelun tarjoajan velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta

Ehdotus

8) asetettava julkisesti saataville toimintaperiaatteet ja menettelyt, joilla varmistetaan verkkotunnusrekisterin tietojen olevan 167 §:n 1 momentissa säädetyn 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 1 momentin 8 ja 11 kohdassa tarkoitetuista toimintaperiaatteista ja menettelyistä,* toiminnan tietoturvallisuudesta sekä siitä, milloin 1 momentin 7 kohdassa tarkoitettu häiriö on merkittävä sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

Kyberturvallisuuslain 2 §:n 3 kohdassa tarkoitetun DNS-palveluntarjoajan velvollisuudesta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja poikkeamien ilmoittamisesta säädetään kyberturvallisuuslaissa.

247 §

Viestinnän välittäjän ja lisäarvopalvelun tarjoajan velvollisuus huolehtia tietoturvasta

— — — — — — — — — — — — — — —

Tietoturvasta huolehtimiseen sovelletaan lisäksi, mitä kyberturvallisuuslaissa säädetään sellaisen viestinnän välittäjän ja

Voimassa oleva laki	*Ehdotus*
Verkossa toimivan markkinapaikan, hakukonepalvelun ja pilvipalvelun tarjoajan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. Riskienhallinnassa on huomioitava: *1) järjestelmien ja tilojen turvallisuus;* *2) tietoturvauhkien ja häiriöiden käsittely;* *3) liiketoiminnan jatkuvuuden hallinta;* *4) seuranta, tarkastukset ja testaukset;* *5) kansainvälisten standardien noudattaminen.* *Edellä 1 momentissa tarkoitettu riskienhallintavelvoite ei koske toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/1148, jäljempänä verkko- ja tietoturvadirektiivi, 16 artiklan 11 kohdassa tarkoitettuja mikroyrityksiä tai pieniä yrityksiä.*	*lisäarvopalvelun tarjoajan osalta, joka kuuluu NIS 2-direktiivin soveltamisalaan.* *(kumotaan)*
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. *Liikenne- ja viestintävirasto toimittaa komissiolle ja Euroopan unionin kyberturvallisuusvirastolle vuosittain tiivistelmäraportin ilmoituksista.* *Edellä 247 a §:ssä tarkoitetun verkossa toimivan markkinapaikan tarjoajan, hakukonepalvelun tarjoajan sekä pilvipalvelun tarjoajan on ilmoitettava viipymättä Liikenne- ja viestintävirastolle sen palveluun kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä.*	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.

Voimassa oleva laki

Jos häiriöistä ilmoittaminen on yleisen edun mukaista, Liikenne- ja viestintävirasto voi velvoittaa teleyrityksen tai palvelun tarjoajan 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 ja 2 momentissa* tarkoitettujen ilmoitusten sisällöstä, muodosta ja toimittamisesta.

Liikenne- ja viestintäviraston on arvioitava, koskeeko *1 ja 2 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.

308 §

Yhteistyö eri viranomaisten kanssa

— — — — — — — — — — — — — — —

Liikenne- ja viestintäviraston on toimittava yhteistyössä muiden Euroopan unionin jäsenvaltioiden verkko- ja tietoturvallisuutta valvovien viranomaisten, tietoturvaloukkauksiin reagoivien yksiköiden sekä *verkko- ja tietoturvadirektiivin 11 artiklassa tarkoitetun yhteistyöryhmän kanssa. Liikenne- ja viestintävirasto toimittaa yhteistyöryhmälle vuosittain verkko- ja tietoturvadirektiivin 10 artiklan 3 kohdan mukaisen tiivistelmäraportin.*

313 §

Valvonta-asioiden käsittely Liikenne- ja viestintävirastossa

— — — — — — — — — — — — — — —

Liikenne- ja viestintävirasto voi asettaa tässä laissa säädetyt valvontatehtävänsä tärkeysjärjestykseen. Liikenne- ja viestintävirasto voi jättää asian tutkimatta, jos:

Ehdotus

(muutetaan)

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 kyberturvallisuuslaissa 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.*

Voimassa oleva laki

— — — — — — — — — — — — — — —

2) asialla on epäillystä virheestä tai laiminlyönnistä huolimatta viestintämarkkinoiden toimivuuden, viestintäpalvelujen luotettavuuden tai sähköisen viestinnän häiriöttömyyden turvaamisen ja palveluja käyttävien edun *taikka 247 a §:ssä tarkoitettujen palveluiden riskinhallinnan* 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 ja 2 momentin* nojalla saamansa salassa pidettävä asiakirja sekä ilmaista salassa pidettävä tieto toisen ETA-valtion valvontaviranomaiselle *ja verkko-ja tietoturvadirektiivin 11 artiklassa tarkoitetulle yhteistyöryhmälle,* 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.

— — — — — — — — — — — — — — —

342 §

Oikaisuvaatimus

— — — — — — — — — — — — — — —

Ehdotus

313 §

Valvonta-asioiden käsittely Liikenne- ja viestintävirastossa

— — — — — — — — — — — — — — —

Liikenne- ja viestintävirasto voi asettaa tässä laissa säädetyt valvontatehtävänsä tärkeysjärjestykseen. Liikenne- ja viestintävirasto voi jättää asian tutkimatta, jos:

— — — — — — — — — — — — — — —

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 mainitun direktiivin 15 artiklassa tarkoitetulle CSIRT-verkostolle,* jos se on verkko- ja tietoturvallisuuden valvonnan kannalta välttämätöntä, eikä luovuttaminen vaaranna mainituissa pykälissä tarkoitettujen toimijoiden turvallisuuteen ja

Voimassa oleva laki	*Ehdotus*
Liikenne- ja viestintäviraston päätökseen, joka koskee 39 §:ssä tarkoitettua radiolupaa, 44 §:ssä tarkoitettua radiotaajuuksien varausta koskevaa päätöstä, 100 §:ssä tarkoitettua numerointipäätöstä, 288 §:ssä tarkoitettua markkinaehtoista taajuusmaksua, 289 §:ssä tarkoitettua tietoyhteiskuntamaksua, 293 §:ssä tarkoitettua televisio- ja radiotoiminnan valvontamaksua tai datanhallinta-asetuksen 19 artiklan 5 kohdassa tarkoitettua rekisteröintiä, saa vaatia oikaisua.	liikesalaisuuksiin liittyviä etuja tai annettujen tietojen luottamuksellisuutta.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
	342 §
	Oikaisuvaatimus
	— — — — — — — — — — — — — — —
	Liikenne- ja viestintäviraston päätökseen, joka koskee 39 §:ssä tarkoitettua radiolupaa, 44 §:ssä tarkoitettua radiotaajuuksien varausta koskevaa päätöstä, 100 §:ssä tarkoitettua numerointipäätöstä, *167 §:n 2 momentissa tarkoitettua verkkotunnuksen rekisteröinnin estämistä, 169 §:n 1 momentissa tarkoitettua verkkotunnuksen poistamista*, 288 §:ssä tarkoitettua markkinaehtoista taajuusmaksua, 289 §:ssä tarkoitettua tietoyhteiskuntamaksua, 293 §:ssä tarkoitettua televisio- ja radiotoiminnan valvontamaksua tai datanhallinta-asetuksen 19 artiklan 5 kohdassa tarkoitettua rekisteröintiä, saa vaatia oikaisua.
	— — — — — — — — — — — — — — —
	Tämä laki tulee voimaan päivänä kuuta 20 .

4

Laki

ilmailulain 128 a ja 128 b §:n kumoamisesta

Eduskunnan päätöksen mukaisesti säädetään:

Tällä lailla kumotaan ilmailulain (864/2014) 128 a ja 128 b §, sellaisina kuin ne ovat laissa 965/2018.

Voimassa oleva laki	*Ehdotus*
128 a §	
Velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta	*(kumotaan)*
Lennonvarmistuspalvelun tarjoajan sekä yhteiskunnan toiminnan kannalta merkittävän lentoaseman pitäjän on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. *Liikenne- ja viestintäviraston on arvioitava 1 momentissa tarkoitetun riskienhallinnan vaikutuksia ilmailun turvallisuuteen. Lennonvarmistuspalvelun tarjoajan sekä yhteiskunnan toiminnan kannalta merkittävän lentoaseman pitäjän on annettava Liikenne- ja viestintävirastolle arvioinnin kannalta tarpeelliset tiedot. Virasto voi velvoittaa lennonvarmistuspalvelun tarjoajan sekä yhteiskunnan toiminnan kannalta merkittävän lentoaseman pitäjän ryhtymään korjaaviin toimenpiteisiin ilmailun turvallisuuteen kohdistuvan merkittävän riskin poistamiseksi.* *Valtioneuvoston asetuksella säädetään, milloin lentoasemaa on pidettävä yhteiskunnan toiminnan kannalta merkittävänä.*	
128 b §	*(kumotaan)*
Tietoturvapoikkeamista ilmoittaminen	
Lennonvarmistuspalvelun tarjoajan sekä yhteiskunnan toiminnan kannalta merkittävän lentoaseman pitäjän on ilmoitettava viipymättä Liikenne- ja viestintävirastolle	

Voimassa oleva laki	*Ehdotus*
viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä poikkeamasta. *Jos poikkeamasta ilmoittaminen on yleisen edun mukaista, Liikenne- ja viestintävirasto voi velvoittaa palvelun tarjoajan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.* *Liikenne- ja viestintäviraston on arvioitava, koskeeko 1 momentissa tarkoitettu poikkeama muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.* *Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu poikkeama on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.*	
	Tämä laki tulee voimaan päivänä kuuta 20

5

Laki

raideliikennelain 169 §:n kumoamisesta

Eduskunnan päätöksen mukaisesti säädetään:
Tällä lailla kumotaan raideliikennelain (1302/2018) 169 §.

Voimassa oleva laki	*Ehdotus*
169 §	
Velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen	*(kumotaan)*
Valtion rataverkon haltijan sekä liikenteenohjauspalvelun tarjoajan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. *Valtion rataverkon haltijan sekä liikenteenohjauspalvelun tarjoajan on ilmoitettava viipymättä Liikenne- ja viestintävirastolle viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä.* *Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Liikenne- ja viestintävirasto voi velvoittaa palvelun tarjoajan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.* *Liikenne- ja viestintäviraston on arvioitava, koskeeko 2 momentissa tarkoitettu häiriö muita ETA-valtioita ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.* *Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä siitä, milloin 2 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.*	

Voimassa oleva laki	*Ehdotus*
	Tämä laki tulee voimaan päivänä kuuta 20

6

Laki

liikenteen palveluista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan liikenteen palveluista annetun lain (320/2017) 161 §, sellaisena kuin se on laissa 1256/2020, sekä

muutetaan 140 §, sellaisena kuin se on laeissa 579/2018, 984/2018 ja 371/2019 seuraavasti:

Voimassa oleva laki	*Ehdotus*
15 luku	15 luku
140 §	140 §
Tietoturva tieliikenteen ohjaus- ja hallintapalvelussa	*Tietoturva tieliikenteen ohjaus- ja hallintapalvelussa*
Tieliikenteen ohjaus- ja hallintapalvelun tarjoajan on huolehdittava käyttämiinsä liikenteen turvallisuuden kannalta merkittäviin viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.	*Tieliikenteen ohjaus- ja hallintapalvelun tarjoajan velvollisuudesta huolehtia käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja poikkeamien ilmoittamisesta säädetään kyberturvallisuuslaissa (/).*
Tieliikenteen ohjaus- ja hallintapalvelun tarjoajan on ilmoitettava viipymättä Liikenne- ja viestintävirastolle sellaisesta sen järjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, joka voi aiheuttaa merkittävän vaaran liikenteen turvallisuudelle. Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä ilmoituksen sisällöstä, muodosta ja toimittamisesta.	*(muutetaan)*
Jos poikkeamasta ilmoittaminen on yleisen edun mukaista, Liikenne- ja viestintävirasto voi velvoittaa palvelun tarjoajan	

Voimassa oleva laki	*Ehdotus*
tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse. (23.11.2018/984) *Liikenne- ja viestintäviraston on arvioitava, koskeeko 1 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltiota ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.* Tieliikenteen ohjaus- ja hallintapalvelun tarjoajan on tallennettava ja säilytettävä tieliikenteen tilannekuva tavalla, joka turvaa tallenteet oikeudettomalta puuttumiselta. Tallenteita on säilytettävä 14 vuorokautta.	Tieliikenteen ohjaus- ja hallintapalvelun tarjoajan on tallennettava ja säilytettävä tieliikenteen tilannekuva tavalla, joka turvaa tallenteet oikeudettomalta puuttumiselta. Tallenteita on säilytettävä 14 vuorokautta.
18 luku	
161 §	*(kumotaan)*
Älykkään liikennejärjestelmän ylläpitäjän velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen	
Älykkään liikennejärjestelmän ylläpitäjän on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. *Älykkään liikennejärjestelmän ylläpitäjän on ilmoitettava viipymättä Liikenne- ja viestintävirastolle sen käyttämiin viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä.* *Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Liikenne- ja viestintävirasto voi velvoittaa palvelun tarjoajan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.* *Liikenne- ja viestintäviraston on arvioitava, koskeeko 2 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.* *Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä siitä, milloin 2 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.*	

Voimassa oleva laki	*Ehdotus*
	Tämä laki tulee voimaan päivänä kuuta 20

7

Laki

alusliikennepalvelulain 18 a §:n kumoamisesta

Eduskunnan päätöksen mukaisesti säädetään:

Tällä lailla kumotaan alusliikennepalvelulain (623/2005) 18 a §, sellaisena kuin se on laissa 947/2018.

Voimassa oleva laki	*Ehdotus*
18 a §	
Tietoturvaan liittyvistä häiriöistä ilmoittaminen	*(kumotaan)*
VTS-palveluntarjoajan on ilmoitettava viipymättä Liikenne- ja viestintävirastolle käyttämiinsä viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä.	
Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Liikenne- ja viestintävirasto voi velvoittaa palvelun tarjoajan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.	
Liikenne- ja viestintäviraston on arvioitava, koskeeko 1 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.	
Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.	

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:

Tällä lailla kumotaan eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain (485/2004) 7 e ja 7 f §, sellaisina kuin ne ovat laissa 955/2018.

Voimassa oleva laki	*Ehdotus*
7 e §	
Satamanpitäjän velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta	*(kumotaan)*
Yhteiskunnan toiminnan kannalta merkittävän satamanpitäjä on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. *Liikenne- ja viestintäviraston on arvioitava 1 momentissa tarkoitetun riskienhallinnan vaikutuksia merenkulun turvallisuuteen. Virasto voi velvoittaa 1 momentissa tarkoitetun satamanpitäjän ryhtymään korjaaviin toimenpiteisiin merenkulun turvallisuuteen kohdistuvan merkittävän riskin poistamiseksi. Velvoitteen tehosteeksi voidaan asettaa uhkasakko. Uhkasakosta säädetään uhkasakkolaissa (1113/1990).* *Valtioneuvoston asetuksella säädetään, milloin 1 momentissa tarkoitettua satamaa on pidettävä yhteiskunnan toiminnan kannalta merkittävänä.*	
7 f §	
Tietoturvallisuuteen liittyvistä häiriöistä ilmoittaminen	*(kumotaan)*
Yhteiskunnan toiminnan kannalta merkittävän satamanpitäjän on ilmoitettava viipymättä Liikenne- ja viestintävirastolle sen käyttämiin viestintäverkkoihin tai	

Voimassa oleva laki	*Ehdotus*
tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä. *Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Liikenne- ja viestintävirasto voi velvoittaa palvelun tarjoajan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.* *Liikenne- ja viestintäviraston on arvioitava, koskeeko 1 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.* *Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.*	
	Tämä laki tulee voimaan päivänä kuuta 20

9

Laki

sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain 2 ja 90 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain (703/2023), 2 §:n 3 momentti ja 90 § seuraavasti:

Voimassa oleva laki	*Ehdotus*
2 §	2 §
Soveltamisala ja suhde muuhun lainsäädäntöön	*Soveltamisala ja suhde muuhun lainsäädäntöön*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Tällä lailla pannaan sosiaali- ja terveydenhuollossa täytäntöön toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148.	*Tällä 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 kyberturvallisuuslakia (/) täydentävät ja täsmentävät säännökset käsiteltäessä sosiaali- ja terveydenhuollon asiakastietoja ja asiakkaan itsensä tuottamia hyvinvointitietoja sosiaali- ja terveyspalveluita järjestettäessä ja toteutettaessa.*
(muutetaan)	
90 §	90 §
Ilmoittaminen tietojärjestelmän ja hyvinvointisovelluksen olennaisten vaatimusten poikkeamista sekä tietoverkkoihin kohdistuvista tietoturvallisuuden häiriöistä	*Ilmoittaminen tietojärjestelmän ja hyvinvointisovelluksen olennaisten vaatimusten poikkeamista sekä tietoverkkoihin kohdistuvista tietoturvallisuuden häiriöistä*
Jos palvelunantaja tai apteekki havaitsee, että tietojärjestelmän olennaisten vaatimusten täyttymisessä on merkittäviä poikkeamia, sen on ilmoitettava asiasta tietojärjestelmäpalvelun tuottajalle. Jos tietojärjestelmän tai hyvinvointisovelluksen	Jos palvelunantaja tai apteekki havaitsee, että tietojärjestelmän olennaisten vaatimusten täyttymisessä on merkittäviä poikkeamia, sen on ilmoitettava asiasta tietojärjestelmäpalvelun tuottajalle. Jos tietojärjestelmän tai hyvinvointisovelluksen poikkeama voi aiheuttaa merkittävän riskin

Voimassa oleva laki	*Ehdotus*
poikkeama voi aiheuttaa merkittävän riskin asiakas- tai potilasturvallisuudelle tai tietoturvalle, on palvelunantajan, apteekin, tietojärjestelmäpalvelun tuottajan tai tietojärjestelmän valmistajan, hyvinvointisovelluksen valmistajan, Kansaneläkelaitoksen tai Terveyden ja hyvinvoinnin laitoksen ilmoitettava siitä Sosiaali- ja terveysalan lupa- ja valvontavirastolle. Myös muu taho voi ilmoittaa Sosiaali- ja terveysalan lupa- ja valvontavirastolle havaitsemistaan riskeistä. Henkilötietojen tietoturvaloukkauksista ilmoittamisesta tietosuojavaltuutetulle säädetään tietosuoja-asetuksen 33 artiklassa.	asiakas- tai potilasturvallisuudelle tai tietoturvalle, on palvelunantajan, apteekin, tietojärjestelmäpalvelun tuottajan tai tietojärjestelmän valmistajan, hyvinvointisovelluksen valmistajan, Kansaneläkelaitoksen tai Terveyden ja hyvinvoinnin laitoksen ilmoitettava siitä Sosiaali- ja terveysalan lupa- ja valvontavirastolle. Myös muu taho voi ilmoittaa Sosiaali- ja terveysalan lupa- ja valvontavirastolle havaitsemistaan riskeistä. *Jos tietojärjestelmän poikkeama voi aiheuttaa merkittävän riskin apteekin toiminnalle, on apteekin ilmoitettava siitä lisäksi Lääkealan turvallisuus- ja kehittämiskeskukselle.* Henkilötietojen tietoturvaloukkauksista ilmoittamisesta tietosuojavaltuutetulle säädetään tietosuoja-asetuksen 33 artiklassa.
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 sosiaali- ja terveyspalveluiden toteuttaminen voi merkittävästi vaarantua. *Terveyden ja hyvinvoinnin laitos voi antaa tarkempia määräyksiä siitä, milloin häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.*	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 sosiaali- ja terveyspalveluiden toteuttaminen voi merkittävästi vaarantua. *Sosiaali- ja terveysalan lupa- ja valvontavirasto voi antaa tarkempia määräyksiä siitä, milloin häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.*
(muutetaan)	*Apteekin on lisäksi ilmoitettava viipymättä Lääkealan turvallisuus- ja kehittämiskeskukselle sellaisesta sen käyttämiin käyttöympäristöihin ja tietoverkkoihin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena apteekin toiminta voi merkittävästi vaarantua. Lääkealan turvallisuus- ja kehittämiskeskus 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	Jos 1 ja 2 momentissa tarkoitetusta tietoturvallisuuteen liittyvästä poikkeamasta tai häiriöstä ilmoittaminen on yleisen edun mukaista, Sosiaali- ja terveysalan lupa- ja

Voimassa oleva laki	*Ehdotus*
valvontavirasto voi velvoittaa palvelunantajan, apteekin, Kansaneläkelaitoksen, tietojärjestelmäpalvelun tuottajan tai tietojärjestelmän valmistajan taikka välittäjän tiedottamaan yleisölle asiasta taikka kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.	valvontavirasto voi velvoittaa palvelunantajan, apteekin, Kansaneläkelaitoksen, tietojärjestelmäpalvelun tuottajan tai tietojärjestelmän valmistajan taikka välittäjän tiedottamaan yleisölle asiasta taikka kuultuaan ilmoitusvelvollista tiedottaa asiasta itse. *Lisäksi Lääkealan turvallisuus- ja kehittämiskeskus voi velvoittaa apteekin tiedottamaan yleisölle 3 momentissa tarkoitetusta häiriöstä taikka kuultuaan ilmoitusvelvollista tiedottaa häiriöstä itse.*
Sosiaali- ja terveysalan lupa- ja valvontaviraston on arvioitava, koskeeko 1 ja 2 momentissa tarkoitettu julkista terveydenhuoltoa koskeva tietoturvallisuuteen liittyvä poikkeama tai häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille jäsenvaltioille.	*(muutetaan)*
	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, sellaisina 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:

Voimassa oleva laki	*Ehdotus*
29 a §	
Verkonhaltijan velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen	*(kumotaan)*
Verkonhaltijan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. *Verkonhaltijan on ilmoitettava viipymättä Energiavirastolle sellaisesta sen käyttämiin viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena sähkönjakelu voi keskeytyä jakeluverkossa merkittävässä laajuudessa.* *Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Energiavirasto voi velvoittaa palvelun tarjoajan tiedottamaan yleisölle asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.* *Energiaviraston on arvioitava, koskeeko 2 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille jäsenvaltioille.* *Energiavirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.*	

Voimassa oleva laki

49 a §

Sähkökaupan keskitetyn tiedonvaihdon palvelut

— — — — — — — — — — — — — —

Järjestelmävastaavan siirtoverkonhaltijan on ilmoitettava viipymättä Energiavirastolle sähkökaupan keskitetyn tiedonvaihdon palvelujen tuottamisessa käyttämiinsä tietojärjestelmiin kohdistuvista merkittävistä häiriöistä ja sähkökaupan keskitetyn tiedonvaihdon palveluihin kohdistuvista tai niitä uhkaavista merkittävistä tietoturvaloukkauksista taikka muista tapahtumista, jotka estävät näiden palvelujen toimivuuden tai häiritsevät niitä olennaisesti. Ilmoituksen käsittelyyn sovelletaan 29 a §:ssä säädettyä menettelyä. Energiavirasto voi antaa tarkempia määräyksiä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

62 §

Suljettua jakeluverkkoa koskevat erityissäännökset

Suljettuun jakeluverkkoon ja suljetun jakeluverkonhaltijaan ei sovelleta 23, 23 a eikä 26 a §:ää, 27 §:n 3 momenttia, 28, 29, ***29 a***, 29 b, 50–52, 52 a, 53, 53 a, 54–56, 56 a, 58 eikä 59 §:ää ja 61 a §:ä:n 2 momenttia.

— — — — — — — — — — — — — —

Ehdotus

49 a §

Sähkökaupan keskitetyn tiedonvaihdon palvelut

— — — — — — — — — — — — — —

(kumotaan)

62 §

Suljettua jakeluverkkoa koskevat erityissäännökset

Suljettuun jakeluverkkoon ja suljetun jakeluverkonhaltijaan ei sovelleta 23, 23 a eikä 26 a §:ää, 27 §:n 3 momenttia, 28, 29, 29 b, 50–52, 52 a, 53, 53 a, 54–56, 56 a, 58 eikä 59 §:ää ja 61 a §:n 2 momenttia.

— — — — — — — — — — — — — —

Tämä laki tulee voimaan päivänä kuuta 20

11

Laki

maakaasumarkkinalain 34 a §:n kumoamisesta

Eduskunnan päätöksen mukaisesti säädetään:

Tällä lailla kumotaan maakaasumarkkinalain (587/2017) 34 a §, sellaisena kuin se on laeissa 288/2018 ja 327/2020.

Voimassa oleva laki	*Ehdotus*
34 a §	
Siirtoverkonhaltijan velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen	(*kumotaan*)
Siirtoverkonhaltijan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. Riskienhallinnassa on otettava huomioon: *1) järjestelmien ja tilojen turvallisuus;* *2) tietoturvauhkien ja häiriöiden käsittely;* *3) liiketoiminnan jatkuvuuden hallinta;* *4) riskien seuranta sekä järjestelmien tarkastukset ja testaukset;* *5) mahdollisten kansainvälisten standardien noudattaminen.* *Siirtoverkonhaltijan on ilmoitettava viipymättä Energiavirastolle palvelujen tuottamisessa käyttämiinsä tietojärjestelmiin kohdistuvista merkittävistä häiriöistä ja palveluihin kohdistuvista tai niitä uhkaavista merkittävistä tietoturvaloukkauksista sekä muista tapahtumista, jotka estävät näiden palvelujen toimivuuden tai häiritsevät niitä olennaisesti.* *Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Energiavirasto voi velvoittaa siirtoverkonhaltijan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.*	

Voimassa oleva laki	*Ehdotus*
Energiaviraston on arvioitava, koskeeko 2 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille jäsenvaltioille. *Energiavirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta*.	
	Tämä laki tulee voimaan päivänä kuuta 20

12

Laki

Energiavirastosta annetun lain 1 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan Energiavirastosta annetun lain (870/2013) 1 §:n 2 momentin 19 kohta, sellaisena kuin se on laissa 418/2019, sekä

lisätään 1 §:n 2 momenttiin, sellaisena kuin se on osaksi laeissa 634/2020, 804/2020, 606/2021 ja 500/2023, uusi 20 kohta

seuraavasti:

Voimassa oleva laki	*Ehdotus*
1 §	1 §
Tehtävät	*Tehtävät*
— — — — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — — — —
Energiavirasto hoitaa tehtävät, jotka sille on annettu:	Energiavirasto hoitaa tehtävät, jotka sille on annettu:
— — — — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — — — —
(lisätään)	*19) biopolttoöljyn käytön edistämisestä annetussa laissa (418/2019);* *20) kyberturvallisuuslaissa (/).*
— — — — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — — — —

Tämä laki tulee voimaan päivänä kuuta 20

13

Laki

sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain (590/2013) 9 §, 23 §:n 4 ja 5 kohta sekä 28 §:n 1 momentin 1 kohta, sellaisina kuin niistä ovat 23 §:n 4 ja 5 kohta laissa 589/2017 ja 28 §:n 1 momentin 1 kohta laissa 1002/2018, sekä

lisätään 2 §:ään, sellaisena kuin se on laeissa 633/2020 ja 49/2023, uusi 2 momentti ja 23 §:ään, sellaisena kuin se on laissa 589/2017, uusi 6 kohta

seuraavasti:

Voimassa oleva laki	*Ehdotus*
2 §	2 §
Soveltamisala	*Soveltamisala*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
(lisätään)	Tämän lain 23 ja 24 §:ää sovelletaan lisäksi niiden tehtävien hoitamiseen, jotka säädetään Energiaviraston tehtäviksi kyberturvallisuuslaissa (/).
9 §	9 §
Energiamarkkinaviraston toimivalta valvonta-asioissa	*Energiamarkkinaviraston toimivalta valvonta-asioissa*
Jos joku rikkoo tai laiminlyö *2 §:ssä* tarkoitetussa kansallisessa tai Euroopan unionin lainsäädännössä säädettyjä velvoitteitaan, Energiamarkkinaviraston on velvoitettava hänet korjaamaan rikkomuksensa tai laiminlyöntinsä. Päätöksessä voidaan määrätä, millä tavoin rikkomus tai laiminlyönti tulee korjata. Päätöksessä voidaan myös määrätä palauttamaan asiakkaalle virheellisesti peritty maksu, jos palautukseen ei sovelleta 14 §:ssä säädettyä palautusmenettelyä	Jos joku rikkoo tai laiminlyö *2 §:n 1 momentissa* tarkoitetussa kansallisessa tai Euroopan unionin lainsäädännössä säädettyjä velvoitteitaan, Energiamarkkinaviraston on velvoitettava hänet korjaamaan rikkomuksensa tai laiminlyöntinsä. Päätöksessä voidaan määrätä, millä tavoin rikkomus tai laiminlyönti tulee korjata. Päätöksessä voidaan myös määrätä palauttamaan asiakkaalle virheellisesti peritty maksu, jos palautukseen ei sovelleta 14 §:ssä säädettyä palautusmenettelyä
23 §	23 §
Sähkö- ja maakaasuverkkoluvan peruuttaminen	*Sähkö- ja maakaasuverkkoluvan peruuttaminen*

Voimassa oleva laki	*Ehdotus*
Energiavirasto voi peruuttaa sähköverkkoluvan, maakaasuverkkoluvan sekä sähkömarkkinalain 12 §:ssä ja maakaasumarkkinalain 11 §:ssä säädetyn vapautuksen tai poikkeusluvan:	Energiavirasto voi peruuttaa sähköverkkoluvan, maakaasuverkkoluvan sekä sähkömarkkinalain 12 §:ssä ja maakaasumarkkinalain 11 §:ssä säädetyn vapautuksen tai poikkeusluvan:
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
4) jos luvanhaltija toistuvasti ja oleellisesti rikkoo maakaasuverkkoasetusta tai sen nojalla annettujen, suuntaviivoja koskevien komission asetusten tai päätösten säännöksiä, siltä osin kuin niitä sovelletaan Suomessa, eikä luvanhaltijalle etukäteen annettu varoitus luvan peruuttamisesta ole johtanut toiminnassa esiintyneiden puutteiden korjaamiseen; *tai*	4) jos luvanhaltija toistuvasti ja oleellisesti rikkoo maakaasuverkkoasetusta tai sen nojalla annettujen, suuntaviivoja koskevien komission asetusten tai päätösten säännöksiä, siltä osin kuin niitä sovelletaan Suomessa, eikä luvanhaltijalle etukäteen annettu varoitus luvan peruuttamisesta ole johtanut toiminnassa esiintyneiden puutteiden korjaamiseen;
5) jos luvanhaltija toistuvasti ja oleellisesti rikkoo maakaasun siirtoverkonhaltijan eriyttämisestä annetun lain säännöksiä eikä luvanhaltijalle etukäteen annettu varoitus luvan peruuttamisesta ole johtanut toiminnassa esiintyneiden puutteiden korjaamiseen.	5) jos luvanhaltija toistuvasti ja oleellisesti rikkoo maakaasun siirtoverkonhaltijan eriyttämisestä annetun lain säännöksiä eikä luvanhaltijalle etukäteen annettu varoitus luvan peruuttamisesta ole johtanut toiminnassa esiintyneiden puutteiden korjaamiseen*; tai*
(lisätään)	*6) jos luvanhaltija toistuvasti ja oleellisesti rikkoo kyberturvallisuuslakia, eikä luvanhaltijalle etukäteen annettu varoitus luvan peruuttamisesta ole johtanut toiminnassa esiintyneiden puutteiden korjaamiseen.*
28 §	28 §
Energiaviraston oikeus luovuttaa tietoja toiselle viranomaiselle	*Energiaviraston oikeus luovuttaa tietoja toiselle viranomaiselle*
Sen lisäksi, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetään, Energiavirastolla on oikeus luovuttaa salassapitosäännösten estämättä tietoja:	Sen lisäksi, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetään, Energiavirastolla on oikeus luovuttaa salassapitosäännösten estämättä tietoja:
1) Finanssivalvonnalle, Kilpailu- ja kuluttajavirastolle ja kuluttaja-asiamiehelle niiden tehtävien hoitamista varten *sekä Liikenne- ja viestintävirastolle, jos se on välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi;*	*1) Finanssivalvonnalle, Kilpailu- ja kuluttajavirastolle ja kuluttaja-asiamiehelle niiden tehtävien hoitamista varten;*
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —

Voimassa oleva laki	*Ehdotus*
	Tämä laki tulee voimaan päivänä kuuta 20

14

Laki

vesihuoltolain 35 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan vesihuoltolain (119/2001) 35 §:n 2 momentti, sellaisena kuin se on laissa 1013/2018, seuraavasti:

Voimassa oleva laki	*Ehdotus*
35 §	35 §
Salassapitovelvollisuus	*Salassapitovelvollisuus*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Viranomaisten toiminnan julkisuudesta annetussa laissa säädetyn salassapitovelvollisuuden estämättä saa tämän lain mukaisia tehtäviä suoritettaessa saatuja tietoja yksityisen ja yhteisön taloudellisesta asemasta, liikesalaisuudesta sekä yksityisen henkilökohtaisista oloista luovuttaa:	Viranomaisten toiminnan julkisuudesta annetussa laissa säädetyn salassapitovelvollisuuden estämättä saa tämän lain mukaisia tehtäviä suoritettaessa saatuja tietoja yksityisen ja yhteisön taloudellisesta asemasta, liikesalaisuudesta sekä yksityisen henkilökohtaisista oloista luovuttaa:
1) valvontaviranomaiselle tämän lain mukaisten tehtävien suorittamista varten;	1) valvontaviranomaiselle tämän lain mukaisten tehtävien suorittamista varten; *sekä*
2) rikoksen selvittämiseksi syyttäjä- ja poliisiviranomaiselle; *sekä*	2) rikoksen selvittämiseksi syyttäjä- tai poliisiviranomaiselle.
3) Liikenne- ja viestintävirastolle, jos se on välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi.	
	Tämä laki tulee voimaan päivänä kuuta 20

15

Laki

sakon täytäntöönpanosta annetun lain 1 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

lisätään sakon täytäntöönpanosta annetun lain (672/2002) 1 §:n 2 momenttiin, sellaisena kuin se on laeissa 1183/2023, 23/2024 ja 36/2024, uusi 31 kohta seuraavasti:

Voimassa oleva laki	*Ehdotus*
1 §	1 §
Lain soveltamisala	*Lain soveltamisala*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
Siten kuin tässä laissa säädetään, pannaan täytäntöön myös:	Siten kuin tässä laissa säädetään, pannaan täytäntöön myös:
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
(lisätään)	*31) kyberturvallisuuslain (/) 35 §:ssä tarkoitettu seuraamusmaksu.*

Tämä laki tulee voimaan päivänä kuuta 20

16

Laki

maa-asemista ja eräistä tutkista annetun lain 8 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan maa-asemista ja eräistä tutkista annetun lain (96/2023) 8 §:n 1 momentin 3 kohta seuraavasti:

Voimassa oleva laki	*Ehdotus*
8 §	8 §
Luvan muuttaminen ja peruuttaminen	*Luvan muuttaminen ja peruuttaminen*
Luvan myöntänyt viranomainen voi muuttaa maa-asema- tai tutkatoiminnan harjoittamiseen myönnettyä lupaa tai peruuttaa luvan, jos:	Luvan myöntänyt viranomainen voi muuttaa maa-asema- tai tutkatoiminnan harjoittamiseen myönnettyä lupaa tai peruuttaa luvan, jos:
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
3) toiminnanharjoittaja on olennaisella tavalla laiminlyönyt tai rikkonut tässä laissa säädettyä velvollisuutta tai rajoitusta taikka luvan ehtoja;	3) toiminnanharjoittaja on olennaisella tavalla laiminlyönyt tai rikkonut tässä laissa *tai kyberturvallisuuslaissa (/)* säädettyä velvollisuutta tai rajoitusta taikka luvan ehtoja;
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

Tämä laki tulee voimaan päivänä kuuta 20

17

Laki

vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

lisätään vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annetun lain (390/2005) 5 §:ään, sellaisena kuin se on laeissa 358/2015 ja 794/2020, uusi 10 momentti sekä lakiin uusi 109 a § seuraavasti:

Voimassa oleva laki	*Ehdotus*
5 §	5 §
Suhde muuhun lainsäädäntöön	*Suhde muuhun lainsäädäntöön*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
(lisätään)	*Kyberturvallisuuden riskienhallinta- ja raportointivelvoitteista sekä viranomaisten yhteistyöstä kyberturvallisuuspoikkeamien ja –riskien hallitsemiseksi säädetään kyberturvallisuuslaissa (/).*
	109 a §
(lisätään)	*Kyberturvallisuutta koskevien velvoitteiden laiminlyömisestä johtuva luvan peruuttaminen*
	Jos toiminnanharjoittaja olennaisesti ja vakavasti laiminlyö kyberturvallisuuslaissa säädettyjä velvollisuuksia, on valvontaviranomaisen asetettava toiminnanharjoittajalle riittävä määräaika asian korjaamiseksi. Jos toiminnanharjoittaja ei ole korjannut puutteita määräajan kuluessa, valvontaviranomainen voi peruuttaa myöntämänsä toiminnanharjoittamista koskevan luvan osittain tai kokonaan.
	Tämä pykälä koskee toimintaa, jossa turvallisuus- ja kemikaalivirasto on valvova viranomainen 115 §:n mukaisesti.
	Tämä laki tulee voimaan päivänä kuuta 20