HE 179/2025 vp

Hallituksen esitys eduskunnalle kyberkestävyysasetuksen toimeenpanoa koskevaksi lainsäädännöksi

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan säädettäväksi laki eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista sekä muutettavaksi eräiden tuotteiden markkinavalvonnasta annettua lakia, kyberturvallisuuslakia, sähköisen viestinnän palveluista annettua lakia ja sakon täytäntöönpanosta annettua lakia.

Esityksen tavoitteena on antaa eräiden tuotteiden kyberkestävyyttä koskevan Euroopan unionin asetuksen eli niin kutsutun kyberkestävyyssäädöksen tai -asetuksen soveltamista täydentävät ja täsmentävät kansalliset säännökset. Kyberkestävyysasetus asettaa tietoturvaa koskevat horisontaaliset vähimmäisvaatimukset digitaalisen elementin sisältäville tuotteille eli laitteille ja ohjelmistoille, jotka ovat kytkettävissä internetiin tai toiseen laitteeseen. Ehdotetut säännökset koskevat kyberkestävyysasetuksen markkinavalvontaa, vaatimustenmukaisuuden arviointilaitoksien ilmoittamista ja valvontaa sekä hallinnollisia seuraamuksia.

Esityksen tavoitteena on myös täydentää kansallista sääntelyä eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä koskevan EU:n niin kutsutun kyberturvallisuusasetuksen soveltamiseksi. Ehdotetut säännökset koskevat kansallisen kyberturvallisuussertifioinnin viranomaisen tehtäviä ja toimivaltuuksia sekä vaatimustenmukaisuuden arviointilaitoksia.

Esityksen tavoitteena on myös täydentää EU:n niin kutsutun kyberturvallisuusdirektiivin kansallista täytäntöönpanoa verkkotunnuksien rekisteröintitietoja ja verkkotunnusvälittäjiä koskevilta osin direktiivissä edellytetyllä vähimmäistasolla. Täydennykset koskevat verkkotunnuksiin liittyvien tietojen käsittelyä ja luovuttamista.

Liikenne- ja viestintävirastolle osoitettaisiin uusina tehtävinä kyberkestävyysasetuksen markkinavalvonta sekä vaatimustenmukaisuuden arviointilaitoksien nimeäminen ja valvonta. Korkean riskin tekoälyjärjestelmien osalta markkinavalvontaviranomaisena toimisi eräiden tekoälyjärjestelmien valvonnasta annetun lain nojalla toimivaltainen viranomainen. Kyberturvallisuussertifiointien osalta kansallisen viranomaisen tehtävässä jatkaisi Liikenne- ja viestintävirasto.

Kyberkestävyysasetuksen sujuva ja tehokas toimeenpano laitteiden ja ohjelmistojen tietoturvan parantamiseksi sisältyy Suomen kyberturvallisuusstrategian toimeenpanosuunnitelman priorisoituihin toimenpiteisiin. Suomen uusi kyberturvallisuusstrategia vuosille 2024–2035 on hyväksytty valtioneuvoston periaatepäätöksenä lokakuussa 2024. 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 pääosin 1.6.2026, EU:n kyberturvallisuusdirektiivin kansalliseen täytäntöönpanoon liittyviltä osin kuitenkin mahdollisimman pian. Eräiden säännösten osalta ehdotetaan soveltamisen porrastamista kyberkestävyysasetusta vastaavasti.

SISÄLLYS

PERUSTELUT

1 Asian tausta ja valmistelu

1.1 Tausta

Esityksen valmisteluun on johtanut Euroopan parlamentin ja neuvoston asetus (EU) 2024/2847, annettu 23 päivänä lokakuuta 2024, digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) N:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta (kyberkestävyyssäädös), jäljempänä *kyberkestävyysasetus*. Asetus on tullut voimaan 10.12.2024 ja sen soveltaminen alkaa vaiheittain vuosien 2026–2027 aikana, kuitenkin pääosin 11.12.2027. Tällä esityksellä ehdotetaan säädettäväksi asetuksen soveltamiseksi tarpeelliset kansalliset säännökset.

Kyberkestävyysasetuksen taustalla on kyberturvallisuuteen liittyvä kehitys, jossa laitteet ja ohjelmistot joutuvat enenevässä määrin kyberhyökkäysten kohteeksi. Kyberhyökkäykset aiheuttavat merkittäviä kustannuksia sekä hyökkäyksen kohteeksi joutuneelle että sivullisille esimerkiksi henkilötietojen vaarantumisena. Haasteena tuotteissa ovat matala tietoturvallisuuden taso, haavoittuvuudet ja tietoturvapäivitysten puutteet sekä käyttäjien vajaa tietämys tuotteiden turvallisuusominaisuuksista ja rajoitettu pääsy niitä koskevaan tietoon. Asetuksen tavoitteena onkin puuttua näihin haasteisiin ja varmistaa, että laitteisto- ja ohjelmistotuotteet saatetaan markkinoille nykyistä vähemmin haavoittuvuuksin, valmistajat suhtautuvat tietoturvaan vakavasti tuotteen koko elinkaaren ajan ja käyttäjät voivat ottaa kyberturvallisuutta koskevat ominaisuudet huomioon valitessaan ja käyttäessään tuotteita ja ohjelmistoja.

Euroopan unionissa tai Suomessa kansallisesti ei ole ennestään ollut horisontaalista sääntelykehystä, jossa vahvistettaisiin kyberturvallisuutta koskevia vaatimuksia kaikille digitaalisia elementtejä sisältäville tuotteille.

Esityksen valmisteluun on lisäksi johtanut viranomaistoiminnassa havaittu tarve kansalliselle täydentävälle sääntelylle Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus) annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 soveltamiseksi kansallisen kyberturvallisuussertifioinnin viranomaisen tehtävässä. Tämä tehtävä on Suomessa osoitettu Liikenne- ja viestintävirastolle sähköisen viestinnän palveluista annetussa laissa (917/2014, viestintäpalvelulaki). Kyberturvallisuuden sertifiointikehystä koskevat kyberturvallisuusasetuksen säännökset ovat tulleet sovellettavaksi pääosin kesäkuussa 2021. Kyberkestävyysasetuksen soveltamisen ennakoidaan lisäävän kyberturvallisuussertifiointiin liittyviä viranomaistehtäviä nykyisestä.

Suomen kyberturvallisuusstrategia on uudistettu pääministeri Orpon hallitusohjelman mukaisesti vastaamaan muuttunutta toimintaympäristöä. Suomen uusi kyberturvallisuusstrategia vuosille 2024–2035 hyväksyttiin valtioneuvoston periaatepäätöksenä 10.10.2024. Kyberturvallisuusstrategian hyväksymisen jälkeen on valmisteltu sen toimeenpanosuunnitelma, jossa määritellään kehittämistoimet strategian tavoitteiden saavuttamiseksi. Kyberkestävyysasetuksen sujuva ja tehokas toimeenpano laitteiden ja ohjelmistojen tietoturvan parantamiseksi sisältyy Suomen uudistetun kyberturvallisuusstrategian toimeenpanosuunnitelman priorisoituihin toimenpiteisiin.

1.2 Valmistelu

1.2.1 EU-säädöksen valmistelu

Komissio antoi 15.9.2022 ehdotuksen Euroopan parlamentin ja neuvoston asetukseksi digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetuksen (EU) 2019/1020 muuttamisesta (COM(2022) 454). Komissio teki ehdotuksesta vaikutusten arvioinnin (SWD (2022) 292 final). Komissio järjesti aloitteesta julkisen kuulemisen keväällä 2022. Ehdotuksen neuvottelut käytiin neuvoston horisontaalisessa kybertyöryhmässä keskeisiltä osin vuoden 2023 aikana.

Valtioneuvosto antoi asetusehdotuksesta eduskunnalle U-kirjelmän U 83/2022 vp. Liikenne- ja viestintävaliokunta antoi asiasta lausunnon LiVL 39/2022 vp. Suuri valiokunta yhtyi SuVEK 147/2022 vp mukaan liikenne- ja viestintävaliokunnan lausunnon mukaisesti valtioneuvoston kantaan. Asiasta ei annettu jatkokirjelmiä.

Suomi kannatti ehdotuksen tavoitetta saattaa markkinoille kyberympäristössä turvallisempia tuotteita, joiden turvallisuusominaisuuksilta vaaditaan hyvätasoisuutta sekä turvallisuusominaisuudet ja -vaatimukset ovat läpinäkyvämpiä niitä käyttäville kuluttajille ja yrityksille. Ehdotuksella nähtiin mahdollisena parantaa kaikkien yhteiskunnan toimijoiden tietoturvaa. Suomi piti verkkoon kytkettyjen laitteiden ja ohjelmistojen turvallisuuden parantamista merkittävänä kehityskohteena kyberturvallisuussektorilla.

Suomi piti kannatettavana, että vastuuta tuotteiden turvallisuudesta kyberympäristössä kohdistetaan nykyistä enemmän käyttäjältä valmistajalle riippumatta siitä, missä sisämarkkinoille asetettavat tuotteet valmistetaan. Suomi on pitänyt riskiperusteista lähestymistapaa vaatimustenmukaisuuden osoittamisessa ja markkinavalvonnassa lähtökohtaisesti kannatettavana. Suomi piti tärkeänä myös sitä, että menettelyt muodostuisivat kokonaisuutena selkeiksi suhteissa muihin säädöksiin eikä vaatimuksista aiheutuisi ylimääräistä hallinnollista taakkaa.

Kyberturvallisuusasetuksen valmistelu on kuvattu hallituksen esityksessä eduskunnalle laiksi sähköisen viestinnän palveluista annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi (HE 98/2020 vp, s. 12–13). Kyberturvallisuusasetus on ollut voimassa pääosin kesäkuusta 2019 alkaen. Kyberturvallisuusasetusta on muutettu Euroopan parlamentin ja neuvoston asetuksella (EU) 2025/37, jolla sen soveltamisalaan tuotiin tietoturvapalvelut. Muutokset eivät suoraan vaikuta asetusta täydentävän kansallisen sääntelyn tarpeeseen.

Valtioneuvosto antoi muutosasetuksen (EU) 2025/37 antamiseen johtaneesta ehdotuksesta ja komission ehdotuksesta kybersolidaarisuussäädökseksi eduskunnalle U-kirjelmän U 20/2023 vp. Perustuslakivaliokunta antoi kirjelmän johdosta lausunnon PeVL 6/2023 vp, jossa esitetyt huomiot koskevat kuitenkin lähinnä ehdotusta kybersolidaarisuussäädökseksi. Suuri valiokunta yhtyi erikoisvaliokuntien kannanottojen mukaisesti valtioneuvoston kantaan ja kiinnitti valtioneuvoston huomiota perustuslakivaliokunnan lausunnossa mainittuihin valtiosääntöoikeudellisiin seikkoihin.

Suomen kannan mukaan ehdotetun luotettujen palveluntarjoajien sertifiointikehyksen tavoitteita voitiin pitää kannatettavina siltä osin kuin sääntelyllä pyrittäisiin lisäämään luottamusta digitaalisille sisämarkkinoille, vähentämään yrityksille sertifioinnista aiheutuvia kuluja ja parantamaan kyberturvallisuuspalveluiden laatua ja turvallisuutta.

EU:n kyberturvallisuusdirektiivin (NIS 2 -direktiivi) ja sen kansallisen täytäntöönpanon valmistelu kuvataan hallituksen esityksessä eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi HE 57/2024 vp jaksossa 1.2.

1.2.2 Hallituksen esityksen valmistelu

Esitys on valmisteltu virkatyönä liikenne- ja viestintäministeriössä. Esityksen valmistelussa on tehty yhteistyötä Liikenne- ja viestintäviraston kanssa.

Valmistelun aikana on järjestetty kuulemistilaisuudet koskien markkinavalvontaa ja ilmoitettujen laitoksien valvontaa koskevien viranomaistehtävien järjestämistä sekä viranomaisten kuulemistilaisuuden tekoälyasetuksen ja kyberkestävyysasetuksen valvonnan yhteyksistä.

Liikenne- ja viestintäministeriö järjesti 6.5.2024 kuulemistilaisuuden ilmoitettujen laitoksien nimeämistä ja niiden valvontaa koskevien viranomaistehtävien järjestämisestä. Kuulemistilaisuudessa esitettiin näkemyksiä siitä, että ilmoitettujen laitoksien nimeämistä ja valvontaa koskevat viranomaistehtävät tulisi järjestää keskitetysti ja tehokkaasti. Kuulemistilaisuudessa esitettiin näkemyksiä siitä, että talouden toimijan kannalta merkityksellisempää on tehokas viranomaistoiminta kuin kysymys siitä, minkä viranomaisen yhteydessä tehtävää järjestetään.

Liikenne- ja viestintäministeriö järjesti 7.5.2024 kuulemistilaisuuden kyberkestävyysasetuksen markkinavalvontaa koskevan viranomaistehtävän järjestämisestä. Kuulemistilaisuudessa pidettiin tärkeänä, että markkinavalvontaa koskeva viranomaistehtävä järjestetään tehokkaasti. Kuulemistilaisuudessa pidettiin tärkeänä, että markkinavalvontaviranomainen on asiantunteva ja kykenee antamaan talouden toimijoille ohjausta ja neuvontaa kyberkestävyysasetuksen soveltamisesta. Kuulemistilaisuudessa pidettiin yleisesti perusteltuna markkinavalvontatehtävän keskittämistä yhdelle viranomaiselle päällekkäisyyksien välttämiseksi viranomaistehtävissä.

Liikenne- ja viestintäministeriö järjesti 11.12.2024 kuulemistilaisuuden viranomaisille tekoälyasetuksen ja kyberkestävyysasetuksen välisistä yhteyksistä sekä asetuksien edellyttämän markkinavalvonnan yhteensovittamisesta. Kuulemistilaisuudessa esitettiin näkemyksiä siitä, että tekoälyasetusta valvoville viranomaisille ei tulisi osoittaa muiden kuin tekoälyjärjestelmien markkinavalvontatehtäviä kyberkestävyysasetuksen osalta. Valmistelun aikana on laadittu arviomuistio markkinavalvonnan järjestämisen vaihtoehdoista. Arviomuistion keskeinen sisältö kuvataan jaksossa 5.1.1.

Esitys on ollut lausuntokierroksella suomeksi 17.6.–12.8.2025 ja ruotsiksi 26.6.–21.8.2025. Esitys on ollut lausuttavana Ahvenanmaan maakuntahallituksella kuusi viikkoa ajalla 1.9.–13.10.2025. Esityksestä vastaanotettiin yhteensä 33 lausuntoa. Lausuntopalautteesta on laadittu lausuntoyhteenveto. Lausuntopalautetta käsitellään keskeisiltä osin jäljempänä jaksossa 6.

Hallituksen esityksen valmisteluasiakirjat ovat saatavilla Valtioneuvoston hankeikkunasta hanketunnuksella LVM014:00/2024 (linkki: https://valtioneuvosto.fi/hanke?tunnus=LVM014%3A00/2024).

2 EU-säädöksen tavoitteet ja pääasiallinen sisältö

2.1 Kyberkestävyysasetus

2.1.1 Tavoitteet ja soveltamisala

Kyberkestävyysasetuksen yleisenä tavoitteena on luoda olosuhteet turvallisten digitaalisen elementin sisältävien tuotteiden kehittämiselle ja varmistaa, että laitteissa ja ohjelmistoissa on vähemmän haavoittuvuuksia ja valmistajat ottavat turvallisuusnäkökohdat vakavasti tuotteen elinkaaren ajan. Toisena tavoitteena on lisätä laitteiden käyttäjille näkyvyyttä tuotteiden tietoturvaominaisuuksiin. Ehdotuksen tavoitteena on luoda kehys turvallisuusvaatimuksille, edistää turvallisuusominaisuuksien läpinäkyvyyttä ja mahdollistaa tuotteiden turvallinen käyttö.

Tavoitteiden saavuttamiseksi asetuksella luodaan sääntelykehys, jolla yhdenmukaistetaan digitaalisen elementin sisältävien tuotteiden turvallisuusvaatimuksia EU:n sisämarkkinoilla.

Asetuksella säädetään digitaalisen elementin tuotteille sekä niiden valmistajille, jakelijoille ja maahantuojille asetettavista vähimmäisvaatimuksista sekä vaatimustenmukaisuuden osoittamisesta ja valvonnasta. Kyberkestävyysasetuksen soveltamisala on horisontaalinen. Asetusta sovelletaan sen 2 artiklan 1 kohdan nojalla kaikkiin markkinoilla saataville asetettuihin digitaalisia elementtejä sisältäviin tuotteisiin, joiden käyttötarkoitus tai kohtuudella ennakoitavissa oleva käyttö sisältää suoran tai välillisen loogisen tai fyysisen datayhteyden johonkin laitteeseen tai verkkoon.

Digitaalisen elementin sisältävällä tuotteella tarkoitetaan asetuksen 3 artiklan 1 kohdan mukaan ohjelmisto- tai laitteistotuotetta ja siihen sisältyviä datan etäkäsittelyratkaisuja, mukaan lukien toisistaan erillään markkinoille saatettavat ohjelmisto- ja laitteistokomponentit. Soveltamisalaan liittyviä määritelmiä datan etäkäsittelystä, ohjelmistosta, laitteistosta, komponentista, kohtuudella ennakoitavissa olevasta käytöstä ja yhteyksistä tarkennetaan asetuksen 3 artiklassa.

Asetuksen johdantokappaleen 11 mukaan datan etäkäsittelyratkaisu olisi määriteltävä etäältä tapahtuvaksi datan käsittelyksi, jota varten on suunniteltu ja kehitetty ohjelmisto kyseisen digitaalisia elementtejä sisältävän tuotteen valmistajan toimesta tai puolesta ja jota ilman digitaalisia elementtejä sisältävä tuote ei kykenisi suorittamaan jotakin toimintoaan. Tällä lähestymistavalla varmistetaan, että valmistajat suojaavat tällaiset tuotteet asianmukaisesti kokonaisuudessaan riippumatta siitä, suoritetaanko tietojen käsittely ja tallentaminen paikallisesti käyttäjän laitteella vai suorittaako valmistaja sen etäältä. Toisaalta etäältä suoritettu käsittely tai tallennus kuuluu asetuksen soveltamisalaan vain sikäli kuin se on välttämätöntä, jotta digitaalisia elementtejä sisältävä tuote voi suorittaa toimintonsa. Tällainen etäältä suoritettu käsittely tai tallennus käsittää tilanteen, jossa mobiilisovellus edellyttää pääsyä ohjelmistosovellusrajapintaan tai tietokantaan, joka tarjotaan valmistajan kehittämän palvelun avulla. Tällaisessa tapauksessa palvelu kuuluu asetuksen soveltamisalaan datan etäkäsittelyratkaisuna. Asetuksen johdantokappaleen 12 mukaan pilvipalvelut ovat asetuksessa tarkoitettuja datan etäkäsittelyratkaisuja vain, jos ne ovat asetuksessa vahvistetun määritelmän mukaisia. Esimerkiksi älykotilaitteiden valmistajien tarjoamat pilvikäyttöiset toiminnot, joiden avulla käyttäjät voivat käyttää laitetta etäältä, kuuluvat tämän asetuksen soveltamisalaan. Toisaalta verkkosivustot, jotka eivät tue digitaalisia elementtejä sisältävän tuotteen toimintoa, tai pilvipalvelut, joita ei ole suunniteltu ja kehitetty digitaalisia elementtejä sisältävän tuotteen valmistajan vastuulla, eivät kuulu asetuksen soveltamisalaan.

Asetuksen soveltamisalan rajauksista säädetään tyhjentävästi sen 2 artiklan 2–7 kohdassa. Asetusta ei sovelleta asetuksien (EU) 2017/745 ja (EU) 2017/246 mukaisiin lääkinnällisiin laitteisiin eikä (EU) 2019/2114 soveltamisalaan kuuluviin ajonenuvoihin. Lisäksi asetusta ei sovelleta sellaisiin ilma-aluksiin, jotka on sertifioitu asetuksen (EU) 2018/1139 nojalla, eikä direktiivin 2014/90/EU mukaisiin laivavarusteisiin. Lisäksi asetusta ei sovelleta yksinomaan kansallisen turvallisuuden tai maanpuolustuksen tarkoituksiin valmistettuihin tuotteisiin eikä tuotteisiin, jotka on valmistettu yksinomaan käsittelemään salassa pidettävää tietoa. Lisäksi soveltamisalan ulkopuolelle jäävät myös varaosat, joilla on tarkoitus korvata komponentteja, jotka sisältyvät digitaalisen elementin sisältävään tuotteeseen ja jotka on valmistettu samojen eritelmien mukaan kuin alkuperäiset komponentit. Komissiolla olisi soveltamisalaan liittyvää siirrettyä säädösvaltaa eräiden tuotteiden rajaamisesta soveltamisalan ulkopuolelle sekä asetuksen liitteiden III ja IV muuttamisesta, mikä kuvataan luvussa 2.1.9.

Asetuksen yleinen soveltamisala koskee markkinoilla saataville asettamista eli tuotteen tai ohjelmiston toimittamista EU:n markkinoille. Osa asetuksen velvoitteista rajautuu markkinoille saattamiseen eli siihen hetkeen, kun tuote asetetaan ensimmäistä kertaa saataville EU:n markkinoilla. Markkinoille saataville asettaminen ja markkinoille saattaminen määritellään asetuksen 3 artiklan 21 ja 22 kohdassa.

2.1.2 Tuotteen vaatimustenmukaisuus

Kyberkestävyysasetuksen 6 artiklan nojalla digitaalisia elementtejä sisältäviä tuotteita saa asettaa saataville markkinoilla ainoastaan, jos ne täyttävät liitteen I osassa I vahvistetut olennaiset kyberturvallisuusvaatimukset ja valmistajan käyttöönottamat prosessit täyttävät liitteen I osassa II vahvistetut olennaiset kyberturvallisuusvaatimukset.

Liitteen I osassa I vahvistettujen olennaisten kyberturvallisuusvaatimuksien nojalla tuotteet on suunniteltava, kehitettävä ja tuotettava siten, että sen kyberturvallisuuden taso on oikeassa suhteessa riskeihin. Tuote on muun ohella asetettava saataville markkinoilla oletusarvoisesti tietoturvallisin asetuksin sekä ilman tiedossa olevia hyödynnettävissä olevia haavoittuvuuksia.

Liitteen I osassa II vahvistettujen olennaisten kyberturvallisuusvaatimuksien täyttämiseksi valmistajien on otettava käyttöön prosesseja koskien haavoittuvuuksien käsittelyä. Valmistajilta edellytetään muun muassa tuotteeseen sisältyvien haavoittuvuuksien tunnistamista ja dokumentointia sekä haavoittuvuuksien korjaamista esimerkiksi tietoturvapäivityksiä tarjoamalla, jos se on mahdollista, sekä säännöllisiä tuotteen tietoturvaan liittyviä testauksia.

Tärkeällä tuotteella tarkoitetaan asetuksen 7 artiklan mukaisesti tuotetta, jolla on jokin asetuksen liitteessä III vahvistetun tuoteryhmän ydintoiminto. Tärkeiltä tuotteilta edellytettäisiin muita tuotteita korkeampaa vaatimustenmukaisuuden arviointimenettelyä. Kriittisellä tuotteella tarkoitetaan asetuksen 8 artiklan mukaisesti tuotetta, jolla on jokin liitteessä IV vahvistetun tuoteryhmän ydintoiminto. Kriittisille tuotteille olisi hankittava vaatimustenmukaisuuden osoittamiseksi kyberturvallisuusasetuksen mukainen vähintään korotetun varmuustason kyberturvallisuussertifikaatti edellyttäen, että kyberturvallisuusasetuksen nojalla on hyväksytty tuoteryhmän kattava soveltuva sertifiointijärjestelmä, joka on valmistajien käytettävissä. Komissiolle on siirretty lainsäädäntövaltaa koskien tärkeitä ja kriittisiä tuotteita määrittäviä III ja IV, mikä kuvataan jäljempänä jaksossa 2.1.9.

Kyberkestävyysasetuksen 11 artiklan nojalla digitaalisia elementtejä sisältäviin tuotteisiin sovellettaisiin yleisen tuoteturvallisuusasetuksen (EU) 2023/988 2 artiklan 1 kohdan kolmannen alakohdan b alakohdasta poiketen yleisen tuoteturvallisuusasetuksen III luvun 1 jaksoa

(talouden toimijoiden velvoitteet), V ja VII lukua (markkinavalvonta, komission rooli ja täytäntöönpanon valvonnan koordinointi) sekä IX–XI lukua (kansainvälinen yhteistyö, rahoitussäännökset ja loppusäännökset) niiden näkökohtien ja riskien tai riskiluokkien osalta, jotka eivät kuulu kyberkestävyysasetuksen soveltamisalaan. Edellytyksenä on lisäksi, että tuotteisiin ei sovelleta muussa unionin yhdenmukaistamislainsäädännössä säädettyjä erityisiä turvallisuusvaatimuksia.

Kyberkestävyysasetuksen 12 artiklassa on erityissäännöksiä soveltamisalaan kuuluvista suuririskisistä tekoälyjärjestelmistä. Tekoälyasetuksen 6 artiklassa tarkoitetut suuririskisten tekoälyjärjestelmien on katsottava täyttävän tekoälyasetuksen 15 artiklassa säädetyt kyberturvallisuusvaatimukset silloin, kun kyberkestävyysasetuksen mukaiset vaatimukset on täytetty ja niiden täyttyminen osoitettu kyberkestävyysasetuksen 12 artiklan mukaisesti. Kyberkestävyysasetuksen 52 artiklaan sisältyy erityissäännös suuririskisten tekoälyjärjestelmien markkinavalvonnasta, mikä kuvataan jaksossa 2.1.6.

2.1.3 Talouden toimijoita ja avoimen lähdekoodin ohjelmistovastaavia koskevat vaatimukset

2.1.3.1 Valmistajat

Valmistajien keskeisistä velvollisuuksista säädetään kyberkestävyysasetuksen 13 ja 14 artikloissa.

Valmistajan velvollisuudet (13 artikla)

Kyberkestävyysasetuksen 13 artiklan nojalla saattaessaan digitaalisen elementin sisältävää tuotetta markkinoille valmistajien on varmistettava, että se on suunniteltu, kehitetty ja tuotettu asetuksen liitteessä I olevassa I osassa vahvistettujen olennaisten kyberturvallisuusvaatimusten mukaisesti. Valmistajien on arvioitava tuotteeseen liittyvät kyberturvallisuusriskit ja huomioitava arvioinnin tulokset osana tuotteen suunnittelua, kehitystä, tuotantoa, toimitusta ja ylläpitoa. Riskien arviointi on dokumentoitava, sitä on päivitettävä tukiajan aikana tarvittaessa, ja siinä on ilmoitettava, sovelletaanko tuotteeseen asetuksen liitteessä I olevan I osan 2 kohdan mukaisia vaatimuksia ja jos sovelletaan, millä tavalla ja miten vaatimukset pannaan täytäntöön riskiarvioinnin perusteella. Arvioinnissa on lisäksi ilmoitettava, miten valmistaja soveltaa liitteessä I olevan I osan 1 kohtaa ja liitteessä I olevassa II osassa vahvistettuja haavoittuvuuksien käsittelyä koskevia vaatimuksia. Valmistajan on sisällytettävä kyberturvallisuusriskien arviointi 31 artiklan ja liitteen VII nojalla vaadittuihin teknisiin asiakirjoihin sekä perusteltava teknisissä asiakirjoissa, jos tietyt olennaiset kyberturvallisuusvaatimukset eivät sovellu tiettyyn digitaalisia elementtejä sisältävään tuotteeseen. Mikroyritykset ja pienet yritykset voivat toimittaa tekniset asiakirjat yksinkertaistetussa muodossa komission täytäntöönpanoasetuksella täsmennetyllä tavalla (33(5) artikla).

Kyberkestävyysasetuksen 13 artiklan nojalla valmistajien olisi lisäksi järjestelmällisesti dokumentoitava tuotteiden kyberturvallisuuteen liittyviä seikkoja, mukaan lukien niiden tietoon tulleita haavoittuvuuksia tai kolmansien osapuolien toimittamia tietoja. Valmistajien olisi määritettävä tuotteen tukiaika ja varmistettava, että tukiajan ajan tuotteen ja sen komponenttien haavoittuvuudet käsitellään tehokkaasti ja liitteessä I olevan II osan mukaisesti. Tukiaika olisi määritettävä tuotteen odotettavissa olevaa käyttöikää vastaavaksi, kuitenkin vähintään viideksi vuodeksi tai – käyttöiän ollessa alle viisi vuotta – käyttöaikaa vastaavaksi. Tukiajan pituuden määrittämiseen liittyisi komissiolle siirrettyä säädösvaltaa, joka kuvataan luvussa 2.1.9. Valmistajien olisi pidettävä tietoturvapäivityksiä saatavilla julkaisun jälkeen tukiajan ajan tai vähintään kymmenen vuotta sen mukaan, kumpi ajanjaksoista on pidempi. Valmistajien on

noudatettava asianmukaista huolellisuutta integroidessaan tuotteeseensa kolmansilta osapuolilta hankittuja komponentteja sekä ilmoitettava toteamastaan haavoittuvuudesta integroidussa komponentissa sen valmistajalle tai ylläpitäjälle sekä puututtava haavoittuvuuteen ja korjattava se.

Kyberkestävyysasetuksen 13 artiklan nojalla ennen tuotteen saattamista markkinoille, valmistajien olisi laadittava 31 artiklassa tarkoitetut tekniset asiakirjat ja suoritettava valintansa mukaan jokin 32 artiklassa tarkoitetuista vaatimustenmukaisuuden arviointimenettelyistä. Lisäksi valmistajien olisi laadittava EU-vaatimustenmukaisuusvakuutus 28 artiklan mukaisesti ja osoituksena vaatimustenmukaisuudesta kiinnitettävä tai liitettävä CE-merkintä tuotteeseen 30 artiklan mukaisesti. Valmistajien olisi pidettävä tekniset asiakirjat ja EU-vaatimustenmukaisuusvakuutus markkinavalvontaviranomaisten saatavilla.

Kyberkestävyysasetuksen 13 artiklan nojalla valmistajien on varmistettava, että digitaalisia elementtejä sisältävien tuotteiden mukana on asetuksen liitteen II mukaiset tiedot käyttäjälle. Valmistajan olisi nimettävä keskitetty yhteyspiste muun muassa haavoittuvuuksista ilmoittamista varten, sekä ilmoitettava nimensä ja yhteystietonsa käyttäjille ja markkinavalvontaviranomaisille.

Valmistaja voisi nimittää kirjallisella toimeksiannolla valtuutetun edustajan, jonka on suoritettava valmistajan sille osoittamat tehtävät. Valtuutetun edustajan nimittämistä koskee kyberkestävyysasetuksen 18 artikla, jossa säädetään 13 artiklan velvollisuuksista, jotka eivät saa kuulua valtuutetun edustajan toimeksiantoon.

Raportointivelvoitteet ja haavoittuvuuskoordinaatio (14–17 artikla)

Kyberkestävyysasetuksen 14 artiklassa säädetään valmistajien velvollisuudesta raportoida:

- digitaalisen elementin sisältävien tuotteiden sisältämistä aktiivisesti hyödynnetyistä haavoittuvuuksista ja vakavista poikkeamista; ja

- tuotteen tietoturvaan vaikuttavista vakavista poikkeamista, joista valmistaja on tullut tietoiseksi.

Artiklan 1–5 kohdan mukaisesti valmistajan on ilmoitettava kaikista tuotteiden sisältämistä aktiivisesti hyödynnetyistä haavoittuvuuksista ja vakavista poikkeamista samanaikaisesti sekä kansalliselle CSIRT-yksikölle että ENISAlle. Ilmoitus tehdään ENISA:n keskitetyn raportointialustan yhteyteen perustettavan kansallisen sähköisen ilmoituspalvelun kautta. Koordinaattoriksi nimetty CSIRT-yksikkö voisi tarvittaessa pyytää valmistajaa toimittamaan väliraportin aktiivisesti hyödynnetyn haavoittuvuuden tai poikkeaman tilanteesta.

Raportointia koskevan 65 johdantokappaleen mukaan valmistajien olisi ilmoitettava keskitetyn raportointialustan kautta samanaikaisesti sekä koordinaattoriksi nimetylle CSIRT-yksiköille että ENISAlle digitaalisia elementtejä sisältäviin tuotteisiin sisältyvistä aktiivisesti hyödynnetyistä haavoittuvuuksista sekä kyseisten tuotteiden tietoturvaan vaikuttavista vakavista poikkeamista.

Kyberkestävyysasetuksen 14 artiklan 8 kohdan nojalla valmistajien olisi lisäksi tiedotettava aktiivisesti hyödynnetystä haavoittuvuudesta tai tuotteen tietoturvaan vaikuttavasta vakavasta poikkeamasta digitaalisia elementtejä sisältävän tuotteen käyttäjiä, joihin vaikutukset kohdistuvat. Valmistajan olisi tarvittaessa tiedotettava kaikkia käyttäjiä kyseisestä haavoittuvuudesta tai poikkeamasta ja tarpeen mukaan mahdollisista

riskinhallintatoimenpiteistä ja korjaavista toimenpiteistä, joita käyttäjät voivat toteuttaa lieventääkseen haavoittuvuuden tai poikkeaman vaikutuksia.

Asetuksen 15 artiklassa säädetään vapaaehtoisesta ilmoitusmenettelystä. Artiklan mukaisesti valmistajat ja muut luonnolliset henkilöt ja oikeushenkilöt voivat ilmoittaa CSIRT-yksikölle tai ENISAlle mahdollisista tuotteeseen sisältyvistä haavoittuvuuksista tai kyberuhkista, jota voivat vaikuttaa tuotteen riskiprofiiliin. Vapaaehtoisen ilmoitusmenettelyn piirissä ovat myös tilanteet, joissa on kyse mahdollisista tuotteen tietoturvaan vaikuttavista poikkeamista sekä läheltä piti -tilanteista, jotka olisivat voineet johtaa poikkeamaan.

Koordinaattoriksi nimetty kansallinen CSIRT-yksikkö vastaanottaisi asetuksen 14 ja 15 tarkoitetut ilmoitukset ENISA:n perustaman keskitetyn raportointialustan välityksellä. CSIRT-yksikön olisi 16(2) artiklan nojalla välitettävä ilmoitus keskitetyn raportointialustan kautta ilman aiheetonta viivytystä koordinaattoreiksi nimetyille CSIRT-yksiköille sillä alueella, jolla valmistaja on ilmoittanut asettaneensa digitaalisia elementtejä sisältävän tuotteen saataville. Valmistajan pyynnöstä, poikkeuksellisissa olosuhteissa, ilmoituksen välittämistä voidaan lykätä kyberturvallisuuteen liittyvistä syistä ehdottoman välttämättömän ajan, myös silloin, kun haavoittuvuuteen sovelletaan NIS 2 -direktiivin 12 artiklassa tarkoitettua koordinoitua haavoittuvuuden julkistamismenettelyä. Jos CSIRT-yksikkö ei välitä ilmoitusta, sen on ilmoitettava päätöksestä ja perusteltava se ENISA:lle. Erityisen poikkeuksellisissa olosuhteissa, jotka koskevat aktiivisesti hyödynnettyä haavoittuvuutta, voitaisiin turvallisuussyistä jättää antamatta samanaikaisesti tarkkoja tietoja ENISA:lle samanaikaisesti kuin CSIRT-yksikölle. CSIRT-yksikön olisi lisäksi välitettävä markkinavalvonnan toteuttamiseksi tarvittavat tiedot asianomaiselle markkinavalvontaviranomaiselle asetuksen 16(3) artiklan mukaisesti. Asetuksen 17(2) artiklan nojalla, jos yleinen tietoisuus on tarpeen digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavan vakavan poikkeaman ehkäisemiseksi tai lieventämiseksi tai meneillään olevan poikkeaman käsittelemiseksi tai jos poikkeaman julkistaminen on muutoin yleisen edun mukaista, asiaankuuluvan jäsenvaltion koordinaattoriksi nimetty CSIRT-yksikkö voi asianomaista valmistajaa kuultuaan ja tarvittaessa yhteistyössä ENISA:n kanssa tiedottaa poikkeamasta yleisölle tai vaatia valmistajaa tekemään niin.

Sen jälkeen, kun tietoturvapäivitys tai muu korjaava tai lieventävä toimenpide on saatavilla, ENISA lisää kyseisen digitaalisia elementtejä sisältävän tuotteen valmistajan suostumuksella 14 tai 15 artiklan nojalla ilmoitetun yleisesti tiedossa olevan haavoittuvuuden ENISA:n ylläpitämään Euroopan haavoittuvuustietokantaan kyberkestävyysasetuksen 17 artiklan 5 kohdan mukaisesti. Lisäksi ENISA voi toimittaa ilmoitettuja tietoja Euroopan kyberkriisien yhteysorganisaatioiden verkostolle (EU-CyCLONe), jos nämä tiedot ovat operatiivisella tasolla merkityksellisiä laajamittaisten kyberturvapoikkeamien ja -kriisien koordinoidun hallinnan kannalta (17(1) artikla). ENISA laatisi myös saamiensa ilmoitusten perusteella 24 kuukauden välein teknisen raportin digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuusriskien uusista suuntauksista ja toimittaa sen NIS-yhteistyöryhmälle.

2.1.3.2 Maahantuojat, jakelijat, valtuutetut edustajat ja muut talouden toimijat

Digitaalisia elementtejä sisältäviin tuotteisiin liittyviä vaatimuksia kohdistuu valmistajien lisäksi maahantuojiin, jakelijoihin ja valmistajan valtuuttamiin edustajiin kyberkestävyysasetuksen 18–22 artiklan nojalla. Maahantuojien ja jakelijoiden vastuulla on lähtökohtaisesti varmistaa, että tuotteessa on asianmukaiset merkinnät ja dokumentaatio, kun se saatetaan markkinoille. Lisäksi vaatimuksia asetetaan valtuutetuille edustajille silloin kun valmistaja on osoittanut sille valmistajan vastuulle kuuluvia tehtäviä (18 artikla). Valmistajien velvollisuuksia voitaisiin soveltaa 21–22 artiklan nojalla maahantuojiin, jakelijoihin tai muihin

toimijoihin silloin, kun ne tekevät tuotteeseen merkittävän muutoksen ja saattavat sen markkinoille tai asettavat sen saataville markkinoilla.

Tuotteiden maahantuojiin sovellettavat vaatimukset

Asetuksen 19 artiklassa säädetään maahantuojien velvollisuuksista, kun ne saattavat markkinoille digitaalisia elementtejä sisältäviä tuotteita. Ennen tuotteen saattamista markkinoille maahantuojan tulee tarkistaa, että valmistaja on suorittanut asianmukaiset vaatimustenmukaisuuden arviointimenettelyt, laatinut tekniset asiakirjat, tuotteeseen on liitetty CE-merkintä, tuotteen mukana on EU-vaatimustenmukaisuusvakuutuksesta sekä tuotteessa on sarjanumero tai yksilöintitieto, valmistajan tiedot ja tukiajan päättymisaikaa koskeva tieto. Jos maahantuoja on tietoinen tai sillä on syytä epäillä, että digitaalisen elementin sisältävä tuote tai valmistajan käyttöönottamat prosessit eivät täytä asetuksen vaatimuksia, sen on välittömästi toteutettava tarvittavat korjaavat toimenpiteet tuotteen saattamiseksi asetuksen mukaiseksi tai tarvittaessa poistettava tuote markkinoilta. Maahantuojan olisi liitettävä tuotteeseen yhteystietonsa sekä ilmoitettava valmistajalle ja markkinavalvontaviranomaisille, jos tuote aiheuttaa merkittävän kyberturvallisuusriskin.

Jakelijoihin sovellettavat vaatimukset

Asetuksen 20 artiklassa säädetään jakelijoiden velvollisuuksista, kun ne asettavat digitaalisia elementtejä sisältäviä tuotteita saataville markkinoilla. Ennen tuotteen asettamista saataville markkinoilla, jakelijoiden on varmistettava, että tuotteessa on CE-merkintä, valmistaja ja maahantuoja liittäneet tuotteeseen vaadittavat tiedot ja toimittaneet tarvittavat asiakirjat jakelijalle. Jos jakelija katsoo tai sillä on hallussaan olevien tietojen perusteella syytä uskoa, että tuote tai valmistajan prosessit eivät täytä liitteessä I vahvistettuja olennaisia vaatimuksia, jakelija ei saa asettaa tuotetta saataville markkinoilla ennen kuin tuote tai valmistajan prosessit on saatettu asetuksen mukaisiksi. Lisäksi jakelijan on ilmoitettava merkittävän kyberturvallisuusriskin sisältävästä tuotteesta ilman aiheetonta viivytystä valmistajalle ja markkinavalvontaviranomaiselle. Jos tuote on jo asetettu saataville markkinoilla, jakelijan on varmistettava, että kaikki tarvittavat korjaustoimenpiteet suoritetaan tai vaatimustenvastainen tuote tarvittaessa poistetaan markkinoilta. Jakelijan olisi lisäksi ilmoitettava valmistajalle ilman aiheetonta viivytystä tietoonsa tullut digitaalisia elementtejä sisältävän tuotteen haavoittuvuus.

Valmistajien velvoitteiden soveltaminen maahantuojiin, jakelijoihin ja muihin toimijoihin

Asetuksen 21 artiklan nojalla jakelijaa tai maahantuojaa pidetään kyberkestävyysasetusta sovellettaessa valmistajana silloin, jos maahantuoja tai jakelija saattaa digitaalisia elementtejä sisältävän tuotteen markkinoille omalla nimellään tai tavaramerkillään tai tekee merkittävän muutoksen markkinoille jo saatettuun digitaalisia elementtejä sisältävään tuotteeseen. Maahantuojaan tai jakelijaan sovelletaan tällöin 13 ja 14 artiklan mukaisia valmistajan velvollisuuksia.

Jos muu luonnollinen henkilö tai oikeushenkilö kuin valmistaja, maahantuoja tai jakelija tekee merkittäviä muutoksia tuotteeseen ja asettaa sen saataville markkinoilla, pidetään kyseistä toimijaa asetuksen 22 artiklan nojalla valmistajana. Tällaiseen muuhun henkilöön sovelletaan tällöin 13 ja 14 artiklan mukaisia valmistajan velvollisuuksia tuotteen sen osan osalta, johon merkittävä muutos vaikuttaa. Jos muutos vaikuttaa tuotteen kyberturvallisuuteen kokonaisuudessaan, velvoitteita sovelletaan koko tuotteen osalta.

Valtuutetut edustajat

Asetuksen 18 artiklan mukaisesti valmistaja voi kirjallisella toimeksiannolla nimittää valtuutetun edustajan. Valtuutetun edustajan on suoritettava valmistajalta saadussa toimeksiannossa eritellyt tehtävät sekä pyynnöstä toimitettava markkinavalvontaviranomaisille jäljennös toimeksiannosta. Artiklan 2 kohdassa säädetään valmistajan velvollisuuksista, jotka eivät saa kuulua valtuutetun edustajan toimeksiantoon. Artiklan 3 kohdassa säädetään tehtävistä, jotka valtuutetun edustajan on toimeksiannon perusteella vähintään voitava suorittaa.

2.1.3.3 Avoimen lähdekoodin ohjelmistovastaavat

Asetuksen 24 artiklassa säädetään avoimen lähdekoodin ohjelmistovastaavien velvollisuuksista. Avoimen lähdekoodin ohjelmistovastaavalla tarkoitetaan asetuksen 3 artiklan 14 kohdan mukaisesti muuta oikeushenkilöä kuin valmistajaa, jonka tarkoituksena tai tavoitteena on järjestelmällisesti ja pitkäjänteisesti tarjota tukea sellaisten tiettyjen digitaalisia elementtejä sisältävien tuotteiden kehittämistä varten, jotka luokitellaan vapaiksi ja avoimen lähdekoodin ohjelmistoiksi ja jotka on tarkoitettu kaupalliseen toimintaan, ja joka varmistaa kyseisten tuotteiden toimintakelpoisuuden.

Avoimen lähdekoodin ohjelmistovastaaviin sovellettaisiin asetuksen johdanto-osan 19 kohdassa todetulla tavoin kevennettyjä vaatimuksia, eikä niihin sovelleta samoja velvoitteita kuin valmistajina toimiviin. Asetuksen 24 artiklan nojalla avoimen lähdekoodin ohjelmistovastaavien on otettava käyttöön ja dokumentoitava kyberturvallisuusperiaatteet, joilla edistetään turvallisen digitaalisia elementtejä sisältävän tuotteen kehittämistä ja haavoittuvuuksien tehokasta käsittelyä. Avoimen lähdekoodin ohjelmistovastaavan olisi tehtävä yhteistyötä markkinavalvontaviranomaisten kanssa sekä pyynnöstä annettava sille dokumentoidut kyberturvallisuusperiaatteensa.

Avoimen lähdekoodin ohjelmistovastaaviin sovellettaisiin velvoitteita digitaalisen elementin sisältävään tuotteeseen sisältyvistä aktiivisista haavoittuvuuksista raportoinnista siltä osin kuin ne osallistuvat digitaalisia elementtejä sisältävien tuotteiden kehittämiseen. Lisäksi sovellettaisiin velvoitteita tuotteen tietoturvaan vaikuttavista vakavista poikkeamista raportoinnista ja käyttäjien tiedottamisesta siltä osin kuin digitaalisia elementtejä sisältävien tuotteiden tietoturvaan vaikuttavat vakavat poikkeamat vaikuttavat verkko- ja tietojärjestelmiin, jotka avoimen lähdekoodin ohjelmistovastaavat antavat käyttöön tällaisten tuotteiden kehittämistä varten

Komissio voisi perustaa vapaaehtoisia tietoturvatodistusohjelmia vapaiksi ja avoimen lähdekoodin ohjelmistoiksi luokiteltavien digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuusominaisuuksien arvioimiseksi. Tähän liittyvä komissiolle delegoitu säädösvalta kuvataan jäljempänä luvussa 2.1.9.

2.1.4 Vaatimustenmukaisuuden osoittaminen

Vaatimustenmukaisuus

Kyberkestävyysasetuksen 27 artiklassa säädetään vaatimustenmukaisuusolettamasta. Artiklan 1 kohdan nojalla liitteessä I vahvistettujen olennaisten kyberturvallisuusvaatimusten mukaisina on pidettävä sellaisia digitaalisia elementtejä sisältäviä tuotteita ja valmistajan käyttöön ottamia prosesseja, jotka ovat yhdenmukaistettujen standardien tai niiden osien mukaisia, joiden viitetiedot on julkaistu Euroopan unionin virallisessa lehdessä, sen osalta, mitä kyseinen standardi tai sen osa kattaa.

Lisäksi 27 artiklan 8 kohdan nojalla liitteessä I vahvistettujen olennaisten kyberturvallisuusvaatimusten mukaisina on pidettävä myös sellaisia digitaalisia elementtejä sisältäviä tuotteita ja valmistajan käyttöön ottamia prosesseja, joille on annettu eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukainen EU-vaatimustenmukaisuusilmoitus tai kyberturvallisuussertifikaatti, jos vaatimustenmukaisuusilmoitus tai sertifikaatti kattaa kyseiset vaatimukset.

Komissiolla olisi 27 artiklan nojalla siirrettyä säädösvaltaa koskien teknisiä vaatimuksia koskevien yhteisten eritelmien hyväksymistä silloin kun standardia ei ole julkaistu sekä yhteensopivien eurooppalaisten kyberturvallisuussertifiointijärjestelmien yksilöimisestä. Siirretty säädösvalta kuvataan jäljempänä luvussa 2.1.9.

EU-vaatimustenmukaisuusvakuutus, CE-merkintä ja tekniset asiakirjat

Valmistajan on laadittava asetuksen 13(12) ja 28 artiklan mukaisesti EU-vaatimustenmukaisuusvakuutus, jossa todetaan, että liitteessä I vahvistettujen olennaisten kyberturvallisuusvaatimusten täyttyminen on osoitettu. Laatimalla EU-vaatimustenmukaisuusvakuutuksen valmistaja ottaa vastuun digitaalisia elementtejä sisältävän tuotteen vaatimustenmukaisuudesta asetuksen 28(4) artiklan nojalla. EU-vaatimustenmukaisuusvakuutuksen tulee olla asetuksen 28 artiklan nojalla liitteessä V vahvistetun rakenteen mukainen ja sen tulee sisältää liitteessä VIII vahvistetuissa arviointimenettelyissä eritellyt tekijät. EU-vaatimustenmukaisuusvakuutus tulee asettaa kansallisten viranomaisten saataville niiden jäsenvaltioiden vaatimilla kielillä, joissa tuote saatetaan markkinoille tai asetetaan saataville markkinoilla. Jos digitaalisia elementtejä sisältävään tuotteeseen sovelletaan useampia unionin säädöksiä, joissa edellytetään EU-vaatimustenmukaisuusvakuutusta, kaikkien tällaisten unionin säädösten osalta laaditaan yksi ainoa EU-vaatimustenmukaisuusvakuutus. Komissiolla olisi 28(5) artiklan nojalla siirrettyä säädösvaltaa liittyen EU-vaatimustenmukaisuusvakuutuksen vähimmäissisältöön.

CE-merkintää koskevat säännökset sisältyvät kyberkestävyysasetuksen 29 ja 30 artikloihin. CE-merkintä olisi kiinnitettävä digitaalisia elementtejä sisältävään tuotteeseen kyberkestävyysasetuksen 30 artiklan mukaisesti.

Digitaalisen elementin sisältävään tuotteeseen liitettävistä teknisistä asiakirjoista säädetään asetuksen 31 artiklassa. Tekniset asiakirjat on laadittava ennen tuotteen saattamista markkinoille ja niitä on tarvittaessa päivitettävä vähintään tuotteen tukiajan ajan. Teknisten asiakirjojen on sisällettävä vähintään asetuksen liitteessä VII vahvistetut osat sekä kaikki asiaankuuluvat tiedot tai yksityiskohtaiset kuvaukset keinoista, joilla valmistaja on varmistanut, että tuote ja valmistajan käyttöön ottamat prosessit täyttävät liitteessä I vahvistetut olennaiset kyberturvallisuusvaatimukset. Komissiolla olisi siirrettyä säädösvaltaa täydentää teknisiin asiakirjoihin sisällytettäviä osia.

Vaatimustenmukaisuuden arviointi

Vaatimustenmukaisuuden arviointimenettelystä digitaalisen elementin sisältävälle tuotteelle säädetään asetuksen 32 artiklassa. Vaatimustenmukaisuus osoitetaan jollakin liitteessä VIII esitetyistä vaatimusmukaisuuden arviointimenettelyistä, jotka perustuvat Euroopan parlamentin ja neuvoston päätöksessä N:o 768/2008/EY vahvistettuihin moduuleihin. Arviointimenettelyt on jaettu liitteessä neljään moduuliin (A, B, C ja H) sen perusteella, minkä riskitason tuotteen arviointiin kyseinen menettely soveltuu. Artiklan 1 kohdan nojalla valmistajan on osoitettava kyberturvallisuusvaatimusten täyttyminen jollakin seuraavista menettelyistä:

- liitteessä VIII esitetty sisäiseen valvontaan perustuva menettely (perustuen moduuliin A)

- liitteessä VIII esitetty EU-tyyppitarkastusmenettely (perustuen moduuliin B), jota seuraa liitteessä VIII esitetty sisäiseen tuotannonvalvontaan perustuva EU-tyypinmukaisuus (perustuen moduuliin C);

- liitteessä VIII esitetty täydelliseen laadunvarmistukseen perustuva vaatimustenmukaisuusarviointi (perustuen moduuliin H); tai

- jos saatavilla ja sovellettavissa, 27 artiklan 9 kohdan mukainen eurooppalainen kyberturvallisuuden sertifiointijärjestelmä.

Muiden kuin liitteen III tärkeiden tuotteiden ja liitteen IV kriittisten tuotteiden osalta vaatimuksenmukaisuus voidaan siten osoittaa muun ohella valmistajan itsearvioinnin perusteella.

Liitteen III mukaisten tärkeiden tuotteiden vaatimustenmukaisuuden osoittamista koskevat artiklan kohdat 2 ja 3. Soveltuva menettely määräytyy sen perusteella, kuuluko tuote liitteessä III luokkaan I vai II. Luokkaan I kuuluvilta tärkeiltä tuotteilta edellytetään 32(2) artiklan nojalla joko yhdenmukaistetun standardin soveltamista tai sertifiointia taikka kolmannen osapuolen arviointiin nojaavaa EU-tyyppitarkastusmenettelyä tai täydellistä laadunvarmistusta. Luokkaan II kuuluvilta tärkeiltä tuotteilta edellytetään 32(3) artiklan nojalla aina kolmannen osapuolen tekemää arviointia, vaikka tuote olisi yhdenmukaistettujen standardien tai eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukainen.

Liitteen IV mukaisten kriittisten tuotteiden osalta on 32(4) artiklan nojalla hankittava EU:n kyberturvallisuusasetuksen mukainen, vähintään korotetun varmuustason sertifikaatti. Jos sellaista ei ole käytettävissä, tuote on arvioitava jollakin vastaavalla kolmannen osapuolen arviointiin nojaavista arviointimenettelyistä, mitä liitteen III tuotteiden luokassa II sovelletaan.

Komissiolla olisi 7 ja 8 artikloiden nojalla siirrettyä säädösvaltaa liitteen III ja IV tuotteiden ryhmistä siten kuin jäljempänä luvussa 2.1.9 kuvataan.

Vapaiksi ja avoimen lähdekoodin ohjelmistoiksi luokiteltavien digitaalisia elementtejä sisältävien tuotteiden osalta valmistajan on voitava osoittaa, silloin kun tällainen tuote kuuluu liitteessä III vahvistettuihin ryhmiin, että tuotteet täyttävät liitteessä I vahvistetut olennaiset kyberturvallisuusvaatimukset, käyttäen jotakin 35(1) artiklassa tarkoitetuista menettelyistä edellyttäen, että 31 artiklassa tarkoitetut tekniset asiakirjat ovat yleisesti saatavilla näiden tuotteiden markkinoille saattamisen ajankohtana.

Asetuksen 33 artikla koskee jäsenvaltioiden tukitoimia erityisesti mikroyrityksille ja pienille yrityksille. Artiklan 1 kohdan nojalla jäsenvaltioiden on tarvittaessa toteutettava mikroyritysten ja pienten yritysten tarpeisiin räätälöityjä tukitoimia, kuten tiedotusta, koulutusta, viestintää ja testauksen tukemista. Lisäksi 2 kohdan nojalla jäsenvaltiot voivat tarvittaessa perustaa kyberkestävyyden sääntelyn testiympäristöjä. Asetuksen johdantokappaleen 97 mukaan sääntelyn testiympäristöjä koskevan kohdan tavoitteena olisi oltava yritysten innovoinnin ja kilpailukyvyn edistäminen perustamalla valvottuja testiympäristöjä ennen digitaalisia elementtejä sisältävien tuotteiden markkinoille saattamista. Sääntelyn testiympäristöjen olisi osaltaan parannettava oikeusvarmuutta kaikkien asetuksen soveltamisalaan kuuluvien toimijoiden kannalta ja helpotettava ja nopeutettava digitaalisia elementtejä sisältävien

tuotteiden pääsyä unionin markkinoille erityisesti silloin, kun niitä tarjoavat mikroyritykset ja pienet yritykset, mukaan lukien startup-yritykset.

2.1.5 Ilmoitetut laitokset

Kyberkestävyysasetuksen IV luvussa (35–51 artikloissa) säädetään vaatimustenmukaisuuden arviointilaitosten hyväksymisestä ja ilmoittamisesta ilmoitetuiksi laitoksiksi, jotka suorittavat kolmannen osapuolen vaatimustenmukaisuuden arviointia digitaalisia elementtejä sisältäville tuotteille. Luvussa säädetään myös muun muassa ilmoittamisesta vastaavan viranomaisen nimeämisestä ja tehtävistä, ilmoitusmenettelystä sekä ilmoitettujen laitosten pätevyydestä ja velvollisuuksista.

Asetuksen 35 artiklan nojalla jäsenvaltioiden on ilmoitettava komissiolle ja muille jäsenvaltioille laitokset, joille on annettu lupa suorittaa asetuksessa säädettyjä vaatimustenmukaisuuden arviointeja. Lisäksi jäsenvaltioiden on pyrittävä varmistamaan 11.6.2026 mennessä, että unionissa on riittävä määrä ilmoitettuja laitoksia vaatimustenmukaisuuden arviointien suorittamiseksi markkinoille pääsyn esteiden välttämiseksi.

Jäsenvaltioiden on 36 artiklan nojalla nimettävä ilmoittamisesta vastaava viranomainen, jonka vastuulla on laatia ja toteuttaa tarvittavat menettelyt, jotka liittyvä vaatimustenmukaisuuden arviointilaitosten arviointiin, nimeämiseen ja ilmoittamiseen, sekä niiden valvontaan. Lisäksi jäsenvaltiot voivat päättää kansallisen akkreditointielimen käyttämisestä ilmoitettujen laitosten arvioinnin ja valvonnan suorittamisessa. Ilmoittamisesta vastaavan viranomaisen on täytettävä 37 artiklan mukaiset vaatimukset. Jäsenvaltioiden on tiedotettava komissiolle 38 mukaisista menettelyistä liittyen vaatimustenmukaisuuden arviointilaitosten arviointiin, ilmoittamiseen ja valvontaan.

Ilmoitettuja laitoksia koskevista vaatimuksista säädetään kyberkestävyysasetuksen 39 artiklassa. Jotta vaatimustenmukaisuuden arviointilaitos voidaan ilmoittaa, sen on täytettävä 39 artiklan 2–12 kohdassa säädetyt vaatimukset. Vaatimustenmukaisuuden arviointilaitoksen on muun ohella kyettävä suorittamaan kaikki liitteen VII mukaiset vaatimustenmukaisuuden arviointimenettelyt niiden tuotteiden tai tuoteryhmien osalta, joita varten se on ilmoitettu. Milloin vaatimustenmukaisuuden arviointilaitos voi osoittaa olevansa sellaisissa olennaisissa yhdenmukaistetuissa standardeissa tai niiden osissa vahvistettujen edellytysten mukainen, joiden viitetiedot on julkaistu Euroopan unionin virallisessa lehdessä, sen oletetaan täyttävän 39 artiklassa säädetyt vaatimukset siltä osin kuin sovellettavat yhdenmukaistetut standardit kattavat nämä vaatimukset, kyberkestävyysasetuksen 40 artiklan nojalla. Kyberkestävyysasetuksen 41 artiklassa säädetään ehdoista ilmoitetun laitoksen tehtävien teettämiseksi alihankintana tai tytäryhtiönä. Muun ohella alihankkijan tai tytäryhtiön on myös täytettävä 39 artiklassa säädetyt vaatimukset. Lisäksi ilmoitetun laitoksen on otettava vastuu alihankkijan tai tytäryhtiön työstä, ilmoitettava teettämisestä ilmoittamisesta vastaavalle viranomaiselle ja sovittava siitä valmistajan kanssa.

Vaatimustenmukaisuuden arviointilaitoksen ilmoittamista koskevasta hakemuksesta säädetään kyberkestävyysasetuksen 42 artiklassa ja ilmoitusmenettelystä 43 artiklassa. Hakemus vaatimustenmukaisuuden arviointilaitoksen ilmoittamisesta toimitetaan ilmoittamisesta vastaavalle viranomaiselle siinä jäsenvaltiossa, johon vaatimustenmukaisuuden arviointilaitos on sijoittunut. Ilmoitetun laitoksen tehtäviä voi suorittaa 43(5) artiklan nojalla ainoastaan, jos komissio ja muut jäsenvaltiot eivät esitä vastalauseita kahden viikon kuluessa ilmoittamisesta siinä tapauksessa, että käytetään akkreditointitodistusta, tai kahden kuukauden kuluessa ilmoittamisesta siinä tapauksessa, että akkreditointia ei käytetä.

Milloin ilmoittamisesta vastaava viranomainen toteaa tai saa tietää, että ilmoitettu laitos ei täytä 39 artiklassa säädettyjä vaatimuksia tai noudata velvollisuuksiaan, ilmoittamisesta vastaavan viranomaisen on 45 artiklan nojalla rajoitettava ilmoitusta taikka peruutettava se toistaiseksi tai kokonaan sen mukaan, miten vakavaa vaatimusten täyttämättä jättäminen tai velvollisuuksien noudattamatta jättäminen on ollut. Lisäksi rajauksesta tai peruutuksesta on välittömästi ilmoitettava komissiolle ja muille jäsenvaltioille. Kyberkestävyysasetuksen 46 artiklassa säädetään ilmoitettujen laitosten pätevyyden riitauttamisesta komissiossa. Jos komissio toteaa, että ilmoitettu laitos ei ole täyttänyt tai ei enää täytä sen ilmoittamiselle asetettuja vaatimuksia, se ilmoittaa asiasta ilmoituksen tehneelle jäsenvaltiolle ja pyytää sitä toteuttamaan tarvittavat korjaavat toimenpiteet, mukaan lukien ilmoituksen peruuttaminen tarvittaessa.

Ilmoitettujen laitoksien velvollisuuksista säädetään kyberkestävyysasetuksen 47 artiklassa. Ilmoitettujen laitosten on suoritettava vaatimustenmukaisuuden arvioinnit 32 artiklassa ja liitteessä VIII säädettyjen vaatimustenmukaisuuden arviointimenettelyjen mukaisesti. Ilmoitettujen laitosten tiedotusvelvollisuudesta ilmoittavalle viranomaiselle ja muille ilmoitetuille laitoksille säädetään kyberkestävyysasetuksen 49 artiklassa.

Jäsenvaltion on varmistettava, että ilmoitettujen laitoksien päätöksiin on käytettävissä muutoksenhakumenettely kyberkestävyysasetuksen 48 artiklan nojalla. Lisäksi jäsenvaltion on varmistettava, että sen ilmoittamat laitokset osallistuvat yhteistyöhön, jota komissio koordinoi 51 artiklan mukaisesti.

2.1.6 Markkinavalvonta ja täytäntöönpano

Markkinavalvontaviranomainen

Kyberkestävyysasetuksen soveltamisalaan kuuluvien tuotteiden markkinavalvonnasta säädetään asetuksen V luvussa (artiklat 52–60). Asetuksen 52 artiklan mukaan tuotteiden markkinavalvontaan sovelletaan asetuksen soveltamisalaan kuuluvien tuotteiden osalta lisäksi asetusta (EU) 2019/1020 (ns. *markkinavalvonta-asetus*).

Asetuksen 52 artiklan 2 kohta edellyttää, että jäsenvaltiot nimeävät yhden tai useamman markkinavalvontaviranomaisen asetuksen tehokkaan täytäntöönpanon varmistamiseksi. Markkinavalvontatehtävän osoittaminen yhdelle tai useammalle viranomaiselle jää siten kansallisen liikkumavaran alaan. Markkinavalvonnan ohella markkinavalvontaviranomaiset vastaavat myös avoimen lähdekoodin ohjelmistovastaaville 24 artiklassa säädettyjen velvollisuuksien valvonnasta.

Asetuksen 52 artiklan 8 kohdan nojalla jäsenvaltioiden on varmistettava, että nimetyille markkinavalvontaviranomaisille annetaan riittävät taloudelliset ja tekniset resurssit, mukaan lukien tarvittaessa käsittelyn automatisointivälineet, sekä henkilöstöresurssit, joilla on riittävät kyberturvallisuustaidot, jotta markkinavalvontaviranomaiset voivat hoitaa tämän asetuksen mukaiset tehtävänsä.

Asetuksen 52 artiklan 14 kohtaan sisältyy erityissäännös suuririskisten tekoälyjärjestelmien markkinavalvonnasta. Kohdan nojalla silloin kun on kyse kyberkestävyysasetuksen soveltamisalaan kuuluvista digitaalisia elementtejä sisältävistä tuotteista, jotka luokitellaan suuririskisiksi tekoälyjärjestelmiksi EU:n tekoälyasetuksen 6 artiklan nojalla, tekoälyasetusta varten nimetyt markkinavalvontaviranomaiset vastaavat myös kyberkestävyysasetuksen nojalla vaadituista markkinavalvontatoimista. Markkinavalvonnan järjestämiseen ei tältä osin liity kansallista liikkumavaraa. Tekoälyasetuksen nojalla nimettyjen markkinavalvontaviranomaisten on tarvittaessa tehtävä yhteistyötä kyberkestävyysasetuksen

nojalla nimettyjen markkinavalvontaviranomaisten kanssa sekä kyberkestävyysasetuksen mukaisten raportointivelvoitteiden noudattamisen valvonnan osalta koordinaattoreiksi nimettyjen CSIRT-yksiköiden ja ENISA:n kanssa.

Asetuksen 52 artiklassa säädetään myös markkinavalvontaviranomaisten yhteistyöstä ja tietojenvaihdosta, markkinavalvontaviranomaisen velvollisuudesta tiedottaa kuluttajia asianmukaisesta valituskanavasta, markkinavalvontaviranomaisen raportointivelvollisuudesta, CSIRT-yksiköiden ja ENISA:n neuvonta- ja arviointiavusta sekä markkinavalvontaviranomaisen mahdollisuudesta antaa talouden toimijoille ohjeita ja neuvontaa asetuksen täytäntöönpanoon liittyen. Markkinavalvontaviranomaisten on tehtävä tarvittaessa yhteistyötä muun ohella kyberturvallisuusasetuksen mukaisten kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten kanssa, CSIRT-yksikön ja ENISA:n kanssa, muiden markkinavalvontaviranomaisten kanssa, tietosuojasääntelyä valvovien viranomaisten kanssa sekä asiaankuuluvien sidosryhmien kanssa (52 artiklan 4–12 kohdat). Lisäksi artiklassa säädetään markkinavalvontaviranomaisten edustajista koostuvan hallinnollisen yhteistyöryhmän perustamisesta. Lisäksi 52 artiklan 16 kohtaan sisältyy erityissäännös koskien markkinavalvontaviranomaisen velvollisuutta seurata tukiajan määrittämistä.

Asetuksen 53 artiklassa säädetään velvollisuudesta antaa markkinavalvontaviranomaiselle pääsy sen helposti ymmärtämällä kielellä dokumentaatioon tai tietoihin, joita tarvitaan tuotteiden ja valmistajien käyttöönottamien prosessien vaatimustenmukaisuuden arvioimiseksi, jos se on tarpeen sen arvioimiseksi, täyttävätkö digitaalisia elementtejä sisältävät tuotteet ja valmistajien käyttöönottamat prosessit kyberkestävyysasetuksen vaatimukset.

Kansallisen tason menettely

Asetuksen 54 artiklassa säädetään kansallisen tason menettelystä merkittävän kyberturvallisuusriskin aiheuttavien tuotteiden osalta. Artikla asettaa markkinavalvontaviranomaiselle arviointivelvoitteen tilanteissa, joissa sillä on riittävä peruste katsoa, että asetuksen soveltamisalaan kuuluva tuote aiheuttaa merkittävän kyberturvallisuusriskin. Arviointi on tehtävä ilman aiheetonta viivytystä ja tarvittaessa yhteistyössä CSIRT-yksikön kanssa. Jos markkinavalvontaviranomainen toteaa tuotteen vaatimustenvastaiseksi, sen on vaadittava talouden toimijaa toteuttamaan tarvittavat toimenpiteet tuotteen saattamiseksi vaatimustenmukaiseksi tai sen poistamiseksi markkinoilta taikka sitä koskevan palautusmenettelyn järjestämiseksi. Markkinavalvontaviranomaisella on velvollisuus ilmoittaa arvioinnin tuloksista ja toimenpiteistä asianomaiselle ilmoitetulle laitokselle. Jos vaatimustenvastaisuus ei rajoitu asianomaisen jäsenvaltion alueelle, ilmoitus on tehtävä myös komissiolle ja muille jäsenvaltioille. Artiklassa säädetään lisäksi markkinavalvontaviranomaisen velvollisuudesta ryhtyä väliaikaisiin toimenpiteisiin, mikäli talouden toimija ei toteuta vaadittuja toimenpiteitä. Markkinavalvontaviranomaisen on ilmoitettava väliaikaisista toimenpiteistä komissiolle ja muille jäsenvaltioille.

Markkinavalvontaviranomaisen olisi tuotteen kyberturvallisuusriskin merkittävyyttä arvioidessa otettava huomioon myös muut kuin tekniset riskitekijät erityisesti, jos niitä on vahvistettu NIS 2 -direktiivin 22 artiklan mukaisesti tehtyjen kriittisiä toimitusketjuja koskevien unionin tason koordinoitujen turvallisuusriskinarviointien tuloksena. Jos markkinavalvontaviranomaisella on riittävä peruste katsoa, että digitaalisia elementtejä sisältävä tuote aiheuttaa merkittävän kyberturvallisuusriskin muiden kuin teknisten riskitekijöiden vuoksi, sen on ilmoitettava tästä NIS 2 -direktiivin nojalla toimivaltaisille viranomaisille.

Unionin suojamenettely

Asetuksen 55 artiklassa säädetään unionin suojamenettelystä. Unionin suojamenettelyä sovelletaan tilanteisiin, joissa jonkin jäsenvaltion markkinavalvontaviranomaisen toteuttamaa väliaikaista toimenpidettä vastaan on esitetty vastalauseita tai komissio katsoo, että väliaikainen toimenpide on unionin oikeuden vastainen. Jos komissio katsoo markkinavalvontaviranomaisen toimenpiteen oikeutetuksi, kaikkien jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että vaatimustenvastainen tuote poistetaan niiden markkinoilta.

Unionin tason menettely merkittävän kyberturvallisuusriskin aiheuttavien tuotteiden osalta

Asetuksen 56 artiklassa säädetään unionin tason menettelystä merkittävän kyberturvallisuusriskin aiheuttavien tuotteiden osalta. Jos komissiolla on riittävä peruste katsoa, että merkittävän kyberuhkan sisältävä tuote ei täytä asetuksen vaatimuksia, sen on tehtävä asiasta ilmoitus asianomaisille markkinavalvontaviranomaisille. Markkinavalvontaviranomaisen arviointiin, joka toteutetaan komission ilmoituksen perusteella, sovelletaan 54 ja 55 artiklassa säädettyjä menettelyjä. Välittömiä toimia vaativissa tilanteissa komissio voi suorittaa vaatimustenmukaisuuden arvioinnin sekä päättää unionin tasoisista korjaavista tai rajoittavista toimenpiteistä.

Markkinavalvontaviranomaisten lisäksi komissio ilmoittaa muiden kuin teknisten riskitekijöiden vuoksi merkittävän kyberturvallisuusriskin aiheuttavasta tuotteesta tarvittaessa NIS 2 -direktiivin mukaisille toimivaltaisille viranomaisille ja tekee tarpeen mukaan yhteistyötä kyseisten viranomaisten kanssa. Komissio tarkastelee myös kyseiseen digitaalisia elementtejä sisältävään tuotteeseen liittyvien tunnistettujen riskien merkityksellisyyttä osana tehtäviään, jotka liittyvät NIS 2 -direktiivin 22 artiklassa säädettyihin kriittisten toimitusketjujen unionin tason koordinoituihin turvallisuusriskinarviointeihin, ja kuulee tarvittaessa NIS-yhteistyöryhmää ja ENISA:aa.

Asetuksen 56 artiklan 3–6 kohdassa säädetään komission toimenpiteistä eräissä poikkeuksellisissa tilanteissa. Artiklan 5 kohdan nojalla komissio voi antaa täytäntöönpanosäädöksiä, joissa säädetään unionin tason korjaavista tai rajoittavista toimenpiteistä, joihin voi sisältyä vaatimus asianomaisia digitaalisia elementtejä sisältävien tuotteiden poistamisesta markkinoilta tai niitä koskevan palautusmenettelyn järjestämisestä sellaisen kohtuullisen ajan kuluessa, joka on oikeassa suhteessa riskin luonteeseen.

Merkittävän kyberturvallisuusriskin aiheuttavat vaatimustenmukaiset tuotteet

Asetuksen 57 artiklassa säädetään toimenpiteistä koskien vaatimustenmukaisia tuotteita, jotka sisältävät merkittävän kyberturvallisuusriskin. Artiklan mukaan markkinavalvontaviranomaisen on vaadittava talouden toimijaa toteuttamaan kaikki asianmukaiset toimenpiteet tilanteessa, jossa markkinavalvontaviranomainen on 54 artiklan mukaisen arvioinnin suoritettuaan todennut, että tuote ja valmistajan prosessit täyttävät asetuksen vaatimukset, mutta tuote aiheuttaa merkittävän kyberturvallisuusriskin sekä jonkin artiklan 1 kohdan a–d alakohdassa mainitun muun riskin. Jäsenvaltion on ilmoitettava toimenpiteistä välittömästi komissiolle ja muille jäsenvaltioille jatkotoimien arviointia varten.

Tuotteiden muodollinen vaatimustenvastaisuus

Asetuksen 58 artiklassa säädetään muodollisesta vaatimustenvastaisuudesta. Jos markkinavalvontaviranomainen havaitsee, ettei tuote täytä muodollisia vaatimuksia, sen on vaadittava asianomaista valmistajaa korjaamaan tuotteen vaatimustenvastaisuus. Muodollisia

vaatimustenvastaisuuksia ovat 58 artiklan 1 kohdassa luetellut seikat, kuten CE-merkinnän puutteellinen kiinnittäminen, EU-vaatimustenmukaisuusvakuutuksen puutteellinen laadinta tai teknisten asiakirjojen puutteellisuus. Mikäli valmistaja ei korjaa vaatimustenvastaisuutta, jäsenvaltion toteutettava kaikki tarvittavat toimenpiteet, joilla rajoitetaan tuotteen asettamista markkinoille, kielletään se tai joilla varmistetaan tuotetta koskevan palautusmenettelyn järjestäminen tai tuotteen poistaminen kyseisiltä markkinoilta.

Markkinavalvontaviranomaisten yhteistoimet ja tehotarkastukset

Asetuksen 59 artikla sisältää säännöt markkinavalvontaviranomaisten yhteistoimista. Jäsenvaltioiden markkinavalvontaviranomaiset voivat sopia muiden asianomaisten viranomaisten kanssa yhteisistä toimenpiteistä, joilla pyritään varmistamaan tuotteiden kyberturvallisuus sekä suojaamaan kuluttajia. Myös komissio tai ENISA voivat ehdottaa yhteisiä toimenpiteitä, jos on viitteitä tai tietoja siitä, että asetuksen soveltamisalaan kuuluvat tuotteet eivät täytä useissa jäsenvaltioissa asetuksen vaatimuksia. Markkinavalvontaviranomaisten ja komission on tarvittaessa varmistettava, ettei yhteistoimien toteuttaminen johda kilpailun vääristymiseen taloudellisten toimijoiden välillä. Asetuksen 60 artiklassa säädetään ”tehotarkastuksista”, joita pääsäännön mukaisesti koordinoisi komissio.

2.1.7 Hallinnolliset seuraamukset

Kyberkestävyysasetuksen 64 artiklassa velvoitetaan jäsenvaltiot säätämään asetuksen rikkomiseen sovellettavista seuraamuksista eli hallinnollisesta seuraamusmaksusta.

Kyberkestävyysasetuksen edellyttämä seuraamusjärjestelmä on kolmiportainen 64 artiklan 2–4 kohtien mukaisesti. Kohdissa säädetään hallinnollisten sakkojen määräämisen perusteista sekä vahvistetaan sakkojen enimmäismäärät asetuksen eri velvoitteiden rikkomisen osalta.

Hallinnollisten sakkojen enimmäismäärät on porrastettu kolmeen eri luokkaan. Ensimmäisessä luokassa (2 kohta) liitteessä I vahvistettujen olennaisten kyberturvallisuusvaatimusten ja 13 ja 14 artiklassa säädettyjen velvoitteiden täyttämättä jättämisestä on määrättävä hallinnollinen sakko, joka on enimmillään 15 miljoonaa euroa tai, jos rikkomukseen on syyllistynyt yritys, enimmillään 2,5 prosenttia sen edellisen tilikauden maailmanlaajuisesta liikevaihdosta sen mukaan, kumpi summista on suurempi. Velvoitteet kohdistuvat pääasiassa digitaalisia elementtejä sisältävän tuotteen valmistajaan. Toisessa luokassa (3 kohta) on kyse talouden toimijoita ja ilmoitettuja laitoksia koskevien kohdassa viitattujen velvoitteiden rikkomisesta, josta on määrättävä hallinnollinen sakko, joka on enimmillään 10 miljoonaa euroa tai 2 prosenttia edellisen tilikauden maailmanlaajuisesta liikevaihdosta. Kolmannessa luokassa (4 kohta) on virheellisten, puutteellisten tai harhaanjohtavien tietojen toimittaminen ilmoitetulle laitokselle tai markkinavalvontaviranomaiselle, josta on määrättävä hallinnollinen sakko, joka on enimmillään 5 miljoonaa euroa tai 1 prosentti edellisen tilikauden maailmanlaajuisesta liikevaihdosta sen mukaan, kumpi summista on suurempi.

Artiklan 5 kohdassa säädetään seikoista, jotka seuraamusmaksun määrästä päätettäessä on otettava huomioon kaikkien kyseisen tilanteen kannalta merkittävien olosuhteiden lisäksi. Artiklan 6 kohdan nojalla markkinavalvontaviranomaisen olisi välitettävä tiedot hallinnollisen seuraamusmaksun määräämisestä muiden jäsenvaltioiden markkinavalvontaviranomaisille.

Kyberkestävyysasetuksen 64 artiklan 10 kohdassa säädetään poikkeus hallinnollisten seuraamusmaksujen määräämisestä. Poikkeuksen nojalla hallinnollista seuraamusmaksua ei sovelleta valmistajaan, joka on mikroyritys tai pienyritys, silloin kun teko koskee 14 artiklan 2

tai 4 kohdassa tarkoitetun ilmoituksen tekemistä koskevan 24 tunnin määräajan noudattamatta jättämisen osalta. Lisäksi poikkeuksen nojalla hallinnollista seuraamusmaksua ei sovelleta avoimen lähdekoodin ohjelmistovastaavaan kyberkestävyysasetuksen rikkomisen osalta.

Kyberkestävyysasetuksen 65 artiklan nojalla edustajakannedirektiiviä (EU) 2020/1828 sovelletaan edustajakanteisiin, jotka on nostettu talouden toimijoita vastaan johtuen kyberkestävyysasetuksen rikkomisista, jotka vahingoittavat tai voivat vahingoittaa kuluttajien yhteisiä etuja. Kyberkestävyysasetuksen rikkomisen perusteella olisi siten voitava nostaa edustajakannedirektiivissä tarkoitettu edustajakanne.

2.1.8 Voimaantulo ja siirtymäsäännökset

Kyberkestävyysasetusta sovelletaan sen 71 artiklan mukaisesti 11.12.2027 alkaen. Ilmoitettuja laitoksia koskevaa IV lukua sovelletaan 11.6.2026 alkaen ja raportointivelvollisuuksia koskevaa 14 artiklaa 11.9.2026 alkaen.

Kyberkestävyysasetuksen vaatimuksia sovelletaan ennen 11.12.2027 markkinoille saatettuihin digitaalisia elementtejä sisältäviin tuotteisiin ainoastaan, jos tuotteeseen tehdään tämän ajankohdan jälkeen merkittävä muutos (69 artiklan 2 kohta). Merkittävällä muutoksella tarkoitetaan asetuksen 3 artiklan 30 kohdan määritelmän mukaan tuotteeseen sen markkinoille saattamisen jälkeen tehtyä muutosta, joka vaikuttaa siihen, täyttääkö digitaalisia elementtejä sisältävä tuote liitteessä I olevassa I osassa vahvistetut olennaiset kyberturvallisuusvaatimukset, tai joka muuttaa käyttötarkoitusta, jota varten digitaalisia elementtejä sisältävä tuote on arvioitu.

Raportoinnista 14 artiklassa säädettyjä velvoitteita sovelletaan 69 artiklan 3 kohdan nojalla kaikkiin asetuksen soveltamisalaan kuuluviin digitaalisia elementtejä sisältäviin tuotteisiin, jotka on saatettu markkinoille myös ennen 11.12.2027.

Kyberkestävyysasetuksen 69 artiklan 1 kohdan nojalla EU-tyyppitarkastustodistukset ja hyväksymispäätökset, jotka on annettu digitaalisia elementtejä sisältävien tuotteiden, joihin sovelletaan muuta unionin yhdenmukaistamislainsäädäntöä kuin kyberkestävyysasetusta, kyberturvallisuusvaatimuksista, pysyvät voimassa 11.6.2028 saakka tai niiden voimassaolon mukaisesti.

2.1.9 Komissiolle siirretty säädösvalta

Kyberkestävyysasetus sisältää useita valtuutussäännöksiä komissiolle siirretystä säädösvallasta.

Delegoidut säädökset

2 artiklan 5 kohdan toisen alakohdan nojalla komissio voi antaa delegoituja säädöksiä, joilla täsmennetään asetuksen vaatimusten soveltamisalan rajaamista koskevaa säännöstä, sikäli kuin sektorikohtaisessa lainsäädännössä on jollekin tuoteryhmälle määritelty vastaava tai korkeampi kyberturvallisuuden taso.

7 artiklan 3 kohdan nojalla komissio voi antaa delegoituja säädöksiä, joilla muutetaan liitettä III sisällyttämällä luetteloon uusi tuoteryhmä ja esittämällä sen määritelmä, siirtämällä tuoteryhmä yhdestä luokasta toiseen tai poistamalla luettelosta olemassa oleva tuoteryhmä.

8 artiklan 1 kohdan nojalla komissio voi antaa delegoituja säädöksiä, joilla liitteessä IV tarkoitetuilta tuotteilta edellytetään eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaista kyberturvallisuussertifikaattia.

8 artiklan 2 kohdan nojalla komissio voi antaa delegoituja säädöksiä, joilla muutetaan liitettä IV lisäämällä tai poistamalla digitaalisia elementtejä sisältävien kriittisten tuotteiden ryhmiä.

13 artiklan 8 kohdan neljännen alakohdan nojalla komissio voi antaa delegoituja säädöksiä, joilla määritetään tukiajan vähimmäiskesto tietyille tuoteryhmille.

14 artiklan 9 kohdan nojalla komission on annettava viimeistään 11.12.2025 delegoituja säädöksiä, joilla määritetään ehdot kyberturvallisuuteen liittyvien syiden soveltamiselle lykättäessä ilmoitusten välittämistä kyberkestävyysasetuksen 16 artiklan 2 kohdassa tarkoitetulla tavalla.

25 artiklan nojalla komissio voi antaa delegoituja säädöksiä, joilla perustetaan vapaaehtoisia tietoturvatodistusohjelmia, joiden avulla vapaiksi ja avoimen lähdekoodin ohjelmistoiksi luokiteltavien digitaalisia elementtejä sisältävien tuotteiden kehittäjät tai käyttäjät sekä muut kolmannet osapuolet voivat arvioida, ovatko tuotteet kyberkestävyysasetuksen velvoitteiden mukaisia.

27 artiklan 9 kohdan nojalla komissio voi antaa delegoituja säädöksiä, joilla yksilöidään ne eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät, joita voidaan käyttää osoittamaan, että digitaalisia elementtejä sisältävät tuotteet ovat liitteessä I vahvistettujen olennaisten kyberturvallisuusvaatimusten tai niiden osien mukaisia.

28 artiklan 5 kohdan nojalla komissio voi antaa delegoituja säädöksiä, joilla lisätään teknologian kehittymisen huomioon ottamiseksi elementtejä liitteessä V vahvistetun EU-vaatimustenmukaisuusvakuutuksen vähimmäissisältöön.

31 artiklan 5 kohdan nojalla komissio voi antaa delegoituja säädöksiä, joilla lisätään liitteessä VII vahvistettuihin teknisiin asiakirjoihin sisällytettäviä osia, jotta voidaan ottaa huomioon teknologian kehitys sekä asetuksen täytäntöönpanoprosessissa havaittu kehitys.

Täytäntöönpanosäädökset

7 artiklan 4 kohdan nojalla komission on hyväksyttävä viimeistään 11.12.2025 täytäntöönpanosäädös, jolla täsmennetään tekniset kuvaukset liitteissä III ja IV vahvistetuille digitaalisia elementtejä sisältävien tuotteiden ryhmille.

13 artiklan 24 kohdan nojalla komissio voi antaa täytäntöönpanosäädöksen, jolla täsmennetään ohjelmistojen materiaaliluettelon muoto ja osatekijät.

14 artiklan 10 kohdan nojalla komissio voi antaa täytäntöönpanosäädöksiä, joilla täsmennetään 14–16 artiklassa tarkoitettujen ilmoitusten muotoa ja niihin liittyviä menettelyitä.

27 artiklan 2 kohdan nojalla komissio voi antaa täytäntöönpanosäädöksiä, joissa vahvistetaan teknisiä vaatimuksia koskevia yhteisiä eritelmiä, mikäli saatavilla ei ole tarvittavia standardeja.

30 artiklan 6 kohdan nojalla komissio voi antaa täytäntöönpanosäädöksiä, joilla vahvistetaan teknisiä eritelmiä, jotka koskevat digitaalisia elementtejä sisältävien tuotteiden tietoturvaan liittyviä merkintöjä, kuvamerkkejä tai muita merkkejä, niiden tukiaikoja sekä mekanismeja, joilla edistetään niiden käyttöä ja lisätään yleistä tietoisuutta digitaalisia elementtejä sisältävien tuotteiden tietoturvasta.

34 artiklan 5 kohdan nojalla komissio täsmentää täytäntöönpanosäädöksellä teknisten asiakirjojen yksinkertaistetun muodon mikro- ja pienyrityksiä varten.

56 artiklan 5 kohdan ja 58 artiklan 9 kohdan nojalla komissio voi antaa täytäntöönpanosäädöksiä unionin tason korjaavista tai rajoittavista toimenpiteistä vaatimustenvastaisille digitaalisia elementtejä sisältäville tuotteille.

Ohjeet ja luettelo

Komissio voi lisäksi julkaista 26 artiklan 1 kohdan mukaisesti ohjeita, joilla autetaan talouden toimijoita soveltamaan asetusta.

Komission on 26 artiklan 2 kohdan mukaisesti pidettävä yllä luetteloa kyberkestävyysasetuksen nojalla annetuista delegoiduista säädöksistä ja täytäntöönpanosäädöksistä.

2.1.10 Kansallinen liikkumavara ja täydentävän sääntelyn tarve

Kyberkestävyysasetus on asetuksena suoraan sovellettava, eikä se lähtökohtaisesti sisällä kansallista liikkumavaraa.

Kyberkestävyysasetuksen 4 artiklan 1 kohdan nojalla jäsenvaltiot eivät saa estää kyberkestävyysasetuksen soveltamisalaan kuuluvien seikkojen osalta digitaalisia elementtejä sisältävien tuotteiden asettamista markkinoille silloin, kun tuotteet ovat kyberkestävyysasetuksen mukaisia. Kyberkestävyysasetuksen soveltamisalaan kuuluvia digitaalisen elementin sisältäviä tuotteita voidaan näin ollen jatkossa säädellä kansallisesti ainoastaan siltä osin kuin kyse ei ole kyberkestävyysasetuksen alaan kuuluvasta seikasta. Lisäksi asetus ei estä jäsenvaltioita asettamasta korkeampia kyberturvallisuusvaatimuksia digitaalisen elementin sisältävälle tuotteelle silloin kun se hankitaan tai käytetään kyberkestävyysasetuksen 5(1) artiklassa tarkoitettua tarkoitusta varten.

Kyberkestävyysasetus jättää jäsenvaltion kansalliseen liikkumavaraan vaatimustenmukaisuuden arviointilaitoksien ilmoittamista ja markkinavalvonnan järjestämistä koskevien viranomaistehtävien järjestämisen.

Jäsenvaltioiden on nimettävä 36 artiklan nojalla ilmoittamisesta vastaava viranomainen, jonka vastuulla on laatia ja toteuttaa tarvittavat menettelyt, jotka liittyvät vaatimustenmukaisuuden arviointilaitosten arviointiin, nimeämiseen ja ilmoittamiseen, sekä valvoa niitä. Jäsenvaltiot voivat myös päättää, että vaatimustenmukaisuuden arviointilaitosten arvioinnin ja valvonnan suorittaa kansallinen akkreditointielin (36(2) artikla). Jäsenvaltioiden on ilmoitettava komissiolle ja muille jäsenvaltioille laitokset, joille on annettu lupa suorittaa vaatimustenmukaisuuden arviointeja sekä pyrittävä varmistamaan 11.12.2026 mennessä, että unionissa on riittävä määrä ilmoitettuja laitoksia kyberkestävyysasetuksen mukaisten vaatimustenmukaisuuden arviointien suorittamiseksi (35 artikla). Jäsenvaltioiden tulee lisäksi huolehtia, että kansallisella tasolla on käytettävissä muutoksenhakumenettely ilmoitettujen laitosten päätöksiin (48 artikla).

Markkinavalvontaa varten asetus edellyttää jäsenvaltiota nimeämään yhden tai useamman markkinavalvontaviranomaisen asetuksen tehokkaan täytäntöönpanon varmistamiseksi ja markkinavalvontatoimien täytäntöönpanemiseksi (52(2) artikla). Jäsenvaltioiden on varmistettava, että nimetyille markkinavalvontaviranomaisille annetaan riittävät taloudelliset ja tekniset resurssit, mukaan lukien tarvittaessa käsittelyn automatisointivälineet, sekä henkilöstöresurssit, joilla on riittävät kyberturvallisuustaidot, jotta

markkinavalvontaviranomaiset voivat hoitaa tämän asetuksen mukaiset tehtävänsä (52(8) artikla). Markkinavalvontaviranomaisen tehtävät osoitetaan kyberkestävyysasetuksessa ja markkinavalvonta-asetuksessa.

Kyberkestävyysasetuksen 64 artiklan nojalla jäsenvaltioiden on säädettävä kyberkestävyysasetuksen rikkomiseen sovellettavista seuraamuksista ja toteutettava kaikki tarvittavat toimenpiteet niiden täytäntöönpanon varmistamiseksi. Seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia. Asetuksen 64 artiklan 2–4 kohdissa säädetään rikkomisista, jotka jäsenvaltion on sanktioitava, sekä niistä määrättävien hallinnollisten sakkojen enimmäismääristä. Lisäksi 64(7) artiklan nojalla jäsenvaltion on vahvistettava säännöt siitä, voidaanko viranomaisille tai julkisille elimille määrätä hallinnollisia sakkoja.

Kyberkestävyysasetuksen 5(2) artiklan nojalla jäsenvaltioiden on varmistettava, että julkisia hankintoja koskevassa prosessissa otetaan huomioon tämän asetuksen liitteessä I vahvistettujen olennaisten kyberturvallisuusvaatimusten noudattaminen, mukaan lukien valmistajien kyky käsitellä tehokkaasti haavoittuvuuksia, tämän kuitenkaan rajoittamatta julkisia hankintoja koskevien direktiivien soveltamista.

Kyberkestävyysasetuksen 10 artiklan nojalla jäsenvaltion on tarvittaessa edistettävä komission, Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja ENISA:n tuella toimenpiteitä ja strategioita, joilla pyritään:

a) kehittämään kyberturvallisuustaitoja ja luomaan organisatorisia ja teknologisia välineitä, joilla varmistetaan pätevien ammattihenkilöiden riittävä saatavuus, jotta voidaan tukea markkinavalvontaviranomaisten ja vaatimustenmukaisuuden arviointilaitosten toimintaa;

b) lisäämään yksityisen sektorin, talouden toimijoiden, kuluttajien, koulutuksen tarjoajien sekä julkishallinnon välistä yhteistyötä, muun muassa tarjoamalla valmistajien työntekijöille uudelleen- tai täydennyskoulutusta, ja siten lisäämään nuorten mahdollisuuksia saada työpaikkoja kyberturvallisuusalalta.

Kyberkestävyysasetuksen 33 artiklassa säädetään jäsenvaltioiden tukitoimista mikroyrityksille ja pienille ja keskisuurille yrityksille. Artiklan 1 kohdan nojalla jäsenvaltioiden on tarvittaessa toteutettava seuraavia mikro- ja pienten yritysten tarpeisiin räätälöityjä toimia:

a) järjestettävä erityisiä tiedotus- ja koulutustoimia asetuksen soveltamisesta;

b) perustettava erityinen viestintäkanava mikroyrityksiä ja pieniä yrityksiä ja tarvittaessa paikallisviranomaisia varten, jotta voidaan antaa neuvoja ja vastata asetuksen täytäntöönpanoa koskeviin kysymyksiin;

c) tuettava testausta ja vaatimustenmukaisuuden arviointitoimia tarpeen mukaan myös Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen tuella.

Kyberkestävyysasetuksen 33 artiklan 2 kohdan nojalla jäsenvaltiot voivat tarvittaessa perustaa kyberkestävyyden sääntelyn testiympäristöjä. Tällaisissa sääntelyn testiympäristöissä on oltava innovatiivisille digitaalisia elementtejä sisältäville tuotteille valvottuja testausympäristöjä, joilla helpotetaan niiden kehittämistä, suunnittelua, validointia ja testausta asetuksen noudattamiseksi, rajoitetun ajan ennen markkinoille saattamista. Komissio ja tarvittaessa ENISA voivat tarjota teknistä tukea, neuvontaa ja välineitä sääntelyn testiympäristöjen

perustamista ja toimintaa varten. Sääntelyn testiympäristöt on perustettava markkinavalvontaviranomaisten suorassa valvonnassa, ohjauksessa ja niiden tuella. Jäsenvaltioiden on ilmoitettava komissiolle ja muille markkinavalvontaviranomaisille sääntelyn testiympäristön perustamisesta hallinnollisen yhteistyön ryhmän kautta. Sääntelyn testiympäristöt eivät vaikuta toimivaltaisten viranomaisten valvonta- ja korjausvaltuuksiin. Jäsenvaltioiden on varmistettava avoin, oikeudenmukainen ja läpinäkyvä pääsy sääntelyn testiympäristöihin ja erityisesti helpotettava mikroyritysten ja pienten yritysten, myös startup-yritysten, pääsyä niihin.

Kyberkestävyysasetuksen 65 ja 67 artikloiden nojalla edustajakannedirektiiviä olisi sovellettava myös edustajakanteisiin, jotka nostetaan talouden toimijoita vastaan johtuen kyberkestävyysasetuksen rikkomisista, jotka vahingoittavat tai voivat vahingoittaa kuluttajien yhteisiä etuja.

2.2 Kyberturvallisuusasetus

2.2.1 Eurooppalainen kyberturvallisuuden sertifiointijärjestelmä

Kyberturvallisuusasetuksen tavoitteena on turvata sisämarkkinoiden toimintaa vahvistamalla kyberturvallisuutta, sietokykyä ja luottamusta EU:ssa. Asetus sisältää säännökset kyberturvallisuusvirasto ENISA:sta sekä EU:n kyberturvallisuuden sertifiointikehyksestä, mikä mahdollistaa tieto- ja viestintätekniikan tuotteiden, palveluiden ja prosessien sekä muutosasetuksen EU (EU) 2025/37 myötä myös tietoturvapalvelujen sertifioinnin erikseen laadittavien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien perusteella.

Kyberturvallisuusasetuksen sisältöä on kuvattu aiemmin hallituksen esityksessä eduskunnalle laiksi sähköisen viestinnän palveluista annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi, HE 98/2020 vp, s. 39–40. Tässä jaksossa kuvataan tiiviisti asetuksen sisältöä siltä osin kuin se on merkityksellistä kyberturvallisuussertifiointiin liittyvien ehdotuksien kannalta. Eurooppalaisen kyberturvallisuuden sertifiointikehyksen perustamista koskee kyberturvallisuusasetuksen III osasto.

Kyberturvallisuussertifioinnissa jokin tuote, prosessi tai palvelu saa sertifikaatin osoitukseksi sen siitä, että sen on tietyllä varmuustasolla arvioitu täyttävän tietyt määritellyt kyberturvallisuusvaatimukset. Kyberturvallisuusasetus ei itsessään johda sertifikaatin olemassaoloon eikä siinä säädetä sertifikaattien hankkimista koskevista velvollisuuksista. Asetuksella vahvistetaan mekanismi, jonka avulla laaditaan eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä. Asetuksella vahvistetaan sertifiointijärjestelmien laadintaa, sisältöä ja valvontaa koskevia tehtäviä Euroopan komissiolle, ENISA:lle ja jäsenvaltioiden viranomaisille.

Kyberturvallisuusasetuksen 48 artiklan nojalla komissio julkaisee eurooppalaista kyberturvallisuussertifiointia koskevan unionin jatkuvan työohjelman, johon on sisällytettävä luettelo sellaisista tuotteista, palveluista ja prosesseista, joille voi olla hyötyä eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan kuulumisesta. Komissio voi jatkuvan työohjelman pohjalta pyytää ENISA:a valmistelemaan ehdolla olevan sertifiointijärjestelmän tai tarkistamaan voimassa olevaa sertifiointijärjestelmää. ENISA:lla olisi komission pyynnöstä velvollisuus valmistella sertifiointijärjestelmä kyberturvallisuusasetuksessa säädetyin edellytyksin. Sertifiointijärjestelmien valmistelu on edennyt hitaasti. Ensimmäinen sertifiointijärjestelmä (EUCC) on hyväksytty vuoden 2024 alussa komission täytäntöönpanoasetuksella (EU) 2024/482 Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 soveltamissäännöistä siltä osin kuin on kyse yhteisiin kriteereihin perustuvan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän (EUCC)

hyväksymisestä. EUCC on tieto- ja viestintätekniikan tuotteita koskeva sertifiointijärjestelmä, joka perustuu tietoteknologian turvallisuuden arviointia koskeviin yhteisiin kriteereihin (Common Criteria for Information Technology Security Evaluation, CC) ja tietotekniikan turvallisuuden yhteisiin arviointimenetelmiin (Common Methodology for Information Technology Security Evaluation, CEM), jotka ovat julkaistu esimerkiksi standardeina ISO/IEC 15408 ja ISO/IEC 18405. Valmistelussa ovat lisäksi pilvipalveluita, 5G:tä ja eurooppalaista digitaalista identiteettilompakkoa koskevat sertifiointijärjestelmät.

Eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan kyberturvallisuusasetuksen 52 artiklan mukaisesti määritellä kolmen varmuustason sertifikaatteja: perustason, korotetun tason ja korkean tason sertifikaatit. Perustason ja korotetun tason sertifikaatit myöntävät pääsääntöisesti akkreditoidut ja viranomaisen ilmoittamat ja tarvittaessa valtuuttamat vaatimustenmukaisuuden arviointilaitokset. Valmistajat ja palveluntarjoajat voivat hakea sertifiointia vaatimustenmukaisuuden arviointilaitoksilta tai tapauksen mukaan kyberturvallisuussertifioinnin myöntävältä viranomaiselta. Arviointilaitoksen tulee täyttää asetuksessa ja sen liitteessä määritellyt vaatimukset. Kyberturvallisuusasetuksen 53 artiklan nojalla sertifiointijärjestelmässä voidaan myös sallia, että vaatimustenmukaisuuden itsearviointi on yksinomaan tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien valmistajan tai tarjoajan vastuulla. Itsearviointia voidaan kuitenkin soveltaa vain varmuustasolla perustaso. Kyberturvallisuusasetuksen 55 artiklassa säädetään valmistajan tai tarjoajan velvollisuudesta asettaa julkisesti saataville tietyt tuotteen tai palvelun kyberturvallisuutta tukevat tiedot.

2.2.2 Sertifiointivelvollisuudet

Kyberturvallisuussertifiointi on kyberturvallisuusasetuksen mukaan vapaaehtoista, jollei unionin lainsäädännössä tai jäsenvaltioiden lainsäädännössä toisin säädetä. Kyberturvallisuusasetukseen ei sisälly vaatimuksia sertifiointijärjestelmien käytöstä. Edellä todetusti ensimmäinen sertifiointijärjestelmä (EUCC) on hyväksytty vuoden 2024 alussa.

Kyberkestävyysasetuksen 32 artiklassa säädetään digitaalisia elementtejä sisältävien tuotteiden vaatimustenmukaisuuden arviointimenettelystä. Silloin kun digitaalisen elementin sisältävälle tuotteelle on saatavilla ja sovellettavissa eurooppalainen kyberturvallisuuden sertifiointijärjestelmä, kyberkestävyysasetuksen 32 artiklan nojalla digitaalisen elementin sisältävän tuotteen vaatimustenmukaisuuden kyberkestävyysasetuksen vaatimuksille voi osoittaa muun ohella eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän käyttämisellä. Kyberkestävyysasetuksen liitteessä III tarkoitetuille tärkeille tuotteille vaatimustenmukaisuuden osoittaminen edellyttäisi tällöin vähintään varmuustason ”korotettu” kyberturvallisuussertifikaatin käyttämistä. Kyberkestävyysasetuksen 8 artiklan 1 kohdan ja 32 artiklan 4 kohdan nojalla asetuksen liitteessä IV tarkoitetuilta tuotteilta edellytetään pääsääntönä eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän käyttämistä varmuustasolla ”korotettu”. Komissiolla olisi luvussa 2.1.9 kuvatusti siirrettyä säädösvaltaa tuotteiden listojen muuttamiseen tietyin reunaehdoin ja edellytyksen alaan kuuluvien tuotteiden tarkemmalle määrittelylle. Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien käytön voidaan olettaa lisääntyvän kyberkestävyysasetuksen myötä.

Kyberturvallisuussertifioinnilla on liittymiä myös EU:n kyberturvallisuus- eli NIS 2 -direktiiviin EU (2022/2555). NIS 2 -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 kyberturvallisuusasetuksen 49 artiklan nojalla hyväksyttyjen eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukaisesti. Direktiivin kansallisessa

täytäntöönpanossa tällaisia säännöksiä ei sisällytetty kyberturvallisuuslakiin (124/2025; HE 57/2024 vp), mutta lisävaatimusten asettaminen on jatkossa mahdollista erityislainsäädännössä. Lisäksi EU-oikeuden salliman kansallisen liikkumavaran puitteissa on mahdollista asettaa muita kansallisia edellytyksiä kyberturvallisuussertifiointien käytölle.

Lisäksi NIS 2 -direktiivin 24 artiklan 2 kohdan mukaan komissiolla on valta antaa direktiivin 38 artiklan mukaisesti tietyin edellytyksin delegoituja säädöksiä, joilla voidaan vaatia joitakin keskeisten ja tärkeiden toimijoiden luokkia 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. Komissio ei ole toistaiseksi antanut tällaisia delegoituja säädöksiä.

2.2.3 Kansallinen kyberturvallisuussertifioinnin viranomainen

Kyberturvallisuusasetuksen 58 artikla velvoittaa jäsenvaltiot yhden tai useamman kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen nimeämiseen. Jäsenvaltio voi myös nimetä sopimuksella toisen jäsenvaltion kanssa yhden tai useamman tähän toiseen jäsenvaltioon sijoittautuneen kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen vastaamaan valvontatehtävistä tämän nimeävän jäsenvaltion alueella. Kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten on tarkoitus vastata eurooppalaisen kyberturvallisuuden sertifiointijärjestelmien täytäntöönpanosta ja valvonnasta ja siitä, että näiden järjestelmien mukaisesti myönnetyt sertifikaatit ovat voimassa ja tunnustettuja kaikkialla unionissa. Jäsenvaltioiden on varmistettava, että kansallisilla viranomaisilla on riittävät resurssit käyttää valtuuksiaan ja suorittaa tuloksekkaasti ja tehokkaasti niille osoitetut tehtävät.

Kyberturvallisuusasetuksen suomenkielisen version käyttämästä kyberturvallisuussertifioinnin myöntävän viranomaisen käsitteestä huolimatta kyseisen viranomaisen tehtävissä on kyse tosiasiallisesti myös sertifiointijärjestelmien noudattamista koskevasta valvonnasta eikä ainoastaan sertifikaattien myöntämiseen liittyvistä tehtävistä.

Asetuksen 58 artiklan 3 kohdan nojalla kansallisen viranomaisen on organisaatioltaan, rahoituspäätökseltään, oikeudelliselta rakenteeltaan ja päätöksenteoltaan oltava riippumaton yksiköistä, joita se valvoo. Artiklan 4 kohdan nojalla kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen kyberturvallisuussertifikaattien myöntämiseen liittyvän toiminnan tulee artiklan mukaan olla tiukasti erotettu viranomaisen 58 artiklan mukaisesta valvontatoiminnasta. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen toimivaltaan kuuluu asetuksen 56 artiklan 6 kohdan nojalla korkean varmuustason kyberturvallisuussertifikaattien myöntäminen. Tehtävä voidaan tietyin ehdoin delegoida vaatimustenmukaisuuden arviointilaitokselle.

Kansalliset kyberturvallisuussertifioinnin myöntävät viranomaiset osallistuvat Euroopan kyberturvallisuuden sertifiointiryhmään. Viranomaisten on tehtävä yhteistyötä keskenään ja komission kanssa ja vaihdettava tietoja, kokemuksia ja hyviä käytäntöjä tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien kyberturvallisuussertifioinnista ja niiden kyberturvallisuuteen liittyvistä teknisistä kysymyksistä.

Kyberturvallisuusasetuksen 58 artiklan 7 kohdassa säädetään kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen valvontatehtävistä. Kansallisen viranomaisen tehtäviin kuuluvat ensinnäkin itsearviointiin perustuvien vaatimustenmukaisuusilmoitusten valvonta sekä sen valvominen, että sen alueella myönnettyjen eurooppalaisten kyberturvallisuussertifikaattien vaatimuksia ja

sertifiointijärjestelmien sääntöjä noudatetaan. Toiseksi viranomaisen tehtäviin kuuluu akkreditointielinten tukeminen niiden valvoessa vaatimustenmukaisuuden arviointilaitoksia sekä vaatimustenmukaisuuden arviointilaitosten valtuuttaminen sertifiointijärjestelmien sitä edellyttäessä ja valtuutusten keskeyttäminen tai peruuttaminen, jos asetuksen vaatimuksia ei noudateta. Kolmanneksi viranomaisen tehtävänä on asetuksen 56 artiklan 5 kohdan nojalla valvoa perustason tai korotetun varmuustason eurooppalaisia kyberturvallisuussertifikaatteja poikkeuksellisesti myöntäviä julkisia elimiä. Neljänneksi viranomaisen tehtävänä on käsitellä luonnollisten henkilöiden tai oikeushenkilöiden tekemät valitukset, jotka liittyvät kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten tai vaatimustenmukaisuuden arviointilaitosten 56 artiklan 6 kohdan mukaisesti myöntämiin eurooppalaisiin kyberturvallisuussertifikaatteihin taikka EU-vaatimustenmukaisuusilmoituksiin. Lisäksi viranomainen laatii vuosittain yhteenvedon toimistaan ENISA:lle ja Euroopan kyberturvallisuuden sertifiointiryhmälle, tekee yhteistyötä muiden kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten ja muiden viranomaisten kanssa esimerkiksi jakamalla tietoa mahdollisista tapauksista, joissa tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit taikka tietoturvapalvelut eivät vastaa asetuksen tai yksittäisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien vaatimuksia, sekä seuraa kehitystä kyberturvallisuussertifioinnin alalla.

Kyberturvallisuusasetuksen 58 artiklan 8 kohdan edellyttämiin viranomaisen toimivaltuuksiin kuuluvat muun muassa oikeudet saada tietoja vaatimustenmukaisuuden arviointilaitoksilta, eurooppalaisen kyberturvallisuussertifikaatin haltijoilta ja EU-vaatimustenmukaisuusilmoituksen antajilta, tehdä niitä koskevia tarkastuksia ja päästä niiden tiloihin sekä toteuttaa muita toimenpiteitä kansallisen lainsäädännön mukaisesti sen varmistamiseksi, että ne noudattavat asetuksen tai eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimuksia. Valvontaviranomaisella on myös oikeus peruuttaa kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen myöntämät eurooppalaiset kyberturvallisuussertifikaatit tai vaatimustenmukaisuuden arviointilaitosten delegoinnin perusteella myöntämät korkean varmuustason eurooppalaiset kyberturvallisuussertifikaatit, jos ne eivät täytä asetuksen tai kyseisen eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimuksia. Viranomaisella on lisäksi oikeus määrätä seuraamuksia kansallisen lainsäädännön mukaisesti asetuksen rikkomisesta ja vaatia lopettamaan asetuksen velvoitteiden rikkominen.

2.2.4 Vaatimustenmukaisuuden arviointilaitokset

Kyberturvallisuusasetuksen 60 ja 61 artiklassa säädetään vaatimustenmukaisuuden arviointilaitosten akkreditoinnista, valtuuttamisesta ja ilmoittamisesta komissiolle. Asetuksen liite sisältää kansallisen akkreditointielimen antaman akkreditoinnin edellytyksenä olevat vaatimukset. Sertifiointijärjestelmä voi sisältää erityisiä vaatimuksia tai lisävaatimuksia, jolloin kansallinen kyberturvallisuuden sertifiointiviranomainen valtuuttaa vain nämä vaatimukset täyttävät vaatimustenmukaisuuden arviointilaitokset. Akkreditointi myönnetään enintään viideksi vuodeksi, ja se voidaan uusia. Jos akkreditoinnin edellytykset eivät enää täyty tai jos vaatimustenmukaisuuden arviointilaitoksen toiminta rikkoo asetuksen säännöksiä, kansallisten akkreditointielinten on rajoitettava akkreditointia taikka keskeytettävä tai peruttava se.

Kansallinen kyberturvallissertifioinnin viranomainen ilmoittaa komissiolle vaatimustenmukaisuuden arviointilaitoksista, jotka on akkreditoitu ja valtuutettu myöntämään eurooppalaisia kyberturvallisuussertifikaatteja määritellyillä varmuustasoilla sekä muutoksista. Komissio julkaisee luettelon ilmoitetuista vaatimustenmukaisuuden arviointilaitoksista. Kansallinen kyberturvallisuussertifioinnin viranomainen voi esittää komissiolle pyynnön poistaa ilmoittamansa vaatimustenmukaisuuden arviointilaitos luettelosta.

2.2.5 Komissiolle siirretty säädösvalta

Kyberturvallisuusasetukseen sisältyy komissiolle siirrettyä säädösvaltaa. Komissio antaa eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän täytäntöönpanosäädöksellä asetuksen 49 artiklan nojalla. Edellä todetusti ensimmäinen sertifiointijärjestelmä (EUCC) on hyväksytty vuoden 2024 alussa komission täytäntöönpanoasetuksella (EU) 2024/482.

Komissio voi 61 artiklan 5 kohdan nojalla antaa myös täytäntöönpanosäädöksiä, joilla vahvistetaan olosuhteet, muotoseikat ja menettelyt tämän ilmoituksille, jotka kansallinen kyberturvallisuuden sertifiointiviranomainen antaa vaatimustenmukaisuuden arviointilaitoksista. Komissio on antanut tämän nojalla täytäntöönpanoasetuksen (EU) 2024/3143 Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 61 artiklan 5 kohdan mukaisiin ilmoituksiin liittyvien olosuhteiden, muotoseikkojen ja menettelyjen vahvistamisesta.

Lisäksi komissio voi antaa täytäntöönpanosäädöksiä kansallisille kyberturvallisuussertifioinnin myöntäville viranomaisille tehtävien vertaisarviointien suunnitelmasta asetuksen 59 artiklan 5 kohdan nojalla.

2.2.6 Kansallinen liikkumavara ja täydentävän sääntelyn tarve

Kyberturvallisuusasetukseen ei lähtökohtaisesti sisälly kansallista liikkumavaraa, vaan se on asetuksena suoraan sovellettava. Kansallisesti on kuitenkin mahdollista asettaa vaatimuksia eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien käytölle EU-oikeuden salliman liikkumavaran puitteissa (ks. luku 2.2.2). Kansallista liikkumavaraa on myös sen suhteen, miten kansallisen kyberturvallisuussertifioinnin viranomaistehtävät järjestetään. Tehtävä on nykyisin osoitettu Liikenne- ja viestintävirastolle sähköisen viestinnän palveluista annetussa laissa. Viranomaisen toimivaltuuksista on säädettävä kansallisesti. Tarkastusoikeuden osalta kyberturvallisuusasetus jättää kansalliseen prosessioikeuteen tehdyn viittauksen johdosta kyberkestävyysasetuksen valvontaan sovellettavaksi tulevaa markkinavalvonta-asetusta enemmän kansallista liikkumavaraa sen suhteen, onko tarkastusoikeuden ulotuttava kotirauhan piiriin. Lisäksi asetus edellyttää kansallista täydentävää sääntelyä vaatimustenmukaisuuden arviointilaitosten asemasta niiden hoitaessa julkista hallintotehtävää.

Kansallista liikkumavaraa liittyy myös seuraamusten määrittämiseen. Kyberturvallisuusasetuksen 65 artiklan mukaan jäsenvaltioiden on annettava säännöt seuraamuksista, joita sovelletaan asetuksen kyseisen osaston ja eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien säännösten rikkomiseen, ja toteutettava kaikki tarvittavat toimenpiteet sen varmistamiseksi, että ne pannaan täytäntöön. Säädettyjen seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia.

2.3 Verkkotunnusvälittäjät

Euroopan unionin kyberturvallisuusdirektiivin eli toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2022/2555, jäljempänä NIS 2 -direktiivi, 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 velvoitteet kyberturvallisuutta koskevasta riskienhallinnasta sekä merkittävistä

kyberturvallisuuspoikkeamista ilmoittamisesta. Lisäksi 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 team, jäljempänä *CSIRT-yksikkö*). Lisäksi direktiivissä säädetään verkkotunnusten rekisteröintitietoja koskevasta tietokannasta.

NIS 2 -direktiivin keskeinen sisältö kuvataan tarkemmin hallituksen esityksen HE 57/2024 vp jaksossa 2. Tässä yhteydessä käsitellään NIS 2 -direktiivin keskeiset verkkotunnusvälittäjiä koskevat säännökset.

NIS 2 -direktiivin 6 artiklan 22 kohdan nojalla ”verkkotunnusten rekisteröintipalveluja tarjoavalla toimijalla” tarkoitetaan verkkotunnusvälittäjää tai verkkotunnusvälittäjien puolesta toimivaa tahoa, kuten yksityisyys- tai välityspalvelujen tarjoajaa tai jälleenmyyjää. Verkkotunnusten rekisteröintipalveluja tarjoavat toimijat eivät ole direktiivin 3 artiklassa tarkoitettuja keskeisiä toimijoita, joihin olisi sovellettava direktiivin 21 ja 23 artiklan mukaisia velvollisuuksia kyberturvallisuuden riskienhallinnasta ja merkittävien poikkeamien ilmoittamisesta. Verkkotunnusten rekisteröintipalveluja tarjoaviin toimijoihin liittyvää sääntelyä sisältyy direktiivin 3 artiklan 3 ja 4 kohtaan, 27 artiklaan ja 28 artiklaan.

NIS 2 -direktiivin 3 artiklan 3 kohdan mukaan jäsenvaltioiden on laadittava luettelo keskeisistä ja tärkeistä toimijoista sekä verkkotunnusten rekisteröintipalveluja tarjoavista toimijoista. Saman kohdan mukaan jäsenvaltioiden on tarkasteltava luetteloa uudelleen säännöllisesti ja vähintään kahden vuoden välein ja saatettava se tarvittaessa ajan tasalle. NIS 2 -direktiivin 3 artiklan 4 kohdan mukaan 3 kohdassa tarkoitetun luettelon laatimiseksi jäsenvaltioiden on vaadittava kyseisessä kohdassa tarkoitettuja toimijoita toimittamaan toimivaltaisille viranomaisille eräät tiedot. Lisäksi toimijoiden on ilmoitettava kaikista muutoksista tällaisiin tietoihin viipymättä ja joka tapauksessa kahden viikon kuluessa muutospäivästä.

NIS 2 -direktiivin 27 artiklan 2 ja 3 kohdan nojalla jäsenvaltion on edellytettävä eräiden toimijoiden, mukaan lukien verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden, toimittamaan jäsenvaltion toimivaltaiselle viranomaiselle kohdassa tarkoitetut tiedot. Jäsenvaltioiden on varmistettava, että toimijat ilmoittavat toimivaltaiselle viranomaiselle kaikista muutoksista 2 kohdan mukaisesti toimittamiinsa tietoihin viipymättä ja joka tapauksessa kolmen kuukauden kuluessa muutospäivästä.

NIS 2 -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.

NIS 2 -direktiivin 28 artiklan 2 kohdan nojalla jäsenvaltion tulee edellyttää 28 artiklan 1 kohdan soveltamiseksi, 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.

NIS 2 -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.

NIS 2 -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.

NIS 2 -direktiivin 28 artiklan 6 kohdan nojalla 28 artiklan 1–5 kohdassa säädettyjen velvoitteiden noudattaminen ei saa johtaa päällekkäisyyksiin verkkotunnusten rekisteröintitietojen keruussa. Tätä varten jäsenvaltioiden on edellytettävä, että aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat tekevät yhteistyötä keskenään.

NIS 2 -direktiivin 26 artiklassa säädetään jäsenvaltioiden lainkäyttövallasta verkkotunnusten rekisteröintipalveluja tarjoavia toimijoita koskien. 26 artiklan 1 kohdan nojalla verkkotunnusten rekisteröintipalveluja tarjoava toimija kuuluu sen jäsenvaltion lainkäyttövaltaan, jossa sen päätoimipaikka on. Päätoimipaikasta tai edustajan nimeämisestä unioniin säädetään 26 artiklan 2–5 kohdassa.

3 Nykytila ja sen arviointi

3.1 Kyberkestävyysasetus

3.1.1 Tuotesääntely

Suomessa ei ole voimassa olevaa kansallista tuotesääntelyä, jossa asetettaisiin kyberkestävyysasetuksen kaltaisia horisontaalisia kyberturvallisuusvaatimuksia digitaalisen elementin sisältäville tuotteille tai niiden valmistajille, maahantuojille tai jälleenmyyjille. Horisontaalisia kyberturvallisuutta koskevia vaatimuksia ei nykyisin aseteta laissa laitteille ja ohjelmistoille. Vaatimukset olisivat siten talouden toimijoille lähtökohtaisesti uusia. Vaatimukset kohdistuvat mm. laitteen tai ohjelmiston ominaisuuksiin, kyberturvallisuuteen vaikuttavien seikkojen dokumentointiin sekä haavoittuvuuksien hallintaan.

Tuotekohtaisiin erityissäädöksiin voi sisältyä tuotteiden tietoturvaan liittyviä vaatimuksia. Kyberturvallisuutta tai haavoittuvuuksien hallintaa koskeva tuotekohtainen sääntely on kuitenkin yleisesti ottaen vähäistä ja keskittyy korkean turvallisuusriskin tuotteisiin. Esityksen valmistelussa ei ole tunnistettu sellaista kansallista lainsäädäntöä, joka olisi ristiriidassa kyberkestävyysasetuksen kanssa siten, että kansallista sääntelyä olisi ehdotettava kumottavaksi tai muutoin jätettävä kyberkestävyysasetuksen vastaisena soveltamatta tulevaisuudessa.

Kyberturvallisuutta parantavista tietoturvavaatimuksista on säädetty EU:n radiolaitedirektiivin (2014/53/EU) 3(3) artiklan d, e ja f alakohdissa, joita sovelletaan komission delegoidussa asetuksessa 2022/30 säädettyihin radiolaitteisiin. Radiolaitedirektiivin vaatimukset on pantu täytäntöön sähköisen viestinnän palveluista annetulla lailla (2014/917) ja valtioneuvoston asetuksella radiolaitteiden vaatimustenmukaisuudesta (152/2024). Kyberkestävyysasetus kattaa kaikki radiolaitedirektiivin tietoturvaa koskevat vaatimukset, ja sitä sovelletaan päällekkäin komission delegoidussa asetuksessa säädettyihin tuotteisiin, kunnes komissio kumoaa delegoidun asetuksen tai muuttaa sen soveltamisalaa.

Lainsäädännön ohella nykytilassa kyberturvallisuusvaatimuksia sisältyy lisäksi eri tuotesektorien kyberturvallisuutta koskeviin standardeihin, joita noudattamalla voidaan tietyin edellytyksin osoittaa tuotteen vaatimustenmukaisuus. Standardien hyödyntäminen on lähtökohtaisesti valmistajalle vapaaehtoista ja liiketoimintaintresseihin perustuvaa. Kyberturvallisuutta ja haavoittuvuuksien hallintaa koskevia ehtoja voi sisältyä soveltamisalaan kuuluvien tuotteiden hankintasopimuksiin tai tuotteelle vapaaehtoisesti tarjottavaan takuuseen.

Avoimen lähdekoodin ohjelmistoja tai -ohjelmistovastaavia koskevia kyberturvallisuusvaatimuksia ei ole asetettu nykyisin lainsäädännössä.

Koska kyberkestävyysasetuksen on suoraan sovellettava, nykytilaa arvioidaan tarkemmin vain niiden kokonaisuuksien osalta, joiden osalta on tarve esittää asetusta täydentävää kansallista sääntelyä. Tällaisia kokonaisuuksia ovat kyberkestävyysasetuksen ilmoitettuja laitoksia ja markkinavalvontaa koskevat viranomaistehtävät sekä hallinnolliset seuraamukset. Kyberturvallisuusasetuksen kohdalla arvioidaan vastaavasti vaatimustenmukaisuuden arviointilaitoksia koskevaa sääntelyä sekä viranomaistoimivaltuuksia ja hallinnollisia sanktioita.

3.1.2 Markkinavalvonta

Markkinavalvonnalla tarkoitetaan jälkikäteistä, riskiarviointiin perustuvaa valvontaa markkinoilla. Markkinavalvonnan tarkoituksena on varmistaa, että tuotteita koskevia säännöksiä ja määräyksiä noudatetaan eikä vaarallisia tai turvallisuudeltaan puutteellisia tuotteita ole Euroopan unionin sisämarkkinoilla. Vastuu tuotteiden vaatimustenmukaisuudesta on valmistajilla, maahantuojilla ja jälleenmyyjillä, jotka osoittavat tuotteen vaatimustenmukaisuuden ennen sen saattamista markkinoille.

Markkinavalvontatehtäviä Suomessa on hajautettu tuoteryhmittäin eri viranomaisille eri ministeriöiden hallinnonaloilla. Markkinavalvontaviranomaiset helmikuun 2020 tilanteen mukaan esitetään tuoteryhmittäin työ- ja elinkeinoministeriön muistiossa (linkki). Viranomaisista laajin tehtäväalue markkinavalvontaan liittyen on Turvallisuus- ja kemikaalivirastolla (Tukes). Virasto hoitaa markkinavalvontatehtäviä työ- ja elinkeinoministeriön hallinnonalalla useilla tuotesektoreilla, ja sen yhteydessä toimiva akkreditointiyksikkö eli FINAS-akkreditointipalvelu huolehtii kansallisen akkreditointielimen tehtävistä. Liikenne- ja viestintävirasto Traficomille on nykyisin osoitettu markkinavalvontatehtäviä tuotekohtaisessa sääntelyssä radiolaitteisiin sekä huviveneisiin, laivavarusteisiin, miehittämättömiin ilma-aluksiin ja ajoneuvoihin kohdistuen. Muita tuotekohtaisia markkinavalvontaviranomaisia ovat mm. Poliisihallitus, Tulli, Suomen ympäristökeskus, ELY-keskukset, kunnan ympäristönsuojeluviranomaiset, aluehallintovirastojen työsuojelun vastuualueet ja Ruokavirasto.

Kyberkestävyysasetus edellyttää jäsenvaltiota järjestämään sen soveltamisalaan kuuluvien tuotteiden vaatimustenmukaisuuden markkinavalvonnan. Tehtävä olisi uusi ja järjestettävä

viranomaisessa ensimmäistä kertaa, koska asetus vaatimuksineen on vastaavasti uusi. Kansallisesti ei ole säädetty vastaavista vaatimuksista tai valvontaa koskevasta viranomaistehtävästä.

Liikenne- ja viestintäviraston Kyberturvallisuuskeskus on vuodesta 2019 alkaen myöntänyt ja valvonut Tietoturvamerkin käyttöä osoitukseksi siitä, että merkillä varustettu tuote tai palvelu on suunniteltu tietoturvalliseksi ja täyttää Traficomin asettamat tietoturvavaatimukset. Tietoturvamerkin hankkiminen on tuotteen valmistajalle ja myyjälle vapaaehtoista, eikä Tietoturvamerkin hankkiminen ole ollut markkinoille pääsyn edellytys.

Laki eräiden tuotteiden markkinavalvonnasta

Laki eräiden tuotteiden markkinavalvonnasta (2016/1137, jäljempänä *markkinavalvontalaki*) sisältää perussäännökset sen soveltamisalaan kuuluvien tuoteryhmien markkinavalvonnasta. Markkinavalvontalaki on horisontaalinen markkinavalvontaa sääntelevä yleislaki, jota sovelletaan sen soveltamisalaan säädettyjen tuotesäädösten markkinavalvontaan.

Markkinavalvontalailla on pantu täytäntöön Euroopan parlamentin ja neuvoston asetus (EU) 2019/1020 markkinavalvonnasta ja tuotteiden vaatimustenmukaisuudesta sekä direktiivin 2004/42/EY ja asetusten (EY) N:o 765/2008 ja (EY) N:o 305/2011 muuttamisesta (*markkinavalvonta-asetus*), jossa asetetaan yhdenmukaiset säännöt tiettyjen tuoteryhmien markkinavalvonnalle sekä vähimmäisvaatimukset markkinavalvontaviranomaisten toimivaltuuksille. Markkinavalvonta-asetuksen täytäntöönpanon yhteydessä markkinavalvontalain soveltamisalaan lisättiin useita tuoteryhmiä sekä säännökset markkinavalvontaviranomaisten toimivaltuuksista ja valvontakeinoista.

Markkinavalvontalaissa säädetään sen 1 §:ssä tarkoitettujen tuotteiden markkinavalvonnasta. Muiden kuin markkinavalvontalain soveltamisalaan kuuluvien tuoteryhmien markkinavalvonnasta säädetään tuotekohtaisissa laeissa. Markkinavalvontalaki on luonteeltaan yleislaki, jota sovelletaan sen 1 §:n nojalla silloin, kun tuotekohtaisessa säädöksissä ei toisin säädetä.

Markkinavalvontalain 4 §:ssä säädetään lain mukaisista markkinavalvontaviranomaisista. Markkinavalvontaviranomaisina toimivat Turvallisuus- ja kemikaalivirasto, Tulli, Säteilyturvakeskus, Liikenne- ja viestintävirasto, Suomen ympäristökeskus, Lääkealan turvallisuus- ja kehittämiskeskus, Sosiaali- ja terveysalan lupa- ja valvontavirasto (1.1.2026 lukien Lupa- ja valvontavirasto) ja kunnat sekä Ruokavirasto. Kuvaus keskeisten markkinavalvontaviranomaisten tehtävistä sisältyy hallituksen esitykseen eduskunnalle EU:n tekoälyasetusta täydentäväksi lainsäädännöksi HE 46/2025 vp.

Markkinavalvontalain 4 a §:n nojalla markkinavalvonta-asetuksen 10 artiklan 3 kohdassa tarkoitettuna markkinavalvonnan yhteyspisteenä toimii Turvallisuus- ja kemikaalivirasto. Markkinavalvonnan yhteistyöryhmä toimii markkinavalvonnan yhteyspisteen yhteydessä.

Markkinavalvontalain 4 §:n 4 momentin nojalla Liikenne- ja viestintävirasto toimii markkinavalvontaviranomaisena ilmailulaissa, ajoneuvolaissa, ympäristönsuojelulain 24 a §:n 3 momentissa, huviveneiden turvallisuudesta ja päästövaatimuksista annetussa laissa, sähköisen viestinnän palveluista annetussa laissa, laivavarustelaissa ja eräiden tuotteiden esteettömyysvaatimuksista annetussa laissa tarkoitettujen tuotteiden osalta.

Hallituksen esityksellä HE 46/2025 vp on ehdotettu markkinavalvontalaissa säädettäväksi viittaussäännöksellä myös tekoälyjärjestelmien markkinavalvontaviranomaisista. Ehdotuksen

mukaan eräiden tekoälyjärjestelmien valvonnasta annetun lain 3 §:ssä säädettäisiin suuririskisten tekoälyjärjestelmien markkinavalvontaviranomaisista, joita olisivat tapauksen mukaan Tukes, Tulli, Liikenne- ja viestintävirasto, työsuojeluviranomainen, Lääkealan Turvallisuus- ja kehittämiskeskus, Energiavirasto, tietosuojavaltuutettu, Lupa- ja valvontavirasto, Finanssivalvonta ja Lounais-Suomen aluehallintovirasto.

Kyberkestävyysasetuksen 52 artiklan mukaan asetuksen soveltamisalaan kuuluvien tuotteiden markkinavalvontaan sovelletaan markkinavalvonta-asetusta. Markkinavalvonta-asetuksen kansallinen toimeenpanosääntely sisältyy markkinavalvontalakiin. Lisäksi kyberkestävyysasetuksen soveltamisalaan kuuluu tuotteita, joihin kohdistuu jo voimassa olevaa tuotesääntelyä sekä sen edellyttämää markkinavalvontaa.

Tuotteiden kyberturvallisuutta koskevissa markkinavalvontatehtävissä on kyse uusista viranomaistehtävistä, jotka eivät sisälly minkään viranomaisen lakisääteisiin tehtäviin.

Koska kyberkestävyysasetuksen valvontaan sovelletaan markkinavalvonta-asetusta, jota on kansallisesti täydennetty markkinavalvontalailla, olisi tarpeen laajentaa markkinavalvontalain 1 §:n soveltamisalaa kattamaan myös kyberkestävyysasetuksen soveltamisalaan kuuluvien tuotteiden valvonta. Markkinavalvontalain 4 §:ssä säädetään lain nojalla toimivaltaisista valvontaviranomaisista, minkä vuoksi siihen on tarpeen lisätä viittaus esityksen nojalla ehdotettavan lain nojalla toimivaltaiseksi tuleviin viranomaisiin. Lakiteknisistä syistä muutos on tarpeen tehdä osittain viittaamalla, koska viranomaisia on lukumääräisesti useita toimivallan kuuluessa eräissä tapauksissa tekoälyasetusta valvoville viranomaisille. Ehdotettavan lakimuutoksen tarkoituksena on varmistaa, että ehdotettavan lain nojalla toimivaltaiseksi tulevilla viranomaisilla on kaikki markkinavalvonta-asetukseen perustuvat markkinavalvontalaissa säädetyt toimivaltuudet digitaalisen elementin sisältävien tuotteiden valvontaa koskevien tehtäviensä hoitamiseksi. Muilta osin markkinavalvontalakiin ei katsota tarvittavan muutoksia, koska markkinavalvonta-asetus soveltuu täysimääräisesti kyberkestävyysasetukseen, ja näin ollen myös markkinavalvontalaki soveltuu täysimääräisesti, kun sovelletaan kyberkestävyysasetusta ja sen toimeenpanemiseksi ehdotettavaa lakia. Jäljempänä esitetysti markkinavalvontalain sääntelystä on kuitenkin tarpeen eräiltä osin poiketa ja täydentää sitä.

Markkinavalvonta-asetuksen 10 artiklan 3 kohdassa tarkoitetusta yhteyspisteestä säädetään markkinavalvontalain 4 a §:ssä, ja tehtävässä toimii Turvallisuus- ja kemikaalivirasto. Turvallisuus- ja kemikaalivirasto toimisi markkinavalvonnan yhteyspisteenä myös kyberkestävyysasetuksen osalta, sillä yhteyspisteitä voidaan nimetä vain yksi. Tukesissa yhteyspisteen tehtävä on sijoitettu tuoteyksikön Fipoint-ryhmään. Yhteyspisteen tehtävien hoidossa Fipoint toimii puolueettomasti suhteessa kaikkiin markkinavalvontaviranomaisiin ja Tulliin. Markkinavalvonta-asetuksen 10 artiklan mukaisesti yhteyspiste vastaa markkinavalvontaviranomaisten ja Tullin yhteensovitetun kannan esittämisestä sekä kansallisesta markkinavalvontastrategiasta ilmoittamisesta ICSMS-järjestelmässä. Markkinavalvonta-asetuksessa säädettyjen tehtävien lisäksi yhteyspisteelle on annettu tehtäviä markkinavalvontalain 4 a §:ssä. Markkinavalvontalain mukaan Suomen yhteyspiste koordinoi markkinavalvontaan liittyvää viranomaisyhteistyötä ja auttaa markkinavalvontaviranomaisia kansallisessa ja kansainvälisessä yhteistyössä. Lisäksi yhteyspisteen tehtäviin kuuluu laatia kansallinen markkinavalvontastrategia yhteistyössä markkinavalvonnan yhteistyöryhmän kanssa.

Esityksen valmistelussa ei ole tunnistettu olemassa olevaa viranomaista, jonka olemassa olevien tehtävien yhteyteen kyberkestävyysasetuksen markkinavalvonta olisi erityisen luontevaa ehdottaa lisättäväksi. Sopivia viranomaisia markkinavalvontatehtävään olisivat Turvallisuus- ja

kemikaalivirasto, jolla on nykyisin useita markkinavalvontaan liittyviä tehtäviä, sekä Liikenne- ja viestintävirasto, jonka vastuulla on jo entuudestaan useita kyberturvallisuutta koskevia viranomaistehtäviä. Liikenne- ja viestintävirasto vastaa lisäksi useiden tuoteryhmien markkinavalvontatehtävistä, joista säädetään muun muassa ilmailulaissa (864/2014), ajoneuvolaissa (82/2021), huviveneiden turvallisuudesta ja päästövaatimuksista annetussa laissa (1712/2015) sekä sähköisen viestinnän palveluista annetussa laissa (917/2014). Jäljempänä jaksossa 5.1.1 arvioidaan vaihtoehtoja markkinavalvonnan järjestämisestä.

Suuririskisten tekoälyjärjestelmien valvonnasta on ehdotettu säädettäväksi eräiden tekoälyjärjestelmien valvonnasta annetussa laissa (HE 46/2025 vp). Mainittua lakia valvovat viranomaiset toimisivat suuririskisten tekoälyjärjestelmien osalta myös kyberkestävyysasetuksen vaatimuksien valvojina EU:n tekoälyasetuksen ja kyberkestävyysasetuksen välisestä yhteydestä johtuen, kuten jaksossa 2.1.6 kuvataan. Kyberkestävyysasetuksen mukaisina markkinavalvontaviranomaisina toimisi näin ollen joka tapauksessa useampi viranomaisia sen johdosta, että valvonta on osin hajautettu tekoälyasetuksen valvontaan toimivaltaisille viranomaisille. Markkinavalvontaviranomaisten velvollisuuteen tehdä yhteistyötä myös kyberkestävyysasetuksen valvonnassa tulisi sovellettavaksi nykyisestä sääntelystä markkinavalvonta-asetuksen 22 artiklan 1 kohta, markkinavalvontalain 4 a ja 4 b §:t sekä hallintolain 10 §. Markkinavalvontalaissa säädetään muun muassa kansallisen markkinavalvontastrategian laatimisesta. Strategiaa olisi tarvittaessa päivitettävä niin, että siinä otetaan huomioon kyberkestävyysasetuksen uuden tyyppiset vaatimukset. Markkinavalvontalain 7 §:ssä säädetään lisäksi markkinavalvontaviranomaisen velvollisuudesta laatia valvontasuunnitelma.

Kyberkestävyysasetuksen valvonnassa olisi perusteltua pyrkiä siihen, että kyberkestävyysasetuksen vaatimuksien valvonta olisi mahdollisimman yhdenmukaista markkinavalvontaviranomaisesta riippumatta. Valvonnassa olisi siten kiinnitettävä huomiota markkinavalvontaviranomaisten yhteistyöhön. Liikenne- ja viestintäviraston keskeinen rooli ja asiantuntemus huomioon ottaen voisi olla tarpeen säätää sen mahdollisuudesta antaa asiantuntijatukea muille kyberkestävyysasetuksen markkinavalvontaviranomaisille erityisesti, mikäli niiden markkinavalvontatehtävä on laajuudeltaan rajattu.

Markkinavalvonnan toimivaltuudet

Markkinavalvontaviranomaisten valvontatoimivaltuuksista ja tiedonsaantioikeuksista säädetään markkinavalvontalain 3 luvussa. Toimivaltuuksiin sisältyvät esimerkiksi oikeus saada tietoja, oikeus ottaa tuotteita tutkittavaksi ja oikeus asettaa kieltoja sekä tarpeen vaatiessa oikeus määrätä tuote hävitettäväksi.

Lain 8 §:ssä säädetään viranomaisen oikeudesta saada tietoja talouden toimijalta. Pykälän mukaan markkinavalvontaviranomaisella ja Tullilla on oikeus saada valvontaa varten välttämättömät tiedot, joihin voivat kuulua myös markkinavalvonta-asetuksen 14 artiklan 4 kohdan a ja b alakohdassa tarkoitetut tiedot. Tiedonsaantioikeus koskee myös sellaisia valvonnan kannalta välttämättömiä tietoja, jotka yksityistä liike- tai ammattitoimintaa, yksityisen taloudellista asemaa tai terveydentilaa koskevina taikka muutoin ovat viranomaisen hallussa ollessaan salassa pidettäviä viranomaisten toiminnan julkisuudesta annetun lain (621/1999) nojalla. Pykälän 2 momentin mukaan tiedonsaantioikeus koskee myös sellaisia valvonnan kannalta välttämättömiä tietoja, joita tarvitaan verkkorajapintojen omistajien varmentamiseen.

Markkinavalvontalain 9 §:ssä säädetään viranomaisen oikeudesta tehdä tarkastuksia. Markkinavalvontaviranomaisella on oikeus valvontaa varten päästä kaikkiin tiloihin, joissa

harjoitetaan markkinavalvontalain 1 §:n 1 momentissa mainituissa laeissa tarkoitettua toimintaa tai säilytetään valvonnan kannalta merkityksellisiä tietoja, ja tehdä valvonnassa tarvittavia tarkastuksia. Pysyväisluonteiseen asumiseen käytettäviin tiloihin tarkastuksia ei kuitenkaan pääsääntöisesti saa ulottaa. Tarkastuksissa noudatetaan, mitä hallintolain (434/2003) 39 §:ssä säädetään.

Markkinavalvontalain säännöksistä olisi tarpeen poiketa eräiltä osin. Markkinavalvontalaki on luonteeltaan yleislaki, josta on sen 1 §:n mukaisesti mahdollista poiketa tuotekohtaisissa laeissa.

Markkinavalvontalaista poiketen olisi tarpeen säätää tarkastuksen ulottamisesta pysyväisluonteiseen asumiseen käytettäviin tiloihin. Markkinavalvontalaki ei mahdollista tarkastusten ulottamista pysyväisluonteiseen asumiseen käytettäviin tiloihin, sillä sen 9 §:n 2 momentin mukaan markkinavalvontaviranomaisen oikeudesta ulottaa tarkastus pysyväisluonteiseen asumiseen käytettäviin tiloihin säädetään tarvittaessa erikseen. Toimivaltuus olisi valvonnan toteuttamiseksi tarpeen, sillä kyberkestävyysasetuksen alaan kuuluvaa elinkeinotoimintaa voidaan tavanomaisesti harjoittaa myös kotirauhan piiriin kuuluvissa tiloissa erityisesti ohjelmistotoimialalla. Tiloihin olisi markkinavalvonta-asetuksen mukaisesti kyettävä kohdistamaan tarkastuksia.

Lisäksi markkinavalvontalain 10 §:ssä säädetään markkinavalvontaviranomaisen oikeudesta ottaa tuotteita tutkittavaksi, jos se on tuotteen vaatimustenmukaisuuden valvonnan kannalta tarpeellista. Tuotteen ottamisesta olisi suoritettava korvaus, mikä perustuu esineen menetyksestä talouden toimijalle aiheutuvaan vahinkoon. Säännöstä voidaan soveltaa myös kyberkestävyysasetuksen käsittämiin ohjelmistotuotteisiin, jotka ovat tavanomaisesti aineettomia ja eivät aiheuta vastaavaa vahinkoa talouden toimijalle.

Markkinavalvontalain tiedonvaihtoa koskevia säännöksiä olisi myös tarve täydentää erityisesti kyberkestävyysasetuksen sisältämien ilmoitusvelvollisuuksien mukaisten tietojen käsittelemiseksi. Lisäksi kyberkestävyysasetuksen 52 ja 54 artiklassa säädetään tietojenvaihdosta ja muusta mahdollisesti salassa pidettävän tiedon luovuttamista edellyttävästä yhteistyöstä markkinavalvontaviranomaisten sekä kansallisten kyberturvallisuuden sertifiointiviranomaisten kanssa, CSIRT-yksiköiden ja ENISA:n kanssa, tietosuojaviranomaisten kanssa, komission kanssa sekä NIS 2 -direktiiviä valvoville toimivaltaisten viranomaisten kanssa samoin kuin muiden jäsenvaltioiden ja muiden markkinavalvontaviranomaisten kanssa.

Markkinavalvontalain 11 §:n mukaan markkinavalvontaviranomaisella ja Tullilla on oikeus salassapitosäännösten ja muiden tiedonsaantia koskevien rajoitusten estämättä luovuttaa valvonnan kannalta välttämättömiä tietoja toisilleen ja saada niitä muilta valvontaviranomaisilta. Lisäksi markkinavalvontalain 13 §:ssä säädetään markkinavalvontaviranomaisen oikeudesta luovuttaa tietoja yksityisen ja yhteisön taloudellisesta asemasta, liikesalaisuudesta sekä yksityisen henkilökohtaisista oloista eräille kotimaisille viranomaisille sekä ulkomaisille viranomaisille ja kansanvälisille toimielimille Euroopan unionin säädökseen tai Suomea sitovaan kansainväliseen sopimukseen perustuvan velvoitteen toteuttamiseksi. Näitä säännöksiä on tarpeen täydentää säätämällä oikeudesta luovuttaa tietoja myös sellaisille viranomaisille, joita ei mainita markkinavalvontalaissa mutta joiden kanssa markkinavalvontaviranomaisen olisi tehtävä yhteistyötä. Lisäksi luovutettavien tietojen piiriä on pidettävä liian suppeana ottaen huomioon kyberkestävyysasetuksen kohde. Näin ollen on markkinavalvontalaissa säädetyn tiedonluovutusoikeuden piiriä olisi laajennettava näihin tietoihin.

Sähköisen viestinnän palveluista annetun lain 318 §:n 2 momentissa (laissa 703/2025, voimaan 1.1.2026) säädetään Liikenne- ja viestintäviraston oikeudesta luovuttaa salassa pidettäviä tietoja Energiavirastolle, Finanssivalvonnalle, Lupa- ja valvontavirastolle sekä elinvoimakeskukselle, jos se on näille säädettyjen tietoturvallisuuteen liittyvien tehtävien hoitamiseksi välttämätöntä. Säännöstä sovelletaan myös sellaisiin Liikenne- ja viestintäviraston tehtäviin, joista säädetään muussa laissa kuin viestintäpalvelulaissa. Markkinavalvontaviranomaisen olisi tehtävä näiden viranomaisten kanssa tarvittaessa yhteistyötä niille kuuluvien NIS 2 -direktiivin mukaisen toimivaltaisen viranomaisen tehtävien johdosta. Koska säännös koskee vain Liikenne- ja viestintäviraston tiedonluovutusoikeutta, on olemassa olevaa sääntelyä tarpeen täydentää niin, että otetaan huomioon myös tilanteet, joissa markkinavalvontaviranomaisena toimii poikkeuksellisesti tekoälyasetusta valvova viranomainen.

Kyberkestävyysasetuksen 52 artiklan 7 kohdan toisen alakohdan mukaan unionin tietosuojalainsäädäntöä valvovilla viranomaisilla on oltava valtuudet pyynnöstä tutustua kaikkiin tämän asetuksen nojalla laadittuihin tai ylläpidettyihin asiakirjoihin, jos mahdollisuus tutustua kyseisiin asiakirjoihin on tarpeen niiden tehtävien hoitamiseksi. Niiden on ilmoitettava tällaisesta pyynnöstä asianomaisen jäsenvaltion nimetyille markkinavalvontaviranomaisille, mikä koskee etenkin tilanteita, joissa tietoja pyydetään suoraan valmistajalta tai ilmoitetulta laitokselta. Asiakirja, kuten haavoittuvuus- tai poikkeamailmoitus, voi olla kuitenkin myös markkinavalvontaviranomaisen hallussa. Suomessa tietosuojavaltuutetun tiedonsaantioikeudesta säädetään tietosuojalain 18 §:ssä. Sen mukaan tietosuojavaltuutetulla on oikeus salassapitosäännösten estämättä saada maksutta tehtäviensä hoidon kannalta tarpeelliset tiedot. Kyberkestävyysasetus ei siten edellytä tältä osin uutta kansallista lainsäädäntöä, koska tietosuojavaltuutetulla on tietosuojalain nojalla oikeus saada tieto yksityisen taikka viranomaisen salassa pidettävästä asiakirjasta myös kyberkestävyysasetuksen alalla.

Kyberkestävyysasetuksen 52 artiklan 13 kohdan mukaan markkinavalvontaviranomaisten on raportoitava vuosittain komissiolle asiaankuuluvien markkinavalvontatoimien tuloksista. Kyberkestävyysasetuksen 54 artiklan 3 ja 5–8 kohdassa taas säädetään markkinavalvontaviranomaisen ilmoituksista komissiolle ja muille jäsenvaltioille eräissä tapauksissa, joissa digitaalisia elementtejä sisältävän tuotteen voidaan perustellusti arvioida aiheuttavan merkittävän kyberturvallisuusriskin muiden kuin teknisten riskitekijöiden vuoksi ja vaatimustenvastaisuus ei rajoitu kansalliselle alueelle. Ilmoitukset voivat sisältää salassa pidettäviä tietoja. Markkinavalvontalain 13 §:n 3 kohta mahdollistaisi tähän liittyvän tiedonvaihdon, sillä sen 3 kohdassa säädetään tietojen luovuttamisesta muun ohella toimivaltaiselle ulkomaan viranomaiselle ja kansainväliselle toimielimelle Euroopan unionin säädökseen perustuvan velvoitteen toteuttamiseksi.

Markkinavalvontalain 17 § mahdollistaa toimenpidemääräyksen antamisen talouden toimijalle, jos tuote tai tuotetta koskevat menettelyt eivät ole vaatimusten mukaiset tai jos tuote aiheuttaa siinä määritellyn riskin. Toimenpidemääräys olisi mahdollista antaa myös tilanteissa, joissa valmistaja ei noudata kyberkestävyysasetuksen 14 artiklan mukaisia raportointivelvoitteita.

Markkinavalvontaviranomainen vastaisi myös avoimen lähdekoodin ohjelmistovastaavien velvollisuuksien valvonnasta kyberkestävyysasetuksen 52 artiklan 3 kohdan nojalla. Jos markkinavalvontaviranomainen toteaa, että avoimen lähdekoodin ohjelmistovastaava ei noudata mainitussa artiklassa säädettyjä velvollisuuksia, sen on vaadittava avoimen lähdekoodin ohjelmistovastaavaa varmistamaan, että kaikki asianmukaiset korjaavat toimenpiteet toteutetaan. Avoimen lähdekoodin ohjelmistovastaavien on varmistettava, että kaikki asianmukaiset korjaavat toimenpiteet toteutetaan niiden tämän asetuksen mukaisten velvollisuuksien noudattamiseksi.

Kyberkestävyysasetuksen mukaisesti avoimen lähdekoodin ohjelmistovastaaviin sovelletaan valmistajiin nähden kevennettyjä vaatimuksia, joihin kuuluu yhteistyövelvoite ja velvoite ottaa käyttöön kyberturvallisuusperiaatteet sekä raportoida poikkeamista ja haavoittuvuuksista (ks. luku 2.1.3.3). Avoimen lähdekoodin ohjelmistovastaavan ei kuitenkaan katsota asettavan ohjelmistotuotetta saataville markkinoilla (kyberkestävyysasetuksen johdanto-osan 19 kohta). Kun mahdollisuus antaa toimenpidemääräys markkinavalvontalain 17 §:n nojalla tällaisessa tilanteessa ei ole yksiselitteinen ja kun näihin toimijoihin on tarkoitus soveltaa muuhun kyberkestävyyden valvontaan nähden erityistä sääntelyjärjestelmää, on ehdotukseen perusteltua ottaa selkeyttävät säännökset mahdollisuudesta antaa velvoittava määräys korjaavien toimenpiteiden toteuttamiseksi, jota voitaisiin tehostaa uhkasakolla.

Markkinavalvontalain 28 § mahdollistaa uhkasakon asettamisen markkinavalvontaviranomaisen antaman kiellon tai määräyksen tehosteeksi. Kyberkestävyysasetuksen johdanto-osan 120 kohdan mukaan jäsenvaltiot eivät saisi määrätä mikroyrityksille tai pienille yrityksille eikä avoimen lähdekoodin ohjelmistovastaaville muunlaisiakaan rahallisia seuraamuksia, kun niille ei asetuksen mukaan määrätä hallinnollisia sakkoja. Valmistelussa on arvioitu, ettei tämä kuitenkaan tarkoita uhkasakkoa, joka ei ole luonteeltaan rangaistusluonteinen seuraamus vaan hallintopakon keino, jolla varmistetaan varsinaisen päävelvoitteen noudattaminen.

Kuvaus markkinavalvontalain sisältämistä muista toimivaltuuksista sisältyy esimerkiksi hallituksen esitykseen eduskunnalle EU:n tekoälyasetusta täydentäväksi lainsäädännöksi, HE 46/2025 vp, luku 3.2.

3.1.3 Ilmoitettujen laitosten hyväksyminen, nimeäminen ja valvonta

Eräitä tuoteryhmiä koskevista ilmoitetuista laitoksista annettu laki

Ilmoitetuilla laitoksilla tarkoitetaan yleisesti vaatimustenmukaisuuden arviointilaitoksia, jotka on hyväksytty ja nimetty hoitamaan EU:n tuotesäädöksiin perustuvia vaatimustenmukaisuuden arviointitehtäviä. Ilmoitettu laitos on jäsenvaltion komissiolle ilmoittama toimija, jolla on lupa suorittaa vaatimustenmukaisuuden arviointitehtäviä. Tässä luvussa käsitellään ilmoitettujen laitoksien nykytilaa kyberkestävyysasetuksen kannalta. Kyberturvallisuusasetuksessa tarkoitettuja tehtäviä hoitavia vaatimustenmukaisuuden arviointilaitoksia käsitellään jäljempänä luvussa 3.2.4.

Ilmoitettujen laitosten hyväksymisestä, nimeämisestä ja valvonnasta säädetään kutakin tuoteryhmää koskevassa laissa. Tuotesääntelyä on useamman eri ministeriön hallinnonalalla.

Useiden tuoteryhmien osalta ilmoitetuista laitoksista säädetään eräitä tuoteryhmiä koskevista ilmoitetuista laitoksista annetussa laissa (278/2016), joka tuli voimaan 27.4.2016. Lailla pantiin täytäntöön yhdeksän Euroopan parlamentin ja neuvoston hyväksymää tuotekohtaista direktiiviä (ns. *Alignment Package*), joissa asetetaan yhdenmukaiset säännöt tuotteiden vaatimustenmukaisuuden arviointilaitosten hyväksymisestä niin sanotuiksi ilmoitetuiksi laitoksiksi. Laki on horisontaalinen, ja siinä säädetään ilmoitetuksi laitokseksi hyväksymistä koskevasta hakemuksesta, toimivaltaisista viranomaisista sekä kansallisesta hyväksymis- ja ilmoitusmenettelystä. Lisäksi laki sisältää säännökset muun muassa ilmoitetun laitoksen yleisistä vaatimuksista, laitoksen toimintaa ja sen henkilöstöä koskevista vaatimuksista sekä ilmoitetun laitoksen velvollisuudesta osallistua standardointi- ja koordinaatiotyöhön.

Eräitä tuoteryhmiä koskevista ilmoitetuista laitoksista annettua lakia sovellettiin sen voimaantullessa aluksi seuraaviin tuotelakeihin: hissiturvallisuuslaki (1134/2016),

mittauslaitelaki (707/2011), painelaitelaki (1144/2016), laki pyroteknisten tuotteiden vaatimustenmukaisuudesta (180/2015), laki räjähdysvaarallisissa tiloissa käytettäviksi tarkoitettujen laitteiden ja suojausjärjestelmien vaatimustenmukaisuudesta (1139/2015), laki räjähteiden vaatimustenmukaisuudesta (1140/2016) ja sähköturvallisuuslaki (1135/2016). Myöhemmin lain soveltamisalaa on laajennettu myös muihin tuotelakeihin, kuten kaasulaitelakiin (502/2018), ilmailulakiin (864/2014) ja sähköisen viestinnän palveluista annettuun lain 30 lukuun (917/2014). Muiden kuin lain soveltamisalaan kuuluvien tuoteryhmien osalta ilmoitettuja laitoksia koskeva sääntely perustuu edelleen kyseistä tuoteryhmää koskevaan tuotelakiin.

Ilmoitetun laitoksen hyväksymistä ja nimeämistä koskevaan hakemukseen liitetään pääsääntöisesti kansallisen akkreditointielimen antama akkreditointitodistus. Suomessa kansallisena akkreditointielimenä toimii Turvallisuus- ja kemikaalivirastosta annetun lain (1261/2010) 2 a §:n nojalla Turvallisuus- ja kemikaaliviraston akkreditointiyksikkö (FINAS-akkreditointipalvelu). Akkreditointiyksikön akkreditointiin ja siihen rinnastettavaan pätevyyden arviointiin sovelletaan vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta annettua lakia (920/2005) riippumatta siitä, sovelletaanko tuoteryhmään eräistä tuoteryhmiä koskevista ilmoitetuista laitoksista annettua lakia vai muuta, tuotekohtaista säädöstä.

Kyberkestävyysasetus on säädöksenä uusi. Voimassa ei ole sen soveltamisalaa koskevia päällekkäisiä säännöksiä, jotka koskisivat ilmoitettuja laitoksia. Kyberkestävyysasetuksen 36 artiklassa edellytetään jäsenvaltioita nimeämään arviointilaitosten ilmoittamisesta vastaava viranomainen, jonka vastuulla on laatia ja toteuttaa tarvittavat menettelyt, jotka liittyvät arviointilaitosten hyväksymiseen, nimeämiseen ja ilmoittamiseen sekä ilmoitettujen laitosten valvontaan.

Kansallisesta päällekkäisestä sääntelystä olisi pidättäydyttävä, koska kyberkestävyysasetuksen IV luku sisältää yksityiskohtaiset ja suoraan sovellettavat vaatimustenmukaisuuden arviointilaitosten ilmoittamista koskevat säännökset. Tästä syystä kyberkestävyysasetuksen soveltamisalaan kuuluvia tuoteryhmiä koskevia ilmoitettuja laitoksia ei olisi tarpeen saattaa eräitä tuoteryhmiä koskevista ilmoitetuista laitoksista annetun lain soveltamisalaan. Siltä osin kuin kyberkestävyysasetuksen soveltaminen sitä edellyttää, ilmoitettuja laitoksia koskevia säännöksiä voitaisiin sisällyttää muuhun lakiin.

Arviointi- ja arviointilaitoslait

Tietoturvallisuuden tason arviointia koskee kansallisesti myös tietoturvallisuuden arviointilaitoksista annettu laki (1405/2011, arviointilaitoslaki) ja laki viranomaisten tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011, arviointilaki). Arviointilaitoslakia sovelletaan tietoturvallisuuden arviointipalveluita julkishallinnolle tarjoaviin organisaatioihin, jotka toimeksiannosta arvioivat tietoturvallisuustasoa ja hakevat Liikenne- ja viestintävirastolta hyväksyntää tälle toiminnalle. Lain nojalla on annettu 12 päätöstä neljälle eri yritykselle tietoturvallisuuden arviointilaitoksen hyväksymisestä eri pätevyysalueille.[1] Tietojärjestelmien vaatimustenmukaisuuden arvioinnin ajantasaistamisen ja tehostamisen työryhmässä (VN/36127/2023) on laadittu nykytila-arvio tietojärjestelmien

[1] Lähde: Liikenne- ja viestintävirasto Traficom, Kyberturvallisuuskeskus. Viitattu 31.7.2023. (https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/arviointi-hyvaksynta-ja-neuvonta/hyvaksytyt-tietoturvallisuuden-arviointilaitokset)

tietoturvallisuuden ja varautumisen vaatimustenmukaisuuden arvioinnista. Sen kanssa yhtenevästi hallituksen esityksen valmistelussa on arvioitu, ettei kyberkestävyysasetuksen ja kyberturvallisuusasetuksen osalta ole päällekkäisyyttä suhteessa näihin kansallisiin säädöksiin. Koska säädösten tavoite ja tarkoitus on eri, arviointi- ja arviointilaitoslakien mukaisten menettelyiden hyödyntäminen kyberkestävyysasetuksen vaatimustenmukaisuuden arviointiin edellyttäisi merkittäviä muutoksia mainittuihin lakeihin sekä nykytilassa niiden nojalla tapahtuvaan arviointitoimintaan.

Viranomaisten tietojärjestelmien tietoturvallisuuden ja varautumisen kansallinen arviointisääntely kohdistuu viranomaisen määräämisvallassa olevan tai hankittavaksi suunnitteleman tietojärjestelmän tai tietoliikennejärjestelyn tietoturvallisuuden ja varautumisen tapauskohtaiseen arviointiin, ei siis markkinoilla yleisesti tarjottavien tuotteiden, palveluiden tai prosessien vaatimuksiin. Arviointilaitoslain mukaiset arvioinnin kohdealueet ja arvioinnin tuloksen tarkoitus eroavat EU:n sertifiointisäänteystä. Tästä erillinen asia on, että FINAS-akkreditointipalvelun myöntämä akkreditointi voi olla edellytyksenä sekä EU:n että kansallisen sääntelyn mukaiselle arviointitoiminnalle. Arviointi- ja arviointilaitoslakien mukainen toiminta olisi kyberkestävyysasetuksen 2(7) artiklan nojalla tulkittavissa sen soveltamisalan ulkopuolelle kuuluvaksi.

3.1.4 Haavoittuvuuskoordinaatio

Liikenne- ja viestintäviraston Kyberturvallisuuskeskus toteuttaa nykyisin haavoittuvuuskoordinaatiota osana sille säädettyjä tehtäviä. Haavoittuvuuskoordinaatiolla tarkoitetaan toimintaa, jossa tehtävänä on varmistaa, että tieto havaitusta haavoittuvuudesta tai muusta vakavasta ohjelmistovirheestä päätyy ohjelmiston valmistajalle. Haavoittuvuuskoordinaation toteuttaminen perustuu vapaaehtoisiin ilmoituksiin ohjelmistojen haavoittuvuuksista sekä Kyberturvallisuuskeskuksen tehtäviin selvittää verkkopalveluihin ja tietojärjestelmiin kohdistuvia uhkia.

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen CSIRT-yksikön nykyisen haavoittuvuuskoordinaation tehtävänä on avustaa haavoittuvuuden löytäjää tekemään yhteistyötä ohjelmistovalmistajien kanssa haavoittuvuuden korjaamiseksi. Tavoitteena on siis varmistaa, että tieto haavoittuvuudesta ja sen asianmukaisesta korjauksesta päätyy kaikille relevanteille osapuolille eli myös tuotteen loppukäyttäjille.

Koordinaatioprosessi alkaa yleensä, kun haavoittuvuus raportoidaan Kyberturvallisuuskeskukselle. Ilmoituksen voi tehdä esimerkiksi organisaation nimissä, henkilökohtaisesti tai nimettömästi. Ilmoituksen jälkeen Kyberturvallisuuskeskus analysoi ilmoitetun haavoittuvuuden ja varmistaa tarvittavat tekniset yksityiskohdat ilmoittajan kanssa. Tämän jälkeen Kyberturvallisuuskeskus ottaa yhteydessä laitevalmistajaan tai palveluntarjoajaan, ja sopii haavoittuvuuden korjauksen tavoiteaikatauluista ja haavoittuvuudesta tiedottamisesta. Koordinoinnissa on erityisen tärkeää varmistaa tiedon vastuullinen käsittely kaikkien osapuolten kesken. Kun korjaus on valmis, sovitaan kaikkien osapuolten kanssa haavoittuvuuden julkaisutavasta ja aikatauluista.

Vuonna 2024 Kyberturvallisuuskeskukselle ilmoitettiin 489 haavoittuvuutta. Sen lisäksi Kyberturvallisuuskeskus otti vuoden 2024 aikana ennaltaehkäisevästi yhteyttä yli tuhannen haavoittuvan VPN-laitteen omistajaorganisaatioihin sekä julkaisi yhteensä 26 haavoittuvuustiedotetta.

Suomessa ei ole nykyisin voimassa horisontaalista sääntelyä, jolla velvoitettaisiin ilmoittamaan viranomaiselle ohjelmiston haavoittuvuuksista. Kyberturvallisuuskeskuksen vastaanottamat haavoittuvuusilmoitukset perustuvat vapaaehtoisuuteen ja yhteistyöhön sidosryhmien kanssa.

Kyberkestävyysasetuksella asetetaan CSIRT-yksikölle velvoite käsitellä ja ilmoittaa muiden maiden CSIRT-yksiköille kyberkestävyysasetuksen nojalla tehdyistä pakollisista ja vapaaehtoisista haavoittuvuushavainnoista. Tämä tulee vaikuttamaan CSIRT-yksikön nykyiseen haavoittuvuuskoordinaatioon sen käytännön järjestämisen kannalta. Kyberkestävyysasetus ei kuitenkaan edellytä muutoksia voimassa olevaan lainsäädäntöön nykyisin toteutetun haavoittuvuuskoordinaation osalta. Kyberkestävyysasetus edellyttää täydentävää sääntelyä sen mukaisen haavoittuvuuskoordinaation toteuttamiseksi.

Selvyyden vuoksi todetaan, että jatkossakin CSIRT-yksikön eli Kyberturvallisuuskeskuksen olisi voitava ottaa vastaan vapaaehtoisuuteen ja sidosryhmäyhteistyöhön perustuvia haavoittuvuusilmoituksia. Jatkossa CSIRT-yksikkö vastaanottaisi siis sekä kyberkestävyysasetuksessa tarkoitettuja ilmoituksia että myös muita kuin kyberkestävyysasetuksessa tarkoitettuja vapaaehtoisia haavoittuvuusilmoituksia osana sen olemassa olevien kyberturvallisuuslain mukaisten tehtävien hoitamista. CSIRT-yksikön kyberturvallisuuslain 22 §:n mukainen haavoittuvuuskoordinaatiotehtävä kattaisi kyberkestävyysasetuksen soveltamisalan ulkopuolelle jäävien tuotteiden ja palvelujen sisältämiä haavoittuvuusilmoituksia sekä organisaatioiden toimintaan liittyviä haavoittuvuusilmoituksia. Näin ollen sen jälkeen, kun kyberkestävyysasetuksen haavoittuvuusilmoituksia koskevia säännöksiä sovelletaan, CSIRT-yksikkö vastaanottaisi haavoittuvuusilmoituksia, jotka voidaan jakaa kolmeen luokkaan seuraavasti:

1) kyberkestävyysasetuksen 14 artiklan mukaiset pakolliset haavoittuvuusilmoitukset;

2) kyberkestävyysasetuksen 15 artiklan mukaiset vapaaehtoiset haavoittuvuusilmoitukset; ja

3) muut vapaaehtoiset haavoittuvuusilmoitukset.

Kyberkestävyysasetuksen 16 ja 17 artiklassa säädetään eräistä CSIRT-yksikön velvollisuuksista, jotka voivat edellyttää julkisuuslaissa salassa pidettäväksi säädettyjen tietojen luovuttamista. Näistä tilanteista olisi tarpeen säätää erikseen.

Kyberkestävyysasetuksen 15 artiklan 4 kohdassa säädetään tilanteesta, jossa muu taho kuin valmistaja ilmoittaa aktiivisesti hyödynnetystä haavoittuvuudesta tai digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavasta vakavasta poikkeamasta. Koordinaattoriksi nimetyn CSIRT-yksikön on tällöin ilman aiheetonta viivytystä ilmoitettava asiasta valmistajalle. Valmistajaan sovellettaisiin tällöin julkisuuslain asianosaisen tiedonsaantioikeutta koskevia säännöksiä. Asianosaisella on tietyin rajoituksin oikeus saada asiaa käsittelevältä tai käsitelleeltä viranomaiselta tieto muunkin kuin julkisen asiakirjan sisällöstä, joka voi tai on voinut vaikuttaa hänen asiansa käsittelyyn. Tästä syystä tietojen luovuttamiseksi tältä osin ei tarvittaisi uutta sääntelyä.

Kyberkestävyysasetuksen 15 artiklan 5 kohdan mukaan koordinaattoriksi nimettyjen CSIRT-yksikköjen ja ENISA:n on varmistettava ilmoituksen tehneen luonnollisen henkilön tai oikeushenkilön toimittamien tietojen luottamuksellisuus ja asianmukainen suoja. Julkisuuslain säännösten voidaan katsoa varmistavan CSIRT-yksikön osalta kyseisten tietojen salassapidon niiltä osin kuin se on perusteltua. Salassapito voidaan perustaa joko julkisuuslain 24 §:n 7 kohtaan, jonka mukaan tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevat ja niiden

toteuttamiseen vaikuttavat asiakirjat on pidettävä salassa, 15 kohdassa säädettyyn valvontasalaisuuteen tai 20 kohdassa säädettyyn liikesalaisuuksien ja muiden elinkeinosalaisuuksien salassapitoon.

3.1.5 Tietoturvamerkki

Liikenne- ja viestintäviraston Kyberturvallisuuskeskus julkaisi Tietoturvamerkin älykkäille kuluttajalaitteille eli IoT-laitteille vuonna 2019. Tietoturvamerkki oli Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen myöntämä osoitus siitä, että merkillä varustettu tuote on jo lähtökohtaisesti suunniteltu tietoturvalliseksi ja täyttää Traficomin asettamat tietoturvavaatimukset.

Tietoturvamerkin hakeminen oli tuotteiden valmistajille vapaaehtoista. Tietoturvamerkki ei ole ollut edellytyksenä tuotteen asettamiseksi saataville markkinoilla.

Tietoturvamerkin vaatimukset perustuivat ETSI:n standardiin EN 303 645, joka on kokoelma kuluttajille suunnattujen IoT-laitteiden perustason tietoturvavaatimuksista. Tietoturvamerkin vaatimusten valinnassa kiinnitettiin erityistä huomioita käyttäjän suojaamiseen. Tuotteelta edellytettiin muun muassa tukijakson ilmoittamista, tietoturvallisen käytön ohjeistamista ja turvallisia oletusasetuksia. Tuotteelle asetettiin vaatimuksia salasanakäytäntöihin, salauksiin, haavoittuvuuksien hallintaan ja ohjelmistopäivityksiin sekä hyökkäyspinnan pienentämiseen.

Liikenne- ja viestintävirasto myönsi Tietoturvamerkin tuotteille ja palveluille, joille merkkiä haettiin vapaaehtoisesti ja jotka täyttivät tietoturvavaatimukset sekä läpäisivät kolmannen osapuolen tekemän tarkastuksen. Sidosryhmät arvostivat kolmannen osapuolen tarkastusta tärkeäksi verrattuna itsearvioinnin antamaan varmuuteen tuotteen kyberturvallisuusominaisuuksista. Säännöllisisillä vuosikatselmoinneilla varmistettiin tuotteen kyberturvallisuusominaisuuksien ajantasaisuus muuttuvassa uhkaympäristössä.

Tietoturvamerkki myönnettiin yhteensä 27 kuluttajalaitteelle. Tietoturvamerkkiä haettiin useammalle tuotteelle, mutta noin 40 % hakemuksista jäi ilman lopullista merkintää tuotteessa ilmenneiden puutteiden vuoksi. Tulokset osoittivat, että valmistajan kypsyys tuotteiden kyberturvallisuuden toteuttamisessa vaihtelee. Haasteita aiheuttavat pitkät toimitusketjut, sidosryhmien suuri määrä sekä komponenttien ja ekosysteemien lisääntynyt integraatio.

Liikenne- ja viestintävirasto on lopettanut uusien tietoturvamerkkien myöntämisen. Päätöksen taustalla on muun ohella kyberkestävyysasetuksen ja radiolaitedirektiivin voimaantulo, koska uusi EU-sääntely tuo vastaavia tietoturvavaatimuksia tulevaisuudessa velvoittavaksi kaikille verkkoon liitettäville laitteille. Liikenne- ja viestintävirasto ei aio jatkaa nykyisten tietoturvamerkkien voimassaoloa radiolaitedirektiivin tullessa voimaan 1.8.2025.

3.1.6 Sääntelyn testiympäristö

Suomessa ei ole toteutettu kyberkestävyysasetuksessa tarkoitettuja sääntelyn testiympäristöjä. Muissa EU-jäsenvaltioissa sääntelyn testiympäristöjen tärkeimpiä sovellusalueita ovat olleet rahoituspalvelut (*fintech*), energia ja liikenne.

Kyberkestävyysasetuksen kaltaista sääntelyä sääntelyn testiympäristöstä sisältyy myös EU:n tekoälyasetukseen. Tekoälyasetuksessa säädetään kyberkestävyysasetusta yksityiskohtaisemmin sääntelyn testiympäristöjen käytöstä tekoälyasetuksen soveltamisalaan kuuluville tuotteille.

Lisäksi eräissä muissa viime aikoina annetuissa EU-säädöksissä on säädetty sääntelyn testiympäristöjen perustamisesta. Kyseisten säädösten mukaisten testiympäristöjen perustamisen ja toiminnan yksityiskohdat poikkeavat jonkin verran toisistaan. Esimerkiksi Euroopan parlamentin ja neuvoston asetuksessa (EU) 2024/1735 Euroopan nettonollateknologiatuotteiden valmistusekosysteemiä vahvistavasta toimenpidekehyksestä ja asetuksen (EU) 2018/1724 muuttamisesta (ns. nettonolla-asetus) mahdollistetaan se, että jäsenvaltiot voivat vapaaehtoisesti perustaa nettonollateknologioita koskevia sääntelyn testiympäristöjä. Nettonolla-asetuksen kansallisessa täytäntöönpanossa ei toistaiseksi olla päädytty perustamaan sääntelyn testiympäristöä Suomeen.

3.1.7 Edustajakanteet

Kyberkestävyysasetuksen 65 artiklan nojalla edustajakannedirektiiviä (EU) 2020/1828 sovelletaan edustajakanteisiin, jotka on nostettu talouden toimijoita vastaan johtuen kyberkestävyysasetuksen rikkomisista, jotka vahingoittavat tai voivat vahingoittaa kuluttajien yhteisiä etuja.

Edustajakannedirektiivin mukaisista edustajakanteista säädetään kieltotoimenpiteitä koskevista edustajakanteista annetussa laissa (1101/2022) sekä ryhmäkannelaissa (1103/2022). Edustajakanteella voidaan vaatia elinkeinonharjoittajan toimintatavan kieltämistä sekä hyvitystä kuluttajille aiheutuneesta vahingosta. Edustajakanteita ovat hyvitysvaatimuksia koskevat ryhmäkanteet sekä kieltotoimenpiteitä koskevat edustajakanteet.

Edustajakannedirektiiviä täytäntöönpanevien säännösten soveltaminen myös kyberkestävyysasetuksen rikkomiseen ei edellytä kansallista täydentävää sääntelyä. Kyberkestävyysasetuksen 67 artiklalla lisätään kyberkestävyysasetus edustajakannedirektiivin liitteessä I tarkoitettujen säädösten listaan. Lisäys mahdollistaa edustajakanteita koskevien kansallisten säännösten soveltamisen sellaisenaan myös kyberkestävyysasetuksen rikkomista koskeviin edustajakanteisiin. Kieltotoimenpiteitä koskevista edustajakanteista annetun lain 4 §:n 1 momentin nojalla edustajakanne voidaan panna vireille elinkeinoharjoittajaa vastaan, joka on menetellyt edustajakannedirektiivin liitteessä I mainituissa säädöksissä olevien kuluttajien yhteisiä etuja suojaavien säännösten vastaisesti. Sääntely olisi tältä osin riittävää edustajakanteiden osalta.

3.2 Kyberturvallisuusasetus

3.2.1 Kyberturvallisuussertifioinnin viranomaistehtävät

Kyberturvallisuusasetuksen mukaiset eurooppalaiset kyberturvallisuussertifikaatit ja vaatimustenmukaisuusilmoitukset tulevat arvion mukaan olemaan tärkeitä kyberkestävyysasetuksen vaatimusten täyttämisessä. Lähtökohtaisesti vapaaehtoisen kyberturvallisuussertifioinnin luonne muuttuu, kun kyberkestävyysasetus tulee voimaan. Kyberkestävyysasetuksen 27 artiklan 8 kohdan tarkoittamissa tapauksissa eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisella EU-vaatimustenmukaisuusilmoituksella tai sertifikaatilla voidaan, muiden soveltuvien menettelyjen ohella, osoittaa tuotteen olevan kyberkestävyysasetuksessa asetettujen tietoturvavaatimusten mukainen. Kyberturvallisuussertifiointien kysynnän arvioidaan lisääntyvän ennen kuin kyberkestävyysasetuksen johdosta laadittavat yhdenmukaistetut standardit ovat saatavilla. Lisäksi kyberkestävyysasetuksen 8 ja 32 artiklassa määritellään tilanteet, joissa kriittiseltä tuotteelta vaaditaan korotetun tai korkean tason kyberturvallisuussertifikaattia.

Kyberturvallisuussertifioinnin myöntävän viranomaisen tehtävistä säädetään kyberturvallisuusasetuksen 58 artiklassa. Asetuksen suomenkielisessä versiossa käytetystä käsitteestä huolimatta tehtävä kattaa myös valvontatoiminnan (ks. tarkemmin 1. lakiehdotuksen 21 §:n yksityiskohtaiset perustelut). Kyberturvallisuusasetuksen mukaisen kansallisen kyberturvallisuussertifioinnin viranomaisen tehtävien osoittamisesta Liikenne- ja viestintävirastolle säädettiin lailla 1210/2020 (hallituksen esitys eduskunnalle laiksi sähköisen viestinnän palveluista annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi HE 98/2020 vp). Tällöin otettiin sähköisen viestinnän palveluista annetun lain 304 §:ään säännös siitä, että Liikenne- ja viestintäviraston tehtävänä on toimia kyberturvallisuusasetuksen mukaisena kansallisena kyberturvallisuussertifioinnin viranomaisena. Tämä laissa säädetty tehtävä kattaa sekä kyberturvallisuussertifikaattien myöntämisen että asetuksen mukaiset valvontatehtävät, jotka on asetuksen 58 artiklan 4 kohdan mukaisesti erotettava toisistaan.

Tehtävästä säädettäessä ei kuitenkaan lakiin otettu uusia säännöksiä kansallisen kyberturvallisuussertifioinnin viranomaisen toimivaltuuksista. Käytännössä on sittemmin havaittu, että viestintäpalvelulain viranomaistoimivaltuuksia kuten tarkastuksia sekä seuraamuksia koskevat säännökset edellyttäisivät tässä suhteessa täydentämistä, sillä niitä ei voida kattavasti soveltaa kyberturvallisuusasetuksen edellyttämissä tapauksissa. Keskeisenä syynä tähän on, että viranomaisen toimivaltuudet on viestintäpalvelulaissa lähtökohtaisesti kytketty tilanteisiin, joissa on kyse tuon lain mukaisten oikeuksien tai velvollisuuksien soveltamisesta tai rikkomisesta, mistä ei suoraan sovellettavan asetuksen tapauksessa kuitenkaan olisi suoranaisesti kyse. Viestintäpalvelulakiin ei myöskään otettu säännöksiä vaatimustenmukaisuuden arviointilaitosten asemasta. Tämän takia on tarpeen täydentää kyberturvallisuusasetuksen edellyttämää täydentävää kansallista sääntelyä.

3.2.2 Valvontaan liittyvät kyberturvallisuuden sertifiointiviranomaisen toimivaltuudet

Kyberturvallisuusasetuksen 58 artiklan 8 kohdassa säädetään kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle kuuluvista valtuuksista.

Asetuksen 58 artiklan 8 kohdan a alakohdan mukaan viranomaisella tulee olla valtuus pyytää vaatimustenmukaisuuden arviointilaitoksilta, eurooppalaisen kyberturvallisuussertifikaatin haltijoilta ja EU-vaatimustenmukaisuusilmoituksen antajilta kaikki tiedot, jotka se tarvitsee tehtävänsä suorittamiseksi. Viestintäpalvelulaissa, jossa tällä hetkellä säädetään Liikenne- ja viestintäviraston tehtävästä toimia tällaisena viranomaisena, ei kuitenkaan ole tällä hetkellä tältä osin riittävää täydentävää kansallista sääntelyä. Lain 315 §:n mukainen tiedonsaantioikeus koskee nimittäin vain tahoja, joiden oikeuksista tai velvollisuuksista säädetään viestintäpalvelulaissa, joten se ei sovellu asetuksen valvontaan.

Alakohdan b mukaan viranomaisella tulee olla toimivalta tehdä tarkastusten avulla tutkimuksia vaatimustenmukaisuuden arviointilaitoksista, eurooppalaisen kyberturvallisuussertifikaatin haltijoista ja EU-vaatimustenmukaisuusilmoituksen antajista sen tarkastamiseksi, että ne noudattavat tämän osaston säännöksiä. Alakohdan d mukaan viranomaisen tulee päästä vaatimustenmukaisuuden arviointilaitosten ja eurooppalaisen kyberturvallisuussertifikaatin haltijoiden tiloihin tutkimusten tekemiseksi unionin tai jäsenvaltion prosessioikeuden mukaisesti. Viestintäpalvelulain tarkastuksia koskeva 325 § soveltuu kuitenkin lähinnä teleyrityksiin kohdistuviin tarkastuksiin. Tarkastusten toteuttamiseksi olisi tarpeen olla mahdollisuus saada myös poliisin virka-apua.

Alakohdat c ja f koskevat viranomaisen täytäntöönpanotoimivaltuuksia. Alakohdan c mukaan viranomaisella tulee olla toimivalta toteuttaa asianmukaisia toimenpiteitä kansallisen lainsäädännön mukaisesti varmistaakseen, että vaatimustenmukaisuuden arviointilaitokset,

eurooppalaisen kyberturvallisuussertifikaatin haltijat ja EU-vaatimustenmukaisuusilmoitusten antajat noudattavat tämän asetuksen tai eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimuksia. Lisäksi alakohdan f mukaan tulee olla toimivalta määrätä seuraamuksia kansallisen lainsäädännön mukaisesti 65 artiklassa säädetyllä tavalla ja vaatia lopettamaan tässä asetuksessa säädettyjen velvoitteiden rikkominen välittömästi. Asetuksen 65 artiklassa säädetään vielä, että jäsenvaltioiden on annettava säännöt seuraamuksista, joita sovelletaan tämän osaston ja eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien säännösten rikkomiseen, ja toteutettava kaikki tarvittavat toimenpiteet sen varmistamiseksi, että ne pannaan täytäntöön. Säädettyjen seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia. Viestintäpalvelulain 330–332 §:ssä säädetään nykyisin valvontapäätöksen ja väliaikaisen päätöksen tekemisestä sekä uhkasakosta, keskeyttämisuhasta ja teettämisuhasta. Lisäksi lain 309 §:ssä säädetään Liikenne- ja viestintäviraston oikeudesta saada virka-apua. Nämä säännökset koskevat kuitenkin lähinnä vain mainitun lain rikkomista. Lain seuraamusmaksuja tai rikosoikeudellisia rangaistuksia koskevat säännökset eivät nekään sovellu asetuksen täytäntöönpanoon. Sääntelyn täydentäminen on siten tarpeen.

Alakohdan e mukaan viranomaisella tulee olla toimivaltuus peruuttaa kansallisen lainsäädännön mukaisesti kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen tai 56 artiklan 6 kohdan mukaisesti vaatimustenmukaisuuden arviointilaitosten myöntämät eurooppalaiset kyberturvallisuussertifikaatit, jos ne eivät täytä tämän asetuksen tai eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimuksia. Sähköisen viestinnän palveluista annettu laki ei sisällä tällaisia kansallisia säännöksiä, vaikka tällaista toimivaltuutta on pidettävä tarpeellisena.

Lisäksi kyberturvallisuusasetuksen 58 artiklan 7 kohdan e alakohdassa säädetään kansallista sääntelyä edellyttävällä tavalla siitä, että viranomaisen on myönnettävä soveltuvin osin valtuudet vaatimustenmukaisuuden arviointilaitoksille asetuksen 60 artiklan 3 kohdan mukaisesti ja rajoitettava myönnettyjä valtuutuksia taikka keskeytettävä tai peruutettava ne, jos vaatimustenmukaisuuden arviointilaitokset eivät noudata tämän asetuksen vaatimuksia. Tällaisen tilanteen varalta on lisäksi tarpeen säätää asiakirjojen säilyttämisestä vaatimustenmukaisuuden arviointilaitoksen kyberturvallisuusasetuksen mukaisen toiminnan päättyessä.

3.2.3 Tiedonvaihtoa koskeva sääntely

Kyberturvallisuussertifioinnin myöntävän viranomaisen tehtäviin kuuluisi yhteistyötä ja tiedonvaihtoa useiden tahojen kanssa. Kyberturvallisuusasetuksen 58 artiklan 7 kohdan a alakohta edellyttää valvontayhteistyötä asiaankuuluvien markkinavalvontaviranomaisten kanssa. Alakohta c taas edellyttää, että kyberturvallisuussertifioinnin myöntävä viranomainen aktiivisesti avustaa ja tukee kansallisia akkreditointielimiä näiden seuratessa ja valvoessa vaatimustenmukaisuuden arviointilaitosten toimintaa tämän asetuksen soveltamiseksi. Alakohdan g mukaisesti kyberturvallisuussertifioinnin myöntävän viranomaisen on toimitettava ENISA:lle ja Euroopan kyberturvallisuuden sertifiointiryhmälle vuosittainen yhteenveto tämän kohdan b, c ja d alakohtien tai 8 kohdan nojalla toteutetuista toimista, millä viitataan eri tahoihin kohdistuviin valvontatoimenpiteisiin. Alakohdan h perusteella kyberturvallisuussertifioinnin myöntävän viranomaisen on tehtävä yhteistyötä muiden kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten tai muiden viranomaisten kanssa esimerkiksi jakamalla tietoa mahdollisista tapauksista, joissa tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit taikka tietoturvapalvelut eivät vastaa asetuksen tai yksittäisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien vaatimuksia. Asetuksen johdanto-osan kohdassa 102 todetaan, että komission olisi helpotettava tätä tietojen jakamista asettamalla saataville yleinen sähköinen tietotukijärjestelmä. Lisäksi kyberturvallisuusasetuksen 58 artiklan

9 kohdan mukaan kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten on tehtävä yhteistyötä keskenään ja komission kanssa erityisesti vaihtamalla tietoja, kokemuksia ja hyviä käytäntöjä tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sekä tietoturvapalvelujen kyberturvallisuussertifioinnista ja niiden kyberturvallisuuteen liittyvistä teknisistä kysymyksistä.

Kyberturvallisuusasetuksen 62 artiklalla on perustettu Euroopan kyberturvallisuuden sertifiointiryhmä, joka muodostuu kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten tai muiden asiaankuuluvien kansallisten viranomaisten edustajista. Ryhmän tehtävänä on muun ohella tarkastella merkityksellistä kehitystä kyberturvallisuussertifioinnin alalla ja vaihtaa tietoja ja hyviä käytäntöjä kyberturvallisuuden sertifiointijärjestelmistä (62 artiklan 4 kohdan f alakohta) ja helpottaa kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten välistä, tämän osaston mukaista yhteistyötä valmiuksien kehittämisen ja tietojenvaihdon avulla erityisesti ottamalla käyttöön menetelmiä tietojen vaihtamiseksi tehokkaasti kaikista kyberturvallisuussertifiointia koskevista kysymyksistä (g alakohta).

Kyberturvallisuussertifioinnin myöntävän viranomaisen olisi näin ollen tarpeen pystyä vaihtamaan tarvittaessa myös salassa pidettävää tietoa yllä mainittujen tahojen kanssa. Tietojen salassapito voisi tyypillisesti perustua esimerkiksi julkisuuslain 24 §:n 1 momentin 20 kohdassa tarkoitettuun yksityiseen liikesalaisuuteen tai muuhun elinkeinosalaisuuteen taikka 7 kohdassa tarkoitettuun tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevaan tietoon.

EU-tason yhteistyötä varten tietoja olisi tarpeen voida luovuttaa eri jäsenvaltioiden kansallisten kyberturvallisuussertifioinnin myöntäville viranomaisille ja muille Euroopan kyberturvallisuuden sertifiointiryhmän jäsenille sekä komissiolle. Lisäksi tietoja olisi tarpeen voida luovuttaa kotimaisille ja eurooppalaisille markkinavalvontaviranomaisille sekä akkreditointiyksiköille.

Kyberturvallisuusasetuksen 56 artiklan 8 kohdan nojalla kyberturvallisuussertifioinnin myöntävä viranomainen saisi sertifikaattien haltijoilta ilmoituksia haavoittuvuuksista tai epäsäännönmukaisuuksista, jotka saattavat vaikuttaa sertifiointiin liittyvien vaatimusten mukaisuuteen. Näiden tietojen jakaminen CSIRT-yksikölle olisi välttämätöntä, jotta muun muassa sertifioitujen tuotteiden käyttäjät tavoitetaan tehokkaasti ja toteutetaan tarvittavat toimenpiteet vahinkojen minimoimiseksi.

Sähköisen viestinnän palveluista annetun lain 318 §:n 2 momentissa säädetään (laissa 703/2025) Liikenne- ja viestintäviraston oikeudesta luovuttaa salassa pidettäviä tietoja Energiavirastolle, Finanssivalvonnalle, Lupa- ja valvontavirastolle sekä elinvoimakeskukselle, jos se on näille säädettyjen tietoturvallisuuteen liittyvien tehtävien hoitamiseksi välttämätöntä. Säännöstä voidaan periaatteessa soveltaa myös kyberturvallisuusasetuksen mukaisiin tehtäviin, mutta luettelo ei kata kaikkia kotimaan viranomaisia, joiden kanssa yhteistyötä voidaan pitää tarpeellisena. Näin ollen tiedonvaihdosta olisi säädettävä kattavammin niin kotimaan kuin EU-tason yhteistyönkin kannalta.

3.2.4 Vaatimustenmukaisuuden arviointilaitokset ja julkinen hallintotehtävä

Kyberturvallisuusasetuksen 56 artiklan 4–6 kohdassa säädetään kyberturvallisuussertifikaatin myöntäjästä. Varmuustasoon ”perustaso” tai ”korotettu” viittaavan eurooppalaisen kyberturvallisuussertifikaatin myöntävät 60 artiklassa tarkoitetut vaatimustenmukaisuuden arviointilaitokset perustuen kriteereihin, jotka sisältyvät komission 49 artiklan mukaisesti hyväksymään eurooppalaiseen kyberturvallisuuden sertifiointijärjestelmään. Sertifiointijärjestelmässä voidaan kuitenkin määrätä, että järjestelmästä saatavan

eurooppalaisen kyberturvallisuussertifikaatin myöntää vain julkinen elin, joka voi olla joko kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen tai vaatimustenmukaisuuden arviointilaitoksena akkreditoitu julkinen elin. Korkean varmuustason kyberturvallisuussertifikaatin myöntäjä taas on lähtökohtaisesti kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen. Vaatimustenmukaisuuden arviointilaitos voi myöntää kuitenkin korkean varmuustason sertifikaatin, jos a) kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen hyväksyy ennalta kunkin yksittäisen, vaatimustenmukaisuuden arviointilaitoksen myöntämän eurooppalaisen kyberturvallisuussertifikaatin; tai b) kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen delegoi tämän eurooppalaisten kyberturvallisuussertifikaattien myöntämistä koskevan tehtävän ennalta yleisesti vaatimustenmukaisuuden arviointilaitokselle.

Asetuksen 60–61 artiklassa säädetään vaatimustenmukaisuuden arviointilaitoksista ja niiden ilmoittamisesta. Asetuksen (EY) N:o 765/2008 mukaisesti nimettyjen kansallisten akkreditointielinten on akkreditoitava vaatimustenmukaisuuden arviointilaitos. Kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten on jokaisen eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän osalta ilmoitettava komissiolle vaatimustenmukaisuuden arviointilaitoksista, jotka on akkreditoitu ja soveltuvin osin 60 artiklan 3 kohdan nojalla valtuutettu myöntämään eurooppalaisia kyberturvallisuussertifikaatteja 52 artiklassa tarkoitetuilla määritellyillä varmuustasoilla.

Ilmoitetun vaatimustenmukaisuuden arviointilaitoksen toteuttamaa sertifiointia on pidettävä perustuslain 124 §:ssä tarkoitettuna julkisena hallintotehtävänä. Kansallisessa laissa ei kuitenkaan ole tällä hetkellä perustuslain edellyttämiä säännöksiä siitä, että kyberturvallisuussertifiointia hoitavaan vaatimustenmukaisuuden arviointilaitokseen sovelletaan tässä tehtävässä samoja säännöksiä kuin viranomaisvastuulla vastaavaa tehtävää hoitavaan. Kuten edellä luvussa 3.1.3 todettiin, arviointilaitoslaki ja arviointilaki eivät tule sovellettavaksi kyberturvallisuusasetuksen mukaiseen sertifiointitoimintaan. Toiminta ei kuuluisi myöskään eräitä tuoteryhmiä koskevista ilmoitetuista laitoksista annetun lain soveltamisalaan. Tämän johdosta lakiin olisi tarpeen sisällyttää kyberturvallisuusasetuksen edellyttämät täydentävät säännökset vaatimustenmukaisuuden arviointilaitosten ilmoittamisesta ja valtuuttamisesta sekä niiden velvollisuuksista ja vastuista siltä osin kuin niiden ei voida katsoa seuraavan suoraan asetuksesta. Samoin on tarpeen säätää mahdollisuudesta delegoida korkean varmuustason sertifikaatin myöntäminen vaatimustenmukaisuuden arviointilaitokselle.

3.2.5 Oikeussuojakeinot

Kyberturvallisuusasetuksen 63 artiklassa säädetään valitusoikeudesta. Artiklan 1 kohdan mukaan luonnollisilla henkilöillä ja oikeushenkilöillä on oikeus tehdä valitus eurooppalaisen kyberturvallisuussertifikaatin myöntäjälle tai asianmukaiselle kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle, jos valitus koskee vaatimustenmukaisuuden arviointilaitoksen 56 artiklan 6 kohdan mukaisesti myöntämää eurooppalaista kyberturvallisuussertifikaattia. Viimeksi mainitussa tapauksessa on kyse tilanteesta, jossa vaatimustenmukaisuuden arviointilaitos on myöntänyt korkean tason kyberturvallisuussertifikaatin sertifiointiviranomaisen yksittäistapauksellisen hyväksynnän tai yleisen delegoinnin perusteella. Asetuksen johdanto-osan 102 kohdan mukaan kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten olisi käsiteltävä luonnollisten tai oikeushenkilöiden tekemät valitukset, jotka liittyvät näiden viranomaisten myöntämiin eurooppalaisiin kyberturvallisuussertifikaatteihin tai vaatimustenmukaisuuden arviointilaitosten myöntämiin, varmuustasoa ”korkea” osoittaviin sertifikaatteihin, tutkittava asianmukaisessa määrin valituksen kohde ja ilmoitettava valituksen tekijälle tutkinnan etenemisestä ja tuloksesta kohtuullisessa ajassa. Artiklassa on siten kyse tilanteista, jossa

sivullinen kiinnittää viranomaisen tai arviointilaitoksen huomiota esimerkiksi havaitsemaansa puutteeseen sertifiointijärjestelmän vaatimusten noudattamisessa tai valmistajan tiedonantovelvoitteiden noudattamisessa.

Vaikka asetuksen 63 artiklassa käytetään valituksen käsitettä, tässä yhteydessä kansallisesti olisi kyse valvontailmoituksesta (toimenpidepyynnöstä) eli viranomaiselle osoitetusta pyynnöstä tutkia väitetty lainvastainen menettely. Kyse on hallintoasiasta. Tällä hetkellä valvonta-asioiden käsittelystä Liikenne- ja viestintävirastossa on erityissääntelyä viestintäpalvelulain 313 §:ssä. Sen mukaisesti Liikenne- ja viestintävirasto voi ottaa asian tutkittavakseen asianosaisen pyynnöstä sekä omasta aloitteestaan, minkä lisäksi virasto voi asettaa valvontatehtävänsä tärkeysjärjestykseen ja jättää asian tutkimatta. Viestintäpalvelulain säännökset täyttävät tältä osin nykyisin kyberturvallisuusasetuksen vaatimukset. Artiklan ei kuitenkaan arvioida välttämättä edellyttävän kansallista täydentävää sääntelyä siirrettäessä asetusta täydentävä sääntely ehdotettuun erillislakiin, vaan hallintolakia voidaan pitää tässä suhteessa riittävänä. Hallintolain 19 §:n mukaan asia pannaan vireille ilmoittamalla vaatimukset perusteineen.

Tällainen vaatimus voitaisiin esittää myös sertifikaatin myöntäneelle vaatimustenmukaisuuden arviointilaitokselle niissä tapauksissa, joissa tehtävä kuuluu arviointilaitokselle. Kyberturvallisuusasetuksen 63 artikla koskee myös sellaisia sertifikaatin myöntäjiä, jotka eivät ole viranomaisia. Kyse olisi vaatimustenmukaisuuden arviointilaitoksista, jotka voivat myöntää sertifikaatin eräissä tapauksissa. Tämä katsotaan julkisen hallintotehtävän hoitamiseksi, jolloin toimintaan soveltuvat hallinnon yleislait. Elimen on siten käsiteltävä toimenpidepyyntö hallintolain mukaisesti. Kansallisessa laissa ei kuitenkaan ole säännöksiä siitä, että tehtävää hoitavaan sovelletaan tällöin samoja säännöksiä kuin viranomaisvastuulla vastaavaa tehtävää hoitavaan, joten kansallista lainsäädäntöä olisi tässä täydennettävä tässä suhteessa.

Kyberturvallisuusasetuksen 63 artiklan 2 kohdan mukaan viranomaisen tai elimen, jolle valitus on jätetty, on ilmoitettava valituksen tekijälle valituksen käsittelyn etenemisestä ja siitä tehdystä päätöksestä sekä 64 artiklassa tarkoitetusta oikeudesta tehokkaisiin oikeussuojakeinoihin. Vaatimus ei edellytä täydentävää kansallista sääntelyä. Hallinnon yleislait soveltuvat niin viranomaiseen kuin julkista hallintotehtävää hoitavaan vaatimustenmukaisuuden arviointilaitokseen Hyvän hallinnon periaatteiden ja palveluperiaatteen nojalla (hallintolain 7 ja 8 §) asiallisiin tiedusteluihin esimerkiksi käsittelyn tilanteesta on vastattava. Hallintolaki sisältää säännökset myös valitusosoituksen antamisesta.

Asetuksen 64 artiklassa säädetään oikeudesta tehokkaisiin oikeussuojakeinoihin. Artiklan 1 kohdan mukaan sen estämättä, mitä hallinnollisista tai muista kuin oikeudellisista oikeussuojakeinoista säädetään tai määrätään, luonnollisilla henkilöillä ja oikeushenkilöillä on oltava oikeus tehokkaisiin oikeussuojakeinoihin ensinnäkin 63 artiklan 1 kohdassa tarkoitetun viranomaisen tai elimen päätösten osalta. Tämä sisältää ainakin eurooppalaisen kyberturvallisuussertifikaatin virheellistä myöntämistä koskevat päätökset, päätökset olla myöntämättä eurooppalaista kyberturvallisuussertifikaattia tai päätökset tunnustaa kyseisten luonnollisten henkilöiden ja oikeushenkilöiden hallussa oleva eurooppalainen kyberturvallisuussertifikaatti. Toiseksi oikeus kattaa tilanteen, jossa on kyse 63 artiklan 1 kohdassa tarkoitetulle viranomaiselle tai elimelle tehdyn valituksen käsittelemättä jättäminen. Artiklan 2 kohdan mukaan artiklan mukaiset kanteet on nostettava sen jäsenvaltion tuomioistuimissa, johon kanteen kohteena oleva viranomainen tai elin on sijoittautunut.

Viranomaisten päätöksistä valittamisessa on Suomessa kyse hallintoprosessista. Valitusoikeus on asianosaisilla tai sillä, jonka valitusoikeudesta laissa erikseen säädetään. Vaikka kohdassa käytetään kanteen käsitettä, asia saatetaan Suomessa vireille hallintotuomioistuimeen tehtävällä valituksella. Oikeudenkäynnistä hallintoasioissa annettu laki (808/2019) sisältää

muutoksenhakua koskevan perussääntelyn. Yleislain säännökset oikeudesta valittaa viranomaisen hallintopäätöksestä hallinto-oikeuteen kattavat myös julkista hallintotehtävää hoitavien yksityisten tekemät hallintopäätökset. Muutoksenhausta on nykyisin viestintäpalvelulain 344 §:ssä informatiivinen viittaus edellä mainittuun lakiin. Pykälässä säädetään myös päätöksen tehneen viranomaisen ja ilmoitetun laitoksen mahdollisuudesta määrätä, että päätöstä on noudatettava muutoksenhausta huolimatta, jollei muutoksenhakuviranomainen toisin määrää. Vastaava sääntely on syytä sisällyttää ehdotettuun lakiin kuitenkin siten, että myös vaatimustenmukaisuuden arviointilaitos voi määrätä päätöksen noudattamisesta muutoksenhausta huolimatta.

Jos muutoksenhakukeinona halutaan käyttää kansallisesti ensin oikaisuvaatimusta hallintolain 7 a luvun mukaisesti, tästä on säädettävä erikseen. Vaikka tarkoituksena on, että oikaisuvaatimus olisi muutoksenhaun ensi vaiheena mahdollisimman laajasti, ei oikaisuvaatimusmenettely ei kuitenkaan luontevasti sovellu viranomaisen valvontamenettelyyn, joka perustuu asian yksityiskohtaiseen selvittämiseen. Sen sijaan vaatimustenmukaisuuden arviointilaitosten tekemien päätösten kohdalla oikaisuvaatimusmenettelyä voidaan pitää perusteltuna samoin kuin viranomaisen tekemän maksuvelvollisuutta koskevan päätöksen kohdalla.

Kyberturvallisuusasetuksen mukaan oikeussuojakeinojen tulee kattaa myös tilanne, jossa toimenpidepyyntö jätetään käsittelemättä. Viestintäpalvelulaki ei tunne niin sanottua passiivisuusvalitusta. Kuten jäljempänä vaihtoehtojen arvioinnissa tuodaan tarkemmin esiin, riittävänä oikeussuojakeinona viivästystilanteissa voidaan pitää mahdollisuutta kannella viranomaisen tai julkista hallintotehtävää hoitavan toiminnasta ylimmille laillisuusvalvojille.

Yhteenvetona voidaan todeta, että kyberturvallisuusasetus edellyttää täydentävää kansallista sääntelyä julkisen hallintotehtävän hoitamisesta sekä sertifiointiviranomaisen toimivallasta samoin kuin seuraamuksista ja muutoksenhausta. Lisäksi on tarpeen säätää myös oikeudesta saada virka-apua samoin kuin viranomaisyhteistyöstä ja siihen liittyvästä tietojenvaihdosta.

3.3 Viranomaistoiminnan maksullisuus

Valtion viranomaisten suoritteiden maksullisuuden ja suoritteista perittävien maksujen suuruuden yleisistä perusteista sekä maksujen muista perusteista säädetään valtion maksuperustelaissa (150/1992). Kyseessä on yleislaki, jonka lisäksi maksuista voidaan säätää erikseen. Lakiin sisältyy säännökset suoritteiden maksullisuudesta ja maksujen suuruuden yleisistä perusteista (2 luku), mukaan lukien säännökset tietyistä suoritteista, jotka ovat joko maksullisia tai maksuttomia. Julkisoikeudellisella suoritteella tarkoitetaan maksuperustelaissa valtion viranomaisen suoritetta, jonka kysyntä perustuu lakiin tai asetukseen ja jonka tuottamiseen viranomaisella on tosiasiallinen yksinoikeus. Julkisoikeudellisesta suoritteesta valtiolle perittävän maksun suuruuden tulee maksuperustelain 6 §:n mukaan vastata suoritteen tuottamisesta valtiolle aiheutuvien kokonaiskustannusten määrää. Valtion maksuperustelain 8 §:ssä säädetään asetuksella säädettävistä asioista ja ministeriön toimivallasta. Maksuperustelain 12 §:n mukaan asetuksella voidaan antaa tarkempia säännöksiä omakustannusarvoon kuuluvista kustannuksista.

Valtion maksuperustelain sääntelyn viranomaisten suoritteiden maksullisuudesta ja maksujen suoritteiden perusteista arvioidaan olevan riittävää. Korkean varmuustason sertifikaattien myöntäminen viranomaisen toimesta on maksuperustelain puitteissa katsottava julkisoikeudelliseksi suoritteeksi. Samoin muun muassa vaatimustenmukaisuuden arviointilaitosten nimeäminen ilmoitetuksi laitokseksi kyberkestävyysasetuksen puitteissa, niiden ilmoittaminen kyberturvallisuussertifiointia varten komissiolle sekä niiden valvonta on

katsottava julkisoikeudelliseksi suoritteeksi. Kun mainitut suoritteet liittyvät sertifiointia hakevan tahon tai vaatimustenmukaisuuden arviointilaitoksen taloudelliseen toimintaan, ei niiden maksullisuudesta poikkeamiseen ole maksuperustelaissa tarkoitettua perusteltua syytä. Myös kyberkestävyyden sääntelyn testiympäristön käytön tulisi olla maksuperustelain lähtökohdan mukaisesti oletusarvioisesti maksullista, sillä maksuilla katettaisiin viranomaiselle testiympäristön ylläpidosta ja käytöstä aiheutuvia kustannuksia. Maksuperustelaki mahdollistaa kuitenkin sen, että erityisestä syystä maksu voidaan määrätä tietyltä ryhmältä perittäväksi suoritteen omakustannusarvoa alempana tai jättää kokonaan perimättä. Tämä mahdollistaisi tarvittaessa maksullisuutta koskevat helpotukset etenkin, jos testiympäristö perustettaisiin tekoälyasetuksen mukaisen testiympäristön yhteyteen, sillä pääsy kyseiseen testiympäristöön tulee tekoälyasetuksen mukaan tarjota pk-yrityksille maksutta.

Liikenne- ja viestintäministeriön Liikenne- ja viestintäviraston sähköiseen viestintään liittyvistä suoritteista perittävistä maksuista antaman asetuksen (1190/2023, muutettu asetuksella 905/2024) 3 §:ssä säädetään muun ohella tietoturvatuotteiden ja tietoliikenneyhteyksiä hyödyntävien tuotteiden turvallisuuden tason arviointiin liittyvien suoritteiden maksullisuudesta. Suoritteesta peritään omakustannusarvon mukainen maksu. Saman pykälän 4 kohdan mukaan tietoturvallisuuden arviointilaitosten hyväksyntään liittyvistä toimenpiteistä peritään niin ikään maksu. Asetuksen täsmentämistarvetta siten, että se kattaisi myös kyberkestävyysasetukseen ja kyberturvallisuusasetukseen liittyviä suoritteita, olisi tarpeen arvioida asetuksen päivittämisen yhteydessä.

3.4 Verkkotunnusvälittäjät

NIS 2 -direktiivin verkkotunnusten rekisteröintipalveluja tarjoavia toimijoita koskevat 3 ja 26–28 artiklan säännökset on pantu täytäntöön sähköisen viestinnän palveluista annetun lain muutoksilla (L 126/2025; HE 57/2024 vp).

Sähköisen viestinnän palveluista annetun lain 21 luvussa säädetään Suomen maatunnukseen (*fi-maatunnus*) ja Ahvenanmaan maakuntatunnukseen (*ax-maakuntatunnus*) päättyviin verkkotunnuksiin sekä niihin liittyvästä verkkotunnustoiminnasta ja verkkotunnusten välittämisestä. Verkkotunnusvälittäjän NIS 2 -direktiivin 27 artiklan mukaisista ilmoitusvelvollisuuksista säädetään sähköisen viestinnän palveluista annetun lain 165 §:ssä. NIS 2 -direktiivin 28 artiklaa täytäntöönpanevia säännöksiä sisältyy sähköisen viestinnän palveluista annetun lain 167 §:ään ja 170 §:ään.

Muita kuin verkkotunnusten rekisteröintipalveluja tarjoavia toimijoita koskevat NIS 2 -direktiivin säännökset on pantu täytäntöön kyberturvallisuuslailla (124/2025) ja julkisen hallinnon tiedonhallinnasta annetun lain muutoksilla (L 125/2025). Mainittuihin lakeihin ei sisälly verkkotunnusvälittäjiä koskevia säännöksiä.

Sähköisen viestinnän palveluista annetun lain 21 luvun säännökset soveltuvat ainoastaan fi-maatunnukseen ja ax-maakuntatunnukseen päättyviin verkkotunnuksiin ja niihin liittyvään verkkotunnusten välitystoimintaan verkkotunnusvälittäjien (eng. registrar) toimesta. NIS 2 -direktiivi vaatii jäsenvaltiota edellyttämään 27–28 artiklan mukaisia toimenpiteitä myös muita verkkotunnuksia välittäviltä verkkotunnusvälittäjiltä silloin, jos verkkotunnusvälittäjä kuuluu NIS 2 -direktiivin 26 artiklan nojalla Suomen lainkäyttövaltaan. NIS 2 -direktiivin täytäntöönpanoa olisi näin ollen tarpeen täydentää verkkotunnusten rekisteröintipalveluja tarjoavia toimijoita koskien silloin, kun kysymys on muusta verkkotunnusten rekisteröintipalveluja koskevasta toiminnasta kuin fi-maatunnukseen tai ax-maakuntatunnukseen päättyvään verkkotunnukseen liittyvästä toiminnasta. Lisäksi 21 luvun soveltamista tulisi direktiivin kattavan täytäntöönpanon varmistamiseksi laajentaa eräiltä osin

verkkotunnusvälittäjien puolesta toimiviin tahoihin. Täydennykset edellyttävät muutoksia sähköisen viestinnän palveluista annettuun lakiin tai kyberturvallisuuslakiin.

Suomessa ei nykyisin ole voimassa olevaa sääntelyä muiden kuin fi-maatunnukseen tai ax-maakuntatunnukseen päättyvien verkkotunnusten välittämisestä. Liikenne- ja viestintävirasto on antanut sähköisen viestinnän palveluista annetun lain 21 luvun nojalla verkkotunnusmääräyksen, joka koskee fi-maatunnukseen tai ax-maakuntatunnukseen päättyvien verkkotunnusten välittämistä.

Verkkotunnusten rekisteröintitietojen keräämisestä, saataville saattamisesta ja niihin pääsystä on laadittu useita Internetin vapaaehtoisia standardeja ja toimialan käytänteitä kansainvälisessä yhteistyössä). Näiden pohjalta on syntynyt käytäntö, jonka mukaan jokainen ylimmän tason verkkotunnusrekisteri pitää itse yllä ns. WHOIS-palvelua, jossa rekisterin hallinnassa olevien verkkotunnusten rekisteröintitiedot julkaistaan. Internetin geneerisiä ylimmän tason verkkotunnuksia hallinnoiva ICANN (Internet Corporation for Assigned Names and Numbers) on vienyt tämän periaatteen omiin sopimuksiinsa geneeristen ylimmän tason verkkotunnusrekisterien (gTLD) kanssa siten, että nykyisin rekisteröintitiedon julkaisemisesta ovat vastuussa kyseisen aluetunnusrekisterin ylläpitäjän lisäksi sen valtuuttamat verkkotunnusvälittäjät kukin osaltaan niin, että kummankin toimijan vastuut eri tietotyyppien julkisesti saataville saattamisesta poikkeavat hieman toisistaan. Sopimuksessa määrätään myös rekisteritietojen siirtämisestä verkkotunnusvälittäjältä aluetunnusrekisterin ylläpitäjälle henkilötietojen käsittelyä koskevasta lainsäädännöstä seuraavin edellytyksin. Ylimmän tason maatunnusten (ccTLD) osalta ei sen sijaan ole yhtenäisiä käytäntöjä. NIS 2 -direktiivin täytäntöönpanon täydentämistä sen 28 artiklan osalta koskevat lakimuutokset, jotka koskevat verkkotunnusten rekisteröintitietojen julkisuutta, olisi valmisteltava siten, että ne ovat mahdollisuuksien mukaan linjassa kansainvälisten standardien ja niiden pohjalta syntyneiden käytäntöjen kanssa. Direktiivin voidaan katsoa mahdollistavan erilaiset tekniset toteutusmallit, kunhan direktiivin 28 artiklan edellyttämät tiedot ovat julkisesti saatavilla ja kunhan aluetunnusrekisterin ylläpitäjät ja verkkotunnusvälittäjät kykenevät antamaan direktiivin edellyttämän pääsyn henkilötietoja sisältäviin tietoihin.

Sähköisen viestinnän palveluista annetun lain mukaiset Liikenne- ja viestintäviraston toimivaltuudet kuten tiedonsaantioikeus ja mahdollisuus uhkasakon asettamiseen olisivat kohdistettavissa myös muuhun verkkotunnustustoimintaan kuin 21 luvussa nykyisin säädettyihin verkkotunnusvälittäjiin, mikäli täydentävistä velvoitteista säädettäisiin kyseisessä laissa. Sähköisen viestinnän palveluista annetun lain 312 §:n 2 momentin erityinen verkkotunnuksiin liittyviä asiakirjoja koskeva tiedoksiantosäännös soveltuisi niin ikään myös muihin kuin nykyisin 21 luvussa säädettyihin verkkotunnusasioihin.

4 Ehdotukset ja niiden vaikutukset

4.1 Keskeiset ehdotukset

Esityksellä ehdotetaan säädettäväksi uusi laki eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista.

Laissa säädettäisiin kyberkestävyysasetuksen markkinavalvonnasta, vaatimuksenmukaisuuden arviointilaitoksien ilmoittamisesta kyberkestävyysasetuksen mukaisia arviointitehtäviä varten sekä kyberkestävyysasetuksen rikkomiseen liittyvistä hallinnollisista seuraamuksista. Lisäksi laissa säädettäisiin kyberkestävyyden sääntelyn testiympäristön perustamisesta, keskeneräisten tuotteiden käyttämisestä eräissä olosuhteissa sekä kyberkestävyysasetuksen vaatimuksien huomioimisesta julkisissa hankinnoissa.

Liikenne- ja viestintävirasto vastaisi keskitetysti kyberkestävyysasetuksen markkinavalvontaviranomaisen tehtävistä. Lisäksi suuririskisille tekoälyjärjestelmille markkinavalvontaviranomaisena toimisi eräiden tekoälyjärjestelmien valvonnasta annetun lain nojalla toimivaltainen valvova viranomainen. Kyberkestävyysasetuksen markkinavalvontaan sovellettaisiin eräiden tuotteiden markkinavalvonnasta annettua lakia ja markkinavalvonta-asetusta.

Liikenne- ja viestintävirasto vastaisi myös kyberkestävyysasetuksen mukaisen ilmoittavan viranomaisen tehtävistä. Suomeen sijoittautunut vaatimustenmukaisuuden arviointilaitos hakisi kyberkestävyysasetuksen mukaiseksi ilmoitetuksi laitokseksi ilmoittamista Liikenne- ja viestintävirastolta. Hakemukseen olisi lähtökohtaisesti liitettävä FINAS-akkreditointipalvelun akkreditointitodistus siitä, että arviointilaitos täyttää kyberkestävyysasetuksen vaatimukset.

Esityksellä annettaisiin myös EU:n kyberturvallisuusasetusta täydentäviä säännöksiä kyberturvallisuussertifioinnin kansallisen viranomaisen tehtävistä ja sen toimivaltuuksista. Tehtävä on nykyisin osoitettu Liikenne- ja viestintävirastolle sähköisen viestinnän palveluista annetun lain nojalla. Liikenne- ja viestintävirasto jatkaisi tehtävässä. Tehtävää ja toimivaltuuksia koskevat kansalliset säännökset sisältyisivät kuitenkin uuteen eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista annettavaan lakiin. Ehdotuksella täydennettäisiin ja täsmennettäisiin kyberturvallisuussertifiointiin liittyvien viranomaistehtävien toimivaltuuksia, vaatimustenmukaisuuden arviointilaitosten ilmoittamista sekä hallinnollisten seuraamusmaksujen määräämistä kyberturvallisuussertifiointiin liittyvistä väärinkäytöksistä.

Sähköisen viestinnän palveluista annettuun lakiin ehdotetaan lisättäväksi uusi 21 a luku, jossa säädettäisiin verkkotunnusten rekisteröintitietojen keräämisestä ja luovuttamisesta muiden kuin fi-maatunnukseen ja ax-maakuntatunnukseen päättyvien verkkotunnuksien osalta. Luvussa säädettäisiin myös verkkotunnusvälittäjän ilmoittautumisvelvollisuudesta Liikenne- ja viestintävirastolle. Ehdotuksilla täydennettäisiin EU:n kyberturvallisuusdirektiivin täytäntöönpanoa verkkotunnuksien rekisteröintitietojen osalta.

4.2 Pääasialliset vaikutukset

4.2.1 Yritysvaikutukset

Kyberkestävyysasetus ja sitä täydentävä kansallinen sääntely

Kyberkestävyysasetuksen soveltamisalaan kuuluu huomattavan laaja joukko erilaisia laitteita ja ohjelmistoja. Säädöstä sovelletaan horisontaalisesti kaikkiin laitteisiin ja ohjelmistoihin, jotka sisältävät asetuksen tarkoittaman ”digitaalisen elementin” eli ovat kytkettävissä joko suoraan tai välillisesti verkkoon tai toiseen laitteeseen. Lähtökohtaisesti kaikki internetiin suoraan tai välillisesti kytkettävissä olevat laitteet ja ohjelmistot kuuluisivat soveltamisalaan. Eräitä tuotteita (ajoneuvot, ilma-alukset ja tietyt lääkinnälliset laitteet) on rajattu soveltamisalan ulkopuolelle, koska niissä tuotekohtaisen sääntelyn kattaa myös kyberturvallisuutta koskevia vaatimuksia yksityiskohtaisesti.

Soveltamisalaan kuuluvien tuotteiden määrä on huomattavan suuri. Soveltamisalaan kuuluisivat sekä kuluttaja- että yrityskäytössä olevat laitteet ja ohjelmistot, jotka ovat yhdistettävissä verkkoon tai toiseen laitteeseen. Tuotteille asetettavat vaatimukset koskettavat suoraan tai välillisesti miltei kaikkien nykyisten markkinavalvontaviranomaisten valvontatoimialaan kuuluvia tuotteita, joihin sisältyy digitaalinen elementti. Vaatimukset koskettavat myös merkittävää määrää tuotteita, joihin ei nykyisin kohdistu markkinavalvontaa tai tuotesääntelyyn

perustuvia turvallisuusvaatimuksia. Euroopan komission vaikutusarvion mukaan kyberkestävyysasetuksen soveltamisalaan kuuluvan tuotteiden markkina-arvo on ollut karkeasti 1 485 mrd. € Euroopan unionin tasolla (vuonna 2019).[2]

Kyberkestävyysasetuksella ja sitä täydentävällä kansallisella sääntelyllä on vaikutuksia talouden toimijoille, jotka valmistavat, maahantuovat ja jakelevat kyberkestävyysasetuksen soveltamisalaan kuuluvia tuotteita. Esityksellä on siis vaikutuksia digitaalisen elementin sisältävien tuotteiden valmistajille, maahantuojille ja tuotteita myyville yrityksille. Pääosa vaikutuksista aiheutuu suoraan asetuksesta, mihin ei liity kansallista liikkumavaraa.

Yrityksiin kohdistuvat vaikutukset koostuvat kyberkestävyysasetuksen mukaisten olennaisten kyberturvallisuusvaatimusten täyttämisestä. Digitaalisen elementin sisältävät tuotteiden ominaisuuksien tulee täyttää asetuksen liitteen I osassa I asetetut vaatimukset ja valmistajan käyttöön ottamien prosessien ja haavoittuvuuksien käsittelyn tulee täyttää asetuksen liitteen I osassa II asetut vaatimukset, joita tarkennetaan asetuksen 27 artiklan mukaisesti yhdenmukaistetuin standardein tai komission täytäntöönpanoasetuksin. Valmistajan tulee lisäksi arvioida ja osoittaa vaatimustenmukaisuus kyberkestävyysasetuksen mukaisesti. Valmistajille aiheutuu lisäksi kustannuksia haavoittuvuuksien käsittelystä tuotteen tukiajan aikana sekä kyberkestävyysasetuksen edellyttämien haavoittuvuus- ja poikkeamailmoituksien tekemisestä. Kyberkestävyysasetuksen markkinavalvonnasta aiheutuu talouden toimijoille hallinnollisia kustannuksia.

Kyberkestävyysasetuksen soveltamisalaan kuuluvat digitaalisen elementin sisältävät tuotteet, joiden käyttötarkoitus tai kohtuudella ennakoitavissa oleva käyttö sisältää suoran tai välillisen loogisen tai fyysisen datayhteyden johonkin laitteeseen tai verkkoon. Soveltamisalaan kuuluvia digitaalisen elementin sisältäviä tuotteita ovat esimerkiksi laitteet, joilla on suora tai epäsuora verkkoyhteys (IoT-laitteet, älylaitteet, teollisuuskomponentit), niihin liittyvät ohjelmistot, muut ohjelmistotuotteet ja pelit. Soveltamisalaan kuuluvat esimerkiksi tietokoneet, puhelimet, etäluettavat sensorit, puettavat älylaitteet, verkkoon kytkettävät IoT-laitteet ja kodinelektroniikka sekä verkkoon kytkettävät teollisuusautomaatiojärjestelmät. Soveltamisalaan kuuluvat esimerkiksi myös käyttöjärjestelmät, tietokone- ja mobiiliohjelmat ja pelit. Kyberkestävyysasetuksen soveltamisalaan kuuluu siten huomattavan laaja joukko erilaisia laitteita ja ohjelmistoja. Lähtökohtaisesti kaikki internetiin suoraan tai välillisesti kytkettävissä olevat laitteet ja ohjelmistot kuuluisivat soveltamisalaan. Eräitä tuotteita (ajoneuvot, ilma-alukset ja tietyt lääkinnälliset laitteet) on rajattu soveltamisalan ulkopuolelle, koska niissä tuotekohtaisen sääntelyn kattaa myös kyberturvallisuutta koskevia vaatimuksia

[2] Commission Staff Working Document Impact assessment report accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, SWD/2022/282 final. Kun Euroopan unionin sisämarkkinan koko on ollut 13 900 mrd. € vuonna 2019, voivat kyberkestävyysasetuksen vaatimukset siten komission vaikutusarvion perusteella koskettaa jopa 10,6 prosenttia koko sisämarkkinasta. Vuonna 2021 EU:n sisäisen kaupan arvo oli 6 786 miljardia euroa, joten voidaan karkeasti laskea, että sisäisen kaupan liikevaihdosta 21,8 prosenttiin sisältyy digitaalinen elementti. Suomen markkinoista on tehty arvio, että IoT-markkinoiden arvo olisi 1 903 miljoonaa dollaria (n. 1 742 milj. euroa) vuonna 2024 ja että markkinoiden odotetaan kasvavan 9,3 % vuosittain. Edellä kuvattuihin arvioihin liittyy merkittäviä epävarmuustekijöitä, mutta ne antavat suuntaa soveltamisalan laajuudesta. IoT-laitteiden voidaan arvioida pääsääntöisesti kuuluvan kyberkestävyysasetuksen soveltamisalaan, mutta asetus kattaa paljon myös muita tuotteita, kuten tavanomaiset päätelaitteet ja ohjelmistot.

yksityiskohtaisesti. Soveltamisalaan kuuluvien tuotteiden lukumäärästä tai Suomen markkinan koosta ei ole saatavilla kootusti tilastotietoa. Markkinoilla olevien tuotteiden määrää on hyvin hankala arvioida, sillä tilastotiedot eri tuoteryhmistä eivät erittele, sisältävätkö tuotteet digitaalisen elementin. Soveltamisalaan kuuluvien tuotteiden käyttö on kuitenkin hyvin yleistä. Soveltamisalaan kuuluvien laitteiden ja ohjelmistojen määrä arvioidaan merkittäväksi sekä kotitalouksissa että yrityksissä.

Edellä todetusti soveltamisalaan kuuluvien tuotteiden määrä on huomattavan suuri. Soveltamisalaan kuuluisivat sekä kuluttaja- että yrityskäytössä olevat laitteet ja ohjelmistot, jotka ovat yhdistettävissä verkkoon tai toiseen laitteeseen. Tuotteille asetettavat vaatimukset koskettavat suoraan tai välillisesti miltei kaikkien nykyisten markkinavalvontaviranomaisten valvontatoimialaan kuuluvia tuotteita, joihin sisältyy digitaalinen elementti. Vaatimukset koskettavat myös merkittävää määrää tuotteita, joihin ei nykyisin kohdistu markkinavalvontaa tai tuotesääntelyyn perustuvia turvallisuusvaatimuksia.

Euroopan komission vaikutusarvioinnin mukaan digitaalisen elementin sisältävien tuotteiden markkinan globaali liikevaihto on ollut 550–1 485 miljardia euroa vuonna 2019 riippuen tuoteluokituksista, joita arvioon sisällytetään.[3] Euroopan komission vaikutusarvioinnin mukaan digitaalisen elementin sisältävien tuotteiden kehittämisen kustannuksiin kyberkestävyysasetuksen edellyttämän turvallisuustason vaatimuksilla voi olla keskimäärin 30,5 % (vaihteluväli 19–42 %) tuotteen kehityskustannuksia korottava vaikutus.[4] Euroopan komission 15.9.2022 julkaisema vaikutusarviointi on saatavilla komission verkkosivuilla: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment.

Tilastokeskuksen väestön tieto- ja viestintätekniikan käyttö -tilaston mukaan vuonna 2024 suomalaisista 94 % on käyttänyt internetiä viimeisen 3 kuukauden aikana ja 83 % käyttää internetiä useita kertoja päivässä. Viimeisen 3 kuukauden aikana internetiä on käyttänyt 100 % 16–54-vuotiaiden ikäryhmästä. Näin ollen tästä ikäryhmästä jokainen on käyttänyt yhtä tai useampaa kyberkestävyysasetuksen soveltamisalaan kuuluvaa digitaalisen elementin sisältävää tuotetta. Koko väestön tasolla tuotteita on käytössä 94 %:lla väestöstä. Edelleen tilaston mukaan kosketusnäytöllä varustettu älypuhelin on ollut käytössä 90 prosentilla väestöstä. Tilaston mukaan internetiin liitettyä kodin lämmitys-, valaistus- tai muuta vastaavaa järjestelmää on käyttänyt viimeisen kolmen kuukauden aikana 14 % suomalaisista, internetiin liitettyä kodin hälytysjärjestelmää, esimerkiksi lukkoja, palovaroitinta tai turvakameroita on käyttänyt viimeisen kolmen kuukauden aikana 13 % suomalaisista sekä internetiin liitettyjä kodinkoneita tai laitteita on käyttänyt viimeisen kolmen kuukauden aikana 11 % suomalaisista. Virtuaaliavustajaa älykaiuttimen, tietokoneen tai puhelimen sovelluksen kautta on käyttänyt viimeisen kolmen kuukauden aikana 13 % suomalaisista. Suoraan internetiin liitetyllä SMART-televisiolla tai digiboksin kautta nettiin liitetyllä televisiolla internetiä on käyttänyt viimeisen 3 kuukauden aikana 55 % suomalaisista. Lisäksi 40 % suomalaisista on pelannut tai ladannut pelejä; 16–44-vuotiaiden ikäryhmästä useampi kuin joka toinen ja 44–89-vuotiaiden ikäryhmästä harvempi kuin joka toinen.[5]

---

[3] Commission staff working document. Impact assessment report. SWD(2022) 282 final. Part 2/3, s. 48.
[4] Commission staff working document. Impact assessment report. SWD(2022) 282 final. Part 2/3, s. 55–56.
[5] Lähde: Tilastokeskus. Väestön tieto- ja viestintätekniikan käyttö -tilasto. Tiedot koskevat vuotta 2024. Tilaston perusjoukko kattaa maassa vakituisesti asuvan 16–89-vuotiaan väestön ja kotitaloudet, joissa on vähintään yksi 16–89-vuotias henkilö. Tiedot haettu 1.4.2025.

Kuluttajakäytön lisäksi digitaalisen elementin sisältävien tuotteiden käyttö on yleistä myös yrityksissä. Käytön yleisyyttä kuvaa, että vuonna 2024 yli 100 Mbit/s internetyhteys on ollut käytössä 80 %:lla yrityksistä, mistä on pääteltävissä, että yrityksillä on käytössä vähintään yksi tai useampi digitaalisen elementin sisältävä tuote. Tekoälyteknologioita on ollut käytössä 24 %:lla yrityksistä.[6]

Digitaalisen elementin sisältävien tuotteiden valmistajista, maahantuojista tai jakelijoista ei ole saatavilla kootusti tilastotietoa. Tuotteisiin liittyvä yritystoiminta jakautuu eri toimialoille. Ohjelmistot, konsultointi ja siihen liittyvä toimiala -toimialalla on Suomessa toiminut vuonna 2023 yhteensä 14 095 yritystä ja toimialan yritysten yhteenlaskettu liikevaihto on ollut noin 12,8 miljardia euroa ja henkilöstön määrä noin 65 000 henkilötyövuotta.[7]

Kuten edellä todetaan, keskeiset vaikutukset yrityksille tulevat suoraan asetuksen säännöksistä. Yrityksille aiheutuu tuotekehityksen ja haavoittuvuuksien käsittelyn lisäksi hallinnollisia kustannuksia. Yritysten tulee laatia ja ylläpitää jatkossa teknistä dokumentaatiota, joka osoittaa tuotteen tai ohjelmiston täyttävän asetuksen kyberturvallisuusvaatimukset. Tämä dokumentaatio on keskeinen osa CE-merkintäprosessia ja markkinoille pääsyn ehtoja. Teknisen dokumentaation tulee sisältää tuotekuvauksen, kyberturvallisuusriskien arvioinnin, kuvaus turvallisuustoimenpiteistä ja haavoittuvuuksien hallinnasta. Lisäksi yritysten tulee tehdä tuotteistaan vaatimustenmukaisen arvioinnin joko itsearviointina tai kolmannen osapuolen toteuttama, riippuen tuotteen riskiluokasta. Korkean riskin tuotteille vaaditaan kolmannen osapuolen arviointi, mikä tuo lisäkustannuksia muun muassa auditointien valmistelun, vaatimustenmukaisuuden arviointilaitoksien perimien maksujen ja mahdollisten uusintatarkastuksien osalta.

Kyberkestävyysasetuksen vaatimusten täyttäminen osoitetaan liittämällä laitteeseen CE-merkintä. Jatkossa digitaalisen elementin sisältävät tuotteet eivät pääse EU:n sisämarkkinoille ilman riittävän kyberturvallisuustason osoittamista kyberkestävyysasetuksen mukaisesti. Asetuksella tai sitä täydentävällä kansallisella sääntelyllä ei tunnisteta olevan kilpailua vääristävää vaikutusta, koska vaatimukset tulevat kaikille yrityksille koosta ja toimialasta riippumatta. Koska kyberkestävyysasetuksen vaatimukset koskettavat kaikkia yrityksiä tasapuolisesti, sääntely harmonisoi markkinoita. Kustannuksia ei synny sellaisten tuotteiden valmistajille ja tuojille, joiden laitteissa on jo huolehdittu kyberturvallisuudesta riittävällä tasolla. Sen sijaan useat toimijat voivat joutua investoimaan ja tekemään tuotekehitystä kyberturvallisuuden parantamiseksi. Toisaalta kyberkestävyysasetuksesta aiheutuvat kustannukset ovat liikevaihtoon suhteutettuna korkeampia mikro-, pien- ja keskisuurille talouden toimijoille kuin suuryrityksille, minkä johdosta toimeenpanossa olisi tarpeen keskittyä erityisesti näille yrityksille kohdistettuun neuvontaan ja viranomaistukeen.

Vaikka kyberkestävyysasetuksesta aiheutuvien vaatimuksien tasoon tai niistä aiheutuviin kustannuksiin ei voida vaikuttaa kansallisessa lainsäädännössä, hallituksen esityksen 1. lakiehdotuksella mahdollistettaisiin kuitenkin kyberkestävyysasetuksen mukaisten kyberkestävyyden sääntelyn testiympäristön perustaminen markkinavalvontaviranomaisen päätöksellä. Kyberkestävyyden sääntelyn testiympäristön hyödyntäminen tuotekehityksessä

---

[6] Lähde: Tilastokeskus. Tietotekniikan käyttö yrityksissä -tilasto. Tiedot koskevat vuotta 2024. Tilaston perusjoukko kattaa vähintään 10 henkilöä työllistävät yritykset toimialoilta, jotka kuvataan tilaston perustiedoissa. Tiedot haettu 1.4.2025.

[7] Lähde: Tilastokeskus. Yritysten rakenne- ja tilinpäätöstilasto. Tiedot koskevat vuotta 2023. Tilaston perusjoukko kattaa kaikki Suomessa liiketoimintaa harjoittavat yritykset. Tiedot haettu 1.4.2025.

voisi vaikuttaa erityisesti pk-yrityksille aiheutuviin tuotekehityskustannuksiin niitä alentavasti. Lisäksi kyberkestävyyden sääntelyn testiympäristön yhteydessä viranomainen voisi tarjota neuvontaa ja tukea pk-yrityksille sääntelyn vaatimuksista.

Hallituksen esityksen nojalla yrityksille voitaisiin määrätä kyberkestävyysasetuksen edellyttämällä tavalla hallinnollinen seuraamusmaksu, jos se laiminlyö kyberkestävyysasetuksen vaatimuksia. Yritykselle voidaan määrätä hallinnollinen seuraamusmaksu, joka on enintään 15 miljoonaa euroa tai 2,5 % yrityksen maailmanlaajuisesta vuotuisesta liikevaihdosta. Tuote voidaan myös määrätä poistettavaksi markkinoilta esimerkiksi sellaisessa tapauksessa, jossa tuotteessa todetaan vakava haavoittuvuus, eikä valmistaja ryhdy korjaaviin toimiin. Markkinavalvonnasta voi aiheutua hallinnollisia kustannuksia yritykselle.

Kyberkestävyysasetuksella on vaikutusta markkinoille sellaisten tuotteiden osalta markkinoille pääsyyn, jotka eivät täytä vaatimuksia. Viranomaiset voivat estää tuotteen markkinoille saattamisen tai myynnin jatkamisen, jos vaatimuksenmukaisuutta ei ole osoitettu. Niiden tuotteiden osalta, jotka eivät jo nykyisellään täytä kyberkestävyysasetuksen vaatimuksia, yritykset voivat joutua tekemään tuotekehitystä. Jatkossa yritystoiminnan aloittaminen ja markkinoille pääsy voi edellyttää suurempia alkuinvestointeja sellaisten yritysten osalta, jotka kehittävät, valmistavat tai maahantuovat EU-markkinoille verkkoon liitettäviä tuotteita ja ohjelmistoja. Uusien yritysten, jotka kehittävät digitaalisia tuotteita, on otettava kyberkestävyysasetuksen vaatimukset huomioon jo tuotekehityksen alkuvaiheessa. Tämä voi lisätä alkuinvestointeja, koska tuotekehitykseen voi tarvita laajempaa kyberturvallisuusosaamista, dokumentaatiota ja mahdollisesti kolmannen osapuolen arviointeja. Erityisesti pk-yrityksille tämä voi luoda suuremman tarpeen ulkopuoliselle asiantuntemukselle.

Kyberkestävyysasetuksen vaatimuksien myötä tuotekehityksessä tulee ottaa kyberturvallisuus huomioon ja markkinoille tulee turvallisempia laitteita. Vaikutuksena arvioidaan, että tietoturvaloukkaukset ja niistä syntyvät kustannukset ja mainehaitat pienenevät pidemmällä aikavälillä.

Verkkotunnusvälittäjät ja aluetunnusrekisterin ylläpitäjät

Sähköisen viestinnän palveluista annettuun lakiin ehdotetulla uudella 21 a luvulla olisi vaikutuksia Suomeen sijoittautuneille ja muille Suomen lainkäyttövaltaan kuuluville aluetunnusrekisterien ylläpitäjille ja verkkotunnusvälittäjille. Vaikutukset aiheutuisivat erityisesti verkkotunnusten rekisteröintitietojen käsittelemisestä ja niihin pääsyä koskeviin pyyntöihin vastaamisesta. Lisäksi verkkotunnusvälittäjille aiheuttaisi kustannuksia velvoite ilmoittaa tietoja Liikenne- ja viestintävirastolle. Ehdotetuilla muutoksilla parannettaisiin pääsyä verkkotunnusten rekisteröintitietoihin, millä voi olla merkittäviä myönteisiä vaikutuksia yhteiskunnalle tilanteissa, joissa viranomaisten ja muiden tahojen mahdollisuudet puuttua lainvastaiseen toimintaan parantuvat. Luvun soveltamisalaan tulevien toimijoiden määrän ennakointi on epävarmaa, mutta sen voidaan arvioida olevan yhteensä muutamia satoja mukaan lukien sekä varsinaiset verkkotunnusvälittäjät että niiden puolesta toimivat tahot, kuten verkkotunnusten rekisteröintipalveluja tarjoavat jälleenmyyjät. Suomeen sijoittautuneita sellaisia aluetunnusrekisterin ylläpitäjiä, jotka eivät käyttäisi aluetunnusta ainoastaan omiin tarkoituksiinsa, arvioidaan olevan hyvin vähäinen määrä.

4.2.2 Viranomaisvaikutukset

4.2.2.1 Liikenne- ja viestintävirasto

Kustannukset

Esityksellä on suoria ja merkittäviä vaikutuksia Liikenne- ja viestintävirastolle sen eri toiminnoissa. Esitys lisäisi Liikenne- ja viestintäviraston tehtävien määrää. Kyberkestävyysasetuksen täytäntöönpanoon ja kyberturvallisuussertifiointiin liittyvien tehtävien osalta arvioitu lisäys Liikenne- ja viestintäviraston tehtävämäärään on laajuudeltaan yhteensä 10 henkilötyövuotta. Tämän lisäksi Liikenne- ja viestintäviraston verkkotunnuksiin liittyvän tehtävämäärän arvioidaan lisääntyvän 0,5 henkilötyövuodella.

Esityksestä aiheutuisi kyberkestävyysasetukseen liittyviä kustannuksia tietojärjestelmien ja palveluiden kehittämisestä sekä markkinavalvontaan liittyvistä laboratoriotarkastuksista seuraavasti:

Kertaluonteiset kustannukset		Jatkuvaluontoiset kustannukset	
Selite	Kustannus	Selite	Kustannus
Haavoittuvuuksien raportointiin liittyvät tietojärjestelmät	150.000 eur	Markkinavalvontaan liittyvät laboratoriotarkastukset	100.000 eur vuosittain
Markkinavalvontaan liittyvät tietojärjestelmät	150.000 eur	Tietojärjestelmien ja palveluiden ylläpito ja kehitys	100.000 eur vuosittain
Akkreditoituminen testauslaboratorioksi	200.000 eur	Arvioitu tehtävämäärän lisäyksen laajuus	10 henkilötyövuotta

Verkkotunnuksiin liittyvistä tehtävistä arvioidaan lisäksi aiheutuvan 150.000 eur kertaluontoinen kustannus tietojärjestelmien kehittämisestä. Esityksestä aiheutuisi siten Liikenne- ja viestintävirastolle arvioidun 10,5 henkilötyövuoden laajuisen tehtävämäärän lisäyksen lisäksi yhteensä 650.000 eur kertaluontoinen kustannus, joka toteutuu vuosien 2026–2027 aikana, sekä 200.000 eur jatkuvaluonteinen kustannus, joka toteutuu täysimääräisenä vuosittain vuodesta 2028 alkaen.

Esityksestä aiheutuva tehtävämäärän lisäys sekä kerta- ja jatkuvaluonteiset kustannukset katetaan Liikenne- ja viestintäviraston nykyisistä kehysmäärärahoista. Esityksellä ei näin ollen ole vaikutuksia valtion talousarvioon.

Liikenne- ja viestintäviraston arvion mukaan uusien tehtävien toteuttaminen nykyisten määrärahojen puitteissa on erittäin haastavaa. Tehtävien hoitaminen vähimmäistasolla on erittäin haastavaa huomioiden mahdollisuus myös nykyisten tehtävien uudelleenjärjestelyn hyödyntämiseen täysimääräisesti.

Uudet tehtävät

Esityksen mukaan Liikenne- ja viestintävirasto vastaisi kyberkestävyysasetuksen markkinavalvonnasta. Tehtävä olisi virastolle uusi.

Liikenne- ja viestintävirasto vastaisi uutena tehtävänä kyberkestävyysasetuksen mukaisia ilmoitetun laitoksen tehtäviä hoitavien vaatimustenmukaisuuden arviointilaitoksien ilmoittamisesta ja valvonnasta. Lisäksi kyberkestävyysasetuksen voimaantulo lisää Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksessa sijaitsevan CSIRT-yksikön tehtävämäärää poikkeama- ja haavoittuvuusilmoituksien käsittelyssä ja koordinaatiossa. Liikenne- ja viestintävirasto jatkaisi kansallisen kyberturvallisuussertifioinnin viranomaisen tehtävässä, mihin liittyvien tehtävien määrän ennakoidaan lisääntyvän kyberkestävyysasetuksen voimaantulon myötä.

Markkinavalvonta on keskeinen osa toimivien markkinoiden varmistamisessa. Sillä varmistetaan, että tuotteet vastaavat vaatimuksia. Liikenne- ja viestintävirasto kohdistaisi tehtävässä digitaalisen elementin sisältäviin tuotteisiin markkinavalvontaa vastaavalla tavoin kuin muidenkin tuotesäädösten perusteella nykyisin toimintaan. Valvontatehtävien lisäksi markkinavalvontaviranomainen ohjaa ja neuvoo talouden toimijoita soveltamiseen liittyvissä kysymyksissä. Aiempina vuosina toteutetun tietoturvamerkin ja vuosina 2023–2024 toteutetun radiolaitedirektiivin mukaisten tuotteiden tietoturvallisuuden arvioinnin pilotin kokemusten perusteella arvioitavaksi otettujen tuotteiden tietoturvallisuuden vaatimuksenmukaisuudessa on ongelmia kaikkien tuotetyyppien tuotteiden osalta. Puutteita ja virheitä on sekä tuotteiden teknisen tietoturvan toteutuksessa että esimerkiksi käyttöehdoissa. Valvontatehtäviä tultaisiin toteuttamaan tiiviissä yhteistyössä muiden toimivaltaisten viranomaisten kanssa. Valvonta kohdistuisi poikkeuksellisen laajaan joukkoon tuotteita, joiden valvonta vaatisi erityistä teknistä osaamista. Kyberkestävyysasetuksen mukaiset tehtävät vaativat lisäresursseja salaus- ja tuoteturvallisuustarkastuksiin. Tarvitaan erityistä asiantuntijuutta ja syvää teknistä ymmärrystä, kun tulkitaan tuotteiden teknisiä ratkaisuja ja arvioidaan ilmoitettujen laitosten kyvykkyyttä. Markkinavalvontaviranomaiselle aiheutuu kustannuksia myös viranomaisohjauksesta ja -neuvonnasta. Laajan horisontaalisen soveltamisalan vuoksi ennakoidaan ohjaus- ja neuvontatarpeen olevan laaja erityisesti kyberkestävyysasetuksen siirtymäajalla ja soveltamisen alkaessa.

Kyberturvallisuuskeskuksen CSIRT-yksikön haavoittuvuuskoordinaatioon liittyvät tehtävät tulevat lisääntymään merkittävästi kyberkestävyysasetuksen soveltamisen myötä. Kyberkestävyysasetuksessa valmistajalla on velvollisuus ilmoittaa aktiivisesti hyväksikäytetyistä haavoittuvuuksista ja vakavista poikkeamista viranomaisille. Lisäksi valmistajat voivat ilmoittaa vapaaehtoisesti havaitsemistaan haavoittuvuuksista CSIRT-yksikölle. Pakollisten haavoittuvuusilmoitusten jättäminen on tiukkoihin aikamääreisiin sidottua, jonka vuoksi CSIRT-yksikön olisi valmistauduttava ilmoitusten nopeaan käsittelyyn. Nykytilassa haavoittuvuuskoordinaatioon tulee keskimäärin n. 100–400 ilmoitusta vuositasolla. Kyberkestävyysasetuksen myötä velvoite ilmoittaa aktiivisesti hyödynnetyistä haavoittuvuuksista ja tuotteen tietoturvaan vaikuttavista vakavista poikkeamista tulee kasvattamaan määrää huomattavasti. Tarkkoja arvioita siitä, kuinka monet haavoittuvuudet jäävät raportoimatta, ei ole olemassa. Asiantuntija-arviot nykytilassa ilmoittamattomien haavoittuvuuksien määrästä liikkuvat noin 50–90 %:n välillä. Tämän lisäksi haavoittuvuuksista ei välttämättä ilmoiteta CSIRT-yksiköille vaan suoraan muille tahoille. Varovaisten arvioiden mukaan ilmoituksia haavoittuvuuksista tulisi viikkotasolla yli 50 kappaletta haavoittuvuuskoordinaatioon. Nämä ilmoitukset tulisivat myös markkinavalvontaviranomaisten käsiteltäväksi.

Kyberkestävyysasetuksessa on myös velvoite tarjota tukea pienemmille organisaatioille haavoittuvuuksien ja poikkeamisen selvittämisessä. Nykyisillä CSIRT-yksikön resursseilla pystytään tutkimaan vain vakavimmat tapaukset, jolloin vaikuttavuudeltaan pienempien tapauksien tutkintaan ei ole resursseja tai vaihtoehtoisesti joudutaan jättämään muita vakavia tapauksia tutkimatta. Tutkinnan kesto vaihtelee suuresti ja arviolta kyberkestävyysasetuksen vaatimusten myötä, tapauksia voi tulla viikoittain tutkittavaksi 1–3 kappaletta nykyisten työtehtävien lisäksi. Haavoittuvuudet ilmoitettaisiin ENISA:n haavoittuvuustietokantaan. Haavoittuvuustietojen käsittely tulisi vaatimaan tiivistä yhteistyötä viranomaisten välillä kansallisesti ja kansainvälisesti. Nykyisestä poiketen erityisesti kansainvälisen koordinoinnin tarve lisääntyy.

Liikenne- ja viestintävirasto vastaisi myös ilmoittavan viranomaisen tehtävästä. Tässä tehtävässä viranomainen hyväksyy laitokset ja vastaa niiden valvonnasta. Tehtävään liittyy hyväksyntämenettelyn lisäksi ilmoitusvelvollisuuksia komissiolle. Kyberkestävyysasetuksessa on muista tuoteturvallisuusvaatimuksista poikkeava vaatimustenmukaisuuden osoittaminen. Osalta tuotteista vaaditaan erityistä vaatimustenmukaisuuden osoittamista, kuten ilmoitetun laitoksen suorittamaa tyyppihyväksyntämenettelyä. Kyberkestävyysasetuksen laaja soveltamisala asettaa omat erityispiirteensä myös ilmoitettujen laitosten hyväksynnästä ja valvonnasta vastaavalle viranomaiselle. Viranomaisen tulisi varmistaa, että ilmoitetulla laitoksella on kyvykkyys suorittaa arviointia kutakin sen ilmoittamaa yhdenmukaistettua standardia vasten. Standardien suuri määrä aiheuttaa toimivaltaiselle viranomaiselle perehtymistaakan ja erityisiä tarpeita tekniselle kyvykkyydelle. Ilmoitettujen laitosten hyväksynnästä vastaavan viranomaisen riittävällä resurssoinnilla varmistettaisiin prosessin sujuminen ja ilmoitettujen laitosten riittävän määrä, sekä ehkäistään markkinoille tulon pullonkauloja.

Liikenne- ja viestintävirasto vastaisi jatkossakin kyberturvallisuusasetuksen mukaisesta kansallisen kyberturvallisuussertifioinnin viranomaisen tehtävästä. Liikenne- ja viestintävirasto toimii tehtävässä nykyisinkin sähköisen viestinnän palveluista annetun lain nojalla. Esityksellä ei näin ollen arvioida olevan välitöntä tähän tehtävään liittyvää Liikenne- ja viestintäviraston työmäärää lisäävää vaikutusta. Kansallisen kyberturvallisuussertifioinnin viranomaisen tehtäviin liittyvän työmäärän ennakoidaan kuitenkin kasvavan kyberkestävyysasetuksen soveltamisen alkamisen jälkeen, mikäli kyberturvallisuussertifiointien määrä ja kysyntä kasvaa ennakoidulla tavalla. Kyberturvallisuussertifikaattien kysyntä sekä vaatimustenmukaisuuden arviointilaitosten hakeutuminen kyberturvallisuussertifiointitehtäviin riippuvat esimerkiksi sertifiointijärjestelmien kehitystyön etenemisestä sekä sertifikaattien hyödyntämisen mahdollisuudesta kyberkestävyysasetuksen tai muun edellytetyn vaatimustenmukaisuuden tason osoittamiseksi. Mikäli tulevaisuudessa kehitetään eurooppalaisia kyberturvallisuussertifiointijärjestelmiä, joita hyödynnetään kyberkestävyysasetuksen mukaisten vaatimuksien vaatimustenmukaisuuden osoittamisessa, ennakoidaan toimintaan liittyvän Liikenne- ja viestintäviraston työmäärän kasvavan olennaisesti. Esitys kuitenkin parantaa Liikenne- ja viestintäviraston mahdollisuuksia toteuttaa vaikuttavaa valvontaa. Lisäksi ehdotus tukee viranomaisen tehtävien tarkoituksenmukaista hoitamista mahdollistamalla korkean tason kyberturvallisuussertifikaattien myöntämisen delegoinnin vaatimustenmukaisuuden arviointilaitokselle. Näiltä osin ehdotus selventäisi ja parantaisi viranomaisen toimintaedellytyksiä tehtävässä.

Sähköisen viestinnän palveluista annettuun lakiin ehdotetulla uudella 21 a luvulla olisi vaikutuksia Liikenne- ja viestintäviraston tehtäviin. Viraston olisi pidettävä toimijaluetteloa luvun soveltamisalaan kuuluvista uusista verkkotunnusvälittäjistä sekä tarvittaessa valvottava uusien velvoitteiden noudattamista toimivaltuuksiensa mukaisesti. Myös 21 luvun soveltamisalan laajentaminen verkkotunnusvälittäjien puolesta toimiviin kuten jälleenmyyjiin

lisäisi vähäisessä määrin viraston tehtäviä, joskin jälleenmyyjistä on ollut toimitettava tieto virastolle jo viraston vuonna 2025 voimaan tulleen uuden verkkotunnusmääräyksen nojalla.

4.2.2.2 Muut viranomaisvaikutukset

Esityksellä olisi vaikutuksia suuririskisiä tekoälyjärjestelmiä valvoville viranomaisille. Viranomaisten työmäärä lisääntyisi, sillä ne toimisivat markkinavalvontaviranomaisena suuririskisille tekoälyjärjestelmille kyberkestävyysasetuksen osalta. Tämän johdosta suuririskisiä tekoälyjärjestelmiä valvovien viranomaisten tulisi hankkia ja kehittää kyvykkyyttä kyberkestävyysasetuksen vaatimuksista ja valvonnasta suuririskisille tekoälyjärjestelmille. Vaikutukset markkinavalvontaviranomaisten tehtäviin toteutuisivat täysimääräisesti kyberkestävyysasetuksen tullessa kokonaisuudessaan sovellettavaksi 11.12.2027.

Viranomaisvaikutusten arviointia hankaloittaa kyberkestävyysasetuksen laajan horisontaalisen soveltamisalan lisäksi se, että suuririskisiksi tekoälyjärjestelmiksi katsottavien digitaalisen elementin sisältävien tuotteiden määrää sektoreittain tulevaisuudessa on erittäin vaikea arvioida. Tämä vaikuttaa siihen, mikä osuus markkinavalvontatehtävistä tulee kuulumaan tekoälyjärjestelmiä valvoville viranomaisille. Resurssitarpeita onkin syytä seurata ja tarkastella uudelleen valvontatehtävien alkamisen jälkeen.

Tekoälyasetuksen markkinavalvonnan resurssitarpeita on arvioitu hallituksen esityksessä eduskunnalle EU:n tekoälyasetusta täydentäväksi lainsäädännöksi HE 46/2025 vp, s. 104–108) Tietosuojavaltuutetun toimiston arvion mukaan tekoälyasetuksen mukaisen tekoälyjärjestelmien markkinavalvonta edellyttää 3,5 henkilötyövuoden resurssia. Kyberkestävyysasetuksen yksityiskohtaisemman kyberturvallisuutta koskevan sääntelyn valvonnan voidaan arvioida lisäävän jossakin määrin tätä arvioitua työmäärää. Energiavirasto puolestaan on arvioinut, että suuririskisten tekoälyjärjestelmien kyberkestävyysasetuksen mukaisten tehtävien hoitaminen edellyttää vähintään 1 henkilötyövuoden lisäresurssia sen lisäksi, mitä tekoälyasetuksen kansallisessa valmistelussa on arvioitu Energiaviraston lisäresurssitarpeiksi. Finanssivalvonta taas on pitänyt suuntaa antavana arviona resurssivaikutuksista tältä osin 0,5 henkilötyövuotta. Tullin arvion mukaan tekoälyominaisuuksien mukaan lukien niiden kyberturvallisuuden markkinavalvonnan lisäresurssitarve on kokonaisuutena 3 henkilötyövuotta (vastaavasti HE 46/2025 vp, s. 108). Tulli toimisi Tukesin ohella markkinavalvontaviranomaisena, kun on kyse suuririskisestä tekoälyjärjestelmästä, johon sovelletaan leludirektiiviä. Lisäksi Tulli toimisi ulkorajatarkastuksista vastaavana viranomaisena. Tukes arvioi kyberkestävyysasetuksen valvonnan lisäresurssitarpeeksi 1–2 henkilötyövuotta, minkä lisäksi valvonta edellyttää kertaluonteista 50 000 euron erää toimenpiteisiin, kuten tietojärjestelmien päivittämiseen. Sosiaali- ja terveysalan lupa- ja valvontaviraston (1.1.2026 alkaen Lupa- ja valvontavirasto) tehtävämäärän lisäyksen voidaan arvioida olevan edellisiin verrattava suhteessa sille tekoälyasetuksen osalta arvioituun 3 henkilötyövuoden resurssitarpeeseen. Hallitus ei esitä määrärahaa kyberkestävyysasetuksen toimeenpanoon valtion vuoden 2026 talousarviossa. Tämän vuoksi asetuksen toimeenpano rahoitettaisiin viranomaisten olemassa olevia resursseja uudelleen kohdentamalla.

Esityksellä olisi vaikutuksia Turvallisuus- ja kemikaaliviraston FINAS-akkreditointiyksikölle. Sen suorittamien akkreditointien määrä kasvaisi, mikäli vaatimustenmukaisuuden arviointilaitokset hakisivat akkreditointeja ilmoittautuakseen kyberkestävyysasetuksen mukaiseksi ilmoitetuksi laitokseksi Suomessa. Lisäksi esityksellä ja kyberkestävyysasetuksen soveltamisen käynnistymisellä olisi työmäärää lisääviä vaikutuksia Turvallisuus- ja kemikaaliviraston yhteydessä toimivan markkinavalvonnan yhteyspisteen sekä yhteistyöryhmän toimintaan.

Esityksestä aiheutuisi lisäksi vähäisessä määrin lisähenkilöstön tarvetta Oikeusrekisterikeskukselle, joka vastaisi hallinnollisten seuraamusmaksujen täytäntöönpanosta. Aiheutuvien vaikutusten määrä riippuu lain nojalla määrättävien hallinnollisten seuraamusmaksujen ja maksettavaksi tuomittujen uhkasakkojen määrästä. Hallinnollisten seuraamusten täytäntöönpanoilmoitusten tekemisen on tarkoitus olla ehdotuksen voimaantullessa mahdollista viranomaisportaalin kautta. Esityksestä aiheutuva työmäärän lisäys olisi katettava olemassa olevista valtion talouden kehyspäätösten ja valtion talousarvion mukaisista määrärahoista. Oikeusrekisterikeskuksen määrärahatarpeita kaikkien uusien seuraamusmaksujen täytäntöönpanossa arvioidaan kehys- ja talousarviovalmistelujen yhteydessä.

Hallinnollisia seuraamusmaksuja arvioidaan määrättävän säännöllisesti vuodesta 2028 alkaen. Seuraamusmaksujen määrä olisi soveltamisen ensimmäisen vuosien aikana matalampi kasvaen vuosittain, kunnes määrä vakiintuisi noin 2–3 vuoden soveltamisen kuluttua. Hallinnollisten seuraamusmaksujen määrään vaikuttaisi kyberkestävyysasetuksen valvonnan resursointi ja aktiivisuus sekä toisaalta Suomessa tapahtuvan soveltamisalaan kuuluvan taloudellisen toiminnan määrä. Hallinnollisten seuraamusmaksujen määrän arvioidaan asettuvan sääntelyn soveltamisen alkuvaiheessa vaihteluvälille 5–50 tapausta vuosittain. Maksettavaksi tuomittavien uhkasakkojen määrä arvioidaan tätä selvästi vähäisemmäksi.

4.2.3 Muut vaikutukset

Kyberkestävyysasetuksella parannetaan verkkoon tai toiseen laitteeseen yhdistettävissä olevien tuotteiden, laitteiden ja ohjelmistojen, tietoturvan tasoa. Kyberkestävyysasetuksella asetetaan vähimmäisvaatimukset tuotteiden kyberturvallisuuteen vaikuttaville ominaisuuksille sekä tuotteiden turvallisuuteen vaikuttavien haavoittuvuuksien ja poikkeamien hallinnalle ja ilmoittamiselle tuotteen markkinoille saattamisen jälkeen. Esityksellä arvioidaan olevan myönteisiä vaikutuksia tuotteiden tietoturvan tasoon. Koska esityksen soveltamisala on laaja, esityksellä on välillisesti laajoja myönteisiä vaikutuksia yhteiskunnassa käytettävien digitaalisen elementin sisältävien laitteiden ja ohjelmistojen tietoturvan tasoon Suomessa.

Kyberturvallisuusasetuksen vaikutusarvio sisältyy hallituksen esitykseen eduskunnalle laiksi sähköisen viestinnän palveluista annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi HE 98/2020 vp, s. 149–150. Kyberturvallisuussertifioinnin osalta esityksellä ei arvioida olevan muita, aiemmasta viranomaisvaikutuksia koskevasta arviosta poikkeavia taloudellisia tai tietoyhteiskuntavaikutuksia. Viranomaisen toimivaltuuksien selkeyttäminen parantaa osaltaan yritysten edellytyksiä hyödyntää eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä sekä viranomaisen mahdollisuuksia huolehtia sertifiointijärjestelmien vaatimusten toteutumisesta, millä on välillisiä myönteisiä tietoyhteiskuntavaikutuksia.

5 Muut toteuttamisvaihtoehdot

5.1 Vaihtoehdot ja niiden vaikutukset

5.1.1 Markkinavalvonta

Esityksen valmistelussa on arvioitu vaihtoehtoina markkinavalvontaa koskevien viranomaistehtävien keskittämistä yhteen viranomaiseen tai hajauttamista osittain useampaan viranomaiseen, jotka tekevät nykyisin markkinavalvontaa muiden tuotesäädösten perusteella. Lisäksi valmistelussa on arvioitu markkinavalvontaa koskevien viranomaistehtävien keskittämisen osalta vaihtoehtoina tehtävien osoittamista Turvallisuus- ja kemikaalivirasto Tukesille sekä Liikenne- ja viestintävirastolle, käytännössä sen Kyberturvallisuuskeskukselle.

Kyberkestävyysasetuksen edellyttämässä markkinavalvonnassa on kysymys kokonaan uudesta viranomaistehtävästä, joka on soveltamisalaltaan laaja ja horisontaalinen. Uuden horisontaalisen EU-asetuksen valvonta ei sovellu suoraan nykyisiin kansallisten viranomaisten tehtäviin tai olemassa oleviin hallinnollisin rakenteisiin. Julkisen talouden haastavan tilanteen johdosta viranomaisten kyvykkyys vastaanottaa uusia tehtäviä on haastava, ja vaihtoehtoarvioinnissa onkin painotettu uusien tehtävien sovittamisen kustannustehokkuutta osaksi viranomaisten nykyistä toimintaa. Valmistelussa on todettu, ettei ole tunnistettavissa vaihtoehtoa, jossa kyberkestävyysasetuksen edellyttämä markkinavalvonta voitaisiin toteuttaa kokonaan ilman uusia kustannus- ja resurssivaikutuksia viranomaiselle.

Keskitetyn valvonnan etuna olisi kyberkestävyysasetusta koskevan osaamisen ja asiantuntemuksen keskittäminen viranomaisessa. Kyberturvallisuutta koskevien ominaisuuksien arviointi on sellaisenaan lähtökohtaisesti samankaltaista tuotteen käyttötarkoituksesta riippumatta erityisesti, kun arviointi kohdistuu tuotteen ohjelmiston ominaisuuksiin. Keskitetyn asiantuntemuksen ennakoidaan johtavan myös kyberkestävyysasetuksen yhdenmukaisempaan soveltamiskäytäntöön. Keskitetyn valvonnan haasteina ovat kyberkestävyysasetuksen soveltamisalaan kuuluvien tuotteiden suuri määrä ja siten valvontatehtävän laajuus. Lisäksi markkinavalvontaviranomaisella ei olisi erityistä tuotekohtaista erityisosaamista esimerkiksi riskiarvioinnin osalta. Valmistajien näkökulmasta valvonnan keskittäminen voisi johtaa päällekkäisyyksiin, kun samaan tuotteeseen voisi kohdistua markkinavalvontaa eri tuotesäädöksien perusteella useammasta kuin yhdestä markkinavalvontaviranomaisesta. Vaikka kuvattu tilanne voisi olla kyberkestävyysasetuksen laajan horisontaalisen soveltamisalan johdosta tyypillinen, päällekkäisyydestä valmistajalle aiheutuvat kustannukset arvioidaan vähäisiksi perustuen kokemuksiin muiden tuotesäädösten markkinavalvonnasta samoihin tuotteisiin kohdistuen. Keskitetty valvonta voisi olla kokonaisuutena arvioiden kustannustehokkain ratkaisu markkinavalvonnan järjestämiseksi

Hajautetun valvonnan etuna olisi mahdollisuus yhdistää kyberkestävyysasetuksen markkinavalvontaa myös muihin samaan tuotteeseen kohdistuvien tuotesäädösten markkinavalvonnan kanssa. Lisäksi valvonnan hajauttaminen mahdollistaisi paremmin nykyisen tuote- ja toimialakohtaista asiantuntemuksen hyödyntämistä viranomaisessa myös kyberkestävyysasetuksen valvonnassa. Hajautettu valvonta laajentaisi ja kehittäisi kyberturvallisuuteen liittyvää osaamista nykyisissä markkinavalvontaviranomaisissa. Hajautetun valvonnan haasteena on kuitenkin kyberturvallisuutta koskevan asiantuntemuksen hankkimista useammalle viranomaiselle. Hajautettu valvonta olisi oletettavasti keskitettyä valvontaa suurempia kustannuksia luova tapa järjestää valvonta. Kyberkestävyysasetuksen soveltamisalaan kuuluu merkittävä määrä tuotteita ja ohjelmistoja, joihin ei ennalta kohdistu muita tuoteturvallisuussäädöksiä tai niiden valvontaa, joiden valvonta tulisi myös hajautetussa mallissa uutena tehtävänä. Lisäksi valvonnan hajauttaminen loisi riskiä kyberkestävyysasetuksen soveltamisen ja tulkinnan hajautumiselle.

Hajautettuun valvontaan liittyvien haasteiden ja keskitetystä valvonnasta aiheutuvista päällekkäisyyksistä valmistajille aiheutuvan merkityksen vähäisyyden vuoksi esityksessä on päädytty ehdottamaan markkinavalvonnan järjestämistä mahdollisimman keskitetysti.

Valvonnan keskittämisen osalta on arvioitu vaihtoehtoina markkinavalvonnan osoittamista joko Liikenne- ja viestintävirasto Traficomin tai Turvallisuus- ja kemikaalivirasto Tukesin tehtäväksi.

Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksella on olemassa olevaa osaamista laitteiden kyberturvallisuusominaisuuksista ja niiden arvioinnista. Liikenne- ja viestintävirasto on vuodesta 2019 alkaen myöntänyt valmistajille vapaaehtoista Tietoturvamerkkiä ja arvioinut

laitteiden kyberturvallisuusominaisuuksia Tietoturvamerkille asettamiensa vaatimuksien osalta. Lisäksi Liikenne- ja viestintävirasto valvoo radiolaitteita koskevan tuotesäädöksen mukaisia tietoturvavaatimuksia 1.8.2025 alkaen. Liikenne- ja viestintävirastolla on myös muuta markkinavalvontaa koskevia viranomaistehtäviä. Liikenne- ja viestintävirasto tekee nykyisin eräiden tuotteiden markkinavalvonnasta annetun lain (1137/2016) nojalla markkinavalvontaa kohdistuen ilma-aluksiin, ajoneuvoihin, huviveneisiin, laivavarusteisiin, radiolaitteisiin, ja eräiden tuotteiden esteettömyysvaatimuksiin. Toisaalta Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksella ei ole markkinavalvontaa koskevaa asiantuntemusta tai nykyisiä markkinavalvontatehtäviä.

Turvallisuus- ja kemikaalivirastolla on vakiintunutta osaamista tuoteturvallisuussäädöksistä ja markkinavalvonnan järjestämisestä. Tukesilla on myös osaamista ja kokemusta markkinavalvontaa koskevasta yhteistyöstä EU-jäsenvaltioiden kesken. Turvallisuus- ja kemikaaliviraston yhteydessä toimii markkinavalvonnan yhteistyöryhmä ja -yhteyspiste. Turvallisuus- ja kemikaalivirastolle on myös osoitettu kyberturvallisuuslain mukainen valvovan viranomaisen tehtävä 8.4.2025 voimaan tulleella kyberturvallisuuslailla eräitä toimialoja koskien. Toisaalta Turvallisuus- ja kemikaalivirastolla ei kuitenkaan ole olemassa olevaa asiantuntemusta ohjelmistojen ja laitteiden kyberturvallisuuteen vaikuttavista ominaisuuksista tai niiden arvioinnista.

Kyberkestävyysasetuksen valvonnan järjestämisen kannalta arvioidaan, että markkinavalvontaa koskevan osaamisen kerryttäminen viranomaiseen on kustannustehokkaampi vaihtoehto kuin kyberturvallisuutta koskevan osaamisen kerryttäminen markkinavalvontaa tuntevalle viranomaiselle. Lisäksi valmistelussa on arvioitu perustelluimmaksi keskittää markkinavalvontatehtävä markkinavalvontaa koskevan osaamisen sijasta valvottavan tuotesäädöksen eli tässä tapauksessa tuotteen kyberturvallisuuteen vaikuttaviin seikkoihin liittyvän asiantuntemuksen perusteella. Näin ollen valmistelussa on päädytty ehdotukseen, jossa kyberkestävyysasetuksen markkinavalvontaa koskeva tehtävä osoitettaisiin mahdollisimman keskitetysti Liikenne- ja viestintävirastolle. Kyberkestävyysasetuksen 52 artiklan johdosta markkinavalvontatehtävää olisi kuitenkin hajautettava suuririskisten tekoälyjärjestelmien osalta niitä kansallisesti valvoville viranomaisille.

Siltä osin kuin on kyse EU:n tekoälyasetuksen (EU) 2024/1689 mukaisista suuririskisistä tekoälyjärjestelmistä, kansallista liikkumavaraa markkinavalvonnan järjestämisestä on rajoitettu kyberkestävyysasetuksessa. Kyberkestävyysasetuksen mukaan tekoälyasetuksen mukaiset markkinavalvontaviranomaiset nimittäin valvovat tässä tapauksessa myös kyberkestävyysasetuksen mukaisia kyberturvallisuusvaatimuksia näiden tekoälyjärjestelmien osalta. Tältä osin toteutuva markkinavalvontamalli riippuu siis tekoälyasetuksen kansallisen täytäntöönpanon yhteydessä tehdystä ratkaisuista siitä, miten tekoälyasetuksen valvonta on järjestetty.

5.1.2 Ilmoittava viranomainen

Esityksen valmistelussa on arvioitu vaihtoehtoina ilmoittavan viranomaisen tehtävään Turvallisuus- ja kemikaalivirasto Tukesia ja Liikenne- ja viestintävirastoa. Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksella on nykyisin tehtäviä, jotka tukevat toimintaa myös kyberkestävyysasetuksen mukaisena ilmoittavana viranomaisena. Lisäksi markkinavalvontaa koskevan toimivallan keskittäminen pääosin Liikenne- ja viestintävirastolle tukee ilmoittavan viranomaisen tehtävän osoittamista niin ikään Liikenne- ja viestintävirastolle.

5.1.3 Seuraamussääntely

Esityksessä ei ole päädytty ehdottamaan rikosoikeudellisia seuraamuksia kyberkestävyysasetuksen tai kyberturvallisuusasetuksen rikkomuksista tai laiminlyönneistä. Rikosoikeudellisen ultima ratio -periaatteen vuoksi rikosoikeudellisia seuraamuksia tulisi käyttää viimeisenä mahdollisena vaihtoehtona rikkomuksen tai laiminlyönnin sanktiointiin. Esityksen valmistelussa ei ole arvioitu, että rikosoikeudellisten seuraamusten määräämiselle olisi painavaa yhteiskunnallista tarvetta, vaan että asetusten rikkomukset on mahdollista sanktioida hallinnollisten seuraamusten keinoin.

Esityksessä ehdotetaan säädettäväksi kyberkestävyysasetuksen 64 artiklan 7 kohdassa annetun kansallisen liikkumavaran sallima poikkeus julkisen hallinnon seuraamusmaksujen osalta niin, ettei hallinnollisia sakkoja voitaisi määrätä viranomaisille tai julkisille elimille. Myöskään kyberturvallisuussertifiointiin liittyvää seuraamusmaksua ei ehdotuksen mukaan voitaisi määrätä viranomaiselle. Kyberturvallisuusasetus jättää asianmukaisten seuraamusten määrittämisen kansalliselle lainsäätäjälle tehokkuus- ja vastaavuusperiaatteiden rajoissa.

Kyberturvallisuusasetus ei sisällä nimenomaisia säännöksiä seuraamusmaksusta vaan edellyttää jäsenvaltioiden antavan säännökset tehokkaista, oikeasuhtaisista ja varoittavista seuraamuksista. Valmistelun yhteydessä on arvioitu, että hallinnollisen seuraamusmaksun sijasta kyseeseen voisivat lähinnä tulla rikosoikeudelliset seuraamukset, jotta niiden voitaisiin katsoa tässä tapauksessa täyttävän asetuksen vaatimukset. Edellä mainitusti esityksessä on päädytty sanktioimaan rikkomukset hallinnollisten seuraamusten kautta.

Valmistelun aikana on arvioitu kyberturvallisuusasetuksen rikkomisesta säädettävän seuraamusmaksun määrää. Seuraamusmaksujen suuruus vaihtelee Suomessa huomattavasti sääntely-yhteyden mukaan. Hallinnollisten sanktioiden sääntelyperiaatteisiin kuuluu, että enimmäismäärältään huomattavan suurten seuraamusmaksujen sääntelyyn tulee suhtautua pidättyvästi yksinomaan kansalliseen harkintaan perustuvassa lainsäädännössä, jollei tällaiselle sääntelylle ole esitettävissä asian luonteeseen liittyviä erityisiä perusteita.

Kansalliseen harkintaan perustuvissa tilanteissa seuraamusmaksun määrä onkin lainsäädännössä usein ollut muutamasta tuhannesta eurosta noin sataan tuhanteen euroon. Viestintäpalvelulain nykyiset seuraamusmaksut ovat suuruudeltaan 1 000–1 000 000 euroa. Viestintäpalvelulaissa korkeimmat seuraamusmaksut määrää markkinaoikeus. Viestintäpalvelulain 334 a §:ssä säädetyn EU:n datanhallinta-asetuksen täytäntöönpanoon liittyvä datan välityspalvelujen tarjoajien seuraamusmaksu taas on määrältään 1 000–100 000 euroa, ja sen määrää Liikenne- ja viestintävirasto. Verkossa tapahtuvaan terroristisen sisällön levittämiseen puuttumisesta annetun lain (99/2023) mukainen oikeushenkilölle määrättävä seuraamusmaksu puolestaan on vähintään 1 000 euroa ja enintään 100 000 euroa.

EU-oikeuteen perustuva sääntely taas sisältää huomattavan korkeita seuraamusmaksuja. Edellä käsitellyn kyberkestävyysasetuksen seuraamusmaksusääntelyn ohella esimerkiksi tietosuoja-asetuksessa ja digitaalisten palvelujen sisämarkkinoista ja direktiivin 2000/31/EY muuttamisesta annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) 2022/2065 (digipalvelusäädös) samoin kuin tekoälyasetuksessa seuraamusmaksun enimmäistaso on miljoonissa euroissa. Tietosuojavaltuutetun toimiston seuraamuskollegio on määrännyt useita seuraamusmaksuja tietosuoja-asetuksen rikkomisesta. Samoin EU:n kyberturvallisuusdirektiivin (NIS 2 -direktiivi) kansallinen täytäntöönpanosääntely (kyberturvallisuuslaki) sisältää korkeita seuraamusmaksuja.

Korkeaakin seuraamusmaksun tasoa kyberturvallisuusasetuksen rikkomisesta voitaisiin perustella sillä, että kyberturvallisuussertifiointiin liittyvillä rikkomuksilla voi olla samankaltaisia vakavia vaikutuksia kuin kyberkestävyysasetuksen tai kyberturvallisuuslain rikkomuksilla. Ruotsissa asianmukaiseksi seuraamusmaksun tasoksi katsottu 10 000–15 000 000 kruunua eli noin 1 300–1 300 000 euroa. Saksassa hallinnollinen sakko taas on enintään 500 000 euroa. Sen sijaan Virossa oikeushenkilölle määrättävä seuraamusmaksu on enintään 20 000 euroa. Vertailumaissa seuraamusmaksun taso vaihtelee siis suuresti.

Ainakin toistaiseksi eurooppalaisten kyberturvallisuussertifiointien on tarkoitus perustua vapaaehtoisuuteen. Sikäli kuin kyberturvallisuussertifiointia käytetään osoittamaan kyberkestävyysasetuksen mukaisuus ja sertifiointiin liittyvä rikkomus merkitsisi samalla myös kyberkestävyysasetuksen vaatimusten rikkomista, tulisi teko kyberkestävyysasetuksen mukaisen seuraamusmaksusääntelyn piiriin. Tämän johdosta valmistelussa on arvioitu, että kyberturvallisuussertifiointia koskeviin rikkomuksiin liitettävän seuraamusmaksun tason kohdalla voidaan lähtökohdaksi asettaa kansalliseen harkintaan perustuvien seuraamusmaksujen taso. Tehokkaana, oikeasuhtaisena ja varoittavana voidaan siten pitää enimmäismäärältään 100 000 euron seuraamusmaksua kyberturvallisuussertifiointia koskevan sääntelyn rikkomisesta. Seuraamusmaksu kohdennettaisiin keskeisimpiin kyberturvallisuusasetuksen sisältämiin velvoitteisiin.

Seuraamusmaksun rajoittaminen 100 000 euroon mahdollista sen, ettei seuraamusmaksusta päättämistä ole tarpeen osoittaa monijäseniselle elimelle. Tällainen seuraamusmaksu rinnastuu hallinnollisiin seuraamuksiin, joita Liikenne- ja viestintäviraston on jo nykyisin mahdollista määrätä. Myöskään muut oikeusturvanäkökohdat eivät tässä tapauksessa edellytä seuraamusmaksusta päättämisen osoittamista monijäseniselle elimelle. Seuraamusmaksun määräämisessä ei arvioida tyypillisesti syntyvän hankalia eri perusoikeuksien keskinäistä punnintaa edellyttäviä tilanteita. Koska tätä seuraamusmaksun tasoa voidaan pitää maltillisena suhteessa muuhun kyberturvallisuutta koskevan EU-sääntelyn mukaisiin seuraamusmaksuihin, olisi tarpeen seurata kyberturvallisuusasetuksen soveltamisesta tulevaisuudessa saatavia kokemuksia Suomessa ja eri jäsenvaltioissa sekä miten eri jäsenvaltioiden sääntely mahdollisesti yhdenmukaistuu tulevaisuudessa.

Esityksessä ei ehdoteta sanktioitavan erikseen tilannetta, jossa markkinatoimija antaisi valheellisen ilmoituksen siitä, että tuotteella, palvelulla tai prosessilla on kyberturvallisuussertifikaatti. Tällainen tilanne voisi tapauksen mukaan tulla arvioitavaksi esimerkiksi sopimattomana menettelynä elinkeinotoiminnassa tai kuluttajansuojalaissa tarkoitettuna harhaanjohtavana markkinointina. Milloin teolla tavoitellaan taloudellista hyötyä tai aiheutetaan taloudellista vahinkoa erehtyneelle, teko voi tulla arvioitavaksi myös petoksena. Ehdotuksessa ei myöskään ehdoteta sanktioitavan totuudenvastaista esiintymistä kyberturvallisuusasetuksen mukaisena komissiolle kyberturvallisuussertifiointia varten ilmoitettuna vaatimustenmukaisuuden arviointilaitoksena. Tällaisen tahon valheellisesti antamilla sertifiointiin liittymillä lausumilla ei olisi oikeusvaikutuksia. Teko voisi niin ikään tulla arvioitavaksi petoksena, ja teko voisi täyttää mahdollisesti myös muun rikoksen kuten virkavallan anastuksen tunnusmerkistön. Näin ollen kuvattujen menettelyiden säätämistä hallinnollisen seuraamusmaksun alaiseksi ei ole pidettävä tarpeellisena kyberturvallisuusasetuksen 65 artiklan kannalta.

Kyberkestävyysasetus ei sisällä kansallista liikkumavaraa hallinnollisen seuraamusmaksun enimmäismäärän osalta 64 artiklan 2–4 kohdissa säädettyjen tekojen osalta.

5.1.4 Passiivisuusvalitus

Kyberturvallisuusasetuksen 64 artiklan 1 kohdan b alakohdan mukaan luonnollisilla henkilöillä ja oikeushenkilöillä on oltava oikeus tehokkaisiin oikeussuojakeinoihin myös kyberturvallisuussertifioinnin viranomaiselle tai tietyissä tapauksissa vaatimustenmukaisuuden arviointilaitokselle tehdyn valituksen (toimenpidepyynnön) käsittelemättä jättämisestä. Tämän johdosta valmistelussa on arvioitu tarvetta säätää ns. passiivisuusvalituksesta.

Esityksessä ei esitettäisi erillisen passiivisuusvalituksen käyttöönottoa. Suomessa passiivisuusvalitus on sisällytetty tietosuojalakiin (21 §) saatettaessa kansallisesti voimaan EU:n tietosuoja-asetusta. Eduskunnan lakivaliokunta on katsonut, että passiivisuusvalitus on Suomen oikeusjärjestelmässä poikkeuksellinen. Voimassa olevaan lainsäädäntöön sisältyy eräitä esimerkkejä viranomaisen viivästystilanteita koskevista oikeussuojakeinoista. Ne kuitenkin liittyvät tilanteisiin, joissa viranomaiselle on säädetty asian ratkaisua koskeva määräaika. (LaVL 15/2023 vp) Tällaista määräaikaa ei kyberturvallisuusasetukseen liity, minkä johdosta on arvioitu, onko passiivisuusvalituksen mahdollistaminen tarpeen EU-lainsäädännöstä johtuvien velvoitteiden täyttämiseksi.

Ensinnäkin eduskunnan lakivaliokunta on katsonut, että kantelumahdollisuus laillisuusvalvojille on tehokas oikeussuojakeino, sillä niiden tehtävänä on ryhtyä kantelun johdosta tarvittaviin toimenpiteisiin (LaVL 5/2018 vp). Toiseksi on mahdollista ymmärtää ”valituksen käsittelemättä jättäminen” (”a failure to act on a complaint”; ”underlåtenhet att vidta åtgärder med anledning av ett klagomål”) siten, että kyse on toimenpidepyynnön tutkimatta jättämistä koskevasta tai vaatimuksen hylkäävästä ratkaisusta eli ratkaisusta, jolla viranomainen päättää olla ryhtymättä toimenpiteisiin valituksen johdosta. Tällaiset ratkaisut ovat valituskelpoisia hallintopäätöksiä.

Edellä mainitut seikat huomioiden uuteen lakiin ei esitetä sisällytettävän passiivisuusvalitusta erillisenä oikeussuojakeinona, sillä käytössä olevan kansallisen kantelumahdollisuuden ylimmälle laillisuusvalvojalle samoin kuin valituksen tutkimatta jättämistä tai hylkäämistä koskevan ratkaisun valituskelpoisuuden voidaan katsoa jo täyttävän sen suojan tarpeen, jota kyberturvallisuusasetuksen 64 artiklan 1 kohdan b alakohta edellyttää.

5.2 Muiden jäsenvaltioiden suunnittelemat tai toteuttamat keinot

5.2.1 Kyberkestävyysasetus

Kyberkestävyysasetusta täydentävää sääntelyä valmistellaan samanaikaisesti myös muissa jäsenvaltioissa. Hallituksen esityksen valmistelun aikana ei ole ollut käytettävissä tietoa siitä, miten kyberkestävyysasetuksen markkinavalvontaa tai sen mukaisten ilmoitettujen laitoksien valvontaa koskevat tehtävät järjestetään muissa jäsenvaltioissa.

Ruotsissa eri tuoteturvallisuussäädösten markkinavalvontatehtäviä on osoitettu yhteensä 17 viranomaiselle. Markkinavalvonta on osoitettu tuotekohtaisesti sille viranomaiselle, jonka toimialaan valvottavat tuotteet liittyvät. Kutakin tuoteturvallisuussäädöstä valvoo eräin poikkeuksin yksi viranomainen. Markkinavalvontaviranomaiset osallistuvat kansalliseen markkinavalvontaneuvostoon (Marknadskontrollrådet), jonka puitteissa tehdään markkinavalvontaan liittyvää yhteistyötä ja tiedonvaihtoa viranomaisten välillä. Ruotsin ja Suomen malli eri tuoteturvallisuussäädösten markkinavalvontatehtävien järjestämisestä viranomaisissa on pääosiltaan toisiaan vastaava. Ruotsissa kyberkestävyysasetuksen markkinavalvontaa on suunniteltu keskitetysti Post- och telestyrelsen -viranomaisen tehtäväksi.

Tanskassa eri tuoteturvallisuussäädösten markkinavalvonta on keskitetympää kuin Suomessa ja Ruotsissa. Suurin osa eri tuoteturvallisuussäädösten mukaisista markkinavalvontatehtävistä on osoitettu turvallisuustekniikkaviranomaiselle (Danish Safety Tehnology Authority). Eräitä tuoteryhmiä on osoitettu toimialakohtaisille viranomaisille, kuten ympäristöviraston kemikaaliturvallisuuspalvelulle. Kutakin tuoteturvallisuussäädöstä valvoo yksi viranomainen pois lukien lelut, joissa valvonta on jaettu kahdelle viranomaiselle.

Saksassa eri tuoteturvallisuussäädösten markkinavalvonta jakautuu liittovaltion ja osavaltioiden viranomaisten kesken. Päävastuu markkinavalvonnan toimeenpanosta on Saksan osavaltioiden viranomaisilla, mutta osa vastuista on jaettu myös liittovaltion viranomaisen kesken. Saksassa markkinavalvonta on siten merkittävästi hajautetumpaa kuin Suomessa ja Ruotsissa. Saksassa kyberkestävyysasetuksen markkinavalvontaa on suunniteltu kuitenkin keskitetysti Bundesamt für Sicherheit in der Informationstechnik (BSI) -viranomaisen tehtäväksi.

Virossa eri tuoteturvallisuussäädösten markkinavalvonta on keskitetympää kuin Suomessa ja Ruotsissa. Suurin osa eri tuoteturvallisuussäädösten mukaisista markkinavalvontatehtävistä on osoitettu kuluttajansuoja- ja tekniikkasääntelyn viranomaiselle (Consumer Protection and Techical Regulatory Authority). Eräitä tuoteryhmiä on osoitettu toimialakohtaisille viranomaisille, kuten terveyslautakunnalle tai merenkulkuviranomaiselle. Kutakin tuoteturvallisuussäädöstä valvoo eräin poikkeuksin yksi viranomainen.

Alankomaissa kyberkestävyysasetuksen markkinavalvonta ja ilmoittavan viranomaisen tehtävä on suunniteltu osoitettavaksi keskitetysti yhdelle viranomaiselle. Tehtävissä toimisi digitaalisen infrastruktuurin virasto (Dutch Authority for Digital Infrastructure). Virastoon on sijoitettu myös kyberturvallisuusasetuksen mukainen kansallisen kyberturvallisuussertifioinnin viranomaisen tehtävä.

Euroopan komission verkkosivuilta on saatavilla tiedot kaikista kansallisista markkinavalvontaviranomaisista eri tuoteturvallisuussäädöksille. Linkki: https://single-market-economy.ec.europa.eu/single-market/goods/building-blocks/market-surveillance/organisation_en.

Markkinavalvonnan sääntelyä Ruotsissa, Tanskassa, Virossa ja Saksassa on arvioitu myös hallituksen esityksen HE 195/2022 vp jaksossa 5.2.

5.2.2 Kyberturvallisuusasetus

Ruotsi

Ruotsissa kyberturvallisuusasetusta täydentävät kansalliset säännökset sisältyvät lakiin 2021:553 (lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt). Laissa säädetään, että kansallisella kyberturvallisuussertifioinnin viranomaisella on kyberturvallisuusasetuksen 58 artiklan 8 kohdassa tarkoitetut toimivaltuudet. Se voi tehostaa päätöstään uhkasakolla, ja sillä on oikeus saada virka-apua ulosottoviranomaiselta. Kyberturvallisuussertifioinnin viranomaisella on oikeus peruuttaa sen tai kyberturvallisuusasetuksen 56 artiklan 6 kohdassa mukaisesti vaatimustenmukaisuuden arviointilaitoksen myöntämä kyberturvallisuussertifikaatti, jos se ei täytä kyberturvallisuusasetuksen tai eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimuksia. Kyseisenä viranomaisena toimii Ruotsin puolustusvoimien materiaalilaitos (Försvarets materielverk) niin, että Swedac (Styrelsen för ackreditering och teknisk kontroll) valvoo vaatimustenmukaisuuden arviointilaitoksia. Laki sisältää säännökset myös

kyberturvallisuussertifiointiin liittyvästä vaatimustenmukaisuuden arviointilaitosten akkreditoinnista. Hallituksella on valta antaa akkreditointivaatimuksista tarkempia määräyksiä.

Ruotsissa on arvioitu, että lain noudattamista on tarkoituksenmukaista tehostaa hallinnollisella seuraamusmaksulla, jonka enimmäismäärän tulee olla riittävän varoittava, sillä rikkomukset voivat vaikuttaa yhteiskunnan elintärkeisiin toimintoihin aiheuttaa vakavia vahinkoja valtion turvallisuudelle (Prop. 2020/21:186, s. 31–32, 37–38). Seuraamusmaksun määrä on lain mukaan 10 000–15 000 000 kruunua eli noin 1 300–1 300 000 euroa. Hallituksen esityksessä vertailukelpoisena pidettiin yhteiskunnan elintärkeisiin toimintoihin ja digitaalisiin palveluihin soveltuvaa seuraamusmaksua, joka oli suuruudeltaan enintään 10 miljoonaa kruunua. Seuraamusmaksun määrääminen on lähtökohtaisesti pakollista, ja se kattaa suhteellisen laajan joukon erilaisia tekoja.

Hallinnollinen seuraamusmaksu määrätään sille, joka on antanut EU-vaatimustenmukaisuusilmoituksen kyberturvallisuusasetuksen 53 artiklan 2 kohdan perusteella, vaikka tieto- ja viestintätekniikan tuotteet, palvelut tai prosessit eivät ole kyberturvallisuuden sertifiointijärjestelmän vaatimusten mukaisia. Seuraamusmaksu määrätään myös väärien tai puutteellisten tietojen antamisesta kyberturvallisuussertifiointia koskevassa hakemuksessa. Seuraamusmaksu määrätään myös, jos sertifikaatin haltija jättää ilmoittamatta viranomaiselle 56 artiklan 8 kohdan mukaisesti haavoittuvuuksista tai epäsäännönmukaisuuksista, jotka saattavat vaikuttaa sertifiointiin liittyvien vaatimusten mukaisuuteen, tai jos tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien, jotka on sertifioitu tai joista on annettu EU-vaatimustenmukaisuusilmoitus, valmistaja tai tarjoaja ei anna 55 artiklan edellyttämiä tietoja, jos se voi aiheuttaa kohonneen alttiuden tietoturvauhille tai vahingon riskin. Lisäksi seuraamusmaksu määrätään sille, joka rikkoo eurooppalaiseen kyberturvallisuussertifikaatin tietynlaisia ehtoja tai käyttää sertifikaattia, joka on peruttu asetuksen 58 artiklan 8 kohdan mukaisesti, sekä sille, joka rikkoo lain 5 §:n nojalla annetussa valvontapäätöksessä asetettua kieltoa. Laissa on säännökset seuraamusmaksun määräämisessä huomioitavista seikoista sekä alentamisesta tai määräämättä jättämisestä, jos siihen on erityistä syytä tai sen määrääminen olisi kohtuutonta.

Viranomaisella on oikeus periä maksuja kyberturvallisuusasetuksen mukaisesta toiminnastaan. Lisäksi laissa säädetään oikeudesta hakea muutosta viranomaisen tai vaatimustenmukaisuuden arviointilaitoksen päätökseen.

Viro

Kyberturvallisuussertifiointia koskevat keskeiset säännökset sisältyvät kyberturvallisuuslakiin (küberturvalisuse seadus). Kansallisena kyberturvallisuussertifioinnin viranomaisena toimii Viron kuluttajansuoja- ja teknisen sääntelyn viranomainen (Tarbijakaitse ja Tehnilise Järelevalve Amet). Hallinnollinen seuraamusmaksu voidaan määrätä, jos EU-vaatimustenmukaisuusilmoitus ei täytä kyberturvallisuusasetuksen 53 artiklan 2 kohdan edellytyksiä tai jos tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien, jotka on sertifioitu tai joista on annettu EU-vaatimustenmukaisuusilmoitus, valmistaja tai tarjoaja rikkoo 55 artiklan 2 kohdan edellytyksiä tietojen antamisesta. Oikeushenkilölle määrättävä seuraamusmaksu on enintään 20 000 euroa.

Saksa

Kyberturvallisuusasetusta täydentävä kansallinen sääntely sisältyy lakiin liittovaltion tietotekniikan turvallisuusvirastosta (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) eli BSI-lakiin. Lain 14 §:ssa säädetään hallinnollisesta sakosta, joka voi

olla enintään 500 000 euroa. Sakko voidaan määrätä tietyistä kyberturvallisuusasetuksen rikkomuksista tai siitä, että vaatimustenmukaisuuden arviointilaitos toimii kyberturvallisuusasetuksen alalla ilman turvallisuusviraston antamaa oikeutta siihen. Asetuksen rikkomisen osalta on sanktioitu 55 artiklan 1 kohdan mukaisen tiedonantovelvoitteen sekä 56 artiklan 8 kohdan mukaisen sertifikaatin haltijan tietojen antamista koskevan velvoitteen laiminlyönnit.

5.2.3 Verkkotunnusvälittäjät

Ruotsi

NIS 2 -direktiivin täytäntöönpano on Ruotsissa kesken. Hallituksen esitys täytäntöönpanolainsäädännöksi on annettu 9.10.2025 (Regeringens proposition 2025/26:28: Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag). Luonnoksen mukaan direktiivin katsotaan edellyttävän, että velvollisuus verkkotunnusrekisterin pitämiseen koskee sekä aluetunnusrekisterin ylläpitäjiä että verkkotunnusvälittäjiä (s. 186). Kyberturvallisuuslakiehdotuksen 2 luvun 11 §:n mukaan toimijan, joka on aluetunnusrekisterin ylläpitäjä tai joka tarjoaa verkkotunnusten rekisteröintipalveluja, on pidettävä yllä rekisteriä verkkotunnuksista ja sen varmuuskopiota. Pykälässä lueteltaisiin tiedot, jotka rekisterin on NIS 2 -direktiivin 28 artiklan 2 kohdan mukaan katettava. Ehdotuksen 2 luvun 12 §:ssä säädettäisiin pääsyn antamisesta maksutta verkkotunnusrekisterin tietoihin erottelematta tilanteita, joissa tietoja pyydetään aluetunnusrekisterin ylläpitäjältä tai verkkotunnusvälittäjältä.

Saksa

Saksan liittohallitus on antanut 25.7.2025 päivätyn lakiehdotuksen NIS 2 -direktiivin täytäntöönpanosta (Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung), jonka mukaan BSI-lain 49–51 §:ssä säädettäisiin jatkossa aluetunnusrekisterin ylläpitäjien ja verkkotunnusvälittäjien velvollisuudesta pitää verkkotunnusrekisteriä ja antaa pääsy tietoihin sekä toimijoiden yhteistyövelvoitteesta. Velvollisuudet koskisivat molempia toimijatyyppejä. Lakiehdotuksen perustelujen (s. 186) mukaan tarkoituksena ei ole kuitenkaan velvoitteiden täyttäminen kaksinkertaisesti vaan niiden toteuttaminen tietyn työnjaon mukaan lakisääteisessä yhteistyössä, mikä pitkälti on jo tilanne käytännössä. Lakiluonnoksen mukaisella yhteistyövelvoitteella pantaisiin täytäntöön NIS 2 -direktiivin 28 artiklan 6 kohta, eikä yhteistyövelvoite lakiehdotuksen perustelujen mukaan koske vain rekisteröintitietojen keruuta vaan kaikkia säädettäviä velvoitteita. Luonnoksessa myös todetaan, että tietojen kaksinkertainen ylläpitäminen voisi tarkoittaa merkittävää tietojen siirtämistä EU:n ulkopuolelle.

6 Lausuntopalaute

Esityksen lausuntokierrosta koskevat tiedot kuvataan edellä jaksossa 1.2.2. Lausuntoyhteenveto on saatavilla Valtioneuvoston hankeikkunasta hanketunnuksella LVM014:00/2024.

Lausuntopalautteessa kannatettiin markkinavalvontaviranomaisen ja ilmoittavan viranomaisen tehtävien osoittamista Liikenne- ja viestintävirastolle. Uusista tehtävistä johtuvia resursointitarpeita korostettiin useissa lausunnoissa niin Liikenne- ja viestintäviraston kuin muidenkin viranomaisten kohdalla. Lausunnoissa esitettiin myös yksityiskohtaisia huomioita esitetystä sääntelystä etenkin viranomaisten toimivaltuuksista ja verkkotunnuksia koskevista ehdotuksista.

Kyberkestävyyden testiympäristöä koskevan säännöksen perusteluja muiden markkinavalvontaviranomaisten kuin Liikenne- ja viestintäviraston roolin kannalta täydennettiin Tullin lausunnon johdosta. Esitykseen ei otettu vaatimusta testiympäristön maksuttomuudesta pk-yrityksille Keskuskauppakamarin esittämällä tavalla, sillä kyberkestävyysasetus ei edellytä tätä ja vaatimus testiympäristön maksuttomuudesta voi käytännössä estää mahdollisuuden sen toteuttamiselle Liikenne- ja viestintäviraston nykyisten määrärahojen puitteissa.

Lausuntojen johdosta tehtiin pieniä tarkennuksia seuraamusmaksun määräämistä koskeviin säännöksiin ja niiden perusteluihin. Esitykseen ei kuitenkaan tehty muutoksia eräässä lausunnossa esitetyllä tavalla sääntelyratkaisun muuttamiseksi siitä, että hallinnollista seuraamusmaksua ei voitaisi määrätä viranomaisille. Tältä osin esitys perustuu perustusvaliokunnan lausuntokäytäntöön koskien hallinnollisten seuraamusmaksujen määräämisen reunaehtoja sekä vastaa esimerkiksi kyberturvallisuuslain ja tietosuojalain voimassa olevia säännöksiä hallinnollisesta seuraamusmaksusta.

Esitykseen ei tehty eräissä lausunnoissa esitettyä muutosta lisätä CSIRT-yksiköllе velvollisuus ilmoittaa saamansa asiakirjan tai tiedon edelleen luovuttamisesta. Valmistelussa on arvioitu, että ilmoitusvelvollisten liikesalaisuuksien salassapito turvataan julkisuuslain ja muun soveltuvan yleislainsäädännön nojalla. Myös mahdollinen tarve kuulla asianosaista asiakirjan luovuttamisesta määräytyy yleislainsäädännön kuten julkisuuslain ja hallintolain perusteella.

Lausuntopalautteen johdosta tehtiin muutoksia ehdotuksen CSIRT-yksikön ja markkinavalvontaviranomaisen välisiä tiedonluovutuksia koskevaan 7 §:n 2 momenttiin ja sen perusteluihin, jotta ehdotus vastaisi tarkemmin kyberkestävyysasetuksen sääntelyä. Samalla muutettiin 9 §:ää ja sen perusteluja.

Esityksen säätämisjärjestysperusteluita on eräiltä osin tarkennettu ja laajennettu. Oikeusministeriön lausunnon johdosta tehtiin tarkennuksia lukuihin, joissa arvioidaan esityksen suhdetta perustuslakiin julkisen hallintotehtävän antamisen ja elinkeinovapauden kannalta. Lisäksi oikeusministeriön lausunnossa ja eräissä muissa lausunnoissa kiinnitettiin huomiota kotirauhan piirissä tapahtuvia tarkastuksia koskeviin toimivaltuuksiin, joita koskevia perusteluja ja säännöksiä muutettiin. Kyberkestävyysasetuksen markkinavalvonnan osalta ehdotuksen 19 §:ään tehtiin sääntelyn oikeasuhtaisuutta varmistavia lisäyksiä. Kyberturvallisuussertifioinnin viranomaisen toimivaltuuksien osalta 25 §:stä puolestaan rajattiin pysyväisluontoiseen asumiseen käytettävät tilat pois tarkastusoikeuden alasta samalla, kun ehdotukseen lisättiin mahdollisuus peruuttaa korkean varmuustason sertifikaatti, jos valvonnassa välttämätöntä tietoa ei saada sertifikaatin haltijalta.

Verkkotunnuksia ja verkkotunnusvälittäjiä koskeviin sähköisen viestinnän palveluista annetun lain muutoksiin ja lisäyksiin tehtiin useita tarkennuksia lausuntopalautteen johdosta. Verkkotunnuksen määritelmään tehtiin tekninen täsmennys. Verkkotunnusvälittäjän määritelmä poistettiin ehdotuksen 3 §:stä tarpeettomana ja selkeytettiin lain uuden 21 a luvun soveltamisalasäännöstä verkkotunnusvälittäjien puolesta toimivien tahojen kannalta. NIS 2 -direktiivin täytäntöönpanon kattavuuden varmistamiseksi ehdotukseen lisättiin samankaltainen soveltamisalan laajennos myös voimassa olevan lain fi- ja ax-päätteisiä verkkotunnuksia koskevan 21 luvun soveltamisalaan. Ehdotukseen lisättiin myös verkkotunnuksiin liittyviä uusia velvoitteita koskevat siirtymäsäännökset.

Verkkotunnusten rekisteröintitietojen keräämistä ja saataville saattamista koskevan lausuntopalautteen johdosta täydennettiin ja täsmennettiin esityksen nykytila-arviota sekä asiaa koskevia säännöksiä ja niiden perusteluja. Lakiehdotukseen lisättiin NIS 2 -direktiivin

perustuva säännös toimijoiden yhteistyövelvollisuudesta sekä täsmennettiin perusteluihin, että rekisteröintitietojen keräämisessä, ylläpitämisessä ja saataville saattamisessa voidaan noudattaa tarkoituksenmukaista työnjakoa päällekkäisyyksien välttämiseksi NIS 2 -direktiivin johdanto-osan 109 johdantokappaleessa kuvatulla tavalla. Verkkotunnusvälittäjien luetteloa koskevaa pykälää täsmennettiin vastaamaan tarkemmin direktiiviä sekä kyberturvallisuuslain sääntelyä, jota vastaavasti pykälään lisättiin myös määräyksenantovaltuus. Verkkotunnustietoihin pääsyn maksuttomuudesta otettiin maininta säännöskohtaisiin perusteluihin.

Ehdotukseen ei sen sijaan lisätty Tekijänoikeuden tiedotus- ja valvontakeskus ry:n lausunnossa esitettyä velvollisuutta kerätä yritysten osalta nimenomaisesti luonnollisen henkilön yhteystiedot sekä verkkotunnusvälittäjien luetteloon että verkkotunnuksen rekisteröineistä yrityksistä verkkotunnusten rekisteröintitietojen tietokantaan. Esityksen jatkovalmistelussa on arvioitu, että NIS 2 -direktiivin 28 artikla ei edellytä tällaisen vaatimuksen asettamista. Esityksellä edellytettäisiin NIS 2 -direktiivin 28 artiklan mukaisten verkkotunnusten rekisteröintitietojen keräämistä ja ylläpitämistä. Vaikka nimenomaisesti luonnollisen henkilön yhteystietojen keräämistä ei edellytettäisi, esityksellä vaadittaisiin verkkotunnuksen haltijan tunnistamiseksi ja siihen yhteyden ottamiseksi tarvittavien tietojen keräämistä. NIS 2 -direktiivin johdanto-osan 111 johdantokappaleen mukaisesti aluetunnusrekisterien ja verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden olisi erityisesti varmennettava ainakin yksi keino ottaa yhteyttä verkkotunnuksen rekisteröijään. . Lisäksi verkkotunnusten rekisteröintitietoihin kohdistuvan oikeutetun pyynnön edellytyksiä ei täsmennetty esitykseen, sillä kysymys on muun kuin käsiteltävänä olevalla esityksellä täydennettävän EU-lainsäädännön soveltamisesta. Pääsyn antamista verkkotunnusten rekisteröintitietoihin käsitellään myös NIS 2 -direktiivin johdanto-osan 109–112 johdantokappaleissa.

Esityksen vaikutusarviointia on täydennetty jatkovalmistelussa lausuntokierroksella esitettyjen arvioiden johdosta erityisesti viranomaisvaikutusten osalta. Esitykseen on tehty lausuntopalautteen johdosta myös muita, pienempiä ja lainsäädäntöteknisiä muutoksia, täsmennyksiä ja täydennyksiä. Lisäksi esitykseen otettiin pykälä avoimen lähdekoodin ohjelmistovastaavien valvonnassa annettavista päätöksistä.

7 Säännöskohtaiset perustelut

7.1 Laki eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista

1 luku – Yleiset säännökset

1 §. *Lain tarkoitus.* Laissa annettaisiin kyberkestävyysasetuksen soveltamista täydentävät ja täsmentävät kansalliset säännökset. Lisäksi laissa säädettäisiin kyberturvallisuusasetuksen mukaisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien täytäntöönpanosta.

Pykälän *1 momentissa* säädettäisiin lain tavoitteesta täsmentää ja täydentää kyberkestävyysasetusta ja sen kansallista soveltamista.

Kyberkestävyysasetuksen soveltamisalasta säädetään asetuksen 1–3 artiklassa. Lakia sovellettaisiin kyberkestävyysasetuksen soveltamisalaan kuuluviin tuotteisiin. Kyberkestävyysasetuksen soveltamisalaan kuuluvat sen 2 artiklan 1 kohdassa tarkoitetut digitaalisen elementin sisältävät tuotteet, joiden käyttötarkoitus tai kohtuudella ennakoitavissa oleva käyttö sisältää suoran tai välillisen loogisen tai fyysisen datayhteyden johonkin laitteeseen tai verkkoon. Kyberkestävyysasetuksen soveltamisalan rajauksista säädetään sen 2 artiklan 2–7 kohdassa ja digitaalisen elementin sisältävän tuotteen määritelmästä asetuksen 3 artiklassa.

Kyberkestävyysasetuksen soveltamisalaan kuuluvia tuotteita ovat esimerkiksi älykellot, turvakamerat, televisiot, lelut, kotitalousreitittimet, palomuurit, pelit sekä ohjelmistot. Soveltamisala kattaa laajasti IoT-laitteita ja ohjelmistoja riippumatta siitä, onko laite tai ohjelmisto tarkoitettu kuluttajan, yrityksen tai julkishallinnon käyttöön. Kyberkestävyysasetusta sovelletaan kaikkiin markkinoilla saataville asetettuihin digitaalisia elementtejä sisältäviin tuotteisiin, joiden käyttötarkoitus tai kohtuudella ennakoitavissa oleva käyttö sisältää suoran tai välillisen loogisen tai fyysisen datayhteyden johonkin laitteeseen tai verkkoon, sen 2 artiklan mukaisesti ja sisältämine poikkeuksineen.

Pykälän *2 momentissa* säädettäisiin lain tavoitteesta täsmentää ja täydentää myös kyberturvallisuusasetusta ja sen kansallista soveltamista. Tavoitteena olisi täydentää kyberturvallisuusasetuksen mukaisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien täytäntöönpanoa. Tällä tarkoitettaisiin sertifiointijärjestelmien valvontaa sekä kyberturvallisuussertifikaattien myöntämistä. Kyberturvallisuusasetuksella on perustettu sertifiointikehys, joka asettaa vaatimukset tieto- ja viestintätekniikan tuotteille, palveluille ja prosesseille laadittaville eurooppalaisille kyberturvallisuuden sertifiointijärjestelmille ja menettelyt niiden laatimiselle.

2 §. *Määritelmät.* Pykälässä säädettäisiin määritelmistä vastaten kyberkestävyysasetuksen ja kyberturvallisuusasetuksen vastaavia määritelmiä.

Momentin *1 kohdassa* säädettäisiin digitaalisen elementin sisältävän tuotteen määritelmästä. Määritelmä vastaisi kyberkestävyysasetuksen 3 artiklan 1 kohdan määritelmää, minkä mukaisesti määritelmä kattaisi myös toisistaan erillään markkinoille saatettavat ohjelmisto- tai laitteistokomponentit. Datan etäkäsittelyratkaisulla tarkoitettaisiin kyberkestävyysasetuksen 3 artiklan 2 kohdan mukaisesti etäältä tapahtuvaa datan käsittelyä, jota varten on suunniteltu ja kehitetty ohjelmisto valmistajan toimesta tai valmistajan vastuulla ja jota ilman digitaalisia elementtejä sisältävä tuote ei kykenisi suorittamaan jotakin toimintoaan. Ohjelmiston, laitteiston, ja komponentin määritelmistä säädetään kyberkestävyysasetuksen 3 artiklan 4–6 kohdassa.

Momentin *2 kohdassa* säädettäisiin ilmoitetun laitoksen määritelmästä. Ilmoitetulla laitoksella tarkoitettaisiin kyberkestävyysasetuksen IV luvun mukaisesti Suomen viranomaisen nimeämää ja Euroopan komissiolle ilmoitettua Suomeen sijoittautunutta vaatimustenmukaisuuden arviointilaitosta.

Momentin *3 kohdassa* säädettäisiin jakelijan määritelmästä. Jakelijalla tarkoitettaisiin kyberkestävyysasetuksen 3 artiklan 17 kohtaa vastaavasti sellaista muuta toimitusketjuun kuuluvaa luonnollista tai oikeushenkilöä kuin valmistajaa tai maahantuojaa, joka asettaa digitaalisia elementtejä sisältävän tuotteen saataville unionin markkinoilla vaikuttamatta sen ominaisuuksiin.

Momentin *4 kohdassa* säädettäisiin maahantuojan määritelmästä. Maahantuojalla tarkoitettaisiin kyberkestävyysasetuksen 3 artiklan 16 kohtaa vastaavasti Euroopan unioniin sijoittautunutta luonnollista tai oikeushenkilöä, joka saattaa markkinoille digitaalisia elementtejä sisältävän tuotteen, jossa on unionin ulkopuolelle sijoittautuneen luonnollisen henkilön tai oikeushenkilön nimi tai tavaramerkki.

Momentin *5 kohdassa* säädettäisiin valmistajan määritelmästä. Valmistajalla tarkoitettaisiin kyberkestävyysasetuksen artiklan 13 kohtaa vastaavasti luonnollista tai oikeushenkilöä, joka kehittää tai valmistaa digitaalisia elementtejä sisältäviä tuotteita tai suunnitteluttaa, kehityttää

tai valmistuttaa digitaalisia elementtejä sisältäviä tuotteita ja pitää niitä kaupan omalla nimellään tai tavaramerkillään joko maksua vastaan, ansaintatarkoituksessa tai maksutta.

Momentin *6 kohdassa* säädettäisiin valtuutetun edustajan määritelmästä. Valtuutetulla edustajalla tarkoitettaisiin kyberkestävyysasetuksen 3 artiklan 15 kohtaa vastaavasti unioniin sijoittautunutta luonnollista henkilöä tai oikeushenkilöä, jolla on valmistajan antama kirjallinen toimeksianto hoitaa valmistajan puolesta tietyt tehtävät.

Momentin *7 kohdassa* säädettäisiin talouden toimijan määritelmästä. Talouden toimijalla tarkoitettaisiin 3–7 kohdassa määriteltyä valmistajaa, valtuutettua edustajaa, maahantuojaa, jakelijaa tai muuta luonnollista henkilöä tai oikeushenkilöä, jota koskevat kyberkestävyysasetuksen mukaiset digitaalisia elementtejä sisältävien tuotteiden valmistamiseen tai markkinoilla saataville asettamiseen liittyvät velvoitteet. Määritelmä vastaisi kyberkestävyysasetuksen 3 artiklan 12 kohtaa.

Momentin *8 kohdassa* säädettäisiin avoimen lähdekoodin ohjelmistovastaavan määritelmästä. Avoimen lähdekoodin ohjelmistovastaavan määritelmä vastaisi kyberkestävyysasetuksen 3 artiklan 14 kohdan määritelmää. Vapaan ja avoimen lähdekoodin ohjelmiston määritelmästä säädetään kyberkestävyysasetuksen 3 artiklan 48 kohdassa.

Momentin *9 kohdassa* säädettäisiin vaatimustenmukaisuuden arviointilaitoksen määritelmästä. Vaatimustenmukaisuuden arviointilaitoksella tarkoitettaisiin elintä, joka suorittaa vaatimustenmukaisuuden arviointitoimia kuten kalibrointia, testausta, sertifiointia ja tarkastuksia. Määritelmä vastaisi Euroopan parlamentin ja neuvoston asetus (EY) n:o 765/2008, akkreditoinnin vaatimusten vahvistamisesta ja asetuksen (ETY) N:o 339/93 kumoamisesta (jäljempänä NLF-asetus) 2 artiklan 13 kohdan määritelmää, johon perustuvat kyberkestävyysasetuksen 3 artiklan 28 kohdan ja kyberturvallisuusasetuksen 2 artiklan 18 kohdan vastaavat määritelmät.

Momentin *10 kohdassa* säädettäisiin akkreditoinnin määritelmästä. Akkreditoinnilla tarkoitettaisiin kansallisen akkreditointielimen antamaa todistusta siitä, että vaatimustenmukaisuuden arviointilaitos täyttää tiettyä vaatimustenmukaisuuden arviointia koskevat, yhdenmukaistetuilla standardeilla vahvistetut vaatimukset, ja tarvittaessa muut vaatimukset, mukaan luettuna ne, jotka on vahvistettu asiaa koskevissa alakohtaisissa ohjelmissa.

Momentin *11 kohdassa* säädettäisiin CSIRT-yksikön määritelmästä. CSIRT-yksiköllä tarkoitettaisiin kyberturvallisuuslain 19 §:ssä tarkoitettua CSIRT-yksikköä.

Momentin *12 kohdassa* säädettäisiin kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen määritelmästä, millä tarkoitettaisiin kyberturvallisuusasetuksen 61 artiklan mukaisesti Euroopan komissiolle ilmoitettua vaatimustenmukaisuuden arviointilaitosta. Vaatimustenmukaisuuden arviointilaitos määritellään edellä 9 kohdassa tavalla, joka vastaa NLF-asetusta ja johon myös kyberturvallisuusasetuksen vastaavassa määritelmässä viitataan. Siinä missä kyberkestävyysasetuksen alalla komissiolle ilmoitettu vaatimustenmukaisuuden arviointilaitos toimii 2 kohdassa tarkoitettuna ilmoitettuna laitoksena NLF-kehikon puitteissa, kyberturvallisuusasetuksessa ei ole kyse unionin yhdenmukaistamislainsäädännöstä eikä sen nojalla komissiolle ilmoitettava vaatimustenmukaisuuden arviointilaitos toimi NLF-kehikon puitteissa, joskin esimerkiksi niiden akkreditointiin sovelletaan kyberturvallisuusasetuksen viittauksen johdosta NLF-asetuksen mukaisia vaatimuksia. Ilmoitettuihin laitoksiin ja kyberturvallisuusasetuksen nojalla ilmoitettuihin vaatimustenmukaisuuden arviointilaitoksiin

kohdistuu samankaltaisia mutta jossain määrin erilaisia vaatimuksia. Tämän erottelun selventämiseksi ehdotetussa laissa käytetään kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen käsitettä yhteyksissä, jotka koskevat kyberturvallisuusasetukseen liittyvää toimintaa. Käytännössä olisi kuitenkin mahdollista, että tietty vaatimustenmukaisuuden arviointilaitos hakeutuisi toimimaan molemmissa rooleissa, jotka voivat tukea toisiaan.

3 §. *Suhde muuhun lainsäädäntöön.* Pykälä sisältäisi informatiiviset viittaukset markkinavalvonta-asetukseen ja markkinavalvontalakiin, joita sovellettaisiin kyberkestävyysasetuksen valvonnassa ehdotetussa laissa säädetyn ohella.

Pykälän *1 momentti* sisältäisi informatiivisen viittauksen markkinavalvonta-asetukseen. Markkinavalvonta-asetusta sovelletaan kyberkestävyysasetuksen 52 artiklan 1 kohdan nojalla digitaalisia elementtejä sisältävien tuotteiden markkinavalvonnassa.

Pykälän *2 momentti* sisältäisi informatiivisen viittauksen eräiden tuotteiden markkinavalvonnasta annettuun lakiin (jäljempänä *markkinavalvontalaki*). Markkinavalvontalakia sovellettaisiin digitaalisia elementtejä sisältävien tuotteiden markkinavalvontaan 2. lakiehdotuksella ehdotettavien muutosten mukaisesti. Markkinavalvontalaissa säädetään tuotteiden markkinavalvonnasta, valvontaviranomaisten toimivaltuuksista ja valvontakeinoista sekä muutoksenhausta viranomaisten päätöksiin.

Pykälän *3 momentti* sisältäisi informatiivisen viittauksen kuluttajatuotteiden turvallisuudesta annettuun lakiin sekä EU:n yleiseen tuoteturvallisuusasetukseen. EU:n yleistä tuoteturvallisuusasetusta sovelletaan sen 2 artiklan mukaisesti tuotteisiin, jotka saatetaan markkinoille tai asetetaan saataville markkinoilla, siltä osin kuin kyseisten tuotteiden turvallisuutta sääntelevässä unionin oikeudessa ei ole erityissäännöksiä, joilla on sama tavoite. Kun tuotteisiin sovelletaan unionin lainsäädännössä asetettuja erityisiä turvallisuusvaatimuksia, asetusta sovelletaan ainoastaan niihin seikkoihin ja riskeihin tai riskiluokkiin, joita kyseiset vaatimukset eivät kata.

Pykälän *4 momentti* sisältäisi informatiivisen viittauksen EU:n tekoälyasetukseen ja eräiden tekoälyjärjestelmien valvonnasta annettuun lakiin, jota koskeva ehdotus sisältyy hallituksen esitykseen eduskunnalle EU:n tekoälyasetusta täydentäväksi lainsäädännöksi (HE 46/2025 vp). Tekoälyasetuksessa ja sitä täydentävässä kansallisessa sääntelyssä säädetään tekoälyjärjestelmiä koskevista vaatimuksista ja niiden valvonnasta tekoälyasetuksen soveltamisalaan kuuluville tuotteille.

Pykälän *5 momentti* sisältäisi informatiivista viittauksen CSIRT-yksikön tehtävistä muualla laissa säädettyyn. CSIRT-yksikön tehtävistä ja haavoittuvuuskoordinaatiosta muuten kuin kyberkestävyysasetuksessa tarkoitettujen tehtävien ja ilmoitusten käsittelyn osalta säädetään kyberturvallisuuslaissa. Kyberkestävyysasetuksen 14–17 artiklassa säädetään digitaalisia elementtejä sisältävään tuotteeseen sisältyvistä haavoittuvuuksista ja eräistä muista seikoista tehtävistä pakollisista ja vapaaehtoisista ilmoituksista ja niiden käsittelystä. Ilmoituksia vastaanottaisi ja käsittelisi kansallisesti CSIRT-yksikkö. Säännösten sisältö on kuvattu tarkemmin luvussa 2.1.3.1.

CSIRT-yksikkö vastaanottaa myös muita kuin kyberkestävyysasetuksessa tarkoitettuja vapaaehtoisia haavoittuvuusilmoituksia osana sen olemassa olevien kyberturvallisuuslain mukaisten tehtävien hoitamista. Asiaa käsitellään myös 8 §:n perusteluissa. CSIRT-yksikön kyberturvallisuuslain 22 §:n mukainen haavoittuvuuskoordinaatiotehtävä kattaisi kyberkestävyysasetuksen soveltamisalan ulkopuolelle jäävien tuotteiden ja palvelujen

sisältämiä haavoittuvuusilmoituksia sekä organisaatioiden toimintaan liittyviä haavoittuvuusilmoituksia.

2 luku – Vaatimustenmukaisuus ja ilmoitukset

4 §. *Digitaalisen elementin sisältävän tuotteen vaatimustenmukaisuus.* Pykälä sisältäisi informatiivisen viittauksen kyberkestävyysasetuksen nojalla asetettuihin vaatimuksiin digitaalisen elementin sisältäville tuotteille.

Kyberkestävyysasetuksen 6 artiklan nojalla digitaalisia elementtejä sisältävän tuotteen saa asettaa markkinoille ainoastaan, jos se täyttää asetuksen liitteessä I olevassa I osassa vahvistetut olennaiset kyberturvallisuusvaatimukset, edellyttäen että sitä käytetään asianmukaisesti asennettuina ja ylläpidettyinä käyttötarkoituksensa mukaisesti tai kohtuudella ennakoitavissa olosuhteissa ja tarvittaessa tarpeelliset tietoturvapäivitykset on asennettu. Lisäksi edellytyksenä on, että valmistajan käyttöön ottamat prosessit täyttävät asetuksen liitteessä I olevassa II osassa vahvistetut olennaiset kyberturvallisuusvaatimukset.

Talouden toimijan velvollisuuksista ja digitaalisen elementin sisältävää tuotetta koskevista vaatimuksista säädetään asetuksen 2 luvussa sekä liitteissä I ja II ja vaatimustenmukaisuuden osoittamisesta asetuksen 3 luvussa.

5 §. *Keskeneräiset tuotteet.* Kyberkestävyysasetuksen 4 artiklan 2 ja 3 kohdissa säädetään tilanteista, joissa jäsenvaltiot eivät saa estää esittelemästä, käyttämästä tai asettamasta saataville markkinoilla digitaalisen elementin sisältäviä tuotteita, jotka eivät täytä kyberkestävyysasetuksen vaatimuksia. EU-oikeuden etusijaperiaatteen nojalla sovellettavaksi ei voisi tulla 4 artiklan vastaista kansallista normia. Sääntelyn selkeyttämiseksi ja oikeustilan tarkentamiseksi erityisesti hallinnollista seuraamusmaksua 6 luvussa koskevien ehdotuksien kannalta ehdotetaan säädettäväksi erikseen 4 artiklan 2 ja 3 kohtien mukaisen keskeneräisen tuotteen esittelyn, käytön tai markkinoilla saattaville asettamisen sallimisesta.

Pykälässä säädettäisiin mahdollisuudesta esitellä, käyttää tai saattaa markkinoille digitaalisen elementin sisältävä tuote, silloin kuin se ei täytä kyberkestävyysasetuksen vaatimuksia. Kyberkestävyysasetuksen 4 artiklan 2 kohdan mukaisesti digitaalisen elementin sisältävää tuotetta sekä sen prototyyppiä, jotka eivät täytä asetuksen vaatimuksia, saisi esitellä tai käyttää messuilla, näyttelyissä, esittelytilaisuuksissa tai vastaavissa tapahtumissa edellyttäen, että tuotteet esitellään sellaisella näkyvällä merkinnällä varustettuna, josta käy selvästi ilmi, että tuote ei ole kyberkestävyysasetuksen vaatimuksien mukainen ja että tuotetta ei saa asettaa saataville markkinoilla ennen kuin se on sitä. Kyberkestävyysasetuksen 4 artiklan 3 kohdan mukaisesti keskeneräisen ohjelmiston, joka ei täytä kyberkestävyysasetuksen vaatimuksia, saisi asettaa saataville markkinoilla edellyttäen, että ohjelmisto asetetaan saataville vain rajoitetuksi ajaksi, joka on tarpeen testausta varten, ja että sillä on näkyvä merkintä, josta käy selvästi ilmi, että ohjelmisto ei ole kyberkestävyysasetuksen mukainen ja että se ei ole saatavilla markkinoilla muita tarkoituksia kuin testausta varten.

Selvyyden vuoksi todetaan, että digitaalisen elementin sisältävän tuotteen käytölle voisi kuitenkin aiheutua muusta sääntelystä aiheutuva este. Esimerkiksi digitaalisen elementin sisältävän tuotteen ollessa radiolaite voi sen käyttö vaatia radioluvan. Säännös koskisi digitaalisen elementin sisältävän tuotteen esittelyä, vaikka kyberkestävyysasetuksen mukainen vaatimustenmukaisuus ei täyttyisi. Säännöksen tarkoituksena ei olisi muodostaa perustetta poiketa muussa sääntelyssä tuotteelle asetettavista vaatimuksista, mikäli sellaisia tuotteeseen soveltuu.

6 §. *Digitaalisen elementin sisältävä tuote julkisessa hankinnassa.* Pykälässä säädettäisiin hankintayksikön velvollisuudesta ottaa huomioon kyberkestävyysasetuksen liitteessä I vahvistettujen kyberturvallisuusvaatimusten noudattaminen, mukaan lukien valmistajien kyky käsitellä tehokkaasti haavoittuvuuksia, silloin, kun julkisen hankinnan kohteena on digitaalisen elementin sisältävä tuote. Säännöksellä täydennettäisiin kyberkestävyysasetuksen 5 artiklan 2 kohtaa, joka edellyttää jäsenvaltiota varmistamaan, että hankittaessa kyberkestävyysasetuksen soveltamisalaan kuuluvia digitaalisia elementtejä sisältäviä tuotteita, hankintaprosessissa on otettava huomioon kyberkestävyysasetuksen liitteessä I vahvistettujen olennaisten kyberturvallisuusvaatimusten noudattaminen, mukaan lukien valmistajien kyky käsitellä tehokkaasti haavoittuvuuksia, tämän kuitenkaan rajoittamatta julkisia hankintoja koskevien direktiivien 2014/24/EU ja 2014/25/EU soveltamista. Käytännössä hankintayksikkö voisi huomioida kyberturvallisuutta koskevien vaatimuksien noudattamista esimerkiksi hankintaa ja tarjouspyyntöä valmisteltaessa, hankinnan kohteelle asetettavia vaatimuksia harkitessa sekä ehdokkaan tai tarjoajan soveltuvuuskriteereitä asetettaessa. Säännös olisi tarkoitettu sovellettavaksi julkisista hankinnoista ja käyttöoikeussopimuksista annetun lain soveltamisalaan kuuluviin hankintoihin, joissa hankinnan kohteena on tuote, johon sovelletaan kyberkestävyysasetuksen vaatimuksia.

7 §. *Valmistajan ilmoitusvelvollisuus.* Pykälän *1 momentti* sisältäisi informatiivisen viittauksen kyberkestävyysasetuksen 14 artiklassa säädettyyn velvollisuuteen ilmoittaa digitaalisen elementin sisältävään tuotteeseen sisältyvästä aktiivisesti hyödynnetystä haavoittuvuudesta tai digitaalisen elementin sisältävän tuotteen tietoturvaan vaikuttavasta vakavasta poikkeamasta. Ilmoitus olisi tehtävä kyberkestävyysasetuksen 16 artiklassa tarkoitetun keskitetyn raportointialustan kautta CSIRT-yksikölle ja Euroopan unionin kyberturvallisuusvirasto ENISA:lle. Aktiivisesti hyödynnetyn haavoittuvuuden määritelmästä säädetään asetuksen 3 artiklan 40 ja 42 kohdissa ja vakavan poikkeaman määritelmästä asetuksen 3 artiklan 43 ja 44 kohdissa ja 14 artiklan 5 kohdassa. Ilmoitukset olisi tehtävä asetuksen 14 artiklan 2 ja 4 kohdissa säädettyjen määräaikojen ja tietosisältöjen mukaisina. Liikenne- ja viestintävirastossa sijaitseva CSIRT-yksikkö voisi tarvittaessa pyytää lisätietoja väliraportilla digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavan aktiivisesti hyödynnetyn haavoittuvuuden tai vakavan poikkeaman tilanteesta kyberkestävyysasetuksen 14 artiklan 6 kohdan mukaisesti. Lisäksi valmistajan olisi tiedotettava asetuksen 14 artiklan 8 kohdan mukaisesti tuotteen käyttäjiä. Ilmoitusvelvollisuuksia sovelletaan lisäksi myös avoimen lähdekoodin ohjelmistovastaaviin asetuksen 24 artiklan 3 kohdan nojalla.

Pykälän *2 momentissa* säädettäisiin selvyyden vuoksi CSIRT-yksikön ja markkinavalvontaviranomaisen yhteistyöstä. Momentti sisältäisi informatiivisen viittauksen kyberkestävyysasetuksen 16 artiklan 3 kohtaan, jonka mukaisesti koordinaattoreiksi nimettyjen CSIRT-yksiköiden on annettava jäsenvaltioidensa markkinavalvontaviranomaisille aktiivisesti hyödynnetystä haavoittuvuudesta tai vakavasta poikkeamasta ilmoitetut tiedot, joita markkinavalvontaviranomaiset tarvitsevat täyttääkseen asetuksen mukaiset velvoitteensa. CSIRT-yksikön tiedonantovelvollisuus kohdistuisi käytännössä kyberkestävyysasetuksen 14 artiklassa yksilöityihin tietotyyppeihin, jotka valmistajan on sisällytettävä ilmoitukseensa. Markkinavalvontaviranomaisella olisi kyberkestävyysasetuksen 16 artiklan 3 kohdassa säädetyn johdosta oikeus saada myös tarvitsemansa salassa pidettävät tiedot ilmoituksesta. CSIRT-yksikön oikeudesta luovuttaa salassa pidettäviä tietoja säädettäisiin jäljempänä 9 §:n 1 kohdassa. Markkinavalvontaviranomaisen voidaan katsoa tarvitsevan kaikki haavoittuvuus- tai poikkeamailmoitukseen sisältyvät, kyberkestävyysasetuksen edellyttämät tiedot.

8 §. *Vapaaehtoinen ilmoittaminen*. Pykälässä säädettäisiin kyberkestävyysasetuksen 15 artiklan mukaisista vapaaehtoisista ilmoituksista, joita CSIRT-yksikkö ottaisi *1 momentin* mukaisesti vastaan Euroopan unionin kyberturvallisuusvirasto ENISA:n ohella valmistajilta ja muilta

tahoilta. Kyberkestävyysasetuksen 15 artiklan 1 tai 2 kohdan mukainen vapaaehtoisen ilmoitus voi koskea 1) digitaalisia elementtejä sisältävään tuotteeseen sisältyvää haavoittuvuutta; 2) kyberuhkaa, joka voi vaikuttaa digitaalisia elementtejä sisältävän tuotteen riskiprofiiliin; tai 3) mahdollisista digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavista poikkeamista sekä läheltä piti -tilanteista, jotka olisivat voineet johtaa tällaiseen poikkeamaan.

Vapaaehtoiset ilmoitukset olisi käsiteltävä kyberkestävyysasetuksen 15 ja 16 artiklassa säädetyn menettelyn mukaisesti. Jos muu kuin valmistaja ilmoittaisi aktiivisesti hyödynnetystä haavoittuvuudesta tai digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavasta vakavasta poikkeamasta, koordinaattoriksi nimetyn CSIRT-yksikön olisi ilmoitettava siitä valmistajalle ilman aiheetonta viivytystä. CSIRT-yksikkö voisi asettaa etusijalle pakollisten ilmoitusten eli kyberkestävyysasetuksen 14 artiklassa tarkoitettujen ilmoitusten käsittelyn vapaaehtoisiin ilmoituksiin nähden.

Selvyyden vuoksi todetaan, että kyberkestävyysasetuksen haavoittuvuusilmoituksia koskevien säännösten soveltamisen alkaessa CSIRT-yksikön vastaanottamia haavoittuvuusilmoitukset voidaan jakaa kolmeen luokkaan: 1) kyberkestävyysasetuksen 14 artiklan mukaiset pakolliset haavoittuvuusilmoitukset; 2) kyberkestävyysasetuksen 15 artiklan mukaiset vapaaehtoiset haavoittuvuusilmoitukset ja 3) muut vapaaehtoiset haavoittuvuusilmoitukset. Luokkien 1 ja 2 mukaisten ilmoitusten käsittelyyn sovelletaan kyberkestävyysasetuksen mukaisia toimenpiteitä, kuten velvoitetta ilmoittaa haavoittuvuusilmoituksista muille jäsenvaltioille. Luokan 3 mukaisten vapaaehtoisten haavoittuvuusilmoituksien käsittelyyn ei sovellettaisi kyberkestävyysasetuksen sääntelyä, vaan niitä koskevasta haavoittuvuuskoordinaatiosta säädettäisiin kyberturvallisuuslain 22 §:ssä.

CSIRT-yksikölle voitaisiin siten ilmoittaa myös muutenkin kuin kyberkestävyysasetuksen 15 artiklassa tarkoitettuna vapaaehtoisena ilmoituksena vapaaehtoisesti haavoittuvuuksista, kyberuhkista, poikkeamista ja läheltä piti -tilanteista. Tällaiset ilmoitukset eivät kuuluisi säännöksen tai kyberkestävyysasetuksen ilmoituksien käsittelyä koskevien velvoitteiden soveltamisalaan.

Pykälän *2 momentin* nojalla kyberkestävyysasetuksen 15 artiklan mukaisesti CSIRT-yksikölle vapaaehtoisesti ilmoitettua tietoa ei saa ilman ilmoittajan suostumusta käyttää ilmoittajaan kohdistuvassa rikostutkinnassa eikä hallinnollisessa tai muussa tiedon luovuttajaan kohdistuvassa päätöksenteossa. Kyberkestävyysasetuksen 15 artiklan 5 kohdan mukaisesti vapaaehtoinen ilmoittaminen ei saisi johtaa sellaisten lisävelvoitteiden asettamiseen ilmoituksen tehneelle luonnolliselle henkilölle tai oikeushenkilölle, joita siihen ei olisi sovellettu, jos se ei olisi toimittanut kyseistä ilmoitusta, sanotun kuitenkaan rajoittamatta rikosten ennaltaehkäisemistä, tutkimista, paljastamista ja rikoksiin liittyviä syytetoimia. Säännöksen tarkoitus olisi suojata vapaaehtoista ilmoittajaa sekä kannustaa vapaaehtoiseen ilmoittamiseen turvallisuuden parantamiseksi.

9 §. *CSIRT-yksikön oikeus luovuttaa salassa pidettäviä tietoja.* Pykälässä säädettäisiin CSIRT-yksikön oikeudesta luovuttaa salassapitovelvoitteiden ja muiden tietojen luovuttamista koskevien rajoitusten estämättä tietoja sen hoitaessa kyberkestävyysasetuksen 14–17 artiklan mukaisia haavoittuvuus- ja poikkeamailmoitusten käsittelyyn liittyviä tehtäviä. Säännös olisi tarpeen kyberkestävyysasetuksella CSIRT-yksikölle osoitettujen tehtävien hoitamiseksi. Artiklojen sisältö kuvataan tarkemmin luvussa 2.1.3.1. Pykälän nojalla CSIRT-yksikkö voisi luovuttaa tietoja oma-aloitteisesti kyseisten haavoittuvuus- ja poikkeamailmoitusten käsittelyyn liittyvien tehtävien hoitamiseksi kyberkestävyysasetuksen mukaisesti.

Tiedonluovutusoikeus olisi välttämätön, jotta CSIRT-yksikkö voi välittää ilmoituspalvelussa vastaanottamansa ilmoitukset kyberkestävyysasetuksen 16 artiklan 2 kohdan mukaisesti toisille koordinaattoreiksi nimetyille CSIRT-yksiköille alueella, jolla valmistaja on ilmoittanut asettaneensa digitaalisia elementtejä sisältävän tuotteen saataville. Ilmoitukset tulisivat lähtökohtaisesti samanaikaisesti myös ENISA:n saataville, kun ne tehdään CSIRT-yksikölle. Kyberkestävyysasetuksen 16 artiklan 2 kohdassa säädetyssä poikkeustilanteessa ilmoituksen välittämistä voidaan kuitenkin lykätä.

Pykälän *1 momentti* olisi soveltamisalaltaan rajattu CSIRT-yksikön kyberkestävyysasetuksen 14 artiklan 2, 4 ja 6 kohdissa yksilöityihin pakollisten haavoittuvuus- ja poikkeamailmoitusten tietotyyppeihin sekä vastaaviin 15 artiklan nojalla annettujen vapaaehtoisten ilmoitusten sisältämiin tietoihin. Tiedonluovutusoikeus olisi sidottu tarpeellisuusedellytykseen ja koskisi tietoja, joita sisältyisi CSIRT-yksikön vastaanottamiin pakollisiin ennakkovaroitusilmoituksiin, poikkeamailmoituksiin, haavoittuvuusilmoituksiin ja mahdollisiin väliraportteihin sekä loppuraportteihin samoin kuin haavoittuvuuksia, poikkeamia ja lähellä piti -tilanteita koskeviin vapaaehtoisiin ilmoituksiin.

Pakollisten ilmoitusten sisältämät tietotyypit on yksilöity 14 artiklassa. Haavoittuvuudesta annetaan artiklan 2 kohdan nojalla ennakkovaroitusilmoitus (so. tieto haavoittuvuuden olemassaolosta ja tulevasta ilmoituksesta), jossa ilmoitetaan tarvittaessa jäsenvaltiot, joiden alueella valmistaja tietää digitaalisia elementtejä sisältävää tuotettaan asetetun saataville. Varsinaisessa haavoittuvuusilmoituksessa annetaan yleiset tiedot kyseisestä digitaalisia elementtejä sisältävästä tuotteesta, kyseisen hyödyntämisen ja haavoittuvuuden yleisestä luonteesta sekä toteutetuista korjaavista tai lieventävistä toimenpiteistä ja korjaavista tai lieventävistä toimenpiteistä, joita käyttäjät voivat toteuttaa. Haavoittuvuutta koskevassa loppuraportissa puolestaan on annettava kuvaus haavoittuvuudesta, sen vakavuudesta ja vaikutuksesta, mahdolliset tiedot mahdollisista pahantahtoisista toimijoista, jotka ovat hyödyntäneet tai hyödyntävät haavoittuvuutta sekä yksityiskohtaiset tiedot tietoturvapäivityksestä tai muista korjaavista toimenpiteistä, jotka on asetettu saataville haavoittuvuuden korjaamiseksi. Poikkeamia koskien artiklan 4 kohdan nojalla ennakkovaroituksen olisi puolestaan sisällettävä tieto, epäilläänkö poikkeamaa laittomien tai pahantahtoisten tekojen aiheuttamaksi, ja siinä ilmoitetaan tarvittaessa jäsenvaltiot, joiden alueella valmistaja tietää digitaalisia elementtejä sisältävää tuotettaan asetetun saataville. Varsinaisessa poikkeamailmoituksessa tulisi antaa yleisiä tietoja poikkeaman luonteesta, alustava arvio poikkeamasta sekä tietoa toteutetuista korjaavista tai lieventävistä toimenpiteistä ja korjaavista tai lieventävistä toimenpiteistä, joita käyttäjät voivat toteuttaa. Poikkeamaa koskevan loppuraportin puolestaan tulee sisältää yksityiskohtainen kuvaus poikkeamasta, mukaan lukien sen vakavuus ja vaikutukset, uhkan tyyppi tai poikkeaman todennäköisesti aiheuttanut perimmäinen syy sekä toteutetut ja meneillään olevat lieventämistoimenpiteet. Artiklan 6 kohdan nojalla CSIRT-yksikkö voi pyytää valmistajia toimittamaan väliraportin, joka sisältää merkityksellisiä ajantasaisia tietoja digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavan aktiivisesti hyödynnetyn haavoittuvuuden tai vakavan poikkeaman tilanteesta. Väliraportti sisältäisi siis päivityksen 2 ja 4 kohdan nojalla annettuihin tietoihin.

Vapaaehtoisten ilmoitusten osalta CSIRT-yksikölle voidaan ilmoittaa mahdollisista digitaalisia elementtejä sisältävään tuotteeseen sisältyvistä haavoittuvuuksista tai kyberuhkista, jotka voisivat vaikuttaa digitaalisia elementtejä sisältävän tuotteen riskiprofiiliin, sekä mahdollisista digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavista poikkeamista ja läheltä piti -tilanteista, jotka olisivat voineet johtaa tällaiseen poikkeamaan. Luovutettavia tietotyyppejä täsmennettäisiin ehdotuksessa edellyttämällä, että kyseessä on 14 artiklan 2, 4 ja 6 kohdissa mainittuja tietoja vastaava tieto, jotta on selvää, että tiedonluovutukset voidaan sitoa tarpeellisuusedellytykseen.

Pykälän *2 momentissa* säädettäisiin lisäksi mahdollisuudesta luovuttaa muitakin kuin edellä yksilöityjä, CSIRT-yksikön kyberkestävyysasetuksen mukaisia tehtäviä hoitaessaan saamia tietoja. Tietoja voitaisiin tällöin luovuttaa momentin mukaan vain 1 momentissa tarkoitetuille tahoille. Edellytyksenä olisi, että tiedon luovuttaminen on 1 momentista poiketen välttämätöntä kyberkestävyysasetuksen 14–17 artiklassa säädettyjen tehtävien toteuttamiseksi. Ehdotus on tarpeellinen, sillä ilmoitusten käsittelyssä voi syntyä myös sellaista olennaista liitännäistietoa, joka ei välttämättä kuulu kyberkestävyysasetuksen 14 ja 15 artiklassa yksilöityihin tietoihin. Tietojen luovutus tapahtuisi pääsäännön mukaan 1 momentissa säädetyllä tavalla, ja 2 momentti on tarkoitettu sovellettavaksi vain poikkeuksellisesti.

Kyberkestävyysasetuksen 15 artiklan 5 kohdan mukaisesti koordinaattoriksi nimettyjen CSIRT-yksikköjen ja ENISA:n on varmistettava vapaaehtoisesti ilmoituksen tehneen luonnollisen henkilön tai oikeushenkilön toimittamien tietojen luottamuksellisuus ja asianmukainen suoja. Kuten luvussa 3.1.4 arvioitiin, julkisuuslain säännösten voidaan katsoa varmistavan CSIRT-yksikön osalta kyseisten tietojen salassapidon niiltä osin kuin se on perusteltua. CSIRT-yksikön olisi luovuttaessaan vapaaehtoisesti saamansa ilmoituksen tietoja käsiteltävä tietoja niin, että nämä edut eivät vaarannu. Tahoja, joille tietoja voitaisiin ehdotuksen mukaan luovuttaa, sitoisi julkisuuslain mukainen salassapitovelvollisuus tai tämä sama kyberkestävyysasetuksen mukainen velvollisuus.

Salassapitosäännös tai muu tiedon luovuttamista koskeva rajoitus, josta ehdotetun säännöksen nojalla poiketaan, voisi koskea esimerkiksi tietoa yksityisestä liikesalaisuudesta taikka tieto- ja viestintäjärjestelmien turvajärjestelyistä. Haavoittuvuuteen tai poikkeamaan liittyvään tietoon voisi kohdistua myös muita julkisuuslain mukaisia salassapitoperusteita, kuten julkisuuslain 24 §:n 1 momentin 9 kohta (valtion turvallisuuden ylläpitämistä koskevat asiakirjat) tai 17 kohta (julkisyhteisön liikesalaisuus). Toiseen jäsenvaltioon sijoittautunutta elinkeinonharjoittajaa koskeva tieto voisi olla joissakin oloissa salassa pidettävä myös julkisuuslain 24 §:n 1 momentin 2 kohdan nojalla.

Pykälän *1 kohdassa* säädettäisiin tietojen luovuttamisesta kyberkestävyysasetuksen valvonnassa Suomessa toimivaltaiselle markkinavalvontaviranomaiselle. Markkinavalvontatehtävien osoittamisesta säädettäisiin ehdotetun lain 15 ja 16 §:ssä. Kohta täydentäisi kyberkestävyysasetuksen 16 artiklan 3 kohtaa, jossa säädetään CSIRT-yksiköiden velvollisuudesta antaa jäsenvaltioidensa markkinavalvontaviranomaisille haavoittuvuusilmoituksessa tai poikkeamailmoituksessa ilmoitetut tiedot, joita markkinavalvontaviranomaiset tarvitsevat täyttääkseen asetuksen mukaiset velvoitteensa. Tietoja voitaisiin luovuttaa myös väliraporttiin tai loppuraporttiin sisältyvistä tiedoista.

Pykälän *2 kohdassa* säädettäisiin puolestaan tietojen luovuttamisesta Euroopan unionin kyberturvallisuusvirastolle ENISA:lle ja *3 kohdassa* toisessa jäsenvaltiossa koordinaattoreiksi nimetyille CSIRT-yksiköille. CSIRT-yksikön velvollisuudesta välittää ilmoitukset ENISA:lle ja muille CSIRT-yksiköille säädetään kyberkestävyysasetuksen 16 artiklassa. Tämän lisäksi tietoja voisi tapauskohtaisesti olla tarpeen vaihtaa ENISA:n kanssa, kun tarkoitus on tiedottaa yleisölle poikkeamasta kyberkestävyysasetuksen 17 artiklan 2 kohdassa tarkoitetulla tavalla.

Pykälä ei rajoittaisi CSIRT-yksikön oikeutta luovuttaa kyseisiä tietoja julkisuuslain vahinkoedellytyslausekkeiden puitteissa eikä tietojen luovuttamista muussa laissa kuten kyberturvallisuuslaissa tai sähköisen viestinnän palveluista annetun lain 319 §:ssä säädetyn perusteella.

10 §. *Kyberkestävyyden sääntelyn testiympäristö*. Pykälässä säädettäisiin kyberkestävyysasetuksen 33 artiklan 2 kohdassa tarkoitetun testiympäristön perustamisesta.

Säännös ei velvoittaisi kyberkestävyyden sääntelyn testiympäristön perustamiseen vaan mahdollistaisi testiympäristön perustamisen Liikenne- ja viestintäviraston päätöksellä tarvittaessa. Säännöksellä ei rajattaisi perustettavien testiympäristöjen määrää. Testiympäristöjä voisi olla tarvittaessa useampia, esimerkiksi erilaisten tuotteiden tai olosuhteiden testaamista varten. Testiympäristön perustaminen olisi Liikenne- ja viestintäviraston harkintavallassa. Testiympäristön hyödyntäminen tuotteen kehittämisessä olisi talouden toimijalle vapaaehtoista ja lähtökohtaisesti maksullista valtion maksuperustelaissa säädetyn mukaisesti. Testiympäristön hyödyntäminen olisi tarkoitettu määräaikaiseksi talouden toimijan kehitystyön tueksi silloin, kun digitaalisia elementtejä sisältävä tuote tai sen osa ei ole saatavilla markkinoilla.

Pykälän *1 momentin* nojalla testiympäristön perustaisi Liikenne- ja viestintävirasto. Testiympäristön perustamisesta olisi tehtävä päätös, jossa määritetään testiympäristön voimassaoloaika ja -paikka, soveltuva tekninen rajaus, toimintasuunnitelma sekä testiympäristöön soveltuva testauksen kohde. Testauksen kohteen voisi määrittää esimerkiksi tuotekategorian tai -tyypin, tuotteen käyttötarkoituksen tai tuotteen ominaisuuksien perusteella taikka muulla soveltuvalla tavalla. Testauksen kohteen voisi rajata esimerkiksi myös tiettyyn komponenttiin, ominaisuuteen, käyttötarkoitukseen tai ohjelmiston osaan. Toimintasuunnitelmassa voitaisiin tarkentaa testiympäristön kapasiteettia ja resursointia. Päätöksellä voitaisiin asettaa myös testiympäristöä koskevia ehtoja, jotka ovat tarpeellisia sen toiminnan järjestämisen tai turvallisuuden kannalta. Ehdot voisivat liittyä esimerkiksi testauksen ajalliseen rajaamiseen tai testauksen turvajärjestelyihin. Ehtojen olisi oltava tasapuolisia talouden toimijoille sekä tarpeellisia testiympäristön tai turvallisuuden kannalta. Testiympäristö voitaisiin perustaa myös tekoälyasetuksen mukaisen testiympäristön yhteyteen, mikäli se olisi testauksen vuoksi tarkoituksenmukaista, kuten suuririskiseen tekoälyjärjestelmään liittyvän testauksen vuoksi. Tekoälyn sääntelyn testiympäristöistä on tarkoitus esittää säännöksiä eräiden tekoälyjärjestelmien valvonnasta annettuun lakiin osana tekoälyasetuksen II vaiheen täytäntöönpanoa (VN/31658/2024).

Pykälän *2 momentin* nojalla Liikenne- ja viestintävirasto myöntäisi hakemuksesta talouden toimijalle oikeuden toimintaan eli testaukseen testiympäristössä. Testiympäristön perustaminen tai olemassaolo ei siten perustaisi talouden toimijalle oikeutta sen käyttöön ilman erillistä hakemusta. Hakemuksessa olisi esitettävä sen käsittelemiseksi tarpeelliset tiedot. Liikenne- ja viestintäviraston olisi hakemuksesta myönnettävä oikeus toimintaan testiympäristössä, ellei momentissa tarkoitettua perustetta oikeuden myöntämättä jättämiselle olisi käsillä. Liikenne- ja viestintäviraston olisi kohdeltava talouden toimijoita tasapuolisesti, kuten hallintolain 6 §:ssä edellytetään.

Pykälän *3 momentin* informatiivisesta viittauksesta kävisi ilmi, että Liikenne- ja viestintäviraston velvollisuutena olisi tehdä testiympäristön perustamisesta kyberkestävyysasetuksen 33 artiklan 2 kohdassa tarkoitettu ilmoitus Euroopan komissiolle ja muille markkinavalvontaviranomaisille hallinnollisen yhteistyön ryhmän kautta. Lisäksi pykälässä säädettäisiin viraston tehtäväksi valvoa ja ohjata toimintaa testiympäristössä. Mikäli testattavana olisi suuririskisen tekoälyjärjestelmän kyberkestävyys, voisi sen markkinavalvonnasta vastaava viranomainen osallistua kyberkestävyyden testiympäristössä tapahtuvan toiminnan ohjaamiseen toimivaltuuksiensa ja resurssiensa puitteissa, mutta ehdotus ei asettaisi sille velvollisuutta tähän. Tekoälyjärjestelmien markkinavalvonnasta vastaavien viranomaisten tehtävistä tekoälyasetuksen mukaisessa testiympäristössä on tarkoitus säätää eräiden tekoälyjärjestelmien valvonnasta annetussa laissa.

Pykälän *4 momentin* nojalla Liikenne- ja viestintävirasto voisi määräyksellä antaa tarkempia teknisiä säännöksiä kyberkestävyyden sääntelyn testiympäristön järjestämisestä ja toiminnasta sekä talouden toimijan hakemuksesta.

3 luku – Ilmoitetut laitokset

11 §. *Ilmoittava viranomainen.* Pykälässä säädettäisiin kyberkestävyysasetuksen 36 artiklassa tarkoitetun ilmoittamisesta vastaavan viranomaisen tehtävästä, joka osoitettaisiin Liikenne- ja viestintävirastolle. Ilmoittavan viranomaisen tehtävänä olisi huolehtia sille kyberkestävyysasetuksen IV luvussa säädetyistä tehtävistä. Ilmoittavan viranomaisen vastuulla olisi siten laatia ja toteuttaa tarvittavat menettelyt, jotka liittyvät vaatimustenmukaisuuden arviointilaitosten arviointiin, nimeämiseen ja ilmoittamiseen, sekä valvoa niitä. Kyberkestävyysasetuksen 41 artiklan mukaisesti tehtäviin kuuluisi myös ilmoitettujen laitosten valvonta niiden käyttäessä apuna alihankkijaa tai tytäryhtiötä. Ilmoittava viranomainen vastaisi myös kyberkestävyysasetuksen 35 artiklan 1 kohdassa, 38 artiklan 1 kohdassa ja 46 artiklan 2 kohdassa tarkoitettujen tietojen ilmoittamisesta komissiolle ja muille jäsenvaltioille silloin kun jäsenvaltiolla on velvollisuus niiden ilmoittamiseksi. Ilmoittavan viranomaisen toiminnassa olisi täytettävä kyberkestävyysasetuksen 37 artiklassa säädetyt vaatimukset.

12 §. *Ilmoittamista koskeva hakemus.* Pykälän nojalla kyberkestävyysasetuksen mukaiseksi ilmoitetuksi laitokseksi ilmoittamista koskeva hakemus osoitettaisiin ilmoittavalle viranomaiselle eli Liikenne- ja viestintävirastolle. Sellaisen vaatimustenmukaisuuden arviointilaitoksen, joka ei ole sijoittautunut Suomeen, olisi haettava ilmoittamista kyberkestävyysasetuksen 42 artiklan 1 kohdan mukaisesti siitä jäsenvaltiosta, johon arviointilaitos on sijoittautunut.

Hakemukseen olisi liitettävä kyberkestävyysasetuksen 42 artiklassa tarkoitetut tiedot. Näitä tietoja ovat kuvaus vaatimustenmukaisuuden arviointitoimista, vaatimustenmukaisuuden arviointimenettelystä tai -menettelyistä ja yhdestä tai useammasta digitaalisia elementtejä sisältävästä tuotteesta, jonka osalta laitos katsoo olevansa pätevä, sekä tapauksen mukaan akkreditointitodistus, jonka kansallinen akkreditointielin on antanut ja jossa todistetaan, että vaatimustenmukaisuuden arviointilaitos täyttää kyberkestävyysasetuksen 39 artiklassa säädetyt vaatimukset. Suomessa kansallinen akkreditointielin on Turvallisuus- ja kemikaalivirastosta annetun lain (1261/2010) 2 a §:n nojalla Turvallisuus- ja kemikaaliviraston akkreditointiyksikkö (FINAS-akkreditointipalvelu).

Akkreditointitodistuksen liittäminen hakemukseen olisi tarkoitettu pääsääntöiseksi ja ensisijaiseksi menettelyksi haettaessa nimeämistä ilmoitetuksi laitokseksi. Kyberkestävyysasetuksessa säädetään kuitenkin myös vaihtoehtoisesta menettelystä, jota voitaisiin soveltaa, jos akkreditointitodistuksen hankkiminen ei poikkeuksellisesti olisi mahdollista. Jos hakemukseen ei voitaisi liittää FINAS-akkreditointipalvelun antamaa akkreditointitodistusta siitä, että vaatimustenmukaisuuden arviointilaitos täyttää kyberkestävyysasetuksen vaatimukset, olisi vaatimustenmukaisuuden arviointilaitoksen toimitettava kyberkestävyysasetuksen 42(3) artiklan mukaisesti Liikenne- ja viestintävirastolle kaikki tarpeelliset asiakirjatodisteet, joiden avulla voidaan varmentaa, todeta ja säännöllisesti valvoa, että se täyttää kyberkestävyysasetuksen 39 artiklassa säädetyt vaatimukset.

13 §. *Ilmoitetuksi laitokseksi nimeäminen ja nimeämisen rajaaminen tai peruuttaminen.* Pykälän *1 momentin* nojalla Liikenne- ja viestintävirasto nimeäisi hakemuksesta ilmoitetuksi laitokseksi sellaisen vaatimustenmukaisuuden arviointilaitoksen, joka täyttää kyberkestävyysasetuksessa säädetyt vaatimukset haetun pätevyysalueen osalta. Ilmoitetun laitoksen tehtävien suorittamisen edellytyksenä olisi lisäksi, että kyberkestävyysasetuksen 43 artiklan 5 kohdassa tarkoitettuja vastalauseita nimeämiselle ei ole esitetty. Vaatimustenmukaisuuden arviointilaitos nimettäisiin suorittamaan ilmoitettuna laitoksena vaatimustenmukaisuuden arviointia niiden digitaalisen elementin sisältävien tuotteiden osalta, joiden osalta arviointilaitos on hakenut ilmoittamista ja osoittanut täyttävänsä vaatimukset.

Ilmoitusmenettelystä säädetään kyberkestävyysasetuksen 43 artiklassa. Ilmoitetun laitoksen vaatimuksista säädetään kyberkestävyysasetuksen 39 artiklassa.

Pykälän *2 momentissa* säädettäisiin ilmoitetun laitoksen nimeämistä koskevan päätöksen sisällöstä. Päätöksessä olisi hallintolain 44 §:ssä säädetyn ohella määriteltävä arviointilaitoksen pätevyysalue ja vahvistettava valvontaan liittyvät järjestelyt. Lisäksi päätöksessä voitaisiin tarvittaessa asettaa laitoksen toimintaa koskevia vaatimuksia, rajoituksia ja ehtoja, joilla varmistetaan kyberkestävyysasetuksen mukaisten tehtävien asianmukainen suorittaminen.

Pykälän *3 momentissa* säädettäisiin informatiivinen viittaus kyberkestävyysasetuksen 45 artiklan säännöksiin koskien ilmoitetuksi laitokseksi nimeämistä koskevan päätöksen rajaamista ja peruuttamista.

Pykälän *4 momentin* nojalla ilmoitettuun laitokseen sekä sen käyttämän tytäryhtiön ja alihankkijan henkilöstöön sovellettaisiin rikosoikeudellista virkavastuuta koskevia säännöksiä henkilöstön suorittaessa kyberkestävyysasetuksessa tarkoitettuja ilmoitetulle laitokselle kuuluvia tehtäviä. Säännös olisi tarpeen, koska tehtävien suorittamisessa olisi kysymys julkisesta hallintotehtävästä. Momentti sisältäisi myös informatiivisen viittauksen vahingonkorvauslakiin. Lisäksi ilmoitetun laitoksen tai sen käyttämän tytäryhtiön tai alihankkijan olisi noudatettava julkista hallintotehtävää hoitaessaan hallinnon yleislakeja eli hallintolakia (434/2003), viranomaisten toiminnan julkisuudesta annettua lakia (621/1999), sähköisestä asioinnista viranomaistoiminnassa annettua lakia (13/2003), kielilakia (423/2003), julkisen hallinnon tiedonhallinnasta annettua lakia (906/2019) ja digitaalisten palvelujen tarjoamisesta annettua lakia (306/2019) myös ilman nimenomaista viittausta yleislakeihin. Ilmoitetun laitoksen mahdollisuudesta teettää tehtäviä alihankintana tai käyttää tytäryhtiötä säädettäisiin kyberkestävyysasetuksen 41 artiklassa.

14 §. *Ilmoittavan viranomaisen ja ilmoitetun laitoksen oikeus luovuttaa salassa pidettäviä tietoja.* Pykälässä säädettäisiin ilmoittavan viranomaisen ja ilmoitetun laitoksen oikeudesta luovuttaa tietoja silloin kun se on tarpeen niille kyberkestävyysasetuksen nojalla osoitettujen tehtävien suorittamiseksi.

Pykälän *1 momentissa* säädettäisiin ilmoittavan viranomaisen oikeudesta luovuttaa salassa pidettävää vaatimustenmukaisuuden arviointilaitoksen ilmoittamisen perusteita ja muuta sen pätevyyttä koskevaa tietoa komissiolle sekä toiselle jäsenvaltiolle, jos se on tarpeen ilmoittavan viranomaisen kyberkestävyysasetuksessa säädetyn velvoitteen toteuttamiseksi. Kyseessä olisivat etupäässä vaatimustenmukaisuuden arviointilaitoksen toimintaa koskevat liikesalaisuudet tai muut elinkeinosalaisuudet. Salassa pidettävien tietojen luovuttaminen olisi tarpeen esimerkiksi kyberkestävyysasetuksen 43 artiklan 4 kohdassa tarkoitetussa tilanteessa, jossa laitoksen ilmoittaminen perustuu muuhun selvitykseen kuin akkreditointitodistukseen. Tällöin ilmoittavan viranomaisen olisi toimitettava komissiolle ja muille jäsenvaltioille asiakirjatodisteet, joiden avulla voidaan todistaa vaatimustenmukaisuuden arviointilaitoksen pätevyys ja käytössä olevat järjestelyt, joilla varmistetaan, että laitosta valvotaan säännöllisesti ja että se täyttää edelleen 39 artiklassa säädetyt vaatimukset. Salassa pidettävien tietojen luovuttamisen olisi todennäköisesti tarpeen myös tilanteessa, jossa ilmoitetun laitoksen pätevyys riitautetaan kyberkestävyysasetuksen 46 artiklan mukaisesti. Tällöin ilmoituksen tehneen jäsenvaltion eli 11 §:n 2 momentin nojalla ilmoittavan viranomaisen olisi kyberkestävyysasetuksen 46(2) artiklan mukaisesti toimitettava pyynnöstä komissiolle kaikki tiedot, jotka liittyvät ilmoituksen perusteisiin tai asianomaisen laitoksen pätevyyden ylläpitoon.

Pykälän *2 momentissa* säädettäisiin puolestaan ilmoitetun laitoksen oikeudesta luovuttaa salassa pidettäviä vaatimustenmukaisuuden arviointia ja tarkastuksen tuloksia koskevia tietoja

Euroopan komissiolle, Euroopan unionin jäsenvaltiolle ja toiselle ilmoitetulle laitokselle, jos se on tarpeen ilmoitetun laitoksen kyberkestävyysasetuksessa säädetyn velvoitteen toteuttamiseksi. Tässä tilanteessa olisi pääsääntöisesti kysymys arvioituun tuotteeseen liittyvistä valmistajan liikesalaisuuksista tai muista tuotetta koskevista salassa pidettävistä tiedoista. Tietojen luovuttamisen edellytyksenä olisi sen tarpeellisuus ilmoitetulle laitokselle kyberkestävyysasetuksen nojalla säädetyn velvoitteen toteuttamiseksi. Tietojen antaminen voi olla tarpeen kyberkestävyysasetuksen 49 artiklan 2 kohdan mukaisen ilmoitetun laitoksen velvoitteen täyttämiseksi. Sen mukaan ilmoitettujen laitosten on toimitettava muille ilmoitetuille laitoksille, jotka suorittavat samat digitaalisia elementtejä sisältävät tuotteet kattavia samanlaisia vaatimustenmukaisuuden arviointitoimia, asiaankuuluvat tiedot kysymyksistä, jotka liittyvät vaatimustenmukaisuuden arvioinnin kielteisiin tuloksiin ja pyynnöstä myös myönteisiin tuloksiin. Lisäksi ilmoitetulla laitoksella olisi velvollisuus toimittaa jäljennökset EU-tyyppitarkastukseen liittyvistä teknisistä asiakirjoista ja ilmoitetun laitoksen suorittamien tarkastusten tuloksista pyynnöstä komissiolle tai toiselle jäsenvaltiolle kyberkestävyysasetuksen liitteen VIII osan II kohdan 9 nojalla.

4 luku – Markkinavalvonta

15 §. *Markkinavalvontaviranomaiset*. Pykälässä säädettäisiin kyberkestävyysasetuksen mukaisesta markkinavalvontaviranomaisen tehtävästä. Kyberkestävyysasetuksen mukaisten vaatimusten markkinavalvontaviranomaisena asetuksen soveltamisalaan kuuluville digitaalisen elementin sisältäville tuotteille toimisi Suomessa pääsääntöisesti Liikenne- ja viestintävirasto. Markkinavalvontaviranomainen vastaisi tehtävistä, jotka sille kyberkestävyysasetuksessa osoitetaan. Markkinavalvontaviranomaisen tehtävistä ja toimivaltuuksista säädettäisiin lisäksi markkinavalvonta-asetuksessa ja markkinavalvontalaissa.

16 §. *Suuririskisen tekoälyjärjestelmän markkinavalvonta*. Pykälässä säädettäisiin digitaalisen elementin sisältävien tuotteiden markkinavalvonnasta silloin, kun tuote on tekoälyasetuksessa tarkoitettu suuririskinen tekoälyjärjestelmä. Edellä 15 §:ssä säädetystä poiketen markkinavalvontaviranomaisena suuririskiselle tekoälyjärjestelmälle toimisi myös kyberkestävyysasetuksen vaatimuksien osalta se viranomainen, joka valvoo suuririskistä tekoälyjärjestelmää eräiden tekoälyjärjestelmien valvonnasta annetun lain 3 §:n nojalla.

Kyberkestävyysasetuksen 52(14) artikla edellyttää, että siltä osin kuin on kyse EU:n tekoälyasetuksen (EU) 2024/1689 mukaisista suuririskisistä tekoälyjärjestelmistä, tuotteita valvoo tekoälyasetuksen nojalla toimivaltainen viranomainen myös kyberkestävyysasetuksen vaatimuksien osalta. Asiaan ei liity kansallista liikkumavaraa. Tämän johdosta suuririskisille tekoälyjärjestelmille, siltä osin kuin ne kuuluvat kyberkestävyysasetuksen vaatimusten alaan, markkinavalvontaviranomaisena toimisi eräiden tekoälyjärjestelmien valvonnasta annetun lain 3 §:n nojalla toimivaltainen viranomainen.

Kyberkestävyysasetuksen 52 artiklan 15 kohdassa säädetään hallinnollisen yhteistyön ryhmän perustamisesta. Hallinnollisen yhteistyön ryhmä koostuu nimettyjen markkinavalvontaviranomaisten edustajista ja tarvittaessa yhteyspisteiden edustajista. Edustajan hallinnollisen yhteistyön ryhmään nimeäisi Liikenne- ja viestintävirasto, sillä markkinavalvontatehtävä olisi 16 §:n poikkeusta lukuun ottamatta keskitetty sille. Siinä tapauksessa, että yhteistyöryhmään voitaisiin nimetä useampi kuin yksi edustaja Suomesta, edustajaksi voitaisiin nimetä myös 16 §:ssä tarkoitettu markkinavalvontaviranomainen, jos se on tarkoituksenmukaista kyberkestävyysasetuksen markkinavalvontaa varten.

17 §. *Markkinavalvonnan asiantuntijatuki*. Pykälässä säädettäisiin asiantuntijatuen antamisesta Liikenne- ja viestintävirastosta toiselle viranomaiselle markkinavalvontaa ja hallinnollisen

seuraamusmaksun määräämistä varten. Liikenne- ja viestintävirasto voisi antaa 16 §:ssä tarkoitetulle markkinavalvontaviranomaiselle sekä sille, jolla on toimivalta määrätä 6 luvussa tarkoitettu seuraamusmaksu, sen pyynnöstä asiantuntija-apua, joka koskee kyberkestävyysasetuksen markkinavalvontaa, vaatimustenmukaisuuden arviointia tai kyberturvallisuusriskien arviointia. Tukea voitaisiin antaa toiselle viranomaiselle siten käytännössä suuririskisten tekoälyjärjestelmien markkinavalvontaa tai niitä koskevan hallinnollisen seuraamusmaksun määräämistä varten.

Mahdollisuus asiantuntija-avun käyttöön olisi käytännössä tarpeen sen varmistamiseksi, että valvonnassa kyetään noudattamaan yhtenäisiä arviointiperusteita tuotteiden vaatimustenmukaisuudelle. Asiantuntija-apu olisi olla luonteeltaan esimerkiksi tiedollista tai teknistä tukea vaatimustenmukaisuuden arviointien sekä valvontatoimien suuntaamisen tueksi. Tuki voisi liittyä myös kyberkestävyysasetuksen 54 artiklassa tarkoitettuun menettelyyn, jossa arvioidaan tuotteen mahdollista merkittävää kyberturvallisuusriskiä. Ehdotetun lain 18 §:ssä säädettäisiin asiantuntijatukeen liittyvästä tietojenvaihdosta.

Markkinavalvontaviranomaisten yhteistyöhön muutoin sovellettaisiin, mitä markkinavalvontalaissa, markkinavalvonta-asetuksessa ja kyberkestävyysasetuksessa säädetään.

18 §. *Markkinavalvontaviranomaisen oikeus luovuttaa salassa pidettävää tietoa.* Pykälässä säädettäisiin kyberkestävyysasetuksen markkinavalvonnan edellyttämistä tiedonluovutusoikeuksista.

Säännöksiä sovellettaisiin erityissäännöksinä sen lisäksi, mitä muualla laissa säädetään markkinavalvontaviranomaisen tiedonluovutusoikeuksista. Markkinavalvontalain 11 §:ssä säädetään muun ohella markkinavalvontaviranomaisen oikeudesta luovuttaa tietoja Tullille, ja markkinavalvontalain 13 §:ssä säädetään markkinavalvontaviranomaisen oikeudesta luovuttaa eräitä tietoja tietyille muille kotimaisille ja ulkomaisille viranomaisille sekä kansanväliselle toimielimelle. Markkinavalvontalaissa luetellut tietotyypit (tiedot yksityisen ja yhteisön taloudellisesta asemasta, liikesalaisuudesta sekä yksityisen henkilökohtaisista oloista) eivät ole riittäviä kyberkestävyysasetuksen edellyttämän yhteistyön kannalta (ks. luku 3.1.2), vaikkakin myös kyseisten tietojen luovuttaminen tulisi kyseeseen. Ehdotuksessa täydennettäisiin näitä säännöksiä säätämällä oikeudesta luovuttaa myös eräitä muita tietoja ja tietojen luovuttamisesta sellaisille viranomaisille, joita ei mainita markkinavalvontalaissa.

Pykälän *1 momentissa* laajennettaisiin markkinavalvontalain 11 ja 13 §:n nojalla tietojenluovutusoikeuden piirissä olevia tietotyyppejä myös digitaalisia elementtejä sisältävän tuotteen vaatimustenmukaisuutta, turvajärjestelyjä, haavoittuvuutta ja tietoturvaan vaikuttavaa poikkeamaa koskeviin tietoihin. Kyseiset tiedot voisivat olla salassa pidettäviä erityisesti julkisuuslain 24 §:n 1 momentin 7 kohdassa tarkoitettuina tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevina ja niiden toteuttamiseen vaikuttavina asiakirjoina. Nämä tiedot ovat lähtökohtaisesti salassa pidettäviä salassapito-olettaman mukaisesti. Tiedot olisi välttämätöntä sisällyttää tiedonvaihdon alaan, koska kyberkestävyysasetuksen velvoitteet kohdistuvat siihen, mitä nämä tiedot koskevat. Markkinavalvontaviranomainen voisi luovuttaa tietoja omasta aloitteestaan tai pyynnöstä.

Pykälän *2 momentissa* säädettäisiin markkinavalvontaviranomaisen oikeudesta luovuttaa salassa pidettäviä tietoja 1–6 kohdissa tarkoitetuille tahoille, joiden kanssa markkinavalvontaviranomaisen on tarpeen tehdä yhteistyötä sille säädettyjen tehtävien toteuttamiseksi, mutta jotka eivät sisälly markkinavalvontalain 11 ja 13 §:ään. Markkinavalvontaviranomainen voisi luovuttaa tietoja oma-aloitteisesti tai pyynnöstä.

Momentin *1 kohdassa* säädettäisiin tietojen luovuttamisesta FINAS-akkreditointipalvelulle, jos tiedon luovuttaminen on välttämätöntä vaatimustenmukaisuuden arviointilaitosten pätevyyden arvioimiseksi. Akkreditointia koskevan ns. NLF-asetuksen 5 artiklan 3 kohdan mukaan kansallisten akkreditointielinten on valvottava kaikkia niitä vaatimustenmukaisuuden arviointilaitoksia, joille ne ovat myöntäneet akkreditointitodistuksen. Artiklan 4 kohdan mukaan, jos kansallinen akkreditointielin toteaa, että jokin akkreditointitodistuksen saanut vaatimustenmukaisuuden arviointilaitos ei enää ole pätevä hoitamaan tiettyä vaatimustenmukaisuuden arviointiin liittyvää tehtävää tai on rikkonut vakavasti velvoitteitaan, kansallisen akkreditointielimen on toteutettava tarvittavat toimenpiteet kohtuullisen ajan kuluessa kyseisen laitoksen akkreditointitodistuksen voimassaolon rajoittamiseksi, keskeyttämiseksi tai peruuttamiseksi.

Momentin *2 kohdassa* säädettäisiin tietojen luovuttamisesta kansalliselle kyberturvallisuussertifioinnin viranomaiselle, jos tiedon luovuttaminen on välttämätöntä kyseisen viranomaisen valvontatehtävien suorittamiseksi. Markkinavalvontaviranomaisten on kyberkestävyysasetuksen 52 artiklan 4 kohdan mukaan tehtävä tarvittaessa yhteistyötä kyberturvallisuusasetuksen nojalla nimettyjen kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten kanssa ja vaihdettava säännöllisesti niiden kanssa tietoja. Suomessa tehtävässä jatkaisi Liikenne- ja viestintävirasto ehdotetun lain 21 §:n nojalla. Tietoja voitaisiin luovuttaa lisäksi toisen jäsenvaltion vastaavaa tehtävää hoitavalle viranomaiselle. Tietojen luovuttaminen voisi olla ehdotetulla tavalla välttämätöntä esimerkiksi, jos valvonnassa ilmenisi kyberturvallisuussertifiointia koskeva poikkeama, johon kyberturvallisuussertifioinnin viranomaisen olisi kohdistettava valvontatoimenpiteitä.

Momentin *3 kohdassa* säädettäisiin tietojen luovuttamisesta kyberturvallisuuslain 26 §:ssä ja julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 18 h §:ssä tarkoitetulle valvovalle viranomaiselle, Finanssivalvonnalle tai toisen jäsenvaltion vastaavalle viranomaiselle, jos digitaalisia elementtejä sisältävän tuotteen voidaan perustellusti arvioida aiheuttavan merkittävän kyberturvallisuusriskin muiden kuin teknisten riskitekijöiden vuoksi. Tällä viitattaisiin kyberkestävyysasetuksen 54 artiklan 2 kohdan mukaiseen tilanteeseen. Sen mukaan, jos markkinavalvontaviranomaisella on riittävä peruste katsoa, että digitaalisia elementtejä sisältävä tuote aiheuttaa merkittävän kyberturvallisuusriskin muiden kuin teknisten riskitekijöiden vuoksi, sen on ilmoitettava tästä NIS 2 -direktiivin 8 artiklan nojalla nimetyille tai perustetuille toimivaltaisille viranomaisille sekä tehtävä tarpeen mukaan yhteistyötä kyseisten viranomaisten kanssa. NIS 2 -direktiivin 8 artiklassa tarkoitettuina toimivaltaisina viranomaisina toimivat kansallisesti kyberturvallisuuslain 26 §:ssä ja tiedonhallintalain 18 h §:ssä tarkoitetut valvovat viranomaiset sekä Finanssivalvonnasta annetun lain (878/2008) 50 p §:n (laissa 610/2024) nojalla Finanssivalvonta. Salassa pidettävän tiedon luovuttamisen tulisi olla välttämätöntä kyberkestävyysasetuksen 54 artiklan 2 kohdassa säädetyn ilmoitusvelvollisuuden täyttämiseksi.

Momentin *4 kohdassa* säädettäisiin ensinnäkin tietojen luovuttamisesta Euroopan unionin kyberturvallisuusvirastolle (ENISA) ja Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksessa toimivalle CSIRT-yksikölle, jos se on välttämätöntä kyberkestävyysasetuksessa 52 artiklan 4 ja 5 kohdassa tai 54 artiklan 1 kohdassa säädetyn yhteistyövelvollisuuden, neuvonnan tai tutkimuksen suorittamiseksi. Lisäksi momentissa säädettäisiin tietojen luovuttamisesta CSIRT-yksikölle, jos se on välttämätöntä sille kyberturvallisuuslaissa säädettyjen tehtävien hoitamista varten.

Kyberkestävyysasetuksen 52 artiklan 4 kohdan mukaan markkinavalvontaviranomaisten on tehtävä yhteistyötä ja vaihdettava säännöllisesti tietoja koordinaattoreiksi nimettyjen CSIRT-yksiköiden ja ENISA:n kanssa kyberkestävyysasetuksen 14 artiklan mukaisten

raportointivelvoitteiden noudattamisen valvonnan osalta. Kyberkestävyysasetuksen 52 artiklan 4 kohdan mukaan markkinavalvontaviranomaiset voivat pyytää koordinaattoriksi nimettyä CSIRT-yksikköä tai ENISA:a antamaan teknistä neuvontaa asioissa, jotka liittyvät tämän asetuksen täytäntöönpanoon ja sen noudattamisen valvontaan. Markkinavalvontaviranomaiset voivat 54 artiklan mukaista tutkimusta suorittaessaan pyytää koordinaattoriksi nimettyä CSIRT-yksikköä tai ENISA:a esittämään analyysin digitaalisia elementtejä sisältävien tuotteiden vaatimustenmukaisuuden arviointien tueksi.

Kyberkestävyysasetuksen 54 artiklassa säädetään kansallisen tason menettelystä digitaalisia elementtejä sisältäviä merkittävän kyberturvallisuusriskin aiheuttavia tuotteita varten. Artiklan 1 kohdassa säädetään, että jos jäsenvaltion markkinavalvontaviranomaisella on riittävä peruste katsoa, että digitaalisia elementtejä sisältävä tuote, mukaan lukien sen haavoittuvuuksien käsittely, aiheuttaa merkittävän kyberturvallisuusriskin, sen on arvioitava ilman aiheetonta viivytystä ja tarvittaessa yhteistyössä asiaankuuluvan CSIRT-yksikön kanssa, täyttääkö kyseinen digitaalisia elementtejä sisältävä tuote kaikki tässä asetuksessa säädetyt vaatimukset.

Toiseksi kohdassa säädettäisiin oikeudesta luovuttaa tietoja muissakin tapauksissa CSIRT-yksikölle siinä tapauksessa, että se olisi välttämätöntä CSIRT-yksikön kyberturvallisuuslaissa säädettyjen tehtävien hoitamista varten. CSIRT-yksikön kyberturvallisuuslaissa säädettyjen tehtävien kannalta tiedon luovutus voisi olla välttämätöntä esimerkiksi kyberturvallisuuden tilannekuvan ylläpitämistä, ennakkovaroitusta, haavoittuvuuskoordinaatiota tai haavoittuvuuskartoitusta varten. Tiedonluovutusoikeudessa olisi tältä osin kyse kansallista yhteistyötä ja tiedonvaihtoa parantavasta säädöksestä, jota kyberkestävyysasetuksen markkinavalvonta ei välittömästi edellytä. Markkinavalvontaviranomainen voi kuitenkin todennäköisesti havaita tai vastaanottaa tehtävässään tietoja, jotka olisivat välttämättömiksi CSIRT-yksikön kyberturvallisuuslain 20 §:ssä säädettyjen tehtävien hoitamiseksi. Kyseessä voisivat olla esimerkiksi kyberturvallisuuden tilannekuvan ylläpitämiseksi välttämättömät tiedot esimerkiksi kyberkestävyysasetuksen velvoitteiden puutteelliseen noudattamiseen tilanteista, joista markkinavalvontaviranomaisen käsityksen mukaan CSIRT-yksikkö tulisi saattaa tietoiseksi, tai esimerkiksi markkinavalvontaviranomaisen tietoon tulleet haavoittuvuus- ja uhkatiedot, jotka olisivat tarpeen CSIRT-yksikön haavoittuvuuskoordinaatiotehtävän hoitamiseksi tai ennakkovaroituksen antamiseksi taikka joiden perusteella CSIRT-yksikkö voisi toteuttaa haavoittuvuuskartoituksen. Säännöksellä tuettaisiin kansallisten viranomaisten yhteistyötä ja tiedonvaihtoa kyberpoikkeamien varalta.

Momentin *5 kohdassa* säädettäisiin tietojen luovuttamisesta tietosuojavaltuutetulle, jos tiedon luovuttaminen on välttämätöntä tietosuojavaltuutetulle laissa säädettyjen valvontatehtävien hoitamiseksi. Kyberkestävyysasetuksen 52 artiklan 7 kohdan ensimmäisen alakohdan mukaan markkinavalvontaviranomaisten on tarvittaessa tehtävä yhteistyötä unionin tietosuojalainsäädäntöä valvovien viranomaisten kanssa. Tällaiseen yhteistyöhön sisältyy tiedottaminen kyseisille viranomaisille niiden toimivaltuuksien käytön kannalta merkityksellisistä havainnoista, myös silloin, kun markkinavalvontaviranomainen antaa 52 artiklan 10 kohdan mukaisesti ohjeita ja neuvoja, jos ne koskevat henkilötietojen käsittelyä. Kohta mahdollistaisi tietojen oma-aloitteisen luovuttamisen näissä tapauksissa. Tietojen luovuttaminen olisi rajattava havainnoista tiedottamisen kannalta välttämättömään. Tietosuojavaltuutetulla olisi oikeus pyytää muitakin asiaan liittyviä tietoja alla kuvatun mukaisesti.

Momentin *6 kohdassa* säädettäisiin välttämättömien tietojen luovuttamisesta kilpailulainsäädännön valvomista varten Euroopan komissiolle ja Kilpailu- ja kuluttajavirastolle tai toisen Euroopan unionin jäsenvaltion kansalliselle kilpailuviranomaiselle. Kyberkestävyysasetuksen 52 artiklan 13 kohdassa säädetään markkinavalvontaviranomaisten

velvollisuudesta ilmoittaa viipymättä komissiolle ja asianomaisille kansallisille kilpailuviranomaisille kaikki markkinavalvontatoimien yhteydessä esiin tulleet tiedot, joilla voi olla merkitystä unionin kilpailulainsäädännön soveltamisen kannalta.

Pykälän *3 momentissa* säädettäisiin tietojen vaihtamisesta 17 §:ssä tarkoitettua asiantuntijatukea pyytävän ja antavan viranomaisen välillä. Viranomaisten välillä voitaisiin luovuttaa asiantuntijatuen antamiseksi välttämättömiä tietoja salassapitovelvoitteiden estämättä. Asiantuntijatuen antaminen olisi erillinen tehtävä suhteessa Liikenne- ja viestintäviraston suorittamaan valvontatehtävään, minkä vuoksi olisi selvyyden vuoksi tarve säätää erikseen oikeudesta luovuttaa tietoja myös asiantuntijatuen antamista varten.

19 §. *Markkinavalvontaviranomaisen oikeus tehdä tarkastuksia ja ottaa ohjelmistoja tutkittavaksi*. Pykälän *1 momentissa* säädettäisiin markkinavalvontaviranomaisen oikeudesta tehdä tarkastuksia pysyväisluonteiseen asumiseen käytettyihin tiloihin, joita talouden toimija käyttää elinkeino- tai ammattitoimintaansa liittyviin tarkoituksiin. Säännös täydentäisi markkinavalvontalain 9 §:ssä markkinavalvontaviranomaisen tarkastusoikeutta koskevaa säännöstä, jota sovellettaisiin muilta osin markkinavalvontaviranomaisen oikeuteen tehdä tarkastuksia. Markkinavalvontalain 9 §:n 2 momentti edellyttää, että pysyväisluonteiseen asumiseen käytettäviin tiloihin kohdistettavasta tarkastuksesta säädetään tarvittaessa erikseen.

Kyberkestävyysasetuksen alaan kuuluu tuotteita, joiden kehittämistä ja valmistamista on mahdollista ja jossain määrin tavanomaistakin harjoittaa yrityksen erillisten toimitilojen ohella kotirauhan piiriin kuuluvissa tiloissa. Kyberkestävyysasetuksen alaan kuuluvaa elinkeino- tai ammattitoimintaa kuten ohjelmistokehitystä tai laitteiden kokoonpanoa voidaan harjoittaa myös kotirauhan piiriin kuuluvissa tiloissa. Tällöin voi syntyä tilanteita, joissa ainoa mahdollisuus yritykseen kohdistuvan tarkastuksen tekemiselle on sen toteuttaminen talouden toimijan elinkeinotoimintaansa käyttämissä sinänsä kotirauhan piiriin kuuluvissa tiloissa, joissa toiminnan harjoittamisessa käytettävät järjestelmät ja dokumentaatio sijaitsevat. Säännös mahdollistaisi tarkastuksen ulottamisen tästä syystä myös kotirauhan piiriin kuuluviin tiloihin, kun se olisi välttämätöntä tarkastuksen kohteena olevien seikkojen selvittämiseksi.

Kotirauhan piirissä tapahtuva tarkastus olisi mahdollinen vain, jos se olisi välttämätön tarkastuksen kohteena olevien seikkojen selvittämiseksi, eli jos viranomainen ei voisi hankkia valvonnassa välttämättömiä tietoja tiedonsaantioikeutensa nojalla tai suorittamalla tarkastus muualla kuin pysyväisluonteiseen asumiseen käytetyssä tilassa.

Ulkopuoliset asiantuntijat voisivat tarvittaessa osallistua tarkastukseen markkinavalvontaviranomaisen apuna siten kuin markkinavalvontalain 14 §:n 2 momentissa säädetään. Ulkopuolisen asiantuntijan itsenäisesti suorittama tarkastus ei olisi mahdollinen säännöksen nojalla. Koska säännöksessä viitataan markkinavalvontalain 9 §:ään, myös pysyväisluontoiseen asumiseen käytettyyn tilaan kohdistettavassa tarkastuksessa olisi kyse mainitussa momentissa tarkoitetulla tavalla markkinavalvontalain mukaisesta tarkastuksesta. Viittauksen johdosta myös hallintolain 39 § tulisi sovellettavaksi säännöksen mukaisissa tarkastuksissa.

Momentissa edellytettäisiin, että viranomaisella olisi perusteltu ja yksilöity syy epäillä kyberkestävyysasetusta tai sen nojalla annettuja säädöksiä rikottavan tavalla, josta voi olla seuraamuksena ehdotetussa laissa tarkoitettu seuraamusmaksu. Pysyväisluonteiseen asumiseen käytettävässä tilassa tarkastuksen saisi siten suorittaa vain, jos viranomaisella on ennalta asianmukaiset perusteet epäillä sääntelyä rikottavan. Rikkomuksen vakavuutta ilmentäisi, että siitä tulisi voida määrätä rangaistuksenluonteinen hallinnollinen seuraamusmaksu. Jos olisi ilmeistä, että selvitettävänä olevasta teosta ei tultaisi määräämään seuraamusmaksua sen

vähäisyyden tai muun sellaisen syyn vuoksi, ei tarkastustakaan saisi suorittaa. Tarkastuksen oikeasuhtaisuutta varmistaisi lisäksi momentin edellytys siitä, että epäillyssä rikkomuksessa olisi kyse digitaalisen elementin sisältävän tuotteen tai siihen liittyvän prosessin, kuten haavoittuvuuksien hallinnan, vaatimustenvastaisuudesta taikka että kyse on kyberkestävyysasetuksen 57 artiklassa tarkoitetusta tilanteesta, jossa tuote aiheuttaa vaatimustenmukaisuudestaan huolimatta merkittävän kyberturvallisuusriskin sekä muun artiklassa tarkoitetun riskin, jonka tulee kohdistua ihmisten terveyteen tai turvallisuuteen, perusoikeuksien suojaamiseen tarkoitettujen unionin oikeuden tai kansallisen lainsäädännön mukaisten velvoitteiden noudattamiseen, NIS 2 -direktiivissä tarkoitettujen keskeisten toimijoiden tietoturvaan tai muihin yleisen edun suojaamiseen liittyville näkökohdille. Näin ollen tarkastusoikeutta voitaisiin käyttää kotirauhan piirissä vain siinä määrin vakavissa epäillyissä rikkomustapauksissa, joissa nämä edellytykset täyttyvät.

Pykälän *2 momentissa* säädettäisiin ohjelmistojen tutkittavaksi ottamisesta markkinavalvonnassa. Momentti sisältäisi informatiivisen viittauksen markkinavalvontalakiin. Lisäksi momentissa säädettäisiin rajatusta poikkeuksesta markkinavalvontalain mukaiseen velvollisuuteen korvata tutkittavaksi otettu tuote talouden toimijalle.

Markkinavalvontalain 10 §:ssä säädetään markkinavalvontaviranomaisen oikeudesta ottaa tuotteita tutkittavaksi, jos se on tuotteen vaatimustenmukaisuuden valvonnan kannalta tarpeellista. Markkinavalvontaviranomaisen on markkinavalvontalain 10 §:n 2 momentin mukaan talouden toimijan vaatimuksesta korvattava tarkoitettu tuote käyvän hinnan mukaan, jollei havaita, että tuote on vaatimustenvastainen. Koska kyberkestävyysasetuksen soveltamisalaan kuuluvia tuotteita ovat myös ohjelmistotuotteet sekä tuotteiden ratkaisut datan etäkäsittelystä, mukaan lukien toisistaan erillään markkinoille saatettavat ohjelmisto- ja laitteistokomponentit, markkinavalvontalain mukainen toimivalta soveltuisi myös niihin. Ohjelmistotuotteen ottamisesta tutkittavaksi ei aiheudu talouden toimijalle tutkittavaksi otettavan kappaleen myynnin menetyksestä aiheutuvaa vahinkoa vastaavasti kuin fyysisen tuotteen menetyksestä voi aiheutua, koska ohjelmistotuotteet ovat pääsääntöisesti digitaalisessa muodossa. Näin ollen markkinavalvontaviranomaisen ei olisi suoritettava ohjelmiston tutkittavaksi ottamisesta markkinavalvontalain 10 §:n mukaista korvausta talouden toimijalle riippumatta siitä, todetaanko ohjelmisto vaatimustenmukaiseksi. Säännös ei koskisi Tullin perimää korvausta markkinavalvontalain 10 §:n 2 momentin nojalla.

20 §. *Avoimen lähdekoodin ohjelmistovastaavalle annettava valvontapäätös*. Pykälän *1 momentissa* säädettäisiin mahdollisuudesta antaa avoimen lähdekoodin ohjelmistovastaavalle velvoittava määräys korjata puute sen kyberkestävyysasetuksessa säädettyjen velvollisuuksien noudattamisessa päätöksessä asetettavassa määräajassa. Ohjelmistovastaavan velvoitteista säädetään kyberkestävyysasetuksen 24 artiklassa (ks. luku 2.1.3.3). Markkinavalvontalakia täydentävän sääntelyn tarvetta on arvioitu luvussa 3.1.2. Kyse voisi olla esimerkiksi velvoitteesta korjata puute ohjelmistovastaavan laatimissa kyberturvallisuusperiaatteissa, tehdä puuttuva poikkeama- tai haavoittuvuusilmoitus. Velvoitteella voitaisiin tehostaa myös viranomaisen pyyntöä luovuttaa ohjelmistovastaavan laatimat dokumentoidut kyberturvallisuusperiaatteet, jos niitä ei annettaisi sille vapaaehtoisesti, samoin kuin viranomaisen pyyntöä tehdä kyberkestävyysasetuksen edellyttämää yhteistyötä tuotteen aiheuttamien kyberturvallisuusriskien lieventämiseksi tietyssä tapauksessa, jos pyyntöä ei muutoin noudatettaisi.

Pykälän *2 momentissa* säädettäisiin markkinavalvontaviranomaisen mahdollisuudesta asettaa antamansa päätöksen tehosteeksi uhkasakko. Uhkasakon asettamisesta ja täytäntöönpanosta säädetään uhkasakkolaissa.

5 luku – Kyberturvallisuussertifiointi

21 §. *Kansallinen kyberturvallisuussertifioinnin viranomainen*. Pykälän *1 momentissa* osoitettaisiin kyberturvallisuusasetuksen mukaiset kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen tehtävät Liikenne- ja viestintävirastolle, joka hoitaa tehtävää nykyisinkin sähköisen viestinnän palveluista annetun lain eli viestintäpalvelulain nojalla. Viranomaisen tehtäviin kuuluvat kyberturvallisuusasetuksen 58 artiklan nojalla vaatimustenmukaisuuden arviointilaitosten valtuuttaminen, valvonta ja seuranta, vaatimustenmukaisuuden valvonta sekä korkean varmuustason kyberturvallisuussertifikaattien myöntäminen.

Ehdotuksessa käytettäisiin kyberturvallisuusasetuksen suomenkielisestä toisinnosta poikkeavaa kyberturvallisuussertifioinnin viranomaisen käsitettä, joka on omaksuttu myös käytännössä viranomaisen viestinnässä. Kyberturvallisuusasetuksen suomenkielisessä versiossa käytetään kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen käsitettä, vaikka tämän viranomaisen tehtäviin kuuluvat paitsi eurooppalaisten kyberturvallisuussertifikaattien myöntäminen tietyissä tapauksissa myös kyberturvallisuusasetukseen liittyvä valvontatoiminta, jotka asetus vaatii erottamaan toisistaan. Ruotsinkielisessä toisinnossa käytetty käsite on nationell myndighet för cybersäkerhetscertifiering ja englanninkielisessä national cybersecurity certification authority. Ehdotetusta käsitteestä kävisi asetuksen suomenkielistä toisintoa paremmin ilmi, että viranomaisen tehtäviin kuuluu eurooppalaisten kyberturvallisuussertifikaattien myöntämisen lisäksi kyberturvallisuusasetukseen liittyvä valvontatoiminta.

Pykälän *2 momentissa* säädettäisiin kyberturvallisuussertifikaattien myöntämiseen ja kyberturvallisuusasetukseen liittyvän valvontatoiminnan eriyttämisestä asetuksen edellyttämällä tavalla. Asetuksen mukaan jäsenvaltioiden on varmistettava, että kansallisen kyberturvallisuussertifioinnin myöntävät viranomaisten toiminta, joka liittyy 56 artiklan 5 kohdan a alakohdan ja 56 artiklan 6 kohdan mukaiseen eurooppalaisten kyberturvallisuussertifikaattien myöntämiseen, on tiukasti erotettu tämän artiklan mukaisesta valvontatoiminnasta ja että nämä toiminnot suoritetaan toisistaan riippumattomasti.

Liikenne- ja viestintäviraston olisi järjestettävä toimintansa organisatorisesti niin, että kyberturvallisuussertifikaattien myöntämiseen liittyvä päätöksenteko on eriytetty kyberturvallisuussertifioinnin valvontaan liittyvästä päätöksenteosta niin, etteivät samat henkilöt voi kohdistaa hallinnollista ohjausta sekä sertifikaattien myöntämiseen että valvontatoimintaan. Käytännössä tehtävät voitaisiin osoittaa Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen eri osastoilla toimiviin yksiköihin. Tämä ei kuitenkaan estäisi viranomaisen henkilöstön asiantuntemuksen hyödyntämistä eri tehtävissä.

Kyberturvallisuusasetus ja ehdotuksen 24 § mahdollistaisivat kyberturvallisuussertifioinnin viranomaisen korkean tason sertifikaattien myöntämisen tehtävän delegoinnin vaatimustenmukaisuuden arviointilaitokselle. Euroopan kyberturvallisuuden sertifiointiryhmän tulkinnan mukaan kyberturvallisuusasetuksen 56 artiklan 6 kohdan a alakohdan mukainen vaatimustenmukaisuuden arviointilaitosten myöntämien yksittäisten sertifikaattien etukäteishyväksyntä viranomaisen toimesta olisi sertifioinnin myöntämistä, mikä tulisi siis eriyttää valvontaviranomaisen toiminnasta. Asetuksen 56 artiklan 6 kohdan b alakohdan mukainen ennalta yleisesti tapahtuva delegointi ei ole yhtä ongelmallinen suhteessa valvontatehtävien hoitamiseen, sillä viranomaisella ei olisi roolia yksittäisten sertifikaattien myöntämisessä. Tältäkin osin voidaan kuitenkin katsoa, että delegointi kuuluisi luontevammin organisatorisesti osaksi sertifikaattien myöntämistä, sillä erotuksena arviointilaitoksen ilmoittamisen ja valtuuttamisen sekä valvonnan tehtäviin viranomaiselle jää lähtökohtaisesti

harkintavaltaa siinä, delegoidaanko tehtäviä lainkaan ja mille vaatimustenmukaisuuden arviointilaitoksille niitä delegoidaan. Valvonnan viranomaistehtäviin taas kuuluu yksiselitteisesti kyberturvallisuusasetuksen 58 artiklan 7 kohdan f alakohdassa mainittu vaatimustenmukaisuuden arviointilaitosten delegoinnin perusteella myöntämiin sertifikaatteihin liittyvien sivullisten tekemien valitusten käsittely.

22 §. *Vaatimustenmukaisuuden arviointilaitosten ilmoittaminen ja valtuuttaminen kyberturvallisuussertifiointia varten*. Pykälän *1 momentissa* olisi informatiivinen viittaus kyberturvallisuussertifioinnin viranomaisen tehtävään ilmoittaa vaatimustenmukaisuuden arviointilaitos komissiolle kyberturvallisuussertifiointia varten sen jälkeen, kun laitos on saanut akkreditoinnin. Samoin kuin ehdotetun lain 11 §:ssä kyberkestävyysasetuksen osalta akkreditoinnin myöntäisi Turvallisuus- ja kemikaaliviraston akkreditointiyksikkö (FINAS-akkreditointipalvelu). Lisäksi ilmoittamisen edellytyksenä olisi eräissä tapauksissa kyberturvallisuussertifioinnin viranomaisen arviointilaitokselle antama valtuutus, joka tarvittaisiin, kun sertifiointijärjestelmässä vahvistettaisiin 54 artiklan 1 kohdan f alakohdan mukaisia erityisiä vaatimuksia tai lisävaatimuksia, jotka arviointilaitoksen olisi täytettävä. Tällaisia valtuuttamista koskevia vaatimuksia voi sisältyä komission hyväksymiin sertifiointijärjestelmiin. Tällä hetkellä ns. EUCC-täytäntöönpanoasetus (komission täytäntöönpanoasetus (EU) 2024/482 Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 soveltamissäännöistä siltä osin kuin on kyse yhteisiin kriteereihin perustuvan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän (EUCC) hyväksymisestä) edellyttää valtuutusta sen nojalla tapahtuvaan korkean varmuustason sertifikaattien myöntämiseen.

Akkreditointiin ja siihen rinnastettavaan pätevyyden arviointiin sovelletaan vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta annettua lakia (920/2005). Vaatimuksenmukaisuuden arviointilaitosta koskeviin vaatimuksiin sovelletaan kyberturvallisuusasetuksen 60 artiklan 1 kohdan viittauksen nojalla asetuksen liitettä. Kansallinen akkreditointielin antaa akkreditoinnin vain, jos vaatimukset täyttyvät. Kyberturvallisuussertifioinnin viranomaisella olisi kyberturvallisuusasetuksen mukaiset tehtävät ja toimivalta valvoa, että vaatimustenmukaisuuden arviointilaitokset noudattavat asetuksen vaatimuksia. Tämän lisäksi akkreditointiyksikkö seuraa arviointielimen pätevyyttä ja voisi peruuttaa akkreditoinnin, jos akkreditoinnin edellytykset eivät enää täyty.

Pykälän *2 momentissa* säädettäisiin, että ilmoittamisen ja valtuuttamisen edellytyksenä olisi FINAS-akkreditointipalvelun antama akkreditointitodistus siitä, että vaatimustenmukaisuuden arviointilaitos täyttää kyberturvallisuusasetuksen vaatimukset. Ehdotettu sanamuoto mahdollistaisi sen, että kyberturvallisuussertifioinnin viranomaisen olisi mahdollista käynnistää valtuutukseen liittyvä arviointi akkreditointimenettelyn ollessa vielä kesken, jos viranomainen pitää sitä perusteltuna.

23 §. *Kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen velvollisuudet*.

Pykälän *1 momentissa* säädettäisiin kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen velvollisuudesta suorittaa vaatimustenmukaisuuden arvioinnit kyberturvallisuusasetuksessa ja sen nojalla annettujen säädösten mukaisten vaatimustenmukaisuuden arviointimenettelyjen edellyttämällä tavalla samoin kuin muut edellä tarkoitetuissa säädöksissä säädetyt tehtävät. Ehdotus vastaa osin eräitä tuoteryhmiä koskevista ilmoitetuista laitoksista annetun lain 14 §:n 1 momenttia. Kyseinen laki ei tule sovellettavaksi kyberturvallisuusasetuksen nojalla ilmoitettuihin vaatimustenmukaisuuden arviointilaitoksiin, minkä johdosta lakiehdotukseen on tarpeen ottaa eräitä arviointilaitosten velvollisuuksia koskevia säännöksiä.

Pykälän *2 momentissa* säädettäisiin kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen velvollisuudesta ilmoittaa kyberturvallisuussertifioinnin viranomaiselle kaikista muutoksista, joilla on vaikutusta ilmoittamisen tai valtuuttamisen edellytysten täyttymiseen. Näistä edellytyksistä säädetään kyberturvallisuusasetuksessa ja sen nojalla hyväksytyissä sertifiointijärjestelmissä. Lakiehdotuksen 25 §:ssä säädettäisiin kyberturvallisuussertifioinnin viranomaisen oikeudesta saada muitakin tietoja vaatimustenmukaisuuden arviointilaitokselta.

Pykälän *3 momentissa* säädettäisiin edellä 13 §:ää vastaavasti rikosoikeudellisesta virkavastuusta kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen sekä sen käyttämän tytäryhtiön ja alihankkijan henkilöstön virkavastuusta arviointilaitoksen hoitaman julkisen hallintotehtävän johdosta. Lisäksi momentti sisältäisi informatiivisen viittauksen vahingonkorvauslakiin. Edellä 13 §:n perustelujen yhteydessä mainitusti hallinnon yleislait tulisivat sovellettavaksi ilman eri viittaustakin. Kyberturvallisuusasetuksen liite (vaatimustenmukaisuuden arviointilaitoksia koskevat vaatimukset) sisältää myös tytäryhtiön tai alihankkijan käyttöön liittyviä vaatimuksia.

24 §. *Kyberturvallisuussertifikaatin myöntämiseen liittyvä tehtävien siirtäminen*. Pykälän *1 momentissa* säädettäisiin, että kyberturvallisuussertifioinnin viranomainen voisi siirtää eli delegoida korkean varmuustason kyberturvallisuussertifikaatin myöntämisen vaatimuksenmukaisuuden arviointilaitokselle. Tästä mahdollisuudesta säädetään kyberturvallisuusasetuksen 56 artiklan 6 kohdassa, joka mahdollistaa kaksi erilaista delegoinnin tapaa. Tehtävä voitaisiin siirtää joko niin, että viranomainen hyväksyy ennalta kunkin yksittäisen sertifikaatin myöntämisten erikseen, tai yleisesti ennalta siten, että vaatimustenmukaisuuden arviointilaitos myöntäisi itsenäisesti tietyn sertifiointijärjestelmän puitteissa myönnettävät eurooppalaiset kyberturvallisuussertifikaatit. Kummassakin tapauksessa arviointilaitoksen voitaisiin katsoa toimivan itsenäisesti ja tekevän myöntämistä koskevat päätökset omissa nimissään, eli kyse ei olisi viranomaista avustavasta roolista. Komission täytäntöönpanoasetuksella annettu sertifiointijärjestelmä voi asettaa reunaehtoja delegoinnille tai edellyttää sitä. EUCC-täytäntöönpanoasetuksen 17 artiklan 4 kohdan b alakohta esimerkiksi mahdollistaa vain menettelyn, että viranomainen hyväksyy kunkin yksittäisen sertifioitavan prosessin ennalta. Edellä 21 §:n yhteydessä on tarkasteltu kyberturvallisuussertifioinnin viranomaisen delegointia koskevien tehtävien eriyttämistä valvontatehtävistä.

Tehtävän siirtämiseen liittyvään vaatimustenmukaisuuden arviointilaitoksen palvelun hankintaan voisi tapauskohtaisesti tulla sovellettavaksi laki julkisista hankinnoista ja käyttöoikeussopimuksista (1397/2016). Jos viranomainen hyväksyy tehtävää hoitamaan kaikki ne vaatimustenmukaisuuden arviointilaitokset, jotka täyttävät laissa säädetyt edellytykset, ei kyse ei olisi julkisesta hankinnasta eikä hankintalainsäädäntöä sovellettaisi (ks. vastaavasti HE 108/2016 vp, s. 75). Jos taas ainoastaan osa vaatimustenmukaisuuden arviointilaitoksista voisi osallistua ehdotuksen 1 momentissa tarkoitettujen sertifikaattien myöntämiseen, voisi tilanne tulla arvioitavaksi palveluja koskevana käyttöoikeussopimuksena. Laissa julkisista hankinnoista ja käyttöoikeussopimuksista palveluja koskevalla käyttöoikeussopimuksella tarkoitetaan ”taloudellista vastiketta vastaan tehtyä kirjallista sopimusta, jolla yksi tai usea hankintayksikkö siirtää muiden kuin käyttöoikeusurakkaa koskevien palvelujen tarjoamisen ja hallinnoimisen sekä siihen liittyvän toiminnallisen riskin yhdelle tai usealle toimittajalle ja jossa siirtämisen vastikkeena on joko yksinomaan palvelujen käyttöoikeus tai tällainen oikeus ja maksu yhdessä”. Kun palveluntarjoaja ottaisi riskin palvelun kysynnästä ja sertifiointiviranomainen puolestaan hyötyisi siitä, ettei sen tarvitsisi suorittaa tehtävää itse, voi määritelmä täyttyä.

Pykälän *2 momentissa* säädettäisiin seikoista, joista kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen kanssa tehtävässä sopimuksessa olisi ainakin sovittava. Sopimuksessa tulisi ensinnäkin kuvata delegoitavat tehtävät tarkemmin. Tehtävät olisi mahdollista rajata myös tarkemmin kuin vain tiettyyn sertifiointijärjestelmään. Toiseksi sopimukseen voitaisiin ottaa kyberturvallisuussertifioinnin viranomaisen tarpeellisiksi arvioimia erityisiä vaatimuksia vaatimustenmukaisuuden arviointilaitoksen pätevyydelle ja sen toiminnan turvallisuudelle, kuten tietoturvasta ja fyysisestä turvallisuudesta huolehtimiselle, jos kyberturvallisuusasetuksesta ja sovellettavasta sertifiointijärjestelmästä seuraavia vaatimuksia ei pidettäisi riittävinä. Kolmanneksi sopimuksessa tulisi ottaa kantaa sopimuskauteen, toiminnan aloittamiseen ja sopimuksen päättymiseen kesken sopimuskauden, kuten viranomaisen tai arviointilaitoksen mahdolliseen oikeuteen irtisanoa delegointia koskeva sopimus kesken sopimuskauden. Neljänneksi sopimuksessa tulisi lausua vaatimustenmukaisuuden arviointilaitoksen toimintaan liittyvien asiakirjojen säilyttämisestä ja arkistoinnista etenkin silmällä pitäen sopimuksen päättymistä. Viidenneksi sopimuksessa tulisi sopia vaatimustenmukaisuuden arviointilaitoksen toiminnan puutteista ja laiminlyönneistä aiheutuvista seuraamuksista.

Momentissa ei erikseen mainittaisi henkilötietojen käsittelyä tai maksuja. Vaatimustenmukaisuuden arviointilaitoksen katsottaisiin toimivan itsenäisenä rekisterinpitäjänä siltä osin kuin sertifiointitehtävien hoitamiseen liittyisi esimerkiksi sertifikaatin hakijan henkilöstön henkilötietojen käsittelyä. Tarkoituksena on, että delegoidun tehtävän hoitaminen rahoitettaisiin maksuilla, joita arviointilaitos perisi kaupallisin perustein sertifioinnin hakijoilta.

Pykälän *3 momentin* mukaan kyberturvallisuussertifioinnin viranomainen voisi irtisanoa tai purkaa delegointia koskevan sopimuksen, jos kyberturvallisuussertifiointia varten ilmoitettu vaatimustenmukaisuuden arviointilaitos ei enää täytä arviointilaitokseen kohdistuvia vaatimuksia tai jos se olennaisesti laiminlyö sopimuksessa sovittujen tehtävien suorittamisen tai muutoin rikkoo sopimusta tai toimii olennaisesti tai toistuvasti lainvastaisesti. Ehdotus mahdollistaisi delegoinnin peruuttamisen, jos delegoituja tehtäviä laiminlyödään olennaisella tavalla tai jos arviointilaitos ei enää ole pätevä tehtäviinsä. Vaatimustenmukaisuuden arviointilaitokseen voitaisiin tarvittaessa kohdistaa myös valvontatoimenpiteitä erillisessä menettelyssä ehdotetun lain mukaisesti, mutta delegoinnin peruuttaminen ei periaatteessa olisi riippuvainen valvontaprosessin etenemisestä.

25 §. *Kyberturvallisuussertifioinnin viranomaisen tiedonsaanti- ja tarkastusoikeus.* Pykälän *1 momentissa* säädettäisiin kyberturvallisuussertifioinnin viranomaisen tiedonsaantioikeudesta. Viranomaisella olisi salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada sen ehdotetussa laissa tai kyberturvallisuusasetuksessa säädettyjen tehtävien hoitamiseksi ja kyberturvallisuusasetuksen, sen nojalla annettujen säädösten ja tämän lain noudattamisen valvomiseksi välttämättömät tiedot vaatimustenmukaisuuden arviointilaitokselta, eurooppalaisen kyberturvallisuussertifikaatin haltijalta ja EU-vaatimustenmukaisuusilmoitusten antajalta. Tiedot olisi luovutettava ilman aiheetonta viivytystä, viranomaisen pyytämässä muodossa ja maksutta.

Ehdotus täydentäisi kyberturvallisuusasetuksen 58 artiklan 8 kohdan a alakohtaa, jonka mukaan viranomaisella on oltava valtuus pyytää vaatimustenmukaisuuden arviointilaitoksilta, eurooppalaisen kyberturvallisuussertifikaatin haltijoilta ja EU-vaatimustenmukaisuusilmoituksen antajilta kaikki tiedot, jotka se tarvitsee (eng. ”requires”) tehtävänsä suorittamiseksi. Ilmaisun voidaan katsoa sopivan yhteen ehdotetun välttämättömyysedellytyksen kanssa.

Pykälässä säädettävissä toimivaltuuksissa ei edellytettäisi, että kyseessä olisi kyberturvallisuussertifiointia varten ilmoitettu vaatimustenmukaisuuden arviointilaitos, sillä tietojensaantioikeus koskisi myös tilannetta, jossa arviointilaitos on vasta hakenut ilmoittamista ja toisaalta myös tilanteita, joissa arviointilaitos olisi jäsenvaltion pyynnöstä jo poistettu komission ilmoituksista pitämästä luettelosta.

Ehdotetun pykälän *2 momentissa* säädettäisiin kyberturvallisuussertifioinnin viranomaisen tarkastusoikeudesta. Tarkastus voitaisiin kohdistaa kyberturvallisuusasetuksen 58 artiklan 7 kohdan b alakohdan mukaisesti vaatimustenmukaisuuden arviointilaitokseen, eurooppalaisen kyberturvallisuussertifikaatin haltijaan tai EU-vaatimustenmukaisuusilmoitusten antajaan. Tarkastuksen kohteena olisivat kyberturvallisuusasetuksen, sen nojalla annettujen säädösten ja ehdotetun lain noudattamisen valvontaan liittyvät seikat. Tarkastuksissa tulisi ehdotuksen mukaan noudattaa, mitä hallintolain (434/2003) 39 §:ssä säädetään.

Pykälän *3 momentissa* säädettäisiin kyberturvallisuussertifioinnin viranomaisen oikeudesta teettää tarkastus riippumattomalla asiantuntijalla. Tarkastuksen suorittajalla ja siihen osallistuvalla olisi oltava sellainen koulutus ja kokemus kuin tarkastuksen suorittamiseksi on tarpeen. Tarvittava kokemus on mahdollista hankkia esimerkiksi vaatimustenmukaisuuden arviointilaitoksen palveluksessa. Momentissa säädettäisiin rikosoikeudellisesta virkavastuusta, siinä olisi informatiivinen viittaus vahingonkorvauslakiin.

Pykälän *4 momentissa* ehdotetaan säädettäväksi, että tarkastusta suorittavalla kyberturvallisuussertifioinnin viranomaisella ja riippumattomalla asiantuntijalla olisi oikeus päästä kaikkiin tiloihin, joissa harjoitetaan kyberturvallisuusasetuksessa tarkoitettua toimintaa sekä kaikkiin tiloihin ja tietojärjestelmiin, joissa säilytetään tai käsitellään valvonnan kannalta merkityksellisiä tietoja. Tietojärjestelmissä käsiteltävillä tiedoilla tarkoitettaisiin esimerkiksi asianhallinta- ja arkistointijärjestelmiä, joissa säilytetään arviointilaitoksen arvioinnin kohteena olleen tuotteen tietoja, tai kyberturvallisuussertifikaatin haltijan järjestelmiä, joissa säilytetään tuotetta koskevia tietoja. Tarkastusta ei ole tarkoitettu ulotettavaksi esimerkiksi sähköpostijärjestelmiin tai muihin sen kaltaisiin yrityksen henkilöstön viestintään käyttämiin tietojärjestelmiin, sillä niissä käsiteltäviä tietoja ei yleisesti ottaen pidettäisi säännöksessä tarkoitetulla tavalla kyberturvallisuusasetuksen mukaisten velvoitteiden valvonnan kannalta merkityksellisinä.

Momentissa säädettäisiin, ettei tarkastuksia saisi kuitenkaan ulottaa pysyväisluonteiseen asumiseen käytettäviin tiloihin. Vaikka myös kyberturvallisuusasetuksen alaan kuuluvaa toimintaa voidaan harjoittaa pysyväisluonteiseen asumiseen käytettävissä tiloissa ja kyberturvallisuussertifikaatin haltija voi olla luonnollinen henkilö, toisin kuin edellä 17 §:ssä ei esityksessä ehdoteta tältä osin säädettäväksi tarkastusten ulottamisesta kotirauhan piiriin. Kyberturvallisuusasetukseen katsotaan liittyvän tältä kansallista liikkumavaraa, minkä lisäksi sääntely mahdollistaisi sertifikaatin voimassaolon keskeyttämisen tai peruuttamisen siinä tapauksessa, ettei sertifikaatin haltija täyttäisi tiedonantovelvollisuuttaan. Näin ollen mahdollisuutta tarkastusten ulottamiseen kotirauhan piiriin ei pidetä välttämättömänä.

26 §. *Kyberturvallisuussertifioinnin viranomaisen oikeus luovuttaa salassa pidettäviä tietoja.* Pykälässä säädettäisiin kyberturvallisuussertifioinnin viranomaisen oikeudesta luovuttaa salassa pidettäviä tietoja pyynnöstä tai omasta aloitteestaan. Pykälää sovellettaisiin julkisuuslaissa ja muualla laissa säädetyn lisäksi, minkä johdosta pykälään ei ehdoteta säännöksiä esimerkiksi esitutkintaa varten tapahtuvasta tiedonluovutuksesta. Tietotyyppejä ei yksilöitäisi, mutta pykälän kohdissa tietojen luovuttaminen olisi sidottu välttämättömyyteen tietyn tehtävän kannalta. Käytännössä tiedot voisivat koskea esimerkiksi yhteisön liikesalaisuuksia sekä tieto- ja viestintäjärjestelmien turvajärjestelyjä.

Pykälän *1 kohdassa* säädettäisiin salassa pidettävien tietojen luovuttamisesta ensinnäkin markkinavalvontalain 4 §:ssä tarkoitetulle markkinavalvontaviranomaiselle. Ehdotus on tarpeen kyberturvallisuusasetuksen 58 artiklan 7 kohdan a alakohdan johdosta, sillä se edellyttää valvontayhteistyötä asiaankuuluvien markkinavalvontaviranomaisten kanssa. Myös EUCC-täytäntöönpanoasetuksen 28 artiklan 2 kohdassa edellytetään, että kyberturvallisuussertifioinnin viranomainen ilmoittaa vaatimustenvastaisuudesta markkinavalvontaviranomaiselle. Samoin kyseisen kohdan h alakohta edellyttää tiedonjakoa muiden viranomaisten kanssa mahdollisista tapauksista, joissa sertifioidut hyödykkeet eivät vastaa asetuksen tai yksittäisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien vaatimuksia. Toiseksi kohta mahdollistaisi tietojen luovuttamisen Turvallisuus- ja kemikaaliviraston akkreditointiyksikölle tai toisen jäsenvaltion kansalliselle akkreditointielimelle, jos tiedon luovuttaminen on välttämätöntä kyseisen viranomaisen tehtävien suorittamisen kannalta. Tämä ehdotus on tarpeen kyberturvallisuusasetuksen 58 artiklan 7 kohdan c alakohdan takia, sillä siinä edellytetään viranomaisen avustavan ja tukevan kansallisia akkreditointielimiä.

Pykälän *2 kohdassa* säädettäisiin puolestaan tietojen luovuttamisesta toiselle kansalliselle kyberturvallisuussertifioinnin viranomaiselle ja muulle Euroopan kyberturvallisuuden sertifiointiryhmän jäsenelle, Euroopan unionin kyberturvallisuusvirasto ENISA:lle sekä Euroopan komissiolle, jos se on välttämätöntä kyberturvallisuusasetuksessa tai sen nojalla säädetyn kyberturvallisuussertifioinnin viranomaisen velvoitteen toteuttamiseksi. Tältä osin ehdotettu säännös täydentää erityisesti kyberturvallisuusasetuksen 58 artiklan 7 kohdan g ja h alakohtia sekä 58 artiklan 9 kohtaa, jotka koskevat yhteistyötä ENISA:n, komission, Euroopan kyberturvallisuuden sertifiointiryhmän ja muiden kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten kanssa. Esimerkiksi EUCC-täytäntöönpanoasetuksen 38 artiklassa edellytetään kyberturvallisuussertifioinnin viranomaisen jakavan eräitä haavoittuvuuksiin liittyviä tietoja muiden kansallisten kyberturvallisuussertifioinnin viranomaisten ja ENISA:n kanssa. Lisäksi tietojen luovuttaminen voisi olla tarpeen kyberturvallisuusasetuksen 59 artiklan mukaisen vertaisarvioinnin yhteydessä.

Pykälän *3 kohdassa* taas säädettäisiin eräiden tietojen luovuttamisesta kyberturvallisuuslain 26 §:ssä ja julkisen hallinnon tiedonhallinnasta annetun lain 18 h §:ssä tarkoitetulle valvovalle viranomaiselle, Finanssivalvonnalle sekä CSIRT-yksikölle, jos se on tarpeen sen niille laissa säädettyjen tehtävien hoitamista varten. Finanssivalvonnan kyberturvallisuuteen liittyvästä tehtävistä säädetään Finanssivalvonnasta annetussa laissa ja ns. DORA-asetuksessa (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2554 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). Kohta täydentää kyberturvallisuusasetuksen 58 artiklan 7 kohdan h alakohtaa, jonka mukaan kyberturvallisuussertifioinnin viranomaisen on tehtävä yhteistyötä muiden viranomaisten kanssa esimerkiksi jakamalla tietoa mahdollisista tapauksista, joissa tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit taikka tietoturvapalvelut eivät vastaa tämän asetuksen tai yksittäisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien vaatimuksia. Nämä tiedot samoin kuin tiedot niitä koskevista haavoittuvuuksista voisivat olla tarpeellisia esimerkiksi CSIRT-yksikön kyberturvallisuuslaissa säädetyn kyberuhkien seurantaa koskevan tehtävän kannalta. Tiedot sertifioidun tuotteen tai palvelun puutteista voisivat olla tarpeellisia myös niitä käyttävien toimijoiden kyberturvallisuuslain tai DORA-asetuksen mukaisten riskienhallintavelvoitteiden noudattamisen valvonnan kannalta.

27 §. *Valvontapäätös.* Pykälän *1 momentissa* säädettäisiin kansallisen kyberturvallisuussertifioinnin viranomaisen toimivallasta antaa velvoittava päätös ehdotetun lain tai kyberturvallisuusasetuksen tai sen nojalla säädettyjen velvollisuuksien, kuten soveltuvan

eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisten vaatimusten, vastaisen toiminnan korjaamiseksi. Viranomainen voisi päätöksellään velvoittaa vaatimustenmukaisuuden arviointilaitoksen, eurooppalaisen kyberturvallisuussertifikaatin haltijan tai EU-vaatimustenmukaisuusilmoitusten antajan määräajassa korjaamaan puutteen, jos valvonnassa havaittaisiin virheitä, laiminlyöntejä tai muita puutteita säädettyjen velvoitteiden noudattamisessa. Viranomainen voisi esimerkiksi velvoittaa toimijan korjaamaan havaitut puutteet tai laiminlyönnit, lopettamaan sääntelyn vastaisen toiminnan ja pidättäytymään tästä toiminnasta vastaisuudessa sekä määrätä toimijan täyttämään tietojenantovelvollisuutensa määrätyllä tavalla ja määrätyn ajan kuluessa.

Pykälän *2 momentissa* säädettäisiin kyberturvallisuussertifioinnin viranomaisen mahdollisuudesta asettaa antamansa päätöksen tehosteeksi uhkasakko, teettämisuhka tai keskeyttämisuhka. Hallinnollisen tehosteen asettamisesta ja täytäntöönpanosta säädetään uhkasakkolaissa.

28 §. *Kyberturvallisuussertifikaatin peruuttaminen*. Pykälässä säädettäisiin kyberturvallisuussertifioinnin viranomaisen toimivallasta peruuttaa viranomaisen myöntämä tai kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen kyberturvallisuusasetuksen 56 artiklan 6 kohdan mukaisesti myöntämä eurooppalainen kyberturvallisuussertifikaatti ensinnäkin siinä tapauksessa, jos sertifikaatti ei täytä kyberturvallisuusasetuksessa säädettyjä tai kyseisen eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimuksia. Kyberturvallisuusasetuksen 58 artiklan 8 kohdan e alakohta edellyttää tällaisesta toimivallasta säätämisestä tarkemmin kansallisesti. Edellytyksenä olisi, että puutetta ei korjata kohtuullisessa määräajassa, jos puutteen korjaaminen on mahdollista. Määräaika voisi sisältyä 25 §:n mukaiseen valvontapäätökseen, jos päätös edeltäisi sertifikaatin peruuttamista. Vaihtoehtoisesti sertifikaatin peruuttamista voitaisiin käsitellä omana asianaan, jolloin ilmoitus puutteesta ja korjaamiselta edellytetty määräaika voitaisiin ilmoittaa viranomaisen muulla kuin valituskelpoisella asiakirjalla ennen valituskelpoisen ratkaisun tekemistä sertifikaatin peruuttamisesta.

Kyberturvallisuusasetuksen 56 artiklan 6 kohdan mukaan kyberturvallisuussertifioinnin viranomainen lähtökohtaisesti myöntää korkean varmuustason sertifikaatit. Vaatimustenmukaisuuden arviointilaitos myöntää kuitenkin korkean varmuustason sertifikaatin silloin, jos viranomainen on ennalta delegoinut sille tämän tehtävän joko yleisesti tai yksittäisessä tapauksessa. Lisäksi kyberturvallisuussertifioinnin viranomainen voi poikkeuksellisesti myöntää myös perustason tai korotetun varmuustason sertifikaatin silloin, kun sertifiointijärjestelmässä määrätään niin (56 artiklan 5 kohta). Ehdotus mahdollistaisi sertifikaatin peruuttamisen edellä mainituissa tapauksissa. Sen sijaan tapauksissa, joissa perustason tai korotetun varmuustason sertifikaatin on myöntänyt vaatimustenmukaisuuden arviointilaitos, ei peruuttamistoimivallasta säädettäisi. Tämä ei olisi tarpeen, sillä tällöin sertifikaatin peruuttamisesta vastaisi sen myöntänyt vaatimustenmukaisuuden arviointilaitos soveltuvan sertifiointijärjestelmän määräysten mukaisesti. Lähtökohtaisesti sertifikaatin peruuttaminen kuuluu nimittäin sen myöntäneen vaatimustenmukaisuuden arviointilaitoksen tehtäviin, mikä ilmenee myös ns. EUCC-täytäntöönpanoasetuksen 14 artiklasta, minkä lisäksi arviointilaitos voi keskeyttää sertifikaatin voimassaolon sen 30 artiklan perusteella. Kansallisen kyberturvallisuussertifioinnin viranomaisen peruuttamistoimivalta täydentäisi arviointilaitoksen peruuttamistoimivaltaa yllä mainituissa tilanteissa.

Toiseksi ehdotus mahdollistaisi sertifikaatin peruuttamisen siinä tapauksessa, ettei kyberturvallisuussertifikaatin haltija anna kyberturvallisuussertifioinnin viranomaiselle sen pyytämiä 26 §:n 1 momentissa tarkoitettuja tietoja eikä laiminlyöntiä korjata kohtuullisessa määräajassa. Tältä osin sääntely ei olisi välittömästi kyberturvallisuusasetuksen edellyttämää.

EUCC-täytäntöönpanoasetus kuitenkin mahdollistaa samankaltaiset toimenpiteet eli sertifikaatin voimassaolon keskeyttämisen arviointilaitoksen toimesta siinä tapauksessa, että sertifikaatin haltija jatkuvasti tai toistuvasti rikkoo sitoumustaan antaa tietoja (29 artikla ja 9(2) artikla) tai ei tee yhteistyötä (28(4) artikla). Ehdotetun toimivaltuuden käyttö voisi tulla viime kädessä kyseeseen esimerkiksi tapauksissa, joissa välttämättömiä tietoja ei anneta vapaaehtoisesti eikä niitä voida hankkia myöskään 26 §:ssä tarkoitetulla tarkastuksella sen johdosta, että kyseiset tilat sijaitsevat kotirauhan piirissä tai ulkomailla.

29 §. *Kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen valtuutuksen ja ilmoituksen keskeyttäminen, rajoittaminen tai peruuttaminen.* Pykälän *1 momentissa* säädettäisiin kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen ilmoituksen ja valtuutuksen peruuttamisesta, keskeyttämisestä tai rajoittamisesta sekä arviointilaitoksen poistamista ilmoitettujen vaatimustenmukaisuuden arviointilaitosten luettelosta koskevasta pyynnöstä. Kyberturvallisuussertifioinnin viranomaisen olisi tarvittaessa ryhdyttävä näihin toimenpiteisiin ensinnäkin, jos arviointilaitos ei ole korjannut toimintaansa valvontapäätöksessä edellytetyllä tavalla ja kyseessä on olennainen rikkomus tai laiminlyönti. Toiseksi toimenpiteisiin olisi tarvittaessa ryhdyttävä, jos vaatimustenmukaisuuden arviointilaitos ei täytä sille säädettyjä vaatimuksia tai sen akkreditointia rajoitetaan, akkreditointi peruutetaan tai se keskeytetään. Toimenpiteisiin olisi ryhdyttävä siinäkin tapauksessa, ettei päätös olisi vielä lainvoimainen, jos se olisi täytäntöönpanokelpoinen muutoksenhausta huolimatta. Rikkomuksen, puutteen tai laiminlyönnin luonne ja sen mahdollinen korjaaminen ennen päätöksen tekemistä tulisi ottaa huomioon arvioitaessa, minkä tyyppinen toimenpide olisi tarpeellinen.

Ehdotus on tarpeellinen kyberturvallisuusasetuksen 58 artiklan 7 kohdan e alakohdan johdosta, jossa säädetään viranomaisen velvollisuudesta rajoittaa myönnettyjä valtuutuksia taikka keskeytettävä tai peruutettava ne, jos vaatimustenmukaisuuden arviointilaitokset eivät noudata kyberturvallisuusasetuksen vaatimuksia. Lisäksi se täydentää kyberturvallisuusasetuksen 61 artiklan 1 ja 4 kohtaa. Ensin mainitun johdosta kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten on ilman aiheetonta viivytystä ilmoitettava komissiolle kaikista muutoksista arviointilaitosten akkreditoinneissa ja valtuutuksissa. Jälkimmäisessä puolestaan säädetään, että kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen voi esittää komissiolle pyynnön poistaa kyseisen viranomaisen ilmoittama vaatimustenmukaisuuden arviointilaitos artiklan 2 kohdassa tarkoitetusta sertifiointijärjestelmän mukaisesti ilmoitetuista vaatimustenmukaisuuden arviointilaitoksien luettelosta. Tällainen pyyntö olisi ehdotuksen mukaan tarvittaessa esitettävä, jos ilmoittamisen edellytykset eivät enää täyty.

Momentissa säädettyä sovellettaisiin vain, jos kyberturvallisuusasetuksen nojalla annetusta säädöksestä ei muuta johtuisi. Komission täytäntöönpanoasetuksessa (EU) 2024/3143 säädetään kyberturvallisuusasetuksen 61 artiklan 5 kohdan mukaisiin ilmoituksiin liittyvien olosuhteiden, muotoseikkojen ja menettelyjen vahvistamisesta, ja sen 4 artiklan 2 kohdassa säädetään kyberturvallisuussertifioinnin viranomaisen velvollisuudesta tarvittaessa ryhtyä yllä mainittuihin toimenpiteisiin sen mukaan, miten vakava kyseisten vaatimusten tai velvoitteiden noudattamatta jättäminen on. Lisäksi komission täytäntöönpanoasetuksella annettava sertifiointijärjestelmä voi sisältää yksityiskohtaisempaa sääntelyä kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen valtuutuksen tai ilmoituksen peruuttamisesta. Tällaista sääntelyä sisältyy EUCC-täytäntöönpanoasetuksen 22 artiklan 6 kohtaan.

Ehdotettu *2 momentti* vastaisi osin eräitä tuoteryhmiä koskevista ilmoitetuista laitoksista annetun lain 6 §:n 4 momenttia. Siinä säädettäisiin tilanteesta, jossa kyberturvallisuussertifiointia varten ilmoitettu vaatimustenmukaisuuden arviointilaitos on

lopettanut toimintansa tai se poistetaan komission luettelosta. Tällöin kyberturvallisuussertifioinnin viranomaisen olisi ryhdyttävä asianmukaisiin toimenpiteisiin sen varmistamiseksi, että kyseisen vaatimustenmukaisuuden arviointilaitoksen asiakirjat käsittelee toinen kyberturvallisuussertifiointia varten ilmoitettu vaatimustenmukaisuuden arviointilaitos tai että asiakirjat pidetään muutoin kyberturvallisuussertifioinnin viranomaisen ja markkinavalvonnasta vastaavien viranomaisten saatavilla. Viranomaisen olisi huolehdittava, että asiakirjojen luottamuksellisuus säilyy kyberturvallisuusasetuksen ja sen nojalla annettujen säädösten sekä julkisuuslain mukaisesti.

30 §. *Poliisin virka-apu.* Ehdotetun pykälän mukaan kyberturvallisuussertifioinnin viranomaisella olisi oikeus saada poliisilta virka-apua ehdotetussa laissa tai kyberturvallisuusasetuksessa tai sen nojalla säädettyjen velvollisuuksien noudattamisen valvomiseksi ja täytäntöön panemiseksi. Virka-avun antaminen voisi tulla kyseeseen esimerkiksi, jos viranomaista estettäisiin käyttämästä tarkastustoimivaltuuksiaan. Pykälässä olisi informatiivinen viittaus poliisilakiin, jossa säädetään poliisin antamasta virka-avusta (872/2011).

6 luku – Seuraamusmaksut

31 §. *Valmistajan seuraamusmaksu.* Pykälässä säädettäisiin hallinnollisesta seuraamusmaksusta, joka voitaisiin määrätä valmistajalle kyberkestävyysasetuksen rikkomisen perusteella.

Pykälän *1 momentissa* säädettäisiin kyberkestävyysasetuksen 64 artiklan 2 kohdan edellyttämällä tavalla kyberkestävyysasetuksen liitteessä I vahvistettujen olennaisten kyberturvallisuusvaatimusten ja 13 ja 14 artiklassa säädettyjen velvoitteiden täyttämättä jättämisestä hallinnollisen seuraamusmaksun perusteena. Momentin säännökset kattaisivat myös 64 artiklan 3 kohdan edellyttämällä tavalla 31 artiklan 1–4 kohtien rikkomisen, 32 artiklan 1–3 kohtien rikkomisen ja 33 artiklan 5 kohdan rikkomisen.

Pykälän *2 momentissa* säädettäisiin kyberkestävyysasetuksen 64 artiklan 3 kohdan edellyttämällä tavalla valmistajalle säädetyn velvoitteen rikkomisesta hallinnollisen seuraamusmaksun perusteena silloin, kun valmistajien velvoitteita sovelletaan 21 artiklan nojalla maahantuojaan tai jakelijaan taikka 22 artiklan nojalla muuhun luonnolliseen henkilöön tai oikeushenkilöön kuin valmistajaan, maahantuojaan tai jakelijaan.

32 §. *Valtuutetun edustajan seuraamusmaksu.* Pykälässä säädettäisiin hallinnollisesta seuraamusmaksusta, joka voitaisiin määrätä valtuutetulle edustajalle kyberkestävyysasetuksen rikkomisen perusteella. Pykälässä säädettäisiin kyberkestävyysasetuksen 64 artiklan 3 kohdan edellyttämällä tavalla asetuksen 18 artiklan rikkomisesta. Valtuutetulla edustajalla tarkoitettaisiin luonnollista henkilöä tai oikeushenkilöä, jolla on valmistajan antama kirjallinen toimeksianto hoitaa valmistajan puolesta tietyt, muutoin valmistajalle kuuluvat tehtävät. Valtuutetun edustajan velvollisuuksista säädetään kyberkestävyysasetuksen 18 artiklassa. Milloin valtuutettua edustajaa ei ole nimitetty valmistajan kirjallisella toimeksiannolla tai laiminlyönti ei kuulu toimeksiannon alaan, hallinnollista seuraamusmaksua ei voitaisi määrätä valtuutetun edustajan vastuun perusteella.

33 §. *Maahantuojan seuraamusmaksu.* Pykälässä säädettäisiin hallinnollisesta seuraamusmaksusta, joka voitaisiin määrätä maahantuojalle kyberkestävyysasetuksen rikkomisen perusteella. Pykälässä säädettäisiin kyberkestävyysasetuksen 64 artiklan 3 kohdan edellyttämällä tavalla asetuksen 19 artiklan rikkomisesta.

34 §. *Jakelijan seuraamusmaksu.* Pykälässä säädettäisiin hallinnollisesta seuraamusmaksusta, joka voitaisiin määrätä jakelijalle kyberkestävyysasetuksen rikkomisen perusteella. Pykälässä säädettäisiin kyberkestävyysasetuksen 64 artiklan 3 kohdan edellyttämällä tavalla asetuksen 20 artiklan rikkomisesta.

35 §. *Ilmoitetun laitoksen seuraamusmaksu.* Pykälässä säädettäisiin hallinnollisesta seuraamusmaksusta, joka voitaisiin määrätä ilmoitetulle laitokselle kyberkestävyysasetuksen rikkomisen perusteella sen toimiessa tehtävässään kyberkestävyysasetuksen vastaisella tavalla. Pykälässä säädettäisiin kyberkestävyysasetuksen 64 artiklan 3 kohdan edellyttämällä tavalla asetuksen 39, 41, 47 tai 49 artiklan rikkomisesta määrättävästä hallinnollisesta seuraamusmaksusta.

36 §. *Muut kyberkestävyysasetukseen liittyvät seuraamusmaksut.* Pykälässä säädettäisiin hallinnollisesta seuraamusmaksusta, joka voitaisiin määrätä talouden toimijalle kyberkestävyysasetuksen rikkomisen perusteella muissa kuin 31–35 §:ssä tarkoitetuissa tilanteissa. Pykälässä säädettäisiin kyberkestävyysasetuksen 64 artiklan 3 kohdan edellyttämällä tavalla asetuksen 23 artiklan, 30 artiklan ja 53 artiklan rikkomisesta määrättävästä hallinnollisesta seuraamusmaksusta. Pykälässä säädettäisiin myös kyberkestävyysasetuksen 64 artiklan 4 kohdan edellyttämällä tavalla hallinnollisesta seuraamusmaksusta talouden toimijalle virheellisten, puutteellisten tai harhaanjohtavien tietojen toimittamisesta vastauksena ilmoitettujen laitosten ja markkinavalvontaviranomaisten pyyntöön.

37 §. *Kyberturvallisuussertifiointia koskeva seuraamusmaksu*. Pykälässä säädettäisiin kyberturvallisuusasetuksen rikkomiseen liittyvistä teoista, joista voitaisiin määrätä hallinnollinen seuraamusmaksu. Pykälässä säädettäisiin kyberturvallisuusasetuksen 65 artiklan täytäntöönpanemiseksi asetuksen kyseisen osaston ja eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien säännösten rikkomisen perusteella määrättävästä hallinnollisesta seuraamusmaksusta.

Pykälän *1 kohdassa* säädettäisiin seuraamusmaksulla sanktioitavien tekojen piiriin tilanne, jossa tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien taikka tietoturvapalvelujen valmistaja tai tarjoaja antaa kyberturvallisuusasetuksen 53 artiklan 2 kohdassa tarkoitetun EU-vaatimustenmukaisuusilmoituksen, vaikka kyseiset hyödykkeet eivät ole kyseisen eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimusten mukaisia. EU-vaatimustenmukaisuusilmoituksen antamisen on tarkoitus osoittaa, että järjestelmässä määritellyt vaatimukset täyttyvät. Jos valmistaja tai tarjoaja on antanut EU-vaatimustenmukaisuusilmoituksen väärin perustein, voitaisiin tästä määrätä seuraamusmaksu. EU-vaatimustenmukaisuusilmoituksiin kohdistuvan luottamuksen varmistamiseksi on tärkeää, että niiden väärinkäyttö on sanktioitu siten, että toimijoilla on asianmukaiset kannustimet huolehtia kyberturvallisuusasetuksen asettamien vaatimusten täyttymisestä.

Pykälän *2 kohdassa* sanktioitaisiin laiminlyönti asettaa kyberturvallisuussertifioinnin viranomaisen saataville kyberturvallisuusasetuksen 53 artiklan 3 kohdassa tarkoitetut tiedot samoin kuin laiminlyönti toimittaa siinä tarkoitettu EU-vaatimustenmukaisuusilmoituksen jäljennös tuolle viranomaiselle ja Euroopan unionin kyberturvallisuusvirasto ENISA:lle.

Kyseisen kyberturvallisuusasetuksen kohdan mukaan tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien taikka tietoturvapalvelujen valmistaja tai tarjoajan tulee asettaa EU-vaatimustenmukaisuusilmoituksen, tekniset asiakirjat ja kaikki muut järjestelmässä määriteltyä tieto- ja viestintätekniikan tuotteiden ja palvelujen taikka tietoturvapalvelujen vaatimustenmukaisuutta koskevat asiaankuuluvat tiedot kansallisen kyberturvallisuussertifioinnin viranomaisen saataville asiaankuuluvassa eurooppalaisessa

kyberturvallisuuden sertifiointijärjestelmässä määrätyn ajanjakson ajaksi. Lisäksi jäljennös EU-vaatimustenmukaisuusilmoituksesta tulee toimittaa kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle ja Euroopan unionin kyberturvallisuusvirasto ENISA:lle. Ensin mainittujen osalta sanktio voitaisiin määrätä, jos asianomaisia tietoja ei anneta kyberturvallisuussertifioinnin viranomaisen pyynnöstä, elleivät ne ole muuten saatavilla. Jälkimmäisen osalta seuraamusmaksu voitaisiin määrätä, jos valmistaja tai tarjoaja laiminlyö jäljennöksen oma-aloitteisen toimittamisen.

Pykälän *3 kohdassa* säädettäisiin seuraamusmaksun piiriin tilanteet, joissa sertifikaatin haltija rikkoo eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä asetettuja ehtoja kyberturvallisuussertifikaatille. Tällaisia ehtoja voidaan kyberturvallisuusasetuksen 54 artiklan 1 kohdan k alakohdan mukaan asettaa sertifikaatin antamiselle, voimassa pitämiselle, jatkamiselle ja uusimiselle sekä sertifioinnin soveltamisalan laajentamiselle tai supistamiselle. Ehtojen noudattamista voidaan pitää sertifikaattien luotettavuuden kannalta keskeisenä.

Pykälän *4 kohdassa* säädettäisiin seuraamusmaksun piiriin tilanteet, joissa tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien taikka tietoturvapalvelujen valmistaja tai tarjoaja laiminlyö saattaa kyberturvallisuusasetuksen 55 artiklan 1 kohdassa tarkoitetut tiedot julkisesti saataville artiklan 2 kohdassa säädetyllä tavalla. Kohta koskee tilanteita, joissa kyseiset tuotteet, palvelut tai prosessit on sertifioitu tai joista on annettu EU-vaatimustenmukaisuusilmoitus. Toimijan tulee tällöin julkaista kohdassa luetellut tiedot, jotka eri tavoin tukevat tarkoituksena tuotteen, prosessin tai palvelun kyberturvallisuuden ylläpitämistä. Artiklan 2 kohdan mukaan tiedot on annettava sähköisessä muodossa, ja ne on pidettävä saatavilla ja tarpeen mukaan ajan tasalla vähintään vastaavan eurooppalaisen kyberturvallisuussertifikaatin tai EU-vaatimustenmukaisuusilmoituksen voimassaolon päättymiseen asti.

Ehdotuksessa ei rajattaisi tarkemmin sitä, minkä tietojen antamatta jättäminen voisi johtaa seuraamusmaksun määräämiseen. Rikkomuksen luonne otettaisiin kuitenkin huomioon ehdotetun 40 §:n puitteissa, jonka nojalla seuraamusmaksu jätetään määräämättä esimerkiksi sen ollessa vähäinen.

Pykälän *5 kohdassa* sanktioitaisiin väärien, harhaanjohtavien tai puutteellisten tietojen antaminen kyberturvallisuussertifioinnin viranomaiselle tai vaatimustenmukaisuuden arviointilaitokselle. Sanktiointi liittyy etenkin tilanteeseen, kun toimija jättää tieto- ja viestintätekniikan tuotteita, palveluja tai prosesseja taikka tietoturvapalveluita sertifioitavaksi. Kyberturvallisuusasetuksen 56 artiklan 7 kohdassa säädetään velvollisuudesta asettaa sertifiointia hakiessa viranomaisen tai arviointilaitoksen saataville kaikki sertifiointimenettelyn suorittamiseen tarvittavat tiedot. Ehdotetussa kohdassa edellytettäisiin, että tieto koskee ehdotetussa laissa tai kyberturvallisuusasetuksessa tarkoitetun tehtävän hoitamisen kannalta merkityksellisiä seikkoja, joten epäolennainen virhe ei johtaisi seuraamusmaksun määräämiseen. Sanktioinnilla on tarkoitus huolehtia siitä, ettei sertifikaatin myöntäminen tapahdu virheellisten tietojen perusteella. Vaatimusten täyttymättä jäämisellä voi olla vakavia vahingollisia vaikutuksia tuotteen, palvelun tai prosessin käyttäjiin.

Tahallinen virheellisen tiedon antaminen voisi mahdollisesti tulla arvioitavaksi myös rikoslain 16 luvun 8 §:ssä rangaistavaksi säädettynä väärän todistuksen antamisena viranomaiselle. Tällöin olisi tarvittaessa otettava huomioon, mitä 40 §:n 3 momentissa säädettäisiin kaksoisrangaistavuuden kiellosta.

Pykälän *6 kohdassa* säädettäisiin seuraamusmaksusta tilanteissa, joissa eurooppalaisen kyberturvallisuussertifikaatin haltija jättää tekemättä kyberturvallisuusasetuksen 56 artiklan 8

kohdassa tarkoitetun ilmoituksen sertifioidun tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin taikka tietoturvapalvelun turvallisuutta koskevasta haavoittuvuudesta tai epäsäännönmukaisuudesta, jotka saattavat vaikuttaa sertifiointiin liittyvien vaatimusten mukaisuuteen. Ilmoitus tehdään kyberturvallisuussertifioinnin viranomaiselle tai vaatimustenmukaisuuden arviointilaitokselle sen mukaan, mikä taho on myöntänyt sertifikaatin.

Pykälän *7 kohdassa* sanktioitaisiin tilanne, jossa taho käyttää eurooppalaista kyberturvallisuussertifikaattia, joka on peruutettu tai jonka voimassaolo on päättynyt. Tällaisella sertifikaatin käytöllä tarkoitettaisiin tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin taikka tietoturvapalvelun markkinoimista sertifioituna tai muuta senkaltaista menettelyä, jossa sertifikaatin entinen haltija viittaa sertifikaattiin hyödykkeen turvallisuuden takeena, vaikka kyseinen sertifikaatti olisi peruutettu tai sen voimassaolo olisi päättynyt.

Kyberturvallisuussertifioinnin viranomainen voisi tietyissä tilanteissa peruuttaa sertifikaatin ehdotetun lain 28 §:n mukaisesti. Tällaisesta peruuttamismahdollisuudesta säädetään kyberturvallisuusasetuksen 58 artiklan 8 kohdan e alakohdassa. Muutoin kyberturvallisuussertifikaatin peruuttaa se vaatimustenmukaisuuden arviointilaitos, joka on myöntänyt kyseisen eurooppalaisen kyberturvallisuussertifikaatin. Peruuttamisen jälkeen sertifikaatti ei ole enää voimassa. Sertifikaateilla on lisäksi tietty, sertifiointijärjestelmän puitteissa määritetty voimassaoloaika, jonka päätyttyä sertifikaatti ei ole enää voimassa. Erityisesti turvallisuuskriittisissä yhteyksissä on tärkeää, ettei tuotteiden, palvelujen ja prosessien sertifiointistatuksesta anneta virheellistä tietoa.

38 §. *Seuraamusmaksun määrä.* Pykälässä säädettäisiin 31–37 §:n nojalla määrättävän hallinnollisen seuraamusmaksun määrästä. Jotta seuraamuksella olisi riittävä ennalta estävä vaikutus, tulisi maksun suuruuden olla riittävä. Seuraamusta määräävän viranomaisen tulisi varmistaa, että sanktio ja sen määrä ovat suhteessa tekoon nähden ottaen huomioon kyberkestävyysasetuksen ja kyberturvallisuussertifioinnin ratio. Pykälällä pantaisiin täytäntöön kyberkestävyysasetuksen 64 artikla ja osaltaan kyberturvallisuusasetuksen 65 artikla.

Pykälän *1 momentissa* säädettäisiin valmistajalle 31 §:n 1 momentin eli pääasiassa kyberkestävyysasetuksen 13 tai 14 artiklan rikkomisesta määrättävän hallinnollisen seuraamusmaksun enimmäismäärästä. Enimmäismäärä olisi 15 000 000 euroa tai, milloin valmistaja on yritys, kaksi ja puoli prosenttia yrityksen edeltävän tilikauden maailmanlaajuisesta liikevaihdosta sen mukaan, kumpi näistä määristä on suurempi. Hallinnollisen seuraamusmaksun enimmäismäärä vastaisi kyberkestävyysasetuksen 64 artiklan 2 kohdassa edellytettyä tasoa.

Pykälän *2 momentissa* säädettäisiin kyberkestävyysasetuksen rikkomisesta 31 §:n 2 momentin, 32–35 §:n tai 36 §:n 1–3 kohdan nojalla määrättävän seuraamusmaksun enimmäismäärästä. Enimmäismäärä olisi 10 000 000 euroa tai, milloin valmistaja on yritys, kaksi prosenttia yrityksen edeltävän tilikauden maailmanlaajuisesta liikevaihdosta sen mukaan, kumpi näistä määristä on suurempi. Enimmäismäärä soveltuisi käytännössä kyberkestävyysasetuksen rikkomisiin muiden talouden toimijoiden kuin valmistajan toimesta sekä ilmoitettuihin laitoksiin. Hallinnollisen seuraamusmaksun enimmäismäärä vastaisi kyberkestävyysasetuksen 64 artiklan 3 kohdassa edellytettyä tasoa.

Pykälän *3 momentissa* säädettäisiin kyberkestävyysasetuksen rikkomisesta 36 §:n 4 kohdan nojalla määrättävän seuraamusmaksun enimmäismäärästä. Enimmäismäärä on 5 000 000 euroa tai, milloin valmistaja on yritys, yksi prosentti yrityksen edeltävän tilikauden maailmanlaajuisesta liikevaihdosta sen mukaan, kumpi näistä määristä on suurempi. Enimmäismäärän alaan kuuluisi ilmoitetulle laitokselle tai markkinavalvontaviranomaiselle

tahallisesti väärän, puutteellisen tai harhaanjohtavan tiedon antaminen tavalla, joka on merkityksellinen ilmoitetun laitoksen tai markkinavalvontaviranomaisen tehtävän hoitamiseksi. Hallinnollisen seuraamusmaksun enimmäismäärä vastaisi kyberkestävyysasetuksen 64 artiklan 4 kohdassa edellytettyä tasoa.

Pykälän *4 momentissa* säädettäisiin kyberturvallisuussertifiointia koskevan seuraamusmaksun enimmäismäärästä, joka olisi 100 000 euroa. Kyberturvallisuusasetuksen rikkomisen perusteella määrättävän hallinnollisen seuraamusmaksun määrä vastaisi tasoa, jossa seuraamuksella olisi riittävä, tehokas ja oikeasuhtainen ennalta estävä vaikutus. Seuraamusmaksun tasoa arvioidaan ja perustellaan jaksossa 5.1.3. Hallinnollisen seuraamusmaksun enimmäismäärä täyttäisi kyberturvallisuusasetuksen 65 artiklan edellytykset.

Pykälän *5 momentissa* säädettäisiin seuraamusmaksun kokonaisarvioinnista. Seuraamusmaksun suuruuden määrittäminen tulisi perustua kokonaisarviointiin rikkomuksen vakavuudesta ja menettelyn moitittavuudesta. Seuraamusmaksun määrää arvioitaessa olisi otettava huomioon menettelyn luonne, vakavuus ja kesto sekä sen toistuvuus, rikkomuksen aiheuttama vahinko ja toimijan koko sekä sen mahdolliset aiemmat ehdotetun lain alaan kuuluvat rikkomukset. Toimijan koko olisi otettava huomioon, koska lain soveltamisalaan kuuluvat velvoitteet voisivat kohdistua hyvin eri kokoisiin organisaatioihin.

Myös kyberkestävyysasetuksen 64 artiklan 5 kohdassa säädetään hallinnollisen seuraamusmaksun määräämisessä huomioon otettavista seikoista. Näitä seikkoja olisi sovellettava hallinnollisen seuraamusmaksun määräämiseen 31–36 §:n nojalla. Kyberkestävyysasetuksen 64 artiklan 5 kohdan mukaan, kun päätetään hallinnollisen sakon määrästä, kussakin yksittäisessä tapauksessa on otettava asianmukaisesti huomioon kaikki kyseisen tilanteen kannalta merkittävät olosuhteet sekä seuraavat seikat:

a) rikkomisen ja sen seurausten luonne, vakavuus ja kesto;

b) ovatko samat tai muut markkinavalvontaviranomaiset jo määränneet hallinnollisia sakkoja samalle talouden toimijalle samankaltaisesta rikkomisesta;

c) rikkomiseen syyllistyneen talouden toimijan koko erityisesti mikroyritysten sekä pienten ja keskisuurten yritysten, myös startup-yritysten, osalta ja markkinaosuus.

39 §. *Seuraamusmaksun määrääminen.* Pykälässä säädettäisiin luvussa tarkoitetun hallinnollisen seuraamusmaksun määräämisestä.

Pykälän *1 momentin* nojalla hallinnollisen seuraamusmaksun 31–34 §:n ja 36 §:n nojalla määräisi markkinavalvontaviranomainen. Markkinavalvontaviranomaisena toimisi 15 §:n nojalla Liikenne- ja viestintävirasto sekä 16 §:n nojalla suuririskiselle tekoälyjärjestelmälle, joka kuuluu kyberkestävyysasetuksen soveltamisalaan, eräiden tekoälyjärjestelmien valvonnasta annetun lain nojalla toimivaltainen valvova viranomainen. Milloin toimivaltainen markkinavalvontaviranomainen olisi eräiden tekoälyjärjestelmien valvonnasta annetun lain 3 §:ssä tarkoitettu markkinavalvontaviranomainen, hallinnollinen seuraamusmaksu määrätään mainitun lain 13 §:ssä säädetyssä järjestyksessä. Tällöin eräiden tekoälyjärjestelmien valvonnasta annetun lain nojalla toimivaltainen taho määräisi siis ehdotetun lain mukaisen seuraamusmaksun. Teoissa olisi kysymys kyberkestävyysasetusta koskevista talouden toimijan rikkomuksista.

Milloin Liikenne- ja viestintäviraston toimivaltaan kuuluvan hallinnollisen seuraamusmaksun määrä olisi yli 100 000 euroa, seuraamusmaksu olisi määrättävä Liikenne- ja viestintävirastosta annetun lain 7 a §:n mukaisessa menettelyssä eli seuraamuskollegiossa.

Pykälän *2 momentin* nojalla hallinnollisen seuraamusmaksun 35 §:ssä tarkoitetusta teosta määrää ilmoittava viranomainen eli Liikenne- ja viestintävirasto. Teoissa olisi kysymys kyberkestävyysasetusta koskevista ilmoitetun laitoksen rikkomuksista.

Milloin Liikenne- ja viestintäviraston toimivaltaan kuuluvan hallinnollisen seuraamusmaksun määrä olisi yli 100 000 euroa, seuraamusmaksu olisi määrättävä Liikenne- ja viestintävirastosta annetun lain 7 a §:n mukaisessa menettelyssä eli seuraamuskollegiossa.

Pykälän *3 momentin* nojalla hallinnollisen seuraamusmaksun 37 §:ssä tarkoitetusta teosta määrää kyberturvallisuussertifioinnin viranomainen eli Liikenne- ja viestintävirasto. Teoissa olisi kysymys kyberturvallisuussertifiointia koskevista rikkomuksista.

Pykälän *4 momentissa* säädettäisiin seuraamusmaksun määräävän viranomaisen oikeudesta saada maksutta ja salassapitosäännösten estämättä talouden toimijalta tai muulta viranomaiselta tiedot, jotka ovat välttämättömiä seuraamusmaksun määräämiseksi tai sen määrän arvioimiseksi. Tietojensaantioikeus olisi välttämätön hallinnollista seuraamusmaksun määräämistä koskevan asian käsittelemiseksi ja ratkaisemiseksi. Tiedonsaantioikeus rajautuisi tietoihin, jotka ovat käsiteltävänä olevassa asiassa välttämättömiä seuraamusmaksun määräämiseksi eli sen perusteen tai määrän arvioimiseksi.

40 §. *Seuraamusmaksun määräämättä jättäminen.* Pykälässä säädettäisiin seuraamusmaksun määräämättä jättämisestä.

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 (PeVL 49/2017 vp ja PeVL 39/2017 vp).

Säännöksen tarkoituksena olisi varmistaa, että seuraamusmaksua ei määrättäisi 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. Lisäksi kyberturvallisuussertifiointia koskevaa seuraamusmaksua ei saisi määrätä sille, jolle on määrätty samasta teosta ankarampi seuraamusmaksu kyberkestävyysasetuksen rikkomisen perusteella. Säännökset vastaisivat niin sanottua ne bis in idem -periaatetta eli kaksoisrangaistavuuden kieltoa.

Pykälän *4 momentissa* säädettäisiin kielto määrätä seuraamusmaksu valtion viranomaisille, valtion liikelaitoksille, hyvinvointialueille tai -yhtymille, kunnallisille viranomaisille, itsenäisille julkisoikeudellisille laitoksille, eduskunnan virastoille, tasavallan presidentin kanslialle, Suomen evankelisluterilaiselle kirkolle tai Suomen ortodoksiselle kirkolle tai niiden seurakunnille, seurakuntayhtymille tai muille elimille.

Pykälän *5 momentissa* säädettäisiin kielto määrätä seuraamusmaksu mikro- tai pienyritykselle sillä perusteella, että yritys on ylittänyt 24 tunnin määräajan kyberkestävyysasetuksen 14(1) tai 14(3) artiklan mukaisesta tapahtumasta ilmoittamiselle. Kyberkestävyysasetuksen 14 artiklan velvollisuus ilmoittaa aktiivisesti hyödynnetystä haavoittuvuudesta tai tuotteen tietoturvaan vaikuttavasta vakavasta poikkeamasta soveltuisi kohdasta huolimatta myös mikro- ja pienyrityksiin siten kuin kyberkestävyysasetuksen 14 artiklassa säädetään, ja seuraamusmaksu voitaisiin määrätä 14(2) artiklan tai 14(4) artiklan b ja c alakohdissa tarkoitettujen määräaikojen laiminlyönnin perusteella. Kohta vastaisi kyberkestävyysasetuksen 64 artiklan 10 kohdan a-luetelmakohtaa.

Pykälän *6 momentissa* säädettäisiin kielto määrätä seuraamusmaksu avoimen lähdekoodin ohjelmistovastaavalle. Avoimen lähdekoodin ohjelmistovastaavan määritelmästä säädettäisiin lain 2 §:n 8 kohdassa vastaten kyberkestävyysasetuksen 3 artiklan 14 kohdan määritelmää. Kohta vastaisi kyberkestävyysasetuksen 64 artiklan 10 kohdan b-luetelmakohtaa.

41 §. *Seuraamusmaksun täytäntöönpano.* Pykälässä säädettäisiin seuraamusmaksun täytäntöönpanosta. Lain nojalla maksettavaksi määrätty seuraamusmaksu pannaan täytäntöön siinä järjestyksessä kuin sakon täytäntöönpanosta annetussa laissa (672/2002) säädetään. Seuraamusmaksun täytäntöönpanosta huolehtisi Oikeusrekisterikeskus. Seuraamusmaksu raukeaisi mainitun lain 4 b §:n (laissa 416/2025) nojalla viiden vuoden kuluttua lainvoiman saaneen ratkaisun antamispäivästä. Seuraamusmaksusta ei perittäisi viivästyskorkoa.

7 luku – Erinäiset säännökset

42 §. *Oikaisuvaatimus.* Pykälässä säädettäisiin päätöksistä, joihin saa vaatia hallintolaissa tarkoitettua oikaisua. Oikaisua saisi vaatia ilmoitetun laitoksen antamaan päätökseen, kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen antamaan päätökseen sekä päätökseen, joka koskee viranomaisen suoritteesta perittävää maksua.

Oikaisuvaatimuksen kohteena voisi olla ilmoitetun laitoksen tai kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen antama hallintopäätös, jonka antaminen perustuu tähän lakiin, kyberkestävyysasetukseen tai kyberturvallisuusasetukseen. Oikaisuvaatimuksen kohteena voisi olla siten esimerkiksi vaatimustenmukaisuustodistuksen myöntämistä tai myöntämättä jättämistä koskeva ilmoitetun laitoksen päätös. Oikaisuvaatimuksen kohteena voisi olla myös viranomaisen päätös, joka koskee viranomaisen suoritteesta perittävää maksua.

Oikaisuvaatimuksen käsittelyyn sovellettaisiin hallintolakia. Oikaisuvaatimukseen annetusta päätöksestä saisi valittaa hallinto-oikeuteen oikeudenkäynnistä hallintoasioissa annetussa laissa säädetyssä järjestyksessä. Jäljempänä 43 §:n 5 momenttiin sisältyisi erityissäännös oikaisuvaatimuksesta annetun päätöksen täytäntöönpanokelpoisuudesta.

Säännös vastaisi kyberkestävyysasetuksen 48 artiklan edellytykseen ilmoitetun laitoksen päätöksiin käytettävissä olevasta muutoksenhakumenettelystä.

43 §. *Muutoksenhaku.* Pykälän *1 momentissa* olisi informatiivinen viittaus siihen, että muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa. Muutoksenhaun kohteena voisi olla esimerkiksi ilmoittavan viranomaisen, markkinavalvontaviranomaisen ja kyberturvallisuussertifioinnin viranomaisen päätös. Muutoksenhaun kohteena voisi olla myös tällaisen viranomaisen hallinnollista seuraamusmaksua koskeva päätös taikka oikaisuvaatimuksen johdosta annettu, viranomaisen suoritteen maksullisuutta koskeva päätös.

Pykälän *2–5 momentissa* säädettäisiin lain nojalla annetun hallintopäätöksen täytäntöönpanokelpoisuudesta lainvoimaa vailla olevana.

Pykälän 2 momentissa säädettäisiin, että markkinavalvontaviranomaisen muu kuin seuraamusmaksun määräämistä koskeva päätös voidaan panna täytäntöön muutoksenhausta huolimatta. Päätöksen täytäntöönpanokelpoisuutta koskeva pääsääntö vastaisi markkinavalvontalain 29 §:ää. Hallinnollisten sanktioiden sääntelyperiaatteiden mukaisesti hallinnollista seuraamusmaksua koskeva päätös olisi kuitenkin täytäntöönpanokelpoinen vasta lainvoimaisen päätöksen perusteella.

Pykälän *3–5 momentissa* säädettäisiin tyhjentävästi päätöksistä, joissa voidaan määrätä, että päätöstä on noudatettava muutoksenhausta huolimatta.

Pykälän 3 momentissa säädettäisiin ilmoittavan viranomaisen päätöksen täytäntöönpanokelpoisuudesta. Ilmoittava viranomainen voisi määrätä ilmoitetun laitoksen nimeämistä taikka nimeämisen rajaamista tai peruuttamista koskevassa päätöksessään, että päätöstä on noudatettava muutoksenhausta huolimatta. Ehdotuksella varmistettaisiin, että jos ilmoitettu laitos ei enää täyttäisi nimeämisen edellytyksiä, voisi ilmoittava viranomainen ryhtyä kyberkestävyysasetuksen edellyttämällä tavalla tehokkaisiin toimenpiteisiin muutoksenhausta huolimatta.

Pykälän 4 momentissa taas säädettäisiin kyberturvallisuussertifioinnin viranomaisen mahdollisuudesta määrätä, että sen päätöstä on noudatettava muutoksenhausta huolimatta.

Pykälän 5 momentissa säädettäisiin ilmoitetun laitoksen tai kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen päätöksen täytäntöönpanokelpoisuudesta silloin, kun päätös koskee digitaalisen elementin sisältävän tuotteen valmistajalta tai eurooppalaisen kyberturvallisuussertifikaatin haltijalta vaadittavia korjaavia toimenpiteitä taikka digitaalisen elementin sisältävälle tuotteelle annetun vaatimustenmukaisuustodistuksen tai eurooppalaisen kyberturvallisuussertifikaatin peruuttamista. Muutoksenhaun kohteena voisi olla oikaisuvaatimuksesta annettu päätös. Ehdotuksen tarkoituksena on varmistaa näiden korjaavien toimenpiteiden tehokkuus, kun vakavia puutteita on todettu.

Oikeudenkäynnistä hallintoasioissa annetun lain 123 §:n mukaan hallintotuomioistuin voi valituksen ollessa vireillä kieltää päätöksen täytäntöönpanon, määrätä täytäntöönpanon

keskeytettäväksi tai antaa päätöksen täytäntöönpanoa koskevan muun määräyksen. Tämän johdosta pykälässä ei säädettäisi erikseen muutoksenhakuviranomaisen mahdollisuudesta kieltää sellaisen päätöksen täytäntöönpano, jonka päätöksen tehnyt viranomainen on määrännyt täytäntöönpantavaksi muutoksenhausta huolimatta. Mainittua säännöstä sovellettaisiin pykälän 2–5 momentin ohella.

Pykälän *6 momentissa* säädettäisiin informatiivisesta viittauksesta uhkasakkolakiin. Muutoksenhaussa uhkasakon asettamista ja maksettavaksi tuomitsemista sekä teettämis- tai keskeyttämisuhan asettamista ja täytäntöönpantavaksi määräämistä koskevaan päätökseen sovellettaisiin myös muutoksenhaun osalta, mitä uhkasakkolaissa (1113/1990) säädetään.

44 §. *Maksut.* Pykälän mukaan viranomaisten suoritteiden maksullisuudesta ja suoritteista perittävien maksujen suuruuden yleisistä perusteista sekä maksujen muista perusteista säädetään valtion maksuperustelaissa (150/1992). Pykälä olisi luonteeltaan informatiivinen. Maksuperustelain nojalla maksuja voitaisiin periä ilmoittavan viranomaisen ja kyberturvallisuussertifioinnin viranomaisen suoritteista, millä tarkoitettaisiin erityisesti vaatimustenmukaisuuden arviointilaitosten ilmoittamista ja valvontaa sekä kyberturvallisuussertifikaattien myöntämistä. Lisäksi maksuja voitaisiin periä testiympäristön käytöstä maksuperustelain mukaisin perustein. Maksuperustelain 8 §:n perusteella toimivalta päättää muun muassa suoritteen maksullisuudesta olisi liikenne- ja viestintäministeriöllä Liikenne- ja viestintäviraston suoritteiden osalta.

45 §. *Voimaantulo.* Pykälän *1 momentissa* säädettäisiin lain voimaantulosta. Pykälän *2–4 momenttiin* sisältyisi kyberkestävyysasetuksen soveltamisen alkamisajankohtia vastaavat porrastukset soveltamisen alkamiselle.

Pykälän 2 momentin nojalla 3 luvun säännöksiä ilmoitetuista laitoksista, ilmoittavan viranomaisen tehtävistä ja 35 §:ää ilmoitettuja laitoksia koskevasta seuraamusmaksusta sovellettaisiin 11.6.2026. Soveltamisen alkaminen vastaisin kyberkestävyysasetuksen 71 artiklan 2 kohdan toista alakohtaa.

Pykälän 3 momentin nojalla kyberkestävyysasetuksen 14 artiklassa tarkoitettua ilmoittamista ja valmistajan seuraamusmaksua ilmoittamista koskevalta osin sovellettaisiin 11.9.2026. Soveltamisen alkaminen vastaisi kyberkestävyysasetuksen 71 artiklan 2 kohdan toista alakohtaa.

Pykälän 4 momentin nojalla kyberkestävyysasetuksen mukaisiin talouden toimijoiden velvollisuuksiin ja niiden rikkomiseen liittyviä säännöksiä sekä hallinnollisia seuraamusmaksuja sovellettaisiin 11.12.2027. Soveltamisen alkaminen vastaisi kyberkestävyysasetuksen 71 artiklan 2 kohdan ensimmäistä alakohtaa.

7.2 Laki eräiden tuotteiden markkinavalvonnasta

1 §. *Soveltamisala*. Pykälän *1 momenttia* ehdotetaan muutettavaksi siten, että 1. lakiehdotus lisättäisiin uutena kohtana momentin listaan laeista, joiden soveltamisalaan kuuluvien tuotteiden markkinavalvontaan lakia sovelletaan. Lisäyksen johdosta edeltävään kohtaan tehtäisiin tekninen muutos.

Eräiden tuotteiden markkinavalvonnasta annettua lakia sovellettaisiin myös kyberkestävyysasetuksen soveltamisalaan kuuluvien tuotteiden markkinavalvontaan siltä osin kuin eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista ehdotetussa laissa ei toisin säädetä. Eräiden tuotteiden kyberkestävyydestä sekä

kyberturvallisuussertifioinnista annettu laki olisi siten erityissäädös suhteessa markkinavalvontalakiin. Lain soveltamisalaan kuuluvalla tuotteella tarkoitettaisiin kyberkestävyysasetuksen soveltamisalaan kuuluvia tuotteita. Lain soveltamisalaan kuuluvalla tuotteella ei siten tarkoitettaisi tuotetta, jolle on myönnetty kyberturvallisuussertifiointi, jos tuote ei kuulu kyberkestävyysasetuksen soveltamisalaan.

4 §. *Valvontaviranomaiset*. Pykälän *4 momenttia* ehdotetaan muutettavaksi siten, että momenttiin lisättäisiin eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista ehdotetun lain soveltamisalaan kuuluvat tuotteet momentin listaan tuotteista, joiden markkinavalvontaviranomaisena toimii Liikenne- ja viestintävirasto. Momenttia ei tarkoiteta muutettavaksi muilta osin.

Kyberkestävyysasetuksen soveltamisalaan kuuluvien tuotteiden markkinavalvontaviranomaisena toimisi siten Liikenne- ja viestintävirasto viitatun lain 15 §:n mukaisesti. Poikkeuksellisesti markkinavalvontaviranomaisena voisi toimia eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista annetun lain 16 §:n nojalla myös eräiden tekoälyjärjestelmien valvonnasta annetun lain 3 §:n nojalla toimivaltainen valvova viranomainen silloin, kun markkinavalvonta kohdistuu tekoälyasetuksen 6 artiklan mukaiseen suuririskiseen tekoälyjärjestelmään, joka kuuluu myös kyberkestävyysasetuksen soveltamisalaan. Mainittu poikkeus perustuu kyberkestävyysasetuksen 52 artiklan 14 kohtaan.

7.3 Kyberturvallisuuslaki

20 §. *CSIRT-yksikön tehtävät.* Pykälän *1 momentin* listaukseen CSIRT-yksikön tehtävistä lisättäisiin uusi 10 kohta, joka koskisi kyberkestävyysasetuksessa sekä 1. lakiehdotuksessa CSIRT-yksikölle osoitettuja tehtäviä. CSIRT-yksikön keskeinen tehtävä olisi vastaanottaa ja käsitellä kyberkestävyysasetuksen 14 artiklassa tarkoitettuja ilmoituksia aktiivisesti hyödynnetystä haavoittuvuudesta ja digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavista vakavista poikkeamista. Valmistajat ovat ilmoituksien tekemiseen velvollisia siten kuin kyberkestävyysasetuksessa säädetään. CSIRT-yksikön tehtävänä olisi lisäksi käsitellä kyberkestävyysasetuksen 15 artiklassa tarkoitettuja vapaaehtoisia ilmoituksia.

Muita CSIRT-yksikölle osoitettuja tehtäviä on muun muassa markkinavalvontaviranomaisten avustaminen tarvittaessa. Kyberkestävyysasetuksen 52 artiklan 5 kohdassa säädetään, että markkinavalvontaviranomaiset voivat pyytää koordinaattoriksi nimettyä CSIRT-yksikköä tai ENISA:a antamaan teknistä neuvontaa asioissa, jotka liittyvät tämän asetuksen täytäntöönpanoon ja sen noudattamisen valvontaan. Markkinavalvontaviranomaiset voivat 54 artiklan mukaista tutkimusta suorittaessaan pyytää koordinaattoriksi nimettyä CSIRT-yksikköä tai ENISA:a esittämään analyysin digitaalisia elementtejä sisältävien tuotteiden vaatimustenmukaisuuden arviointien tueksi. Vastaavasti 54 artiklan 1 kohdassa säädetään, että jos jäsenvaltion markkinavalvontaviranomaisella on riittävä peruste katsoa, että digitaalisia elementtejä sisältävä tuote, mukaan lukien sen haavoittuvuuksien käsittely, aiheuttaa merkittävän kyberturvallisuusriskin, sen on arvioitava ilman aiheetonta viivytystä ja tarvittaessa yhteistyössä asiaankuuluvan CSIRT-yksikön kanssa, täyttääkö kyseinen digitaalisia elementtejä sisältävä tuote kaikki asetuksessa säädetyt vaatimukset. CSIRT-yksikön olisi toimittava tarvittaessa kyberkestävyysasetuksen mukaisissa tehtävissä yhteistyössä muiden viranomaisten kanssa.

28 §. *Tiedonsaantioikeus*. Pykälää ehdotetaan muutettavaksi siten, että sen *4 momentissa* säädettyä valvovan viranomaisen tiedonluovutusoikeutta voitaisiin soveltaa myös tietojen luovuttamiseen Finanssivalvonnalle sen Finanssivalvonnasta annetun lain 50 p §:n 1 ja 2 momentissa tarkoitettua toimivaltaisen viranomaisen tehtävää varten. Näiden säännösten

mukaan Finanssivalvonta toimii EU:n DORA-asetuksen 46 artiklassa tarkoitettuna toimivaltaisena viranomaisena ja NIS 2 -direktiivin 8 artiklan 1 kohdassa tarkoitettuna toimivaltaisena viranomaisena mainitun direktiivin liitteen I toimialojen 3 ja 4 osalta. Tämä tarkoittaisi, että kyberturvallisuuslaissa tarkoitettu valvova viranomainen voisi luovuttaa salassapitosäännösten, 28 §:n 2 momentissa säädetyn salassapitovelvollisuuden ja muiden tietojen luovuttamista koskevien rajoitusten estämättä kyberturvallisuuslaissa säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirjan sekä ilmaista salassa pidettävän tiedon myös Finanssivalvonnalle, jos se on välttämätöntä Finanssivalvonnasta annetun lain 50 p §:n 1 ja 2 momentissa tarkoitettua toimivaltaisen viranomaisen tehtävää varten. Tiedonsaantioikeuden käyttämisellä tai tietojen luovuttamisella ei saisi rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.

Kyberturvallisuuslaissa ei säädetä Finanssivalvonnan tehtävistä tai tiedonvaihdosta sen ja kyberturvallisuuslain 26 §:ssä määriteltyjen valvovien viranomaisten välillä, sillä DORA-asetus on NIS 2 -direktiivin 4 artiklassa tarkoitettu alakohtainen unionin säädös, eikä jäsenvaltioiden pitäisi soveltaa sen alalla NIS 2 -direktiivin säännöksiä, jotka koskevat kyberturvallisuusriskien hallintaa ja raportointivelvoitteita sekä valvontaa ja täytäntöönpanoa (HE 57/2024 vp, s. 33).

Finanssivalvonnasta annetun lain 50 p §:ssä säädetään kyberturvallisuuslain 26 §:ään verrattavalla tavalla siitä, että Finanssivalvonta toimii NIS 2 -direktiivin 8 artiklan 1 kohdassa tarkoitettuna toimivaltaisena viranomaisena mainitun direktiivin liitteen I toimialojen 3 ja 4 osalta. Mainitun lain 71 §:n 1 momentissa säädetään Finanssivalvonnan oikeudesta luovuttaa salassapitosäännösten estämättä tietoja tieto- ja viestintätekniikkaan liittyvistä häiriöistä ja uhkista Liikenne- ja viestintävirastolle 3 f §:n 3 momentissa tarkoitetun yhteistyön toteuttamista varten. Viimeksi mainitun säännöksen mukaan Finanssivalvonnan on tehtävä yhteistyötä NIS 2 -direktiivin mukaisten tehtävien hoitamisessa Liikenne- ja viestintäviraston kanssa.

Kyberturvallisuuslain 28 §:ssä ei kuitenkaan säädetä tällä hetkellä valvovien viranomaisten oikeudesta luovuttaa tietoja Finanssivalvonnalle. Sähköisen viestinnän palveluista annetun lain 318 §:n 2 momentin (laissa 703/2025) nojalla Liikenne- ja viestintävirastolla on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa laissa säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto Energiavirastolle, Finanssivalvonnalle, Lupa- ja valvontavirastolle sekä elinvoimakeskukselle, jos se on näille säädettyjen tietoturvallisuuteen liittyvien tehtävien hoitamiseksi välttämätöntä. Säännöksen taustalla on nyttemmin kumotun NIS-direktiivin täytäntöönpano, ja se mahdollistaa tietojen luovuttamisen Liikenne- ja viestintävirastosta Finanssivalvonnalle myös NIS 2 -direktiivin alalla. Säännöstä ei 318 §:n 5 momentin nojalla kuitenkaan voida soveltaa tietoihin viesteistä, välitystiedoista, paikkatiedoista tai luottamuksellisen radiolähetyksen sisällöstä ja olemassaolosta, vaikka Liikenne- ja viestintävirasto voi valvovana viranomaisena saada näitäkin tietoja kyberturvallisuuslain 28 §:n 2 momentin nojalla. Näin ollen kyberturvallisuuslain 28 §:n 4 momentin sääntely tietojen luovuttamisesta on perusteltua laajentaa koskemaan myös Finanssivalvontaa, jotta kaikki NIS 2 -direktiivin tarkoittamat toimivaltaiset viranomaiset olisivat tältä osin samassa asemassa.

7.4 Laki sähköisen viestinnän palveluista

1 luku – Lain tavoitteet ja määritelmät

3 §. *Määritelmät.* Pykälän 35 kohtaa muutettaisiin niin, että verkkotunnuksen määritelmästä poistettaisiin rajaus fi-maatunnuksen ja ax-maakuntatunnuksen alaisiin verkkotunnuksiin. Verkkotunnuksella tarkoitettaisiin jatkossa siis laissa internet-verkossa käytettävää nimimuotoista osoitetietoa riippumatta siitä, minkä aluetunnuksen (eng. top-level domain,

TLD) alaisesta verkkotunnuksesta on kyse. Muutos on tarpeen uuden 21 a luvun lisäämiseksi, koska sen säännökset koskisivat muita kuin fi- tai ax-päätteisiä verkkotunnuksia. Lisäksi määritelmä vastaa paremmin termin yleiskielistä määritelmää.

Muutoksesta huolimatta 21 lukua sovellettaisiin jatkossakin vain Suomen fi-maatunnuksen ja Ahvenanmaan ax-maakuntatunnuksen alaisiin nimimuotoisiin osoitetietoihin. Lain 21 luvun soveltamisalarajaus sisältyisi muuttamattomana 163 §:ään. Muutoksella ei olisi tarkoitus laajentaa lain nykyisten verkkotunnusta koskevien säännösten soveltamista muihin kuin fi-maatunnuksen ja ax-maakuntatunnuksen alaisiin verkkotunnuksiin.

Verkkotunnuksen määritelmään tehtäisiin lisäksi tekninen, vallitsevan tulkintakäytännön mukainen täsmennys siitä, että verkkotunnuksella tarkoitettaisiin toisen asteen osoitetietoa muotoa domain.fi. Tämä vastaisi kumotussa verkkotunnuslaissa (228/2003) säädettyä. Muutoksella selvennettäisiin, että verkkotunnuksella ei tarkoiteta esimerkiksi osoitteen alasivu.domain.fi ensimmäistä pistettä edeltävää osaa, jonka toiseen asteen osoitetietoa hallitseva taho voi itse vapaasti määrittää.

Pykälään lisättäisiin uusi 35 a kohta, jossa määriteltäisiin aluetunnusrekisterin ylläpitäjä samoin kuin kyberturvallisuuslain 2 §:ssä. Määritelmä vastaisi myös NIS 2 -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 ylläpitäjällä tarkoitettaisiin siten ylimmän tason verkkotunnusrekisterin ylläpitäjää (Top-Level Domain Registry). Ylimmän tason verkkotunnukset jaetaan kahteen ryhmään, joita ovat ylimmän tason maatunnukset (ccTLD) sekä geneeriset ylimmän tason verkkotunnukset (gTLD). Määritelmän tarkoituksena ei olisi rajata sen soveltumista tiettyyn maantieteelliseen alueeseen.

21 luku – Suomen ja Ahvenanmaan verkkotunnukset

Luvun otsikkoa tarkistettaisiin, jotta siitä ilmenee säännösten soveltamisala suhteessa ehdotettuun uuteen 21 a lukuun.

164 §. *Liikenne- ja viestintäviraston verkkotunnustoiminta ja verkkotunnusten välittäminen.* Pykälän 2 momenttiin tehtäisiin tekninen muutos, koska verkkotunnusvälittäjän käsitettä käytettäisiin jatkossa uudessa 21 a luvussa myös sellaisista verkkotunnusvälittäjistä, jotka eivät ole tehneet lain 165 §:ssä tarkoitettua ilmoitusta, joka liittyy fi- ja ax-päätteisten tunnusten välittämiseen. Jatkossakin merkintöjä verkkotunnusrekisteriin voisi siten tehdä vain 165 §:ssä tarkoitetun ilmoituksen tehnyt verkkotunnusvälittäjä. Se siis vastaisi merkinnöistä myös silloin, kun niitä tekisi lain 167 §:n 1 momentista mainitulla tavalla verkkotunnusvälittäjän puolesta toimiva taho.

Pykälään lisättäisiin uusi *4 momentti*, jossa säädettäisiin NIS 2 -direktiivin täytäntöönpanon edellyttämällä tavalla eräiden 21 luvun velvoitteiden soveltamisesta myös verkkotunnusvälittäjän puolesta toimivaan verkkotunnusten rekisteröintipalveluja tarjoavaan tahoon. NIS 2 -direktiivissä säädetyt velvoitteet koskevat verkkotunnusten

rekisteröintipalveluja tarjoavia toimijoita, millä tarkoitetaan direktiivin 6 artiklan 22 kohdan mukaan paitsi verkkotunnusvälittäjää myös verkkotunnusvälittäjien puolesta toimivaa tahoa, kuten yksityisyys- tai välityspalvelujen tarjoajaa tai jälleenmyyjää. Koska verkkotunnus on lain 167 §:n mukaan merkittävä käyttäjän nimiin tämän oikeilla tiedoilla, ei kaikkien tällaisten palvelujen tarjoaminen tule kuitenkaan fi- ja ax-päätteisten tunnusten osalta kyseeseen.

Ehdotetussa momentissa säädettäisiin ensinnäkin 165 §:ssä tarkoitetun ilmoitusvelvollisuuden soveltamisesta verkkotunnusvälittäjien puolesta toimiviin tahoihin. Tällä pantaisiin täytäntöön NIS 2 -direktiivin 3 artiklan 3 ja 4 kohta sekä 27 artiklan 2–4 kohta näiden toimijoiden osalta. Toiseksi momentissa säädettäisiin lain 170 §:n mukaisten tietojen saatavuutta koskevien velvoitteiden soveltamisesta näihin toimijoihin siinä laajuudessa kuin direktiivin 28 artiklan 3–5 kohdan täytäntöönpano minimitasolla edellyttää. Pykälän 1 momentin 2 kohta panee osaltaan täytäntöön myös 28 artiklan 1 kohdan. Verkkotunnusvälittäjien puolesta toimiviin tahoihin ei kuitenkaan sovellettaisi esimerkiksi erityisiä kansallisia tietoturvavelvoitteita, jotka eivät perustu NIS 2 -direktiiviin. Kolmanneksi lain 171 §:n soveltaminen merkitsisi, että Liikenne- ja viestintävirasto voisi lain rikkomistilanteissa käyttää siinä säädettyjä toimivaltuuksiaan myös verkkotunnusvälittäjien puolesta toimiviin tahoihin. Ehdotetusta seuraisi myös, että Liikenne- ja viestintäviraston lain 165 §:n 3 momentin ja 170 §:n 2 momentin nojalla antamia määräyksiä voitaisiin soveltaa myös näihin toimijoihin.

21 a luku – Muut verkkotunnukset

172 a §. *Luvun soveltamisala.* Pykälän *1 momentin* nojalla uutta 21 a lukua sovellettaisiin muihin kuin 21 luvun soveltamisalaan kuuluviin verkkotunnuksiin ja niiden välittämiseen.

Uusi 21 a luku olisi tarkoitettu koskemaan yleisesti aluetunnusrekistereitä ja verkkotunnusten välitystoimintaa Suomessa siltä osin kuin toiminta ei kuulu 21 luvun fi- ja ax-päätteisiä verkkotunnuksia koskevien erityissäännösten alaan. Lukua ei sovellettaisi 21 luvun soveltamisalaan kuuluviin verkkotunnuksiin taikka niihin liittyvään verkkotunnustoimintaan tai verkkotunnusten välittämiseen. Uutta 21 a lukua sovellettaisiin näin ollen muihin kuin fi- tai ax-päätteisiin verkkotunnuksiin ja niiden välittämiseen riippumatta verkkotunnuksen päätteestä.

Pykälän *2 momenttiin* sisältyisi säännös luvun alueellisesta soveltamisalasta. Lukua sovellettaisiin verkkotunnusvälittäjään, jonka päätoimipaikka tai Euroopan unioniin nimetty edustaja sijaitsee Suomessa. Jos Euroopan unionin ulkopuolelle sijoittautunut verkkotunnusvälittäjä ei ole nimennyt edustajaa unionissa mutta tarjoaa palvelua Suomessa, verkkotunnusvälittäjä kuuluisi myös luvun soveltamisalaan. Säännös vastaisi NIS 2 -direktiivin 26 artiklan 2 ja 3 kohtaa direktiivin velvoitteiden alueellisesta soveltamisalasta.

Pykälän 3 momentin mukaan mitä tässä luvussa säädetään verkkotunnusvälittäjästä, sovelletaan myös verkkotunnusvälittäjien puolesta toimivaan verkkotunnusten rekisteröintipalveluja tarjoavaan tahoon. Mainita vastaa NIS 2 -direktiivin 28 artiklan edellyttämien velvoitteiden soveltamisalaa, sillä NIS 2 -direktiivin 6 artiklan 22 kohdassa verkkotunnusten rekisteröintipalveluja tarjoavaksi toimijaksi määritellään verkkotunnusvälittäjien lisäksi myös niiden puolesta toimivat tahot. Verkkotunnusvälittäjien puolesta toimivia tahoja voivat olla esimerkiksi yksityisyys- tai välityspalvelujen tarjoajat tai jälleenmyyjät.

172 b §. *Verkkotunnusvälittäjän ilmoitus*. Pykälässä säädettäisiin tiedoista, jotka verkkotunnusvälittäjän on ilmoitettava Liikenne- ja viestintävirastolle. Pykälällä täydennettäisiin NIS 2 -direktiivin 3 artiklan 3 ja 4 kohdan sekä 27 artiklan täytäntöönpanoa sellaisten verkkotunnusvälittäjien osalta, jotka välittävät muita kuin 21 luvun soveltamisalaan

kuuluvia verkkotunnuksia. Verkkotunnusvälittäjien tulisi ilmoittaa Liikenne- ja viestintävirastolle nimensä, osoitteensa, sähköpostiosoitteensa, puhelinnumeronsa ja muut ajantasaiset yhteystietonsa, IP-osoitealueensa sekä luettelo Euroopan unionin jäsenvaltioista, joissa se tarjoaa palvelujaan. Lisäksi sen tulisi ilmoittaa toimipaikkojensa tai edustajansa yhteystiedot Euroopan unionissa. Verkkotunnusvälittäjän olisi viipymättä ilmoitettava muutoksista 1 momentissa tarkoitettuihin tietoihin ja muutoksista niihin direktiivin edellyttämässä kahden viikon tai kolmen kuukauden määräajassa riippuen muuttuneesta tiedosta. Liikenne- ja viestintävirasto voisi antaa tarkempia määräyksiä tietojen ilmoittamisesta samoin kuin kyberturvallisuuslain 41 §:ssä säädetyn vastaavan ilmoitusvelvollisuudenkin osalta, joka koskee muun ohella aluetunnusrekisterin ylläpitäjiä. Kyberturvallisuuslain 18 §:ssä tarkoitettu keskitetty yhteyspiste vastaa NIS 2 -direktiivin 27 artiklan 4 kohdan mukaisten ilmoituksien tekemisestä, minkä johdosta Liikenne- ja viestintäviraston olisi toimitettava ilmoituksen tekemiseksi tarpeelliset tiedot keskitetylle yhteyspisteelle. Keskitetty yhteyspiste sijaitsee Liikenne- ja viestintävirastossa.

172 c §. *Verkkotunnusten rekisteröintitiedot.* Pykälässä säädettäisiin aluetunnusrekisterin ylläpitäjän ja verkkotunnusvälittäjän velvollisuudesta kerätä ja ylläpitää verkkotunnusten rekisteröintitietoja. Tietoja olisi kerättävä ja ylläpidettävä NIS 2 -direktiivin 28 artiklan edellyttämällä tavalla. NIS 2 -direktiivin 28 artiklan 2 kohdan mukaisiin tietoihin on sisällyttävä verkkotunnus, sen rekisteröintipäivä, verkkotunnuksen rekisteröijän nimi, yhteyssähköpostiosoite ja puhelinnumero sekä verkkotunnusta hallinnoivan yhteyspisteen yhteyssähköpostiosoite ja puhelinnumero, jos ne eivät ole samat kuin verkkotunnuksen rekisteröijän. Velvoite kohdistuisi molempiin toimijatyyppeihin, mutta sen toteuttamisessa olisi noudatettava 172 d §:ssä säädettävää yhteistyövelvollisuutta. Aluetunnusrekisterin ylläpitäjän ja verkkotunnusvälittäjän olisi lisäksi otettava käyttöön ja asetettava julkisesti saataville toimintaperiaatteet ja menettelyt, joilla ne varmistavat, että verkkotunnusten rekisteröintitiedot ovat tarkat ja oikeat. Pykälällä pantaisiin täytäntöön NIS 2 -direktiivin 28 artiklan 2 ja 3 kohdat muiden kuin 21 luvun soveltamisalaan kuuluvien verkkotunnusvälittäjien osalta.

172 d §. *Verkkotunnusten rekisteröintitietojen saatavuus.* Pykälässä säädettäisiin pääsyn antamisesta verkkotunnusten rekisteröintitietoihin NIS 2 -direktiivin 28 artiklan 4 ja 5 kohdan edellyttämällä tavalla sekä 6 kohdan edellyttämästä yhteistyöstä.

Pykälän *1 momentissa* säädettäisiin verkkotunnusten rekisteröintitietojen julkisesta saatavuudesta siltä osin kuin tiedot eivät ole henkilötietoja. Momentin nojalla muut verkkotunnuksen rekisteröintitiedot kuin henkilötiedot olisi asetettava julkisesti saataville ilman aiheetonta viivytystä verkkotunnuksen rekisteröinnin jälkeen. Velvoite kohdistuisi molempiin toimijatyyppeihin, mutta sen toteuttamisessa olisi noudatettava 3 momenttiin ehdotettua yhteistyövelvollisuutta.

Pykälän *2 momentissa* säädettäisiin verkkotunnusten rekisteröintitietojen luovuttamisesta siltä osin kuin tiedot ovat henkilötietoja. Momentin nojalla verkkotunnusten rekisteröintitietoihin olisi annettava pääsy, jos tietoihin pääsyä oikeutetusti pyytävä esittää lainmukaisen ja asianmukaisesti perusteluun pyynnön. Pyyntöön olisi vastattava ilman aiheetonta viivytystä ja viimeistään 72 tunnin kuluessa pyynnön vastaanottamisesta. Velvoite ei mahdollistaisi maksun perimistä tietojen luovuttamisesta. Lisäksi aluetunnusrekisterin ja verkkotunnusvälittäjän on asetettava julkisesti saataville käytössään olevat toimintaperiaatteet ja menettelyt verkkotunnusten rekisteröintitietojen luovuttamisesta.

Pykälän *3 momentissa* säädettäisiin aluetunnusrekisterin ylläpitäjän ja verkkotunnusvälittäjän velvollisuudesta tehdä yhteistyötä 172 c ja 172 d §:ssä säädettyjen velvoitteiden toteuttamiseksi ja päällekkäisten rekisteröintitietojen keräämisen välttämiseksi. Momentilla pantaisiin

täytäntöön NIS 2 -direktiivin 28 artiklan 6 kohta, jonka mukaan artiklan 1–5 kohdan velvoitteiden noudattaminen ei saa johtaa päällekkäisyyksiin verkkotunnusten rekisteröintitietojen keruussa. Tätä varten jäsenvaltioiden on edellytettävä, että aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat tekevät yhteistyötä keskenään. Voidaan kuitenkin katsoa, ettei direktiivin edellyttämä yhteistyö rajoitu suppeasti tietojen keruuseen vaan on yleisemminkin tarpeen direktiivin edellyttämien velvoitteiden toteuttamiseksi.

Verkkotunnusten rekisteröintiin ja rekisteröintitietojen julkaisuun on olemassa erilaisia toimintamalleja. Ehdotettujen 172 c ja 172 d §:n on tarkoitus mahdollistaa erilaiset perustellut toteutustavat tietojen keräämiselle, varmistamiselle, ylläpidolle ja niiden saatavuuden toteuttamiselle sekä tarkoituksenmukainen työnjako eri toimijoiden yhteistyönä mahdollisuuksien mukaan niissä puitteissa, jotka kansainvälisessä yhteistyössä syntyneet sopimusperusteiset parhaat käytännöt mahdollistavat, edellyttäen että NIS 2 -direktiivin edellyttämä lopputulos toteutuu. Tapauksen mukaan verkkotunnuksen rekisteröijän tietojen saataville saattamisesta tämän pykälän 1 momentissa säädettävän velvoitteen mukaisesti voisi esimerkiksi käytännössä vastata verkkotunnusvälittäjä siltä osin kuin direktiivin edellyttämät tiedot eivät sisältyisi aluetunnusrekisterin ylläpitäjän saatavilla pitämiin tietoihin, kun taas aluetunnusrekisterin ylläpitäjä voisi vastata verkkotunnuksen perustustietojen ja kyseisen verkkotunnusvälittäjän tietojen saatavuudesta. Mikäli aluetunnusrekisteri taas saattaisi kaikki edellytetyt tiedot saataville, ei olisi aiheellista edellyttää verkkotunnusvälittäjän julkaisevan tietoja toistamiseen. Ei olisi myöskään tarkoituksenmukaista, että verkkotunnusvälittäjän puolesta toimivien tahojen, joihin velvoitteita myös sovellettaisiin, tulisi asettaa tiedot uudestaan itsenäisesti julkisesti saataville, jos ne olisi saatettu saataville aluetunnusrekisterin ylläpitäjän tai verkkotunnusvälittäjän toimesta.

Pykälän *4 momentissa* säädettäisiin informatiivinen viittaus henkilötietojen suojaa koskevaan yleiseen tietosuoja-asetukseen ja tietosuojalakiin.

304 §. Sähköisen viestinnän palveluista annetusta laista ehdotetaan kumottavaksi 304 §:n 1 momentin 14 kohta, joka koskee kyberturvallisuusasetuksen täytäntöönpanoa ja Liikenne- ja viestintäviraston erityistä tehtävää kansallisena kyberturvallisuussertifioinnin viranomaisena. Liikenne- ja viestintäviraston tehtävästä kansallisena kyberturvallisuussertifioinnin viranomaisena säädettäisiin jatkossa eräiden tuotteiden kyberkestävyydestä ja kyberturvallisuussertifioinnista annetussa laissa. Näin ollen säännös ehdotetaan kumottavaksi päällekkäisenä suhteessa uuteen eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista ehdotettuun lakiin.

7.5 Laki sakon täytäntöönpanosta

1 §. *Lain soveltamisala*. Eri lakien nojalla määrättävien laiminlyönti- ja seuraamusmaksujen täytäntöönpanosta huolehtii Oikeusrekisterikeskus sakon täytäntöönpanosta säädettyä menettelyä noudattaen. Pykälän *2 momenttiin* ehdotetaan lisättäväksi uusi 37 kohta, jonka nojalla eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista annetun lain 31–37 §:n §:ssä tarkoitettu seuraamusmaksu pannaan täytäntöön lain mukaisessa järjestyksessä. Muutoksen johdosta 36 kohtaan tehtäisiin tekninen muutos.

8 Lakia alemman asteinen sääntely

Eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista annetun lain 10 §:ssä säädettäisiin mahdollisuudesta perustaa sääntelyn testiympäristö. Ehdotetun 10 §:n 4 momentin nojalla Liikenne- ja viestintäviraston voisi määräyksellä antaa tarkempia teknisiä

säännöksiä kyberkestävyyden sääntelyn testiympäristön järjestämisestä ja toiminnasta sekä talouden toimijan hakemuksesta. Kysymys olisi teknisistä sääntelyn testiympäristön toimintaan liittyvistä määräyksistä, joiden antamisen toimivalta olisi tarkoituksenmukaista osoittaa sääntelyn testiympäristön perustavalle viranomaiselle. Sääntelyn testiympäristön toiminnassa voi ilmetä tarve muuttaa sen toimintaan liittyviä teknisiä määräyksiä ottaen huomioon esimerkiksi kyberturvallisuuden kehittyvää uhkaympäristöä tai muita kyberturvallisuuteen liittyviä erityispiirteitä.

Perussäännökset koskien valtion viranomaisen suoritteiden maksullisuutta ja määrää sisältyvät valtion maksuperustelakiin. Vaikka esitykseen sisältyisi ehdotuksia, jotka koskevat valtion viranomaisten suoritteiden maksullisuutta, niiden osalta esitykseen ei sisälly ehdotuksia uusiksi asetuksenantovaltuuksiksi. Valtion viranomaisten suoritteiden maksullisuutta koskeva asetuksenantovaltuus perustuisi valtion maksuperustelain 8 §:ään sellaisena kuin se on voimassa.

Sähköisen viestinnän palveluista annettuun lakiin lisättävän 172 b §:n 2 momentissa säädettäisiin Liikenne- ja viestintäviraston oikeudesta antaa tarkempia teknisiä määräyksiä tietojen ilmoittamisesta verkkotunnusvälittäjien luetteloa varten, mikä vastaisi kyberturvallisuuslain vastaavaa sääntelyä. Lisäksi lain 21 luvun soveltamisalaan vaikuttava muutos lain 164 §:ään olisi merkityksellinen lain 165 ja 170 §:ssä säädettyjen määräyksenantovaltuuksien kannalta.

9 Voimaantulo

Ehdotetaan, että lait tulevat voimaan 1.6.2026 lukuun ottamatta sähköisen viestinnän palveluista annettuun lakiin ehdotettuja NIS 2 -direktiivin täytäntöönpanoon liittyviä muutoksia, joiden ehdotetaan tulevan voimaan mahdollisimman pian.

Eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista ehdotetun lain soveltamisen alkamista ehdotetaan porrastettavaksi kyberkestävyysasetuksen soveltamisen alkamista vastaavalla tavalla eräiden säännösten osalta. Kyberkestävyysasetusta sovelletaan sen 71 artiklan mukaisesti 11.12.2027 alkaen. Ilmoitettuja laitoksia koskevaa IV lukua sovelletaan 11.6.2026 alkaen ja raportointivelvollisuuksia koskevaa 14 artiklaa 11.9.2026 alkaen.

Sähköisen viestinnän palveluista annetun lain aluetunnusrekistereitä ja verkkotunnusten välittämistä koskeviin muutoksiin ehdotetaan tietyiltä osin kolmen kuukauden siirtymäsäännöksiä. Siirtymäajan kuluessa olisi tehtävä ehdotetun lain edellyttämät ilmoitukset verkkotunnusten rekisteröintipalvelujen tarjoamisesta sekä asetettava julkisesti saataville direktiivin edellyttämät toimintaperiaatteet ja menettelyt.

10 Toimeenpano ja seuranta

Kyberkestävyysasetuksen 70 artikla sisältää velvoitteen asetuksen uudelleenarvioinnista Euroopan komissiolle. Komissio toimittaa viimeistään 11.12.2030 ja sen jälkeen joka neljäs vuosi Euroopan parlamentille ja neuvostolle julkisen kertomuksen kyberkestävyysasetuksen arvioinnista ja uudelleentarkastuksesta.

Kyberkestävyysasetuksen 52 artikla sisältää sääntelyn toimeenpanoa ja seurantaa tukevia tehtäviä markkinavalvontaviranomaisille. Markkinavalvontaviranomaisten on muun ohella raportoitava vuosittain komissiolle asiaankuuluvien markkinavalvontatoimien tuloksista sekä seurattava, miten valmistajat ovat soveltaneet kyberkestävyysasetuksen 13 artiklan 8 kohdassa tarkoitettuja kriteerejä määrittäessään digitaalisia elementtejä sisältävien tuotteidensa tukiaikaa.

Kyberkestävyysasetuksen nojalla perustetaan lisäksi eri jäsenvaltioiden markkinavalvontaviranomaisten välinen hallinnollisen yhteistyön ryhmä. Hallinnollisen yhteistyön ryhmän on julkaistava yleisesti saatavilla olevassa ja käyttäjäystävällisessä muodossa asiaankuuluvat tilastot digitaalisia elementtejä sisältävien tuotteiden ryhmistä, mukaan lukien niiden keskimääräinen tukiaika sellaisena kuin valmistaja on sen määrittänyt 13 artiklan 8 kohdan mukaisesti, sekä annettava ohjeita, joihin sisältyvät digitaalisia elementtejä sisältävien tuotteiden ryhmien ohjeelliset tukiajat.

Myös kyberturvallisuusasetus sisältää säännökset, jotka edellyttävät komissiota antamaan arviointikertomuksen asetuksesta ensimmäisen kerran vuonna 2024. Komissiossa on yhä käynnissä kyberturvallisuusasetuksen uudelleentarkastelu, joka voi johtaa muutosesityksen antamiseen.

11 Suhde muihin esityksiin

Ensimmäinen lakiehdotus sisältää viittauksia eräiden tekoälyjärjestelmien valvonnasta esitettyyn lakiin. Laki on esitetty säädettäväksi hallituksen esityksellä eduskunnalle EU:n tekoälyasetusta täydentäväksi lainsäädännöksi (HE 46/2025 vp). Mainitulla esityksellä on esitetty muutettavaksi myös eräiden tuotteiden markkinavalvonnasta annettua lakia ja sakon täytäntöönpanosta annettua lakia, mikä on merkityksellistä tämän esityksen 2. ja 5. lakiehdotuksien muutoksien kannalta. Mainitun esityksen käsittely on eduskunnassa kesken.

Eduskunnassa on vireillä useita hallituksen esityksiä, joissa ehdotetaan muutettavaksi sakon täytäntöönpanosta annetun lain 1 §:n 2 momenttia. Näitä esityksiä ovat edellisessä kappaleessa mainitun esityksen lisäksi hallituksen esitys eduskunnalle laeiksi valtioneuvoston jäsenen tehtävään liittyvästä karenssista sekä sakon täytäntöönpanosta annetun lain 1 §:n muuttamisesta (HE 90/2024 vp), hallituksen esitys eduskunnalle EU:n poliittisen mainonnan avoimuutta ja kohdentamista koskevaa asetusta täydentäväksi lainsäädännöksi (HE 57/2025 vp), hallituksen esitys eduskunnalle laeiksi erittäin suuren kapasiteetin verkkojen käyttöönoton helpottamisesta, sähköisen viestinnän palveluista annetun lain 249 ja 303 §:n muuttamisesta ja sakon täytäntöönpanosta annetun lain 1 §:n muuttamisesta (HE 74/2025 vp), hallituksen esitys eduskunnalle laiksi EU:n metsäkatoasetuksen velvoitteiden valvonnasta ja seuraamuksista sekä siihen liittyviksi laeiksi (HE 77/2025 vp), hallituksen esitys eduskunnalle EU:n data-asetusta täydentäväksi lainsäädännöksi (HE 128/2025 vp) ja hallituksen esitys eduskunnalle kansainvälistä taksiliikennettä tiellä koskevan Norjan kanssa tehdyn sopimuksen hyväksymiseksi ja voimaansaattamiseksi ja eräiksi muiksi laeiksi (HE 134/2025 vp).

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

12.1 Viranomaistehtävät

Kyberkestävyysasetuksessa velvoitetaan jäsenvaltiot nimeämään markkinavalvontaviranomainen ja ilmoittava viranomainen. Velvoite viranomaisen nimeämiseen tulee suoraan asetuksesta. Kansalliseen harkintavaltaan jää, nimetäänkö yksi vai useampi viranomainen ja mitä nämä viranomaiset ovat.

Perustuslakivaliokunta on viranomaisten toimivaltuuksia koskevaa sääntelyä arvioidessaan pitänyt arvion lähtökohtana myös sitä, että viranomaisen toimivaltuuksien sääntely on merkityksellistä perustuslain 2 §:n 3 momentissa vahvistetun oikeusvaltioperiaatteen kannalta (PeVL 51/2006 vp, s. 2/I). Julkisen vallan käytön tulee perustuslain 2 §:n 3 momentin mukaan perustua lakiin, ja kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia. Lähtökohtana on, että julkisen vallan käytön tulee olla aina palautettavissa eduskunnan säätämässä laissa olevaan toimivaltaperusteeseen. Lailla säätämiseen taas kohdistuu yleinen vaatimus lain täsmällisyydestä ja tarkkuudesta. (PeVL 19/2021 vp, 15 kohta viittauksineen.) Toimivaltaisen päätöksentekijän tulee käydä ilmi laista yksiselitteisesti (PeVL 18/2021 vp, 2 kohta). Toimivaltasääntely on valiokunnan käsityksen mukaan yleensä merkityksellistä myös perustuslaissa turvattujen perusoikeuksien näkökulmasta (ks. PeVL 10/2016 vp, s. 3). Kun viranomaiselle annetaan uusia tehtäviä, niiden tulisi sopia tälle viranomaiselle (ks. PeVL 32/2020 vp, s. 5).

Kyberkestävyysasetuksen mukaiset tehtävät sopivat asiasisältönsä puolesta ehdotetulla tavalla Liikenne- ja viestintäviraston tehtäviin. Suuririskisiin tekoälyjärjestelmiin kohdistuvan kyberkestävyysasetuksen valvonnan osalta se, mille viranomaiselle valvontatehtävä kuuluisi, määräytyisi eräiden tekoälyjärjestelmien valvonnasta annetun lain ja EU:n tekoälyasetuksen perusteella, sillä tekoälyasetusta varten nimetyt markkinavalvontaviranomaiset vastaavat myös kyberkestävyysasetuksen nojalla vaadituista markkinavalvontatoimista, eikä markkinavalvonnan järjestämiseen liity tältä osin kansallista liikkumavaraa. Tehtävien sisältö määräytyisi pääasiassa kyberkestävyysasetuksen perusteella. Kyberkestävyysasetuksen sääntelyä täydentäisivät kansallisten hallinnon yleislakien säännökset, markkinavalvontalaki sekä eräiden tuotteiden kyberkestävyydestä ja kyberturvallisuussertifioinnista annetun lain säännökset muun muassa tietojenvaihdosta. Viranomaisten uudet tehtävät perustuisivat lakiin ja suoraan sovellettavaan EU:n asetukseen. Toimivaltaisen viranomaisen tehtävät on määritelty ehdotettavassa laissa tarkasti ja täsmällisesti.

12.2 Julkisen hallintotehtävän antaminen muulle kuin viranomaiselle

Perustuslain 124 §:n mukaan julkinen hallintotehtävä voidaan antaa muulle kuin viranomaiselle vain lailla tai sen 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 tulkintakäytännön mukaan julkisen hallintotehtävän antaminen muulle kuin viranomaiselle edellyttää, että laissa määritellään ainakin yleisluonteisesti tehtävän hoitajalta edellytetty pätevyys tai kelpoisuus (muun muassa PeVL 28/2001 vp ja PeVL 48/2001 vp). Perustuslakivaliokunnan käytännössä on katsottu, että oikeusturvan ja hyvän hallinnon vaatimusten toteutumisen varmistaminen perustuslain 124 §:n tarkoittamassa merkityksessä edellyttää, että asian käsittelyssä noudatetaan hallinnon yleislakeja ja että asioita käsittelevät toimivat virkavastuulla (PeVL 33/2004 vp, s. 7/II, PeVL 46/2002 vp, s. 10). Hallinnon yleislakeja sovelletaan niiden sisältämien soveltamisalaa, viranomaisten määritelmää tai yksityisen kielellistä palveluvelvollisuutta koskevien säännösten nojalla myös yksityisiin niiden hoitaessa julkisia hallintotehtäviä (PeVL 42/2005 vp, s. 3/II). Myös yhtiön palveluksessa olevaan henkilöön sovelletaan rikosoikeudellista virkavastuuta koskevia säännöksiä hänen hoitaessaan yhtiölle kuuluvia julkisia hallintotehtäviä (PeVL 26/2017 vp, s. 49–50, PeVL 16/2016 vp, s. 2–3, PeVL 8/2014 vp, s. 5/I).

Kyberkestävyysasetuksen mukaiset ilmoitetut laitokset suorittaisivat vaatimustenmukaisuuden arviointitehtäviä, joissa olisi kysymys julkisesta hallintotehtävästä. Kyberkestävyysasetuksen 39 artiklan 2 kohdassa todetaan, että vaatimuksenmukaisuuden arviointilaitoksen on oltava

jäsenvaltion kansallisen lainsäädännön mukaisesti perustettu ja että sen on oltava oikeushenkilö. Lisäksi 39 artiklassa säädetään yksityiskohtaisesti ja tarkasti vaatimuksenmukaisuuden arviointilaitoksen tehtävän hoidossa edellytetyistä vaatimuksista. Jos ilmoitettu vaatimuksenmukaisuuden arviointilaitos antaa alihankintaan tietyt vaatimuksenmukaisuuden arviointiin liittyvät tehtävät tai käyttää tytäryhtiötä, on ilmoitetun vaatimuksenmukaisuuden arviointilaitoksen varmistettava kyberkestävyysasetuksen 41 artiklan nojalla, että alihankkija tai tytäryhtiö täyttää myös kyberkestävyysasetuksen 39 artiklassa säädetyt vaatimukset sekä ilmoitettava siitä viranomaiselle. Myös tilanteet, joissa ilmoitetun vaatimuksenmukaisuuden arviointilaitoksen toimintaa on rajoitettava tai peruutettava, on säännelty mainitun asetuksen 45 artiklassa. Kyberkestävyysasetuksen suoraan sovellettavan yksityiskohtaisen sääntelyn voidaan katsoa muodostavan riittävän säädöspohjan tehtävän hoitajan pätevyydestä ja kelpoisuudesta perustuslain 124 §:n kannalta. Ilmoitetun laitoksen tehtävissä ei olisi kysymys merkittävän julkisen vallan käytöstä.

Kyberturvallisuusasetuksen mukaisia tehtäviä hoitavien, kyberturvallisuussertifiointia varten ilmoitettuja vaatimuksenmukaisuuden arviointilaitoksia koskeviin vaatimuksiin sovelletaan puolestaan kyberturvallisuusasetuksen 60 artiklan 1 kohdan viittauksen johdosta asetuksen liitettä. Myös tässä tehtävässä olisi kysymys julkisesta hallintotehtävästä. Vaatimukset ovat kyberkestävyysasetuksen vastaavien vaatimuksien kaltaisia. Vaatimustenmukaisuuden arviointilaitoksen on oltava perustettu kansallisen lainsäädännön mukaisesti ja sen on oltava oikeushenkilö. Liite sisältää yksityiskohtaiset vaatimukset arviointien suorittamiselle, ja niillä varmistetaan riippumattomuus ja eturistiriitojen poissulkeminen. Vaatimustenmukaisuuden arviointilaitosten on varmistettava, että niiden tytäryhtiöiden ja alihankkijoiden toimet eivät vaikuta niiden suorittamien vaatimustenmukaisuuden arviointitoimien luottamuksellisuuteen, objektiivisuuteen tai puolueettomuuteen. Kyberturvallisuusasetuksen suoraan sovellettavan yksityiskohtaisen sääntelyn voidaan katsoa muodostavan riittävän säädöspohjan tehtävän hoitajan pätevyydestä ja kelpoisuudesta perustuslain 124 §:n kannalta. Tehtävässä ei olisi kysymys merkittävän julkisen vallan käytöstä.

Lisäksi 1. lakiehdotus mahdollistaisi kyberturvallisuussertifioinnin viranomaiselle osoitettujen kyberturvallisuussertifiointiin liittyvien tehtävien delegoimisen kyberturvallisuusasetuksen sääntelyä vastaavasti vaatimustenmukaisuuden arviointilaitokselle. Tehtävät olisivat samankaltaisia kuin kyberturvallisuusasetuksen nojalla kyberturvallisuussertifiointia varten ilmoitettujen vaatimustenmukaisuuden arviointilaitosten tehtävät muutoinkin, ja niissä olisi kysymys julkisen vallan käytöstä, ei kuitenkaan merkittävän julkisen vallan käytöstä. Erotuksena on, että kyse on korkean varmuustason sertifikaattien myöntämisestä, joka on kyberturvallisuusasetuksessa lähtökohtaisesti viranomaiselle varattu tehtävä. Sertifioinnin korkea varmuustaso sellaisenaan ei kuitenkaan tee tehtävästä sellaista merkittävän julkisen vallan käyttöä, jota ei voitaisi osoittaa viranomaiskoneiston ulkopuolelle. Delegointi voisi olla tarpeen erityisesti tehtävässä edellytetyn korkeatasoisen erityisosaamisen vuoksi. Ehdotus mahdollistaisi tarkempien pätevyysvaatimusten asettamisen tehtävän delegointia koskevassa sopimuksessa, mikäli se olisi sovellettavan sertifiointijärjestelmän kannalta tarpeen. Laissa säädettäisiin vaatimustenmukaisuuden arviointilaitoksia koskevat yleiset vaatimukset akkreditointeineen ja mahdollisine valtuutuksineen, jotka varmistaisivat tehtävän hoitajan pätevyyden myös delegoidun tehtävän osalta perustuslain 124 §:n kannalta riittävällä tasolla.

Ilmoitetun laitoksen ja kyberturvallisuussertifiointia varten ilmoitetun vaatimuksenmukaisuuden arviointilaitoksen katsottaisiin toimivan tehtävässään itsenäisenä rekisterinpitäjänä suhteessa sen ilmoittaneeseen viranomaiseen.

Perusoikeuksien, oikeusturvan ja muiden hyvän hallinnon vaatimusten turvaaminen. Edellytyksenä julkisen hallintotehtävän antamiselle muulle kuin viranomaiselle on, ettei se saa

vaarantaa perusoikeuksia, oikeusturvaa eikä muita hyvän hallinnon vaatimuksia. Perustuslain 118 §:ssä säädetään vastuusta virkatoimista. Virkavastuu sisältää sekä vahingonkorvausoikeudellisen että rikosoikeudellisen vastuun. Kun julkinen hallintotehtävä lailla annetaan hoidettavaksi muulle kuin viranomaiselle, tulee perustuslakivaliokunnan vakiintuneen tulkinnan mukaan säädösperusteisesti huolehtia siitä, että tehtävää hoitavaan sovelletaan tässä tehtävässä samoja säännöksiä kuin viranomaisvastuulla vastaavaa tehtävää hoitavaan (PeVL 5/2010 vp, PeVL 3/2009 vp, PeVL 1/2008 vp). Ehdotettu laki sisältäisi perustuslakivaliokunnan tulkintakäytännössään edellyttämän säännöksen virkavastuusta. Rikosoikeudellista virkavastuuta koskevia säännöksiä sovellettaisiin kyberkestävyysasetuksen mukaisen ilmoitetun laitokseen ja kyberturvallisuussertifiointia varten ilmoitettuun vaatimustenmukaisuuden arviointilaitoksen tai niiden käyttämän tytäryhtiön tai alihankkijan henkilöstöön niiden hoitaessa kyberkestävyysasetuksessa taikka kyberturvallisuusasetuksessa ja ehdotetussa laissa tarkoitettuja tehtäviä. Hallinnon yleislait tulisivat sovellettavaksi ilman eri viittaustakin. Ilmoitetun laitoksen tai kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen tekemään päätökseen olisi myös mahdollista hakea oikaisua ja muutosta, mikä varmistaisi perustuslain 21 §:ssä säädetyn oikeusturvan toteutumisen.

Ilmoitetun laitoksen tai kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen tehtävien luvanvaraisuus ja tehtävien rajoittaminen ja peruuttaminen. Ehdotetun sääntelyn mukaan vaatimustenmukaisuuden arviointilaitoksen on haettava kyberkestävyysasetuksessa tarkoitetuksi ilmoitetuksi laitokseksi nimeämistä ja ilmoittamista Liikenne- ja viestintävirastosta. Ilmoitetuksi laitokseksi nimetään arviointilaitos, joka täyttää kyberkestävyysasetuksen 39 artiklassa asetetut vaatimukset niiden digitaalisen elementin sisältävien tuotteiden osalta, joiden osalta arviointilaitos on pätevä. Vastaavasti kyberturvallisuusasetuksen mukainen sertifiointitoiminta edellyttäisi vaatimustenmukaisuuden arviointilaitokselta, että Liikenne- ja viestintävirasto nimeäisi sen kyberturvallisuussertifiointia varten komissiolle. Ilmoittaminen edellyttäisi FINAS-akkreditointipalvelun akkreditointia ja kyberturvallisuusasetuksen liitteen sekä sovellettavan sertifiointijärjestelmän asettamien edellytysten täyttämistä.

Kyberkestävyysasetuksen mukaiset ilmoitetut laitokset ja kyberturvallisuusasetuksen mukaiset kyberturvallisuussertifiointia varten ilmoitetut vaatimuksenmukaisuuden arviointilaitokset suorittaisivat vaatimustenmukaisuuden arviointitehtäviä, joissa olisi kysymys julkisesta hallintotehtävästä. Perustuslakivaliokunta on käytännössään katsonut, ettei viranomaiselle lähtökohtaisesti kuuluvien hallintotehtävien hoitaminen kuulu perustuslain 18 §:n 1 momentissa turvatun elinkeinovapauden piiriin (PeVL 23/2013 vp, PeVL 20/2006 vp, s. 3/I). Valiokunta on kuitenkin pitänyt viranomaisorganisaatioon kuulumattoman yksityisen toimijan oikeuksia ja velvollisuuksia koskevan sääntelyn oikeasuhtaisuuden kannalta välttämättömänä, että hyväksynnän peruuttamismahdollisuus sidotaan vakaviin tai olennaisiin rikkomuksiin tai laiminlyönteihin sekä siihen, että yksityiselle toimijalle annetut huomautukset ja varoitukset eivät ole johtaneet toiminnassa esiintyneiden puutteiden korjaamiseen (PeVL 23/2013 vp, PeVL 20/2006 vp, s. 3/I, PeVL 27/2010 vp, s. 3/II).

Kyberkestävyysasetuksessa säädetään nimeämisen rajaamisesta ja peruuttamisesta. Jos ilmoitettu laitos ei enää täytä säädettyjä vaatimuksia tai se ei noudata velvollisuuksiaan, ilmoittamisesta vastaavan viranomaisen on tarpeen mukaan rajoitettava ilmoitusta taikka peruutettava se toistaiseksi tai kokonaan sen mukaan, miten vakavaa vaatimusten täyttämättä jättäminen tai velvollisuuksien noudattamatta jättäminen on ollut. Tältä osin asiassa ei ole kansallista liikkumavaraa. Kyberturvallisuusasetuksen nojalla annetut täytäntöönpanosäädökset määrittävät osaltaan edellytykset, joiden nojalla viranomaisen olisi eri tavoin rajoitettava kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen

oikeutta suorittaa kyseisten säädösten mukaisia tehtäviä. Siltä osin kuin EU-oikeudessa ei säädettäisi asiasta toisin, ehdotetussa laissa säädettäisiin viranomaisen toimivallasta viime kädessä peruuttaa nimeäminen, jos kyberturvallisuussertifiointia varten ilmoitettu vaatimustenmukaisuuden arviointilaitos ei ole korjannut toimintaansa määräajassa ja kyseessä on olennainen rikkomus tai laiminlyönti taikka jos se ei täytä sille säädettyjä vaatimuksia tai sen akkreditointia rajoitetaan, akkreditointi peruutetaan tai se keskeytetään.

Lisäksi ehdotuksen mukaan kyberturvallisuuden sertifiointiviranomainen voisi irtisanoa tai purkaa korkean varmuustason kyberturvallisuussertifiointia koskevan sopimuksen vaatimustenmukaisuuden arviointilaitoksen kanssa, jos kyberturvallisuussertifiointia varten ilmoitettu vaatimustenmukaisuuden arviointilaitos ei enää täytä siihen kohdistuvia vaatimuksia tai jos se olennaisesti laiminlyö sopimuksessa sovittujen tehtävien suorittamisen tai muutoin rikkoo sopimusta tai toimii olennaisesti tai toistuvasti lainvastaisesti.

Ehdotuksen arvioidaan täyttävän vaatimukset, jotka perustuslakivaliokunnan käytännössä on asetettu toiminnan hyväksynnän peruuttamiselle.

Asiantuntijoiden käyttö tarkastuksessa. Ehdotus mahdollistaisi sen, että kyberturvallisuussertifioinnin viranomainen voisi teettää tarkastuksen riippumattomalla asiantuntijalla, jolla on tarvittava koulutus ja kokemus. Asiantuntijaan sovellettaisiin tällöin ehdotuksen mukaan rikosoikeudellista virkavastuuta koskevia säännöksiä, minkä lisäksi hallinnon yleislakeja sovellettaisiin ilman nimenomaista mainintaakin, mikä turvaisi hyvän hallinnon vaatimusten noudattamisen. Ulkopuolisten asiantuntijoiden rooli olisi täydentävä. Viranomaisen katsottaisiin toimivan tällöin rekisterinpitäjänä ja asiantuntijan henkilötietojen käsittelijänä. Tarkastusten havaintojen perusteella mahdollisesti tehtävät hallinnolliset päätökset tekisi sen sijaan viranomainen. Valvontaan liittyvän erityisen asiantuntemuksen tarpeen ja viranomaisen resurssien tehokkaan käytön turvaamisen johdosta ulkopuolisen asiantuntijan käytön mahdollisuutta on pidettävä tarkoituksenmukaisena. Ulkopuolisen asiantuntijan käyttäminen ei siten olisi ongelmallista perustuslain 124 §:n kannalta.

12.3 Omaisuuden suoja

Ensimmäisen lakiehdotuksen 19 §:n 2 momentti, jonka mukaan ohjelmiston tutkittavaksi ottamisesta ei suoriteta talouden toimijalle korvausta, on merkityksellinen perustuslaissa turvatun omaisuudensuojan kannalta. Perustuslain 15 §:n mukaan jokaisen omaisuus on turvattu. Perustuslakivaliokunnan lausuntokäytännön mukaan omaisuudensuoja kattaa 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). Omistajan oikeuksia voidaan rajoittaa lailla, kunhan sääntely täyttää perusoikeuksien yleiset rajoitusedellytykset.

Ehdotettu säännös kuuluu kansalliseen liikkumavaraan. Kyseessä olisi poikkeus markkinavalvontalain sääntelyyn, jonka mukaan markkinavalvontaviranomaisen on markkinavalvontalain 10 §:n 2 momentin mukaan talouden toimijan vaatimuksesta korvattava tutkittavaksi otettu tuote käyvän hinnan mukaan, jollei havaita, että tuote on vaatimustenvastainen. Perusteena poikkeukselle olisi se, että fyysisistä tuotteista poiketen digitaalisessa muodossa olevien ohjelmistojen tutkittavaksi ottamisesta eli käytännössä ohjelmiston sähköisen kopion luovuttamisesta ei aiheudu talouden toimijalle sellaista myynnin menetystä tai muutakaan korvattavaa vahinkoa, joka olisi korvattava ohjelmiston käyvän arvon mukaan. Koska tällainen tutkittavaksi ottaminen ei rajoita ohjelmiston valmistajan tai muun talouden toimijan mahdollisuutta käyttää omaisuuttaan tai valmistaa siitä uusia kopioita eikä

aiheuttaisi vähäistä vaivaa merkittävämpää taloudellista vahinkoa, ei ehdotuksen arvioida olevan omaisuuden suojan kannalta ongelmallinen.

12.4 Verkkotunnusvälittäjän ilmoitusvelvollisuus

Sähköisen viestinnän palveluista annetun lain uuden 21 a luvun 172 b §:ssä säädettäisiin verkkotunnusvälittäjiin ja niiden puolesta toimiviin kohdistuvasta ilmoitusvelvollisuudesta. Lisäksi 21 luvun mukainen ilmoitusvelvollisuus laajennettaisiin verkkotunnusvälittäjien puolesta toimiviin. Ehdotus tarkoittaisi käytännössä soveltamisalaan kuuluvan toimijan ilmoitusvelvollisuutta toiminnastaan Liikenne- ja viestintävirastolle ja olisi siten merkityksellinen perustuslain 18 §:ssä turvatun elinkeinovapauden kannalta.

NIS 2 -direktiivin 27 artiklan täytäntöönpano edellyttää ilmoitusvelvollisuuden mukaisten tietojen keräämistä verkkotunnusvälittäjiltä. Lisäksi ilmoittautumisvelvollisuus toisi Liikenne- ja viestintäviraston tietoon ne verkkotunnusvälittäjät, jotka kuuluisivat vain uuden 21 a luvun soveltamisalaan, mikä on edellytys valvonnan kohdentamiselle verkkotunnusvälittäjiin. Ilmoitettavat tiedot olisivat toimijan yhteystietoja ja siten kohtuudella ilmoitettavissa ja päivitettävissä.

Perustuslakivaliokunta ei ole pitänyt ilmoitusvelvollisuutta elinkeinovapauden kannalta ongelmallisena, kun ilmoituksen tekemättä jättäminen ei ole merkinnyt kieltoa harjoittaa toimintaa (PeVL 16/2009 vp, s. 3/I) tai kun viranomaisen ei edellytetä tekevän ilmoituksen johdosta päätöstä (PeVL 54/2002 vp, s. 3/I). Liikenne- ja viestintäviraston ei edellytettäisi tekevän päätöstä ilmoituksen johdosta. Ilmoituksen tekemättä jättäminen ei sinänsä merkitsisi kieltoa tarjota palvelua tai harjoittaa toimintaa. Ehdotuksen ei siten arvioida olevan elinkeinovapauden kannalta ongelmallinen.

12.5 Kotirauhan suoja

Ehdotetun 19 §:n nojalla markkinavalvontaviranomainen voisi tietyin edellytyksin suorittaa tarkastuksen pysyväisluonteiseen asumiseen käytettävässä tilassa. Ehdotus on merkityksellinen perustuslain 10 §:ssä turvatun kotirauhan suojan kannalta.

Perustuslain 10 §:n mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Perustuslain 10 §:n 3 momentin mukaan lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä. Euroopan unionin perusoikeuskirjan 7 artiklan mukaan jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejään kunnioitetaan. Perusoikeuskirjan 52 artiklan mukaan näiden oikeuksien käyttämistä voidaan rajoittaa ainoastaan lailla ja ainoastaan, jos ne ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.

Perustuslakivaliokunnan lausuntokäytännön mukaan perustuslain 10 §:ssä suojatun kotirauhan piiri kattaa lähtökohtaisesti kaikenlaiset pysyväisluonteiseen asumiseen käytetyt tilat eli myös sellaiset elinkeinonharjoittajan toimitilat, jotka sijaitsevat esimerkiksi elinkeinonharjoittajan asunnossa. Valiokunnan mukaan kotirauhan piiriin ulottuvat tarkastukset eivät kuitenkaan välttämättä vaaranna kotirauhan suojan varsinaista ydintä silloin, kun tarkastukset kohdistuvat tiloihin, joissa harjoitetaan elinkeino- tai ammattitoimintaa (ks. esim. PeVL 17/2018 vp, s. 5, PeVL 54/2014 vp, s. 2/II, PeVL 21/2010 vp ja PeVL 6/2019 vp).

Perustuslakivaliokunta on EU-sääntelyn täytäntöönpanoon liittyneessä viranomaisten tarkastusoikeutta koskeneessa lausuntokäytännössään katsonut, että sillä ei ole valtiosääntöistä

huomauttamista tarkastuksia koskevaan sääntelyyn, joka kuuluu EU-asetuksen soveltamisalaan ja on EU-sääntelyn edellyttämää (PeVL 12/2019 vp ja PeVL 6/2019 vp). Perustuslakivaliokunta on kiinnittänyt huomiota siihen, että EU:n perusoikeuskirjassa turvattu kotirauhan suoja ei ole kaikilta osin yhteneväinen perustuslain 10 §:n 3 momentin kanssa. Perustuslakivaliokunnan lausunnoissa on kiinnitetty huomiota siihen, että perusoikeuskirja ei sisällä Suomen perustuslain kaltaista kvalifioitua lakivarausta, minkä vuoksi perusoikeuskirjan kanssa yhdenmukaistakin EU-sääntelyä on toisinaan vaikea ongelmitta sovittaa yhteen Suomen valtiosäännön kanssa (ks. esim. PeVL 6/2019 vp ja PeVL 39/2016 vp). Lisäksi perustuslakivaliokunta on pitänyt tärkeänä, että siltä osin kuin Euroopan unionin lainsäädäntö edellyttää kansallista sääntelyä tai mahdollistaa sen, tätä kansallista liikkumavaraa käytettäessä otetaan huomioon perus- ja ihmisoikeuksista seuraavat vaatimukset (PeVL 25/2005 vp). Perustuslakivaliokunta on tältä osin katsonut, että jos kotirauhan piiriin ulottuva tarkastustoimivaltuus ei ole kaikilta osin EU-asetuksen edellyttämä, tarkastustoimivaltuus tulee kotirauhan piiriin ulottuvilta osilta supistaa asetuksen kannalta välttämättömään (esim. PeVL 6/2019 vp).

Ehdotettu tarkastuksia koskeva toimivaltasääntely on EU-sääntelyn edellyttämää, ja siinä on otettu huomioon perustuslakivaliokunnan käytännössä asetetut vaatimukset.

Kyberkestävyysasetuksen 52 artiklan mukaan tuotteiden markkinavalvontaan sovelletaan asetuksen soveltamisalaan kuuluvien tuotteiden osalta lisäksi asetusta (EU) 2019/1020 (ns. markkinavalvonta-asetus). Markkinavalvonta-asetuksen 14 artiklan 4 kohdassa säädetään vähimmäistoimivaltuuksista, jotka jäsenvaltioissa tulee olla markkinavalvontaviranomaisten käytettävissä. Markkinavalvonta-asetuksen 14 artiklan 4 kohdan e alakohdan mukaan markkinavalvontaviranomaisilla tulee olla valtuudet päästä kaikkiin tiloihin, kaikille alueille tai kaikkiin kulkuneuvoihin, joita talouden toimija käyttää tarkoituksessa, joka liittyy talouden toimijan elinkeino- tai ammattitoimintaan, vaatimustenvastaisuuden havaitsemiseksi ja näytön hankkimiseksi.

Markkinavalvonta-asetusta täydentää kansallisesti markkinavalvontalaki. Markkinavalvontalain 9 §:n 1 momentin mukaan markkinavalvontaviranomaisella on oikeus valvontaa varten päästä kaikkiin tiloihin, joissa harjoitetaan 1 §:n 1 momentissa mainituissa laeissa tarkoitettua toimintaa tai säilytetään valvonnan kannalta merkityksellisiä tietoja, ja tehdä valvonnassa tarvittavia tarkastuksia. Pysyväisluonteiseen asumiseen käytettäviin tiloihin tarkastuksia ei kuitenkaan saa ulottaa. Tarkastuksissa noudatetaan, mitä hallintolain (434/2003) 39 §:ssä säädetään. Pykälän 2 momentin mukaan markkinavalvontaviranomaisen oikeudesta ulottaa tarkastus pysyväisluonteiseen asumiseen käytettäviin tiloihin säädetään tarvittaessa erikseen 1 §:n 1 momentissa mainituissa laeissa.

Markkinavalvonta-asetus edellyttää, että markkinavalvontaviranomaisen toimivaltuudet ovat käytettävissä kaikkien kyberkestävyysasetuksen soveltamisalaan kuuluvien tuotteiden valvonnassa. Markkinavalvonta-asetuksen mukaan tarkastuksia tulisi voida ulottaa kaikkiin tiloihin, joita talouden toimija käyttää elinkeino- tai ammattitoiminnassaan. Viranomaisen oikeudesta tehdä tarkastuksia pysyväisluonteiseen asumiseen tarkoitettuihin tiloihin ei kuitenkaan säädetä markkinavalvontalaissa vaan sektorilainsäädännössä. Markkinavalvontalain esitöissä arvioidaan, että milloin toimivaltuus tehdä tarkastuksia pysyväisluonteiseen asumiseen käytettäviin tiloihin olisi jollain tuotesektorilla sen erityispiirteistä takia tarpeen, tästä toimivaltuudesta olisi säädettävä erikseen sektorilaissa (HE 139/2021 vp, s. 12). Useissa tuotelaeissa onkin säädetty tarkastusoikeuden ulottamisesta myös pysyväisluonteiseen asumiseen käytettyihin tiloihin tietyin reunaehdoin (esim. laki kuluttajatuotteiden turvallisuudesta, sähköturvallisuuslaki, laki kosmeettisista valmisteista ja lannoitelaki). Kyberkestävyysasetuksen valvonnan kannalta käsillä olisi markkinavalvontalain esitöissä kuvattu tilanne.

Kyberkestävyysasetuksen alaan kuuluvaa toimintaa kuten ohjelmistokehitystä on mahdollista ja tavanomaistakin harjoittaa myös kotirauhan piiriin kuuluvissa tiloissa. Tällainen toiminta voi olla henkilön pää- tai sivutoimista yritystoimintaa. Tällöin voi syntyä tilanteita, joissa ainoa mahdollisuus tehdä valmistajaan tai muuhun talouden toimijaan kohdistuva tarkastus on toteuttaa se kyseisissä elinkeinotoimintaan käytetyissä mutta sinänsä myös kotirauhan piiriin kuuluvissa tiloissa. On mahdollista, että myös laitteiden kokoonpano tapahtuisi asuintilojen yhteydessä. Näin ollen markkinavalvonta-asetuksen katsotaan edellyttävän, että kyberkestävyysasetuksen valvomiseksi tarkastus olisi tämänkaltaisissa tilanteissa voitava ulottaa rajoitetusti myös kotirauhan piiriin kuuluviin tiloihin.

Perustuslakivaliokunta on vakiintuneesti painottanut, että perustuslain 10 §:n 3 momentin sanamuoto edellyttää, että kotirauhan piiriin ulottuva tarkastus sidotaan välttämättömyysvaatimukseen, ja edellyttänyt toimenpidevaltuuksia koskeviin säännöksiin kirjattavaksi, että esimerkiksi tarkastus asunnossa voidaan toimittaa vain, jos se on välttämätöntä tarkastuksen kohteena olevien seikkojen selvittämiseksi (ks. esim. PeVL 54/2014 vp, s. 3 ja siinä viitatut lausunnot).

Perustuslakivaliokunta on käytännössään katsonut kotirauhan piiriin ulottuvan toimen olevan hyväksyttävä ”rikosten selvittämiseksi”, jos toimi sidotaan siihen, että on olemassa konkreettinen ja yksilöity syy epäillä lakia rikotun tai rikottavan (PeVL 14/2013 vp, s. 3 ja PeVL 69/2002 vp, s. 2). Sääntelyn oikeasuhtaisuuden näkökulmasta valiokunnan lähtökohtana on ollut, ettei kotirauhan suojaan tule puuttua enimmillään sakolla rangaistavien, moitittavuudeltaan vähäisten rikkomusten selvittämiseksi. (PeVL 40/2002 vp, s. 2). Valiokunta on toisaalta pitänyt kotirauhan piiriin ulottuvaa tarkastusta julkisista varoista myönnettyjen tukien ja avustusten asianmukaisen käytön valvomiseksi hyväksyttävänä sellaisiakin rangaistaviksi säädettyjä rikkomuksia koskevien perusteltujen epäilyjen johdosta, joista voi enimmillään seurata sakkorangaistus (ks. PeVL 69/2002 vp, s. 2–3). Tarkastusoikeus on tavallisella lailla voitu kytkeä myös rangaistusluonteisella maksulla sanktioituun käyttäytymiseen (PeVL 7/2004 vp, PeVL 39/2005 vp ja PeVL 14/2013 vp).

Markkinavalvontalain 9 §:ssä viitataan hallintolain 39 §:ään siten kuin perustuslakivaliokunta on edellyttänyt tehtävän valvontatyyppisten tarkastusten sääntelyssä (PeVL 11/2013 vp, s. 2).

Tarkastusoikeus kotirauhan piirissä olisi rajattu tiloihin, joita talouden toimija käyttää elinkeino- tai ammattitoimintaansa liittyviin tarkoituksiin. Ehdotuksen mukaan pysyväisluonteiseen asumiseen käytetyssä tilassa tarkastuksen saisi tehdä vain, jos se on välttämätöntä tarkastuksen kohteena olevien seikkojen selvittämiseksi. Tämä merkitsee, että edellytyksenä olisi, että epäiltyä rikkomusta ei voida selvittää muilla keinoin, kuten tiedonsaantioikeuden avulla tai tekemällä tarkastus kohteessa, joka ei kuulu kotirauhan piiriin. Tarkastusoikeus kotirauhan piiriin kuuluvissa tiloissa kohdistuisi valvontatehtävien hoitamiseksi välttämättömiin tietoihin, jotka liittyvät kyberkestävyysasetuksen tai esityksen 1. lakiehdotukseen perustuvien velvoitteiden rikkomiseen. Ei ole kuitenkaan mahdollista tyhjentävästi luetella tietoja, joiden hankkimiseksi tarkastus olisi välttämätöntä suorittaa kotirauhan piiriin kuuluvissa tiloissa.

Toimenpiteen oikeasuhtaisuus olisi varmistettu säännösperusteisesti. Edellytyksenä olisi ensinnäkin, että on perusteltu ja yksilöity syy epäillä kyberkestävyysasetusta rikotun tai rikottavan tavalla, josta voi olla seuraamuksena ehdotuksen mukainen hallinnollinen seuraamusmaksu. Kyberkestävyysasetuksen rikkomisesta säädettävän seuraamusmaksun enimmäismäärä on enimmäismäärältään huomattava, ja kyseessä on rangaistuksenluonteinen sanktio. Lisäksi edellytyksenä olisi se, että epäillyssä rikkomuksessa tulisi olla kyse digitaalisen elementin sisältävän tuotteen tai prosessin vaatimustenvastaisuudesta tai

kyberkestävyysasetuksen 57 artiklassa tarkoitetusta muusta merkittävän kyberturvallisuusriskin tilanteesta, joka on kuvattu tarkemmin säännöksen perusteluissa. Kyberkestävyysasetuksen tarkoituksena parantaa digitaalisen elementin sisältävien tuotteiden kyberturvallisuutta sekä kuluttajien että yritysten kannalta. Tuotteet voivat aiheuttaa vakavia kyberturvallisuusriskejä ja riskin esimerkiksi ihmisten terveydelle tai turvallisuudelle. Tämän johdosta on oikeasuhtaista, että edellä mainituissa tilanteissa tarkastus voidaan suorittaa myös pysyväisluontoisen asumiseen käytettävissä tiloissa. Nämä edellytykset merkitsevät, että tarkastusta ei voitaisi suorittaa kotirauhan piirissä sellaisissa vähäisemmissä rikkomistapauksissa, joista seuraamusmaksua ei voitaisi määrätä tai joissa ei olisi kyse viimeksi mainituista seikoista.

Oikeasuhtaisuutta varmistaisi myös hallintolain 39 §:n soveltaminen. Sen mukaan tarkastus on suoritettava aiheuttamatta tarkastuksen kohteelle tai sen haltijalle kohtuutonta haittaa. Oikeasuhteisuutta varmistaisi lisäksi muun muassa hallintolain 6 §, jonka mukaan viranomaisen on käytettävä toimivaltaansa yksinomaan lain mukaan hyväksyttäviin tarkoituksiin ja toimien on oltava oikeassa suhteessa tavoiteltuun päämäärään nähden.

Ehdotettu sääntely täyttää siten perustuslakivaliokunnan käytännössä asetetut edellytykset, kun siinä edellytettäisiin välttämättömyyttä sekä konkreettista ja yksilöityä syytä ja tarkastusoikeus olisi kytketty toimintaan, josta voisi olla seuraamuksena rangaistusluontoinen hallinnollinen seuraamusmaksu, minkä lisäksi siinä varmistettaisiin toimenpiteen oikeasuhtaisuus.

Markkinavalvontalain 14 §:n 2 momentin mukaan ulkopuoliset asiantuntijat voivat markkinavalvontaviranomaisen apuna osallistua tämän lain mukaisiin tarkastuksiin. Ulkopuolisella asiantuntijalla ei siten olisi itsenäistä roolia tarkastuksen suorittamisessa. Laissa säädetään myös asiantuntijan rikosoikeudellisesta virkavastuusta. Perustuslakivaliokunta ei ole nähnyt estettä sille, että laissa säädetään viranomaiskoneiston ulkopuolelta nimetyn toimielimen oikeudesta avustaa tarkastuksen toimittamisessa (PeVL 42/2005 vp ja PeVL 46/2001 vp).

Edellä esitetty huomioon ottaen tarkastusoikeutta koskevien ehdotuksien arvioidaan täyttävän ne reunaehdot, joita perustuslakivaliokunnan käytännöstä aiheutuu kotirauhan piirissä tapahtuvan tarkastuksen suorittamiselle.

12.6 Viranomaisen tiedonsaanti- ja tiedonluovutusoikeudet sekä yksityisyyden suoja

Viranomaisen tiedonsaanti- ja tiedonluovutusoikeudet. Perustuslakivaliokunta on arvioinut usein tietojen saamista ja luovuttamista salassapitovelvollisuuden estämättä koskevan sääntelyn kattavuutta, täsmällisyyttä ja sisältöä (ks. esim. PeVL 89/2022 vp, kappale 12). Viranomaisen tietojensaantioikeus ja tietojenluovuttamismahdollisuus ovat valiokunnan mukaan voineet liittyä jonkin tarkoituksen kannalta tarpeellisiin tietoihin, jos tarkoitetut tietosisällöt on pyritty luettelemaan laissa tyhjentävästi. Jos taas tietosisältöjä ei ole samalla tavoin luetteloitu, sääntelyyn on pitänyt sisällyttää vaatimus tietojen välttämättömyydestä jonkin tarkoituksen kannalta (ks. esim. PeVL 8/2021 vp, kappale 24 ja siinä viitatut lausunnot).

Perustuslakivaliokunta on painottanut toistuvasti, että erottelussa tietojen saamisen tai luovuttamisen tarpeellisuuden ja välttämättömyyden välillä on kyse tietosisältöjen laajuuden ohella myös siitä, että tietoihin oikeutettu viranomainen omine tarpeineen syrjäyttää ne perusteet ja intressit, joita tiedot omaavaan viranomaiseen kohdistuvan salassapidon avulla suojataan. Mitä yleisluonteisempi tietojensaantiin oikeuttava sääntely on, sitä suurempi on vaara, että tällaiset intressit voivat syrjäytyä hyvin automaattisesti. Mitä täydellisemmin tietojensaantioikeus kytketään säännöksissä asiallisiin edellytyksiin, sitä todennäköisemmin yksittäistä tietojensaanti-pyyntöä joudutaan käytännössä perustelemaan. Myös tietojen luovuttajan on tällöin mahdollista arvioida pyyntöä luovuttamisen laillisten edellytysten

kannalta. Tietojen luovuttaja voi lisäksi kieltäytymällä tosiasiallisesti tietojen antamisesta saada aikaan tilanteen, jossa tietojen luovuttamisvelvollisuus eli säännösten tulkinta saattaa tulla ulkopuolisen viranomaisen tutkittavaksi. Tämä mahdollisuus on tärkeä tiedonsaannin ja salassapitointressin yhteensovittamiseksi (ks. esim. PeVL 7/2019 vp, s. 7, PeVL 48/2018 vp, s. 5 ja siinä viitatut lausunnot).

Esityksen 1. ja 3. lakiehdotuksessa säädettäisiin viranomaisten tiedonsaanti- ja tiedonluovutusoikeuksia, jotka voivat koskea salassa pidettäviä tietoja, kuten liikesalaisuuksia tai tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevia tietoja. Tiedot voisivat poikkeuksellisesti koskea myös yksityiselämän suojan alaan kuuluvia seikkoja. Näin ollen esitystä on arvioitava perustuslain 15 §:ssä säädetyn omaisuuden suojan ja 10 §:ssä säädetyn yksityiselämän suoja kannalta.

Ehdotetut tiedonsaanti- ja tiedonluovutusoikeudet olisivat pääosin kyberkestävyysasetuksen ja kyberturvallisuusasetuksen määrittelemien tehtävien edellyttämiä.

Esityksen 1. lakiehdotuksen 9 §:ssä säädettäisiin CSIRT-yksikön oikeudesta luovuttaa sen tiettyjen kyberkestävyysasetuksen mukaisten tehtävien yhteydessä saamiaan salassa pidettäviä tietoja näiden tehtävien toteuttamiseksi. Tiedonluovutusoikeus olisi sidottu pääsääntöisesti tarpeellisuusedellytykseen niin, että tiedonluovutusoikeuden kattamat tietotyypit seuraisivat kyberkestävyysasetuksen 14 artiklan 2, 4 ja 6 kohdista. Muiden näiden tehtävien hoidossa mahdollisesti saatujen tietojen luovuttaminen olisi sidottu välttämättömyysedellytykseen. Lakiehdotuksen 14 §:ssä puolestaan säädettäisiin ilmoittavan viranomaisen ja ilmoitetun laitoksen oikeudesta luovuttaa salassa pidettävää tietoa. Ilmoittavan viranomaisen tiedonluovutusoikeus olisi sidottu välttämättömyyteen pykälässä määriteltyjen tehtävien hoitamisen kannalta. Ilmoitetun laitoksen tiedonluovutusoikeus olisi puolestaan sidottu tarpeellisuusedellytykseen siten, että luovutettavat tiedot olisi määritelty koskemaan vaatimustenmukaisuuden arviointia ja tarkastuksen tuloksia. Ehdotuksen 18 §:n 1 momentissa ulotettaisiin markkinavalvontaviranomaisen markkinavalvontalain 11 ja 13 §:n mukainen tiedonluovutusoikeus kattamaan myös digitaalisia elementtejä sisältävän tuotteen vaatimustenmukaisuutta, turvajärjestelyjä sekä haavoittuvuutta ja tietoturvaan vaikuttavaa poikkeamaa koskeviin tietoihin. Markkinavalvontalaki on säädetty perustuslakivaliokunnan myötävaikutuksella (PeVL 36/2016 vp, TaVM 19/2016 vp). Ehdotettu laajennus tiedonluovutusoikeuden kattamiin tietotyyppeihin on välttämätön, koska kyberkestävyysasetuksen velvoitteet kohdistuvat niiden alaan. Ehdotuksen 18 §:n 2 momentissa säädettäisiin markkinavalvontaviranomaisen tiedonluovutusoikeudesta tietyille kotimaisille ja ulkomaisille viranomaisille niiden säädettyjä tehtäviä varten. Tiedonluovutusoikeus olisi sidottu välttämättömyyteen pykälässä määriteltyjen tehtävien hoitamisen kannalta. Ehdotuksen 26 §:ssä taas säädettäisiin kyberturvallisuuden sertifiointiviranomaisen oikeudesta luovuttaa salassa pidettäviä tietoja. Pykälän 1 ja 2 kohdan osalta tiedonluovutusoikeus olisi sidottu välttämättömyyteen kohdissa määriteltyjen tehtävien hoitamisen kannalta. Pykälän 3 kohdan osalta tiedonluovutusoikeus olisi puolestaan sidottu tarpeellisuusedellytykseen tiedot vastaanottavien viranomaisten tehtävien kannalta siten, että luovutettavat tietotyypit olisi lueteltu kohdassa. Ehdotukset tietojen luovuttamisesta CSIRT-yksikölle sen kyberturvallisuuslaissa säädettyjen tehtävien hoitamiseksi eivät ole suoraan kyberkestävyysasetuksen tai kyberturvallisuusasetuksen edellyttämiä, mutta CSIRT-yksikön tehtävien asianmukaisen hoitamisen voidaan katsoa edellyttävän mahdollisuutta näiden tietojen luovuttamiseen sille, sillä se edistää kyberturvallisuuden toteutumista.

Esityksen 3. lakiehdotuksen mukaisesti kyberturvallisuuslain 28 §:ään tehtävän muutoksen johdosta syntyvä tiedonluovutusoikeus olisi niin ikään sidottu välttämättömyyteen

Finanssivalvonnan eräiden sen laissa säädettyjen tehtävien kannalta. Tätä ehdotusta tarkastellaan lisäksi jäljempänä erikseen luottamuksellisen viestinnän suojan kannalta.

Esityksen 1. lakiehdotuksen 25 §:ssä säädettäisiin kyberturvallisuussertifioinnin viranomaisen tiedonsaantioikeudesta, joka olisi rajattu sen ehdotetussa laissa tai kyberturvallisuusasetuksessa säädettyjen tehtävien hoitamiseksi ja kyberturvallisuusasetuksen, sen nojalla annettujen säädösten ja tämän lain noudattamisen valvomiseksi välttämättömiin tietoihin. Tiedonsaantioikeus kohdistuisi vaatimustenmukaisuuden arviointilaitoksiin, eurooppalaisen kyberturvallisuussertifikaatin haltijoihin ja EU-vaatimustenmukaisuusilmoitusten antajiin. Tietotyyppejä ei ole tarkoituksenmukaista luetella tyhjentävästi tai rajata tiettyihin tilanteisiin, koska viranomaisen tiedonsaantitarpeet voivat olla moninaisia. Lisäksi ehdotuksen 39 §:n 4 momentissa säädettäisiin seuraamusmaksun määräävän viranomaisen oikeudesta saada seuraamusmaksun määräämiseksi tai sen määrän arvioimiseksi välttämättömät tiedot.

Näin ollen ehdotettavan sääntelyn voidaan katsoa täyttävän perustuslakivaliokunnan asettamat tiedonsaanti- ja tiedonluovutusoikeuksia koskevat sääntelyedellytykset tältä osin.

Henkilötietojen suoja. Perustuslain 10 §:n 1 momentin mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Yksityiselämän suojaan kohdistuvia rajoituksia on arvioitava kulloisessakin sääntely-yhteydessä perusoikeuksien yleisten rajoitusedellytysten valossa (esim. PeVL 42/2016 vp, s. 2–3). Euroopan unionin perusoikeuskirjan 8 artiklan mukaan henkilötietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Perusoikeuskirjan 52 artiklan 1 kohdan mukaan perusoikeuskirjassa tunnustettujen oikeuksien ja vapauksien käyttämistä voidaan rajoittaa ainoastaan lailla sekä kyseisten oikeuksien ja vapauksien keskeistä sisältöä kunnioittaen. Suhteellisuusperiaatteen mukaisesti rajoituksia voidaan säätää ainoastaan, jos ne ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.

Esityksen 1. ja 3. lakiehdotuksen mukaiset tiedonluovutus- ja tiedonsaantioikeuksia koskevat säännökset eivät sulkisi tiedonluovutuksen tai tiedonsaantioikeuden ulkopuolelle henkilötietoja, joskin tietojen luovutuksen kohteena olisivat henkilötietojen sijasta pääasiassa tekniset tiedot. Henkilötietoja voisi kuitenkin sisältyä esimerkiksi vaatimustenmukaisuuden arviointilaitokselta pyydettäviin selvityksiin, jotka voisivat koskea arviointilaitoksen henkilöstölle asetettujen vaatimusten täyttymistä. Siltä osin kuin ehdotettujen tiedonsaanti- ja tiedonluovutusoikeuksien käytön yhteydessä käsitellään henkilötietoja, tulee henkilötietojen käsittelyssä noudattaa tietosuojalainsäädäntöä, kuten yleistä tietosuoja-asetusta ja tietosuojalakia.

Perustuslakivaliokunnan mukaan henkilötietojen suoja tulee turvata ensisijaisesti yleisen tietosuoja-asetuksen ja säädettävän kansallisen yleislainsäädännön nojalla. Kansallisen erityislainsäädännön säätämiseen tulee siten suhtautua pidättyvästi ja rajata sellainen vain välttämättömään tietosuoja-asetuksen salliman kansallisen liikkumavaran puitteissa (ks. PeVL 14/2018 vp).

Kyseisten tiedonsaanti- ja tiedonluovutusoikeuksien osalta henkilötietojen käsittelyn oikeusperusteena olisi lähtökohtaisesti tietosuoja-asetuksen 6 artiklan 1 kohdan c alakohdassa tarkoitettu rekisterinpitäjän lakisääteinen velvoite. Esitys sisältäisi täydentävää sääntelyä henkilötietojen käsittelystä yleiseen tietosuoja-asetukseen ja tietosuojalakiin nähden. Ehdotettavassa laissa käytettäisiin yleisen tietosuoja-asetuksen 6 artiklan 2 ja 3 kohdan sallimaa kansallista liikkumavaraa määrittelemällä henkilötietojen käsittelyn oikeusperusta ja yhteisöt ja tarkoitukset, joita varten henkilötietoja voidaan luovuttaa. Henkilötietoja voitaisiin luovuttaa

vain, kun se olisi tapauksen mukaan välttämätöntä tai määriteltyjen tietotyyppien osalta tarpeellista viranomaisen tai julkista hallintotehtävää hoitavan yksityisen laissa säädettyjen tehtävien hoitamisen kannalta. Kyseiset tehtävät perustuvat pääosin Euroopan unionin lainsäädäntöön. Näin ollen ehdotettu sääntely täyttäisi yleisen tietosuoja-asetuksen 6 artiklan 3 kohdan edellytyksen siitä, että jäsenvaltion lainsäädännön on täytettävä yleisen edun mukainen tavoite ja oltava oikeasuhteinen sillä tavoiteltuun oikeutettuun päämäärään nähden.

Viestinnän luottamuksellisuus. Perustuslain 10 §:n 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.

Kolmannella lakiehdotuksella muutettaisiin kyberturvallisuuslain 28 §:n 4 momentissa säädettyä tiedonluovutusoikeutta koskemaan myös tiedon luovuttamista Finanssivalvonnalle kyberturvallisuuslain 26 §:ssä määriteltyjen valvovien viranomaisten lisäksi. Tiedonluovutusoikeus koskisi myös kyberturvallisuuslain 28 §:n 2 momentissa tarkoitettua välitystietoa, sijaintitietoa sekä tietoa haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä, johon valvovalla viranomaisella on ollut tiedonsaantioikeus siksi, että tieto on ollut välttämätön kyberturvallisuutta koskevan riskienhallintavelvoitteen noudattamisen tai merkittävistä poikkeamista ilmoittamisen ja raportoinnin valvomista varten. Perustuslakivaliokunta on pitänyt kyseistä sääntelyä perustuslain 10 §:n asettamien reunaehtojen kannalta mahdollisena, sillä haitallisen tietokoneohjelman tai käskyn sisältämän viestin voidaan katsoa jäävän kokonaan perustuslain 10 §:n luottamuksellisen viestin salaisuuden soveltamisalan ulkopuolelle ja kyseistä välitystietoihin kohdistuvaa tiedonsaantioikeutta voidaan pitää suhteellisen vähäisenä puuttumisena luottamuksellisen viestin salaisuuden suojaan, eikä se muodostu ongelmalliseksi perusoikeuksien yleisten rajoitusedellytysten mukaan (PeVL 62/2024 vp).

Ehdotus Finanssivalvonnan rinnastamisesta tässä suhteessa kyberturvallisuuslaissa määriteltyihin valvoviin viranomaisiin on perusteltu, jotta kaikki NIS 2 -direktiivin tarkoittamat toimivaltaiset viranomaiset olisivat tältä osin samassa asemassa. Kyberturvallisuuslaissa ei tällä hetkellä säädetä Finanssivalvonnan tehtävistä tai tiedonvaihdosta sen ja kyberturvallisuuslain 26 §:ssä määriteltyjen valvovien viranomaisten välillä, sillä vaikka sen täytäntöön panema NIS 2 -direktiivi sisältää Finanssivalvonnan valvomiin toimialoihin kohdistuvaa sääntelyä, EU:n DORA-asetus on toimijoiden velvoitteiden osalta erityissäädös suhteessa NIS 2 -direktiiviin. Finanssivalvonnasta annetun lain mukaisesti Finanssivalvonta kuitenkin toimii NIS 2 -direktiivin mukaisena toimivaltaisena viranomaisena samoin kuin DORA-asetuksen mukaisena toimivaltaisena viranomaisena.

Edellä esitetyn perusteella viranomaisten tiedonvaihtoa ja tiedonluovutusoikeuksia koskevien ehdotuksien arvioidaan täyttävän perustuslain asettamat reunaehdot.

12.7 Seuraamussääntely

Ensimmäisen lakiehdotuksen 6 luvussa säädettäisiin kyberkestävyysasetuksen edellyttämällä tavalla hallinnollisen seuraamusmaksun määräämisestä toimijalle, joka rikkoo kyberkestävyysasetuksen asettamia velvoitteita. Lisäksi luku sisältäisi kyberturvallisuusasetuksen rikkomisesta määrättävän seuraamusmaksun, miltä osin esitys sisältää kansallista liikkumavaraa. Ehdotetuissa seuraamusmaksuissa olisi kysymys

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 ja PeVL 9/2012 vp, s. 2). Perustuslain 2 §:n 3 momentin 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 teoista tai laiminlyönneistä, jotka voisivat 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 (PeVL 14/2018 vp).

Hallintoviranomaisen toiminnassa on asian käsittelyssä noudatettava perustuslain 21 §:n 2 momentin mukaisia hyvän hallinnon takeita, joita ovat muun muassa käsittelyn julkisuus, oikeus tulla kuulluksi ja saada perusteltu päätös sekä oikeus hakea muutosta. Perustuslain mukaan hyvän hallinnon takeet turvataan lailla.

Kyberkestävyysasetuksen rikkomisesta johtuvan seuraamusmaksun määräisi ehdotuksen mukaan pääsääntöisesti Liikenne- ja viestintävirasto. Liikenne- ja viestintävirastosta annetun lain 7 a §:n mukaan Liikenne- ja viestintävirastossa on seuraamuskollegio, jonka tehtävänä on määrätä viraston toimivaltaan kuuluva seuraamusmaksu silloin, kun se on suuruudeltaan yli 100 000 euroa. Seuraamuskollegio tekee päätöksensä esittelystä. Laissa on säännökset kollegion perehtyneisyyttä, asiantuntemusta, riippumattomuutta ja puolueettomuutta koskien. Lisäksi ehdotuksen mukaan silloin, kun markkinavalvontaviranomaisena toimii poikkeuksellisesti eräiden tekoälyjärjestelmien valvonnasta annetun lain 3 §:ssä tarkoitettu markkinavalvontaviranomainen, hallinnollinen seuraamusmaksu määrättäisiin mainitun lain 13 §:ssä säädetyssä järjestyksessä. Tämä tarkoittaisi, että seuraamusmaksun määrääminen ohjautuisi kyseisessä laissa säädetyn euromäärän ylittävien seuraamusmaksujen osalta monijäseniselle tekoälyjärjestelmien valvonnan seuraamusmaksulautakunnalle taikka

tietosuojalaissa tarkoitetulle seuraamuskollegiolle. Ehdotus täyttää tältä osin perustuslakivaliokunnan käytännössä asetetut menettelylle asetetut vaatimukset.

Liikenne- ja viestintävirasto määräisi myös kyberturvallisuussertifiointia koskevan seuraamusmaksun kansallisen kyberturvallisuuden sertifiointiviranomaisen roolissa. Koska seuraamusmaksun enimmäismäärä olisi tällöin 100 000 euroa, ei tällainen seuraamusmaksu kuuluisi Liikenne- ja viestintävirastosta annetun lain 7 a §:n nojalla seuraamuskollegion ratkaisuvaltaan. Voidaan arvioida, että kyseinen seuraamusmaksu ei edellytä sen ohjaamista monijäsenisen toimielimen ratkaistavaksi, sillä sitä ei tule pitää enimmäismäärältään suurena ja huomattavan ankarana ottaen huomioon, että kyse on elinkeinotoiminnasta ja että sertifiointi on lähtökohtaisesti vapaaehtoista.

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 ja PeVL 17/2012 vp, s. 6). Ehdotuksessa arvioidaan säädettävän näistä seikoista riittävällä tasolla.

Koska etenkin kyberkestävyysasetuksessa edellytetyt hallinnolliset seuraamusmaksut ovat enimmäismäärältään huomattavia, on erityistä huomiota perustuslakivaliokunnan käytännön mukaisesti kiinnitettävä oikeusturvalle asetettaviin vaatimuksiin (PeVL 14/2018 vp, s. 18). Seuraamusmaksun enimmäismäärä määriteltäisiin 1. lakiehdotuksen 38 §:ssä. Seuraamusmaksun määrä perustuisi 38 §:n mukaan kokonaisarviointiin, jossa olisi huomioitava pykälässä säädetyt seikat. Seuraamusmaksua koskevaan päätökseen haettaisiin muutosta valittamalla oikeudenkäynnistä hallintoasioissa säädetyssä järjestyksessä. 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 40 §:ssä, jonka tarkoituksena on varmistaa, että seuraamusmaksua ei määrättäisi niissä tilanteissa, joissa se olisi ilmeisen kohtuutonta. Seuraamusmaksua koskevaa päätöstä ei voitaisi ehdotuksen 43 §:n nojalla määrätä noudatettavaksi muutoksenhausta huolimatta. Tämän voidaan arvioida turvaavan oikeusturvajärjestelyiden asianmukaisuutta (PeVL 4/2004 vp, s. 7–8).

Kyberturvallisuusasetuksen 65 artiklan mukaan jäsenvaltioiden on annettava säännöt seuraamuksista, joita sovelletaan asetuksen kyseisen osaston ja eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien säännösten rikkomiseen, ja toteutettava kaikki tarvittavat toimenpiteet sen varmistamiseksi, että ne pannaan täytäntöön. Säädettyjen seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia. Muutoin seuraamussääntely jää jäsenvaltion kansalliseen liikkumavaraan, kunhan vilpittömän yhteistyön periaatteesta juontuvat unionioikeuden täytäntöönpanon yleiset vaatimukset täyttyvät (vastaavuus- ja tehokkuusperiaate). Tämä merkitsee muun muassa sitä, että jäsenvaltiot voivat lähtökohtaisesti päättää, toteutetaanko seuraamukset hallinnollisina seuraamuksina vai rikosoikeudellisina rangaistuksina. Ehdotuksessa säädettäisiin hallinnollisesta seuraamusmaksusta, joka voitaisiin määrätä kyberturvallisuussertifiointia koskevista rikkomuksista (1. lakiehdotuksen 37 §).

Hyväksyttävyys ja viimesijaisuus. Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien tarkoituksena on lisätä kyberturvallisuuden tasoa unionissa. Niiden on tarkoitus vahvistaa, että arvioidut tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit ovat niille määritettyjen turvallisuusvaatimusten mukaisia, jotta voidaan suojella tietojen tai toimintojen tai palvelujen käytettävyyttä, aitoutta, eheyttä ja luottamuksellisuutta niiden koko elinkaaren ajan (kyberturvallisuusasetuksen johdanto-osan kappale 95 ja 46 artikla). Tuotteiden kyberturvallisuusriskit voivat muun muassa vaarantaa henkilötietojen ja viestinnän

luottamuksellisuuden. Nämä tavoitteet kytkeytyvät perustuslain 10 §:ssä turvattuun yksityiselämän suojaan. Ne ovat hyväksyttäviä tavoitteita seuraamussääntelylle. Ne niin ikään puoltavat kansallisen liikkumavaran käyttämistä seuraamuksista säätämiseksi. Ehdotetun sääntelyn tarkoituksena on varmistaa, että säännöksiä noudatetaan ja toiminnan harjoittamiselle asetetut velvoitteet täytetään. Sääntely edesauttaisi erityis- ja yleispreventiota. Valvonnan tehokkuuden ja toimivuuden kannalta lievempiä seuraamuksia ei voida pitää riittävinä ottaen huomioon edellä mainitut hyväksyttävät tavoitteet sekä kyberturvallisuuden keskeinen merkitys yhteiskunnassa.

Rikosoikeudellisen rangaistuksen käyttöön tulee ultima ratio -periaatteen mukaisesti turvautua vasta viimesijaisena keinona. Kansallista seuraamuslajia valittaessa on noudatettava niin kutsuttua vastaavuusperiaatetta. Periaatteen mukaan jäsenvaltioiden on huolehdittava siitä, että seuraamus EU-oikeuden rikkomisesta määritellään perusteiltaan ja menettelyiltään vastaavalla tavalla kuin kansallisen oikeuden samanlainen ja vakavuudeltaan rinnastettava rikkominen.

Edellä luvussa 5.1.35.1.2 on kuvattu ne perusteet, joihin ehdotettu kyberturvallisuussertifiointia koskevan rikkomuksen sanktioinnin enimmäismäärä perustuu. Valmistelussa on arvioitu, että hallinnollinen sanktio on vastaavuusperiaatteen mukainen ratkaisu ja rikosoikeudellista sanktiota soveliaampi seuraamus kyberturvallisuusasetuksen rikkomisesta.

Itsekriminointisuoja. Euroopan ihmisoikeustuomioistuimen käytännön mukaan itsekriminointisuoja ei estä tai rajoita sellaisia lakiin perustuvia hallinnollisia valvontamenettelyjä, joissa henkilön edellytetään antavan tietoja tai selvityksiä esimerkiksi verotusta, elinkeinovalvontaa tai ympäristönsuojelua varten (PeVL 39/2014 vp).

Syyttömyysolettama. Ehdotus ei olisi syyttömyysolettaman kannalta ongelmallinen, sillä se ei perustu tuottamuksesta riippumattomaan vastuuseen (ks. PeVL 9/2018 vp, s. 4). Seuraamusmaksun määräämisen edellytyksenä olisi kyberkestävyysasetusta tai kyberturvallisuusasetusta rikkovan teon tai laiminlyönnin johtuminen toimijan tahallisesta tai huolimattomasta menettelystä.

Kaksoisrangaistavuuden kielto. Ehdotettu seuraamusmaksu ei olisi ongelmallinen kaksoisrangaistavuuden kiellon kannalta. 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 ja PeVL 14/2013 vp, s. 2). Kiellon soveltamisala ulottuu Euroopan ihmisoikeustuomioistuimen ratkaisukäytännössä myös rangaistusluonteisiin hallinnollisiin seuraamuksiin (PeVL 9/2012 vp, s. 3). Kaksoisrangaistavuuden kielto on voimassa yleisenä oikeusperiaatteena, eikä siitä ole tarve säätää erikseen. Päällekkäisten menettelyjen mahdollisuutta eri säännöstöjen nojalla ei voida kuitenkaan täysin sulkea pois. Unionin tuomioistuimen mukaan menettelyjen ja seuraamusten päällekkäisyyden mahdollisuus on perusoikeuskirjan 50 artiklan olennaisen sisällön mukainen edellyttäen, ettei kansallisessa säännöstössä sallita menettelyjen aloittamista ja seuraamusten määräämistä samoista teoista saman rikkomisen perusteella tai saman tavoitteen saavuttamiseksi, vaan siinä säädetään yksinomaan, että päällekkäiset menettelyt ja seuraamukset ovat mahdollisia eri säännöstöjen nojalla (asia C-117/20 bpost, 43 kohta ja asia C- 412/21 Dual Prod SRL, 63 kohta). Lisäksi on oltava selkeitä ja täsmällisiä sääntöjä, joiden perusteella voidaan ennakoida, mitkä toimet ja laiminlyönnit voivat olla menettelyjen ja seuraamusten päällekkäisyyden kohteena (asia C-117/20 bpost, 51 kohta, asia C-412/21 Dual Prod SRL, 67 kohta ja asia C-205/23 Engie Romania, 66 kohta).

Esityksen 1. lakiehdotuksessa periaate on huomioitu 40 §: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.

Kyberturvallisuussertifiointia koskevaa seuraamusmaksua ei saisi ehdotuksen mukaan määrätä myöskään sille, jolle on samasta teosta määrätty kyberkestävyysasetuksen rikkomisesta seuraamusmaksu. Kyberturvallisuusasetus ei rajoita kyberkestävyysasetuksen tai esimerkiksi tietosuojasääntelyn soveltamista seuraamuksineen. Kyberkestävyysasetuksen ja kyberturvallisuusasetuksen tavoitteita voidaan pitää siinä määrin samanlaisina, että on perusteltua säätää ehdotetulla tavalla kansallisen liikkumavaran puitteissa siitä, ettei toista seuraamusmaksua voitaisi määrätä saman teon perusteella enää kyberturvallisuussertifiointia koskevasta rikkomuksesta. Ehdotettu säännös on selkeä ja täsmällinen, ja sen perusteella voidaan ennakoida, mitkä toimet ja laiminlyönnit voivat olla menettelyjen ja seuraamusten päällekkäisyyden kohteena.

Yleisen tietosuoja-asetuksen tavoitteet voivat olla eräissä tilanteissa samansuuntaisia kyberturvallisuusasetuksen kanssa, sillä yleinen tietosuoja-asetus edellyttää rekisterinpitäjiä huolehtimaan henkilötietojen käsittelyn turvallisuudesta (32 artikla) sekä sisältää säännökset sertifiointimekanismeista sekä tietosuojasineteistä ja -merkeistä, joiden tarkoituksena on osoittaa, että rekisterinpitäjät ja henkilötietojen käsittelijät noudattavat kyseistä asetusta käsittelytoimia suorittaessaan, kuten kyberturvallisuusasetuksen johdanto-osan kappaleessa 74 todetaan. Viimeksi mainitun mukaan kyberturvallisuusasetus ei rajoita tietojenkäsittelytoimintojen sertifiointia asetuksen (EU) 2016/679 mukaisesti, ei myöskään silloin, kun nämä toimet on sisällytetty tieto- ja viestintätekniikan tuotteisiin, palveluihin ja prosesseihin. Lähtökohtaisesti kyberturvallisuusasetuksen ja tietosuoja-asetuksen mukaisilla sertifiointimekanismeilla voidaan kuitenkin katsoa olevan omat erilliset tavoitteensa. Tapauskohtaisesti on kuitenkin varmistuttava, että viranomaisten vireille panemilla menettelyillä pyritään toisiaan täydentäviin päämääriin, jotka liittyvät kyseessä olevan saman rangaistavan teon eri ulottuvuuksiin (asia C-117/20 bpost, 50 kohta).

Viranomaisia koskevat seuraamukset. Tietosuojalakia koskevan hallituksen esityksen mukaan viranomaiselle määrättävä hallinnollinen seuraamusmaksu on yleisen oikeusjärjestyksemme kannalta vieras menettely. Oikeusjärjestys kohdistaa julkishallintoon muita erityisvaatimuksia, jotka osaltaan perustelevat tätä sääntelyratkaisua (HE 14/2018 vp, s. 20). Perustuslakivaliokunta on katsonut, että seuraamusmaksusääntelyn ulottaminen viranomaistoimintaan ei ole valtiosääntöisesti ongelmatonta (ks. PeVL 14/2018 vp ja PeVL 13/2023 vp). Perustuslakivaliokunta on sittemmin arvioidessaan valtioneuvoston kirjelmää ehdotuksesta tekoälyasetukseksi painottanut sen merkitystä, että hallinnollisten sanktioiden osalta tulisi pyrkiä varmistamaan riittävä kansallinen liikkumavara erityisesti sen huomioimiseksi, että Suomessa ei voida määrätä hallinnollisia seuraamusmaksuja viranomaisille, sillä viranomaisille voidaan määrätä ainoastaan rikosoikeudellisia seuraamuksia (ks. PeVL 37/2021 vp, kappale 40). Näin ollen esityksen 40 §:n 4 momentissa säädettäisiin niistä julkisoikeudellisista toimijoista, joille ei voitaisi määrätä seuraamusmaksuja.

Oikeasuhtaisuus. Perustuslakivaliokunta on pitänyt hallinnollisten sanktioiden oikeasuhtaisuuden kannalta merkittävinä paitsi säännöksiä sanktioiden euromääräisestä suuruudesta myös säännöksiä seuraamuksen suuruuden määräytymisessä huomioon otettavista seikoista ja seuraamusmaksun määräämättä jättämisestä. Valiokunta on myös käytännössään edellyttänyt, että viranomaisen harkinnan sanktion määräämättä jättämisestä tulee olla sidottua harkintaa siten, että seuraamusmaksu on jätettävä määräämättä laissa säädettyjen edellytysten täyttyessä. (PeVL 46/2021 vp, 17 kohta viittauksineen.) Ehdotettu pykälä

kyberturvallisuussertifiointia koskevasta seuraamusmaksusta olisi oikeasuhtainen. Kyberkestävyysasetuksen osalta seuraamusmaksujen enimmäismäärät määritellään kyseissä säädöksessä.

Ehdotus sisältäisi säännökset seuraamusmaksun enimmäismäärästä samoin kuin seuraamusharkinnassa huomioon otettavista seikoista. Kyberturvallisuussertifiointia koskevan seuraamusmaksun ankaruustaso on määritelty suhteessa sanktioitavien tekojen moitittavuuteen ja suojeltavaan oikeushyvään, ja seuraamusmaksu kohdistuu elinkeinonharjoittajiin, käytännössä oikeushenkilöihin. Seuraamusmaksun määrääminen olisi hallintoasian käsittelyä, johon sovelletaan hallintolakia (PeVL 32/2005 vp, s. 3/II). Ehdotetussa 40 §:ssä olisi myös säädetty, milloin seuraamusmaksua ei tulisi määrätä.

Täsmällisyys. Perustuslakivaliokunta on katsonut, että vaikka perustuslain 8 §:n rikosoikeudellisen laillisuusperiaatteen täsmällisyysvaatimus ei sellaisenaan kohdistu hallinnollisten sanktioiden sääntelyyn, ei tarkkuuden yleistä vaatimusta kuitenkaan voida tällaisen sääntelyn yhteydessä sivuuttaa (PeVL 9/2012 vp, PeVL 74/2002 vp ja PeVL 57/2010 vp). Ehdotetuissa seuraamusmaksuja koskevissa säännöksissä luonnehdittaisiin sanktioitavat teot ja laiminlyönnit, ja säännöksistä kävisi yksiselitteisesti ilmi, mistä lainsäädännön vastaisista teoista tai laiminlyönneistä voi olla seuraamuksena sanktio.

Hallinnollisia seuraamusmaksuja koskevien ehdotuksien arvioidaan täyttävän perustuslakivaliokunnan lausuntokäytännössä sekä niistä johdetuissa hallinnollisten seuraamusmaksujen sääntelyperiaatteissa hallinnollisille seuraamuksille asetetut edellytykset.

12.8 Ahvenanmaan asema ja suhde itsehallintoon

Esitys jakautuu osin valtakunnan ja osin maakunnan lainsäädäntövaltaan. Ahvenanmaan itsehallintolain (1144/1991) 18 ja 27 §:ssä säädetään valtakunnan ja Ahvenanmaan maakunnan välisestä toimivallan jaosta. Ahvenanmaan maakuntalakien esittelyssä 27.6.2025 tasavallan presidentille tapahtuneen lainsäädäntövalvonnan yhteydessä on korkeimmalta oikeudelta (13.6.2025 KKO-HD/442/2025) ja Ahvenanmaan valtuuskunnalta (26.5.2025 Nr 22/25) saaduissa lausunnoissa todettu, että kyberturvallisuutta tai vastaavaa käsitettä ei mainita maakunnan ja valtakunnan välisessä lainsäädäntövallan jaossa itsehallintolaissa. Lainsäädäntövaltaa tulisikin arvioida niiden oikeudenalojen näkökulmasta, joita maakuntalainsäädäntö koskee. Ahvenanmaan itsehallintolain 59 b §:ssä säädetään Euroopan unionissa tehtyjen päätösten täytäntöönpanosta. Vastuu Euroopan unionin lainsäädännön täytäntöönpanossa jakautuu itsehallintolaissa säädetyn toimivallanjaon mukaisesti. Maakunta vastaa Euroopan unionin säädösten täytäntöönpanosta siltä osin kuin asia itsehallintolain mukaan kuuluu sen toimivaltaan.

Ahvenanmaan itsehallintolain 59 b §:n 3 momentin mukaan, jos jäsenvaltio yhteisön oikeuden mukaan voi nimetä vain yhden hallintoviranomaisen sellaisessa tilanteessa, jossa sekä maakunnalla että valtakunnalla olisi toimivaltaa, viranomaisen nimeäminen kuuluu valtakunnalle. Tämän viranomaisen sellainen päätös, joka muutoin kuuluisi maakunnan toimivaltaan, tulee tehdä maakunnan hallituksen esittämän kannan mukaisesti. Aiemmassa arviossa kansallisen kyberturvallisuussertifioinnin nimeämisen on katsottu kuuluneen valtakunnan toimivaltaan sillä perusteella, että kyberturvallisuusasetus olisi edellyttänyt yhden kansallisen viranomaisen nimeämistä (hallituksen esitys eduskunnalle laiksi sähköisen viestinnän palveluista annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi HE 98/2020 vp, s. 320). Koska kyberturvallisuusasetus samoin kuin kyberkestävyysasetus kuitenkin mahdollistavat useammankin kuin yhden viranomaisen nimeämisen, ei valtion ja maakunnan toimivallan jakautumista voida ratkaista itsehallintolain 59 b §:n 3 momentin perusteella.

Standardisointi kuuluu valtakunnan lainsäädäntövaltaan (itsehallintolain 27 §:n 19 kohta). Tämän johdosta siltä osin kuin säädökset sisältävät standardisointiin liittyviä viranomaistehtäviä, kuuluvat ne valtakunnan lainsäädäntövaltaan.

Itsehallintolain 18 §:n 22 kohdan maakunnan lainsäädäntövaltaan kuuluvat eräin rajoituksin elinkeinotoimintaa koskevat asiat samoin kuin 25 kohdan mukaan asiat, jotka koskevat teon rangaistavaksi säätämistä ja rangaistuksen määrää, kun on kysymys maakunnan lainsäädäntövaltaan kuuluvasta oikeudenalasta, ja 26 kohdan mukaan uhkasakon asettamista ja tuomitsemista sekä muiden pakkokeinojen käyttöä, kun on kysymys maakunnan lainsäädäntövaltaan kuuluvasta oikeudenalasta. Kyberturvallisuus ja tietoturvallisuus liittyvät siihen lainsäädäntövaltaan, mihin kutakin toimialaa koskeva lainsäädäntövalta kuuluu (vastaavasti HE 57/2024 vp, s. 271). Kyberkestävyysasetuksen ja kyberturvallisuusasetuksen valvontaan ja sertifiointeihin liittyvien viranomaistehtävien ja seuraamusten voidaan siten arvioida lähtökohtaisesti kuuluvan maakunnan toimivaltaan. Kyberkestävyysasetuksen ja kyberturvallisuusasetuksen horisontaaliset soveltamisalat ovat tässä suhteessa kuitenkin ongelmallisia valtakunnan ja maakunnan lainsäädäntötoimivallan alan määrittämisen suhteen.

Kuluttajansuoja (itsehallintolain 27 §:n 10 kohta) kuuluu valtakunnan lainsäädäntövaltaan. Kuluttajansuojanäkökohdat eivät kuitenkaan ole määräviä niin kyberkestävyysasetuksessa kuin kyberturvallisuusasetuksessakaan, eikä kumpikaan säädöksistä rajoitu kuluttajansuojan alaan. Kyberkestävyysasetuksessa säädetyillä olennaisilla kyberturvallisuusvaatimuksilla tosin suojataan kuluttajia ja organisaatioita kyberturvallisuusriskeiltä, ja siten niillä myös pyritään osaltaan parantamaan yksittäisten henkilöiden henkilötietojen ja yksityisyyden suojaa (johdanto-osa, kohta 32). Vastaavasti kyberturvallisuusasetuksessa esimerkiksi todetaan, että yrityksillä ja yksittäisillä kuluttajilla olisi oltava tarkat tiedot varmuustasosta, jolla tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien turvallisuus on sertifioitu (johdanto-osan kohta 10). Sertifiointijärjestelmät voivat periaatteessa kohdistua niin yritys- kuin kuluttajatuotteisiinkin.

Kuluttajaturvallisuusasioiden on puolestaan katsottu kuuluvan maakunnan lainsäädäntövaltaan, kun on ollut kyse kuluttajatuotteiden tuoteturvallisuudesta (HE 195/2022 vp, s. 47). Kuluttajaturvallisuutta koskevassa sääntelyssä on katsottu olevan kyse asioista, jotka itsehallintolain 18 §:n 6 (yleinen järjestys ja turvallisuus), 12 (terveyden- ja sairaanhoito) ja 22 (elinkeinotoiminta) kohtien mukaan kuuluvat Ahvenanmaan maakunnan lainsäädäntövaltaan. Kyberkestävyysasetus on horisontaalisesta soveltamisalastaan ja markkinavalvontasäädöksille uudentyyppisestä sääntelykohteestaan huolimatta kuitenkin luonteeltaan tuoteturvallisuussäädös, joten ainakin sen voidaan tällä perusteella katsoa kuuluvan lähtökohtaisesti maakunnan lainsäädäntövaltaan. Kyberturvallisuusasetuksen mukaiset eurooppalaiset kyberturvallisuussertifikaatit ja vaatimustenmukaisuusilmoitukset tulevat arvion mukaan olemaan tärkeitä myös kyberkestävyysasetuksen vaatimusten täyttämisessä. Kyberturvallisuusasetuksessa on myös samankaltaisia piirteitä kuin markkinavalvontasääntelyssä, joten sen arvioidaan samoin kuuluvan lähtökohtaisesti maakunnan lainsäädäntövaltaan samoilla perusteluilla kuin tuoteturvallisuussääntelyn, sillä kyse voidaan katsoa olevan yleiseen järjestykseen ja turvallisuuteen sekä etenkin elinkeinotoimintaan liittyvistä seikoista.

Poikkeuksena ovat kuitenkin tilanteet, joissa on kyse valtakunnan lainsäädäntövaltaan kuuluvasta elinkeinotoiminnan sääntelystä. Itsehallintolain 27 §:n 40 kohdan mukaan teletoimintaa koskevissa asioissa lainsäädäntövalta kuuluu valtakunnalle. Sähköisen viestinnän palveluista annetun lain 30 luvun (radiolaitteiden vaatimustenmukaisuus ja markkinavalvonta) osalta radiolaitteita koskevan sääntelyn on teletoimintana katsottu itsehallintolain 27 §:n 40 kohdan nojalla kuuluvan valtakunnan lainsäädäntövaltaan (HE 79/2023 vp, s. 30), vaikka

radiolaitteiden markkinoille saattaminen tai asettaminen saataville markkinoilla eivät ole varsinaista teletoimintaa. Tämän johdosta on vastaavasti katsottava, että kyberkestävyysasetuksen ja kyberturvallisuusasetuksen täytäntöönpano Suomessa kuuluu radiolaitteiden samoin kuin muidenkin teletoimintaan liittyvien laitteiden osalta valtakunnan toimivaltaan.

Myös verkkotunnuksia koskevien asioiden katsotaan kuuluvan valtakunnan lainsäädäntövaltaan (hallituksen esitys eduskunnalle laiksi verkkotunnuslain muuttamisesta HE 151/2005 vp, s. 2).

12.9 Lainsäädäntövallan siirtäminen viranomaiselle

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. Valtuutuksen tulee olla soveltamisalaltaan täsmällisesti rajattu. Perustuslakivaliokunnan lausuntokäytännön mukaan erityinen syy säätää viranomaisen määräystenantovallasta on muun muassa tekninen ja vähäisiä yksityiskohtia koskeva sääntely (PeVL 52/2001 vp ja PeVL 46/2001 vp), joka ei sisällä merkittävää harkintavallan käyttöä (PeVL 43/2000 vp).

Kyberkestävyysasetuksen 33 artiklan 2 kohdan mukaan jäsenvaltiot voivat tarvittaessa perustaa kyberkestävyyden sääntelyn testiympäristöjä. Kyberkestävyysasetuksen toimeenpanoa koskevan lakiehdotuksen 10 §:ssä säädetään Liikenne- ja viestintävirastolle asetettavasta testiympäristön perustamista koskevasta määräyksenantovaltuudesta. Ehdotetuissa määräyksenantovaltuuksissa on kyse teknisestä sääntelystä, joka ei sisällä merkittävää harkintavallan käyttöä. Testiympäristöjen perustaminen olisi viranomaisen harkinnassa, ja niihin osallistuminen olisi talouden toimijalle vapaaehtoista. Sääntelyn asiallinen merkitys ei muutoinkaan edellytä, että asiasta säädettäisiin lailla tai asetuksella.

Sähköisen viestinnän palveluista annettuun lakiin ehdotettu uusi 21 a luku sisältäisi määräyksenantovaltuuden liittyen tietojen ilmoittamisesta verkkotunnusvälittäjien toimijaluetteloa varten. Ehdotus olisi samansisältöinen kuin kyberturvallisuuslain 41 §:n 4 momentin sisältämä määräyksenantovaltuus, jonka suhdetta perustuslakiin on arvioitu hallituksen esityksessä eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi (HE 57/2024 vp, s. 266–267) ja joka on säädetty perustuslakivaliokunnan myötävaikutuksella (PeVL 62/2024 vp). Voimassa olevan 21 luvun määräyksenantovaltuuksien alaan tulisivat muiden muutosten johdosta myös verkkotunnusvälittäjien puolesta toimivat tahot, millä ei arvioida olevan vaikutusta määräyksenantovaltuuden valtiosääntöiseen arviointiin.

Esitetyt valtuutussäännökset ovat tarkkarajaisia, yksityiskohtaisia ja soveltamisalaltaan täsmällisesti rajattuja, ja ne täyttävät perustuslain 80 §:n 2 momentin edellytykset.

Edellä mainituilla perusteilla ehdotukset voidaan käsitellä tavallisessa lainsäätämisjärjestyksessä.

Ponsi

Koska kyberkestävyysasetuksessa ja kyberturvallisuusasetuksessa on säännöksiä, joita ehdotetaan täydennettäviksi lailla, ja koska NIS 2 -direktiivissä on säännöksiä, jotka ehdotetaan pantaviksi täytäntöön lailla, annetaan eduskunnan hyväksyttäviksi seuraavat lakiehdotukset:

1.

Laki

eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista

Eduskunnan päätöksen mukaisesti säädetään:

1 luku

Yleiset säännökset

1 §

Lain tarkoitus

Tällä lailla täsmennetään ja täydennetään digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) N:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta annettua Euroopan parlamentin ja neuvoston asetusta (EU) 2024/2847 (kyberkestävyyssäädös), jäljempänä *kyberkestävyysasetus*, ja sen kansallista soveltamista.

Tällä lailla täsmennetään ja täydennetään Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta annettua Euroopan parlamentin ja neuvoston asetusta (EU) 2019/881 (kyberturvallisuusasetus), jäljempänä *kyberturvallisuusasetus*, ja sen kansallista soveltamista.

2 §

Määritelmät

Tässä laissa tarkoitetaan:

1) *digitaalisia elementtejä sisältävällä tuotteella* ohjelmisto- tai laitteistotuotetta ja sen ratkaisuja datan etäkäsittelystä;

2) *ilmoitetulla laitoksella* Suomen viranomaisen nimeämää ja Euroopan komissiolle kyberkestävyysasetuksen 43 artiklan nojalla ilmoitettua Suomeen sijoittautunutta vaatimustenmukaisuuden arviointilaitosta;

3) *jakelijalla* sellaista muuta toimitusketjuun kuuluvaa luonnollista tai oikeushenkilöä kuin valmistajaa tai maahantuojaa, joka asettaa digitaalisia elementtejä sisältävän tuotteen saataville Euroopan unionin markkinoilla vaikuttamatta sen ominaisuuksiin;

4) *maahantuojalla* Euroopan unioniin sijoittautunutta luonnollista tai oikeushenkilöä, joka saattaa markkinoille digitaalisia elementtejä sisältävän tuotteen, jossa on Euroopan unionin ulkopuolelle sijoittautuneen luonnollisen tai oikeushenkilön nimi tai tavaramerkki;

5) *valmistajalla* luonnollista tai oikeushenkilöä, joka kehittää tai valmistaa digitaalisia elementtejä sisältäviä tuotteita tai suunnitteluttaa, kehityttää tai valmistuttaa digitaalisia elementtejä sisältäviä tuotteita ja pitää niitä kaupan omalla nimellään tai tavaramerkillään joko maksua vastaan, ansaintatarkoituksessa tai maksutta;

6) *valtuutetulla edustajalla* Euroopan unioniin sijoittautunutta luonnollista tai oikeushenkilöä, jolla on valmistajan antama kirjallinen toimeksianto hoitaa valmistajan puolesta tietyt tehtävät;

7) *talouden toimijalla* sellaista valmistajaa, valtuutettua edustajaa, maahantuojaa, jakelijaa ja muuta luonnollista tai oikeushenkilöä, jota koskevat kyberkestävyysasetuksen mukaiset digitaalisia elementtejä sisältävien tuotteiden valmistamiseen tai markkinoilla saataville asettamiseen liittyvät velvoitteet;

8) *avoimen lähdekoodin ohjelmistovastaavalla* sellaista muuta oikeushenkilöä kuin valmistajaa, jonka tarkoituksena tai tavoitteena on järjestelmällisesti ja pitkäjänteisesti tarjota tukea sellaisten tiettyjen digitaalisia elementtejä sisältävien tuotteiden kehittämistä varten, jotka luokitellaan kyberkestävyysasetuksen 3 artiklan 48 kohdassa tarkoitetuiksi vapaiksi ja avoimen lähdekoodin ohjelmistoiksi ja jotka on tarkoitettu kaupalliseen toimintaan, ja joka varmistaa kyseisten tuotteiden toimintakelpoisuuden;

9) *vaatimustenmukaisuuden arviointilaitoksella* elintä, joka suorittaa vaatimustenmukaisuuden arviointitoimia kuten kalibrointia, testausta, sertifiointia ja tarkastuksia;

10) *akkreditoinnilla* kansallisen akkreditointielimen antamaa todistusta siitä, että vaatimustenmukaisuuden arviointilaitos täyttää tiettyä vaatimustenmukaisuuden arviointia koskevat, yhdenmukaistetuilla standardeilla vahvistetut vaatimukset, ja tarvittaessa muut vaatimukset, mukaan luettuna ne, jotka on vahvistettu asiaa koskevissa alakohtaisissa ohjelmissa;

11) *CSIRT-yksiköllä* kyberturvallisuuslain (124/2025) 19 §:ssä tarkoitettua yksikköä;

12) *kyberturvallisuussertifiointia varten ilmoitetulla vaatimustenmukaisuuden arviointilaitoksella* kyberturvallisuusasetuksen 61 artiklan mukaisesti Euroopan komissiolle ilmoitettua vaatimustenmukaisuuden arviointilaitosta.

3 §

Suhde muuhun lainsäädäntöön

Markkinavalvonnan, talouden toimijoiden kanssa tehtävän yhteistyön sekä Euroopan unionin markkinoille tulevien tuotteiden valvonnan puitteista säädetään markkinavalvonnasta ja tuotteiden vaatimustenmukaisuudesta sekä direktiivin 2004/42/EY ja asetusten (EY) N:o 765/2008 ja (EU) N:o 305/2011 muuttamisesta annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) 2019/1020, jäljempänä *markkinavalvonta-asetus*.

Markkinavalvontaviranomaisten toimivallasta, markkinavalvonta-asetuksen 25–28 artiklan mukaisesta ulkorajavalvonnasta sekä muutoksenhausta markkinavalvontaviranomaisten päätöksiin säädetään eräiden tuotteiden markkinavalvonnasta annetussa laissa (1137/2016), jäljempänä *markkinavalvontalaki*.

Kuluttajatuotteiden turvallisuudesta säädetään yleisestä tuoteturvallisuudesta, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1025/2012 ja Euroopan parlamentin ja neuvoston direktiivin (EU) 2020/1828 muuttamisesta sekä Euroopan parlamentin ja neuvoston direktiivin 2001/95/EY ja neuvoston direktiivin 87/357/ETY kumoamisesta annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) 2023/988 sekä kuluttajatuotteiden turvallisuudesta annetussa laissa (184/2025).

Tekoälyjärjestelmiä koskevista vaatimuksista säädetään tekoälyä koskevista yhdenmukaistetuista säännöistä ja asetusten (EY) N:o 300/2008, (EU) N:o 167/2013, (EU) N:o 168/2013, (EU) 2018/858, (EU) 2018/1139 ja (EU) 2019/2144 sekä direktiivien 2014/90/EU, (EU) 2016/797 ja (EU) 2020/1828 muuttamisesta annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) 2024/1689 (tekoälysäädös) ja eräiden tekoälyjärjestelmien valvonnasta annetussa laissa (/).

CSIRT-yksikön tehtävistä sekä muiden kuin kyberkestävyysasetuksessa tarkoitettujen haavoittuvuusilmoituksien käsittelystä säädetään kyberturvallisuuslaissa.

2 luku

Vaatimustenmukaisuus ja ilmoitukset

4 §

Digitaalisen elementin sisältävän tuotteen vaatimustenmukaisuus

Digitaalisen elementin sisältävän tuotteen vaatimustenmukaisuudesta säädetään kyberkestävyysasetuksessa.

5 §

Keskeneräiset tuotteet

Digitaalisen elementin sisältävää tuotetta, joka ei täytä kyberkestävyysasetuksessa säädettyjä vaatimuksia, saa esitellä tai käyttää kyberkestävyysasetuksen 4 artiklan 2 kohdassa säädetyllä tavalla. Keskeneräisen ohjelmiston, joka ei täytä kyberkestävyysasetuksessa säädettyjä vaatimuksia, saa asettaa saataville markkinoilla kyberkestävyysasetuksen 4 artiklan 3 kohdassa säädetyllä tavalla rajoitetuksi ajaksi testausta varten.

6 §

Digitaalisen elementin sisältävä tuote julkisessa hankinnassa

Julkisista hankinnoista ja käyttöoikeussopimuksista annetun lain (1397/2016) soveltamisalaan kuuluvassa hankinnassa, jossa hankinnan kohteena on digitaalisen elementin sisältävä tuote, hankintayksikön on huomioitava, mitä kyberkestävyysasetuksen 5 artiklan 2 kohdassa säädetään vaatimusten noudattamisesta ja valmistajan kyvystä käsitellä tehokkaasti haavoittuvuuksia.

7 §

Valmistajan ilmoitusvelvollisuus

Valmistajan velvollisuudesta ilmoittaa digitaalisen elementin sisältävään tuotteeseen sisältyvästä aktiivisesti hyödynnetystä haavoittuvuudesta tai tuotteen tietoturvaan vaikuttavasta vakavasta poikkeamasta säädetään kyberkestävyysasetuksen 14 artiklassa.

CSIRT-yksikön velvollisuudesta ilmoittaa markkinavalvontaviranomaiselle kyberkestävyysasetuksen 14 artiklan nojalla ilmoitetusta tapahtumasta säädetään kyberkestävyysasetuksen 16 artiklan 3 kohdassa.

8 §

Vapaaehtoinen ilmoittaminen

CSIRT-yksikkö ottaa vastaan kyberkestävyysasetuksen 15 artiklan mukaisia vapaaehtoisia ilmoituksia mahdollisista digitaalisia elementtejä sisältävään tuotteeseen sisältyvistä haavoittuvuuksista, kyberuhkista, digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavista vakavista poikkeamista sekä läheltä piti -tilanteista.

Siitä riippumatta, mitä viranomaisten tiedonsaantioikeuksista muualla laissa säädetään, kyberkestävyysasetuksen 15 artiklan mukaisesti CSIRT-yksikölle vapaaehtoisesti ilmoitettua tietoa ei saa ilman ilmoittajan suostumusta käyttää ilmoittajaan kohdistuvassa rikostutkinnassa eikä hallinnollisessa tai muussa tiedon luovuttajaan kohdistuvassa päätöksenteossa.

9 §

CSIRT-yksikön oikeus luovuttaa salassa pidettäviä tietoja

Sen lisäksi, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) ja muualla laissa säädetään, CSIRT-yksiköllä on oikeus omasta aloitteestaan tai pyynnöstä luovuttaa tai ilmaista salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä kyberkestävyysasetuksen 14 artiklan 2, 4 ja 6 kohdan nojalla saamansa tieto tai mainitun asetuksen 15 artiklan nojalla saamansa vastaava tieto, jos se on tarpeen kyberkestävyysasetuksen 14–17 artiklassa säädettyjen tehtävien toteuttamiseksi:

1) 15 ja 16 §:ssä tarkoitetulle markkinavalvontaviranomaiselle;
2) Euroopan unionin kyberturvallisuusvirasto ENISAlle;
3) toisessa Euroopan unionin jäsenvaltiossa koordinaattoriksi nimetylle CSIRT-yksikölle.

CSIRT-yksikkö voi luovuttaa tai ilmaista muunkin kyberkestävyysasetuksen mukaisia tehtäviä hoitaessaan saamansa kuin 1 momentissa tarkoitetun tiedon siten kuin 1 momentissa säädetään, jos se on välttämätöntä kyberkestävyysasetuksen 14–17 artiklassa säädettyjen tehtävien toteuttamiseksi.

10 §

Kyberkestävyyden sääntelyn testiympäristö

Liikenne- ja viestintävirasto voi päätöksellä perustaa kyberkestävyysasetuksen 33 artiklan 2 kohdassa tarkoitetun kyberkestävyyden sääntelyn testiympäristön. Päätöksessä kyberkestävyyden sääntelyn testiympäristön perustamisesta on määritettävä testiympäristön voimassaoloaika ja -paikka, soveltuva tekninen rajaus sekä lisäksi toimintasuunnitelma ja soveltuva testauksen kohde. Päätöksessä voidaan asettaa testiympäristöä koskevia ehtoja, jotka ovat tarpeellisia sen toiminnan järjestämisen tai turvallisuuden kannalta.

Liikenne- ja viestintävirasto myöntää hakemuksesta talouden toimijalle oikeuden toimintaan sääntelyn testiympäristössä. Hakemuksessa on esitettävä tarpeelliset tiedot hakijasta ja sen toiminnasta, testaukseen osallistuvista muista osapuolista, testauksen kohteesta ja testauksen tavoitteista. Oikeutta ei myönnetä, jos testauksen kohde tai suunniteltu toiminta ei ole testiympäristön perustamista koskevan päätöksen ehtojen mukaista, testaus aiheuttaisi kohtuutonta haittaa tai vaaraa muille tahoille taikka talouden toimijalle on määrätty hakemusta edeltävän kolmen vuoden aikana tämän lain nojalla hallinnollinen seuraamusmaksu. Oikeus voidaan jättää myöntämättä myös, jos testaus ei olisi testiympäristön käytettävissä olevien resurssien vuoksi mahdollista.

Liikenne- ja viestintävirasto vastaa kyberkestävyysasetuksen 33 artiklan 2 kohdassa tarkoitetun ilmoituksen tekemisestä testiympäristön perustamisesta sekä talouden toimijoiden valvonnasta, ohjauksesta ja tuesta sääntelyn testiympäristössä yhteistyössä muiden markkinavalvontaviranomaisten kanssa.

Liikenne- ja viestintäviraston määräyksellä voidaan antaa tarkempia säännöksiä kyberkestävyyden sääntelyn testiympäristön teknisestä järjestämisestä ja toiminnasta sekä talouden toimijan hakemuksesta.

3 luku

Ilmoitetut laitokset

11 §

Ilmoittava viranomainen

Liikenne- ja viestintävirasto toimii kyberkestävyysasetuksen 36 artiklassa tarkoitettuna ilmoittamisesta vastaavana viranomaisena (*ilmoittava viranomainen*).

Ilmoittava viranomainen nimeää vaatimustenmukaisuuden arviointilaitoksen ilmoitetuksi laitokseksi, valvoo ilmoittamiaan laitoksia sekä vastaa muista ilmoittavalle viranomaiselle kyberkestävyysasetuksessa säädetyistä tehtävistä. Ilmoittava viranomainen vastaa kyberkestävyysasetuksen 35 artiklan 1 kohdassa, 38 artiklan 1 kohdassa ja 46 artiklan 2 kohdassa tarkoitettujen tietojen ilmoittamisesta Euroopan komissiolle ja muille Euroopan unionin jäsenvaltioille.

Ilmoittavaa viranomaista koskevista vaatimuksista säädetään kyberkestävyysasetuksen 37 artiklassa.

12 §

Ilmoittamista koskeva hakemus

Suomeen sijoittautuneen vaatimustenmukaisuuden arviointilaitoksen on haettava ilmoittamista ilmoittavalta viranomaiselta. Hakemukseen on liitettävä Turvallisuus- ja kemikaaliviraston akkreditointiyksikön (*FINAS-akkreditointipalvelu*) antama akkreditointitodistus siitä, että vaatimustenmukaisuuden arviointilaitos täyttää kyberkestävyysasetuksessa säädetyt vaatimukset, sekä muut kyberkestävyysasetuksen 42 artiklassa tarkoitetut tiedot. Jos vaatimustenmukaisuuden arviointilaitos ei kuitenkaan voi liittää hakemukseen akkreditointitodistusta, sen on toimitettava ilmoittavalle viranomaiselle kaikki tarpeellinen tieto, jonka avulla voidaan varmentaa, todeta ja säännöllisesti valvoa, että se täyttää kyberkestävyysasetuksessa säädetyt vaatimukset.

13 §

Ilmoitetuksi laitokseksi nimeäminen ja nimeämisen rajaaminen tai peruuttaminen

Ilmoittava viranomainen nimeää hakemuksesta ilmoitetuksi laitokseksi vaatimustenmukaisuuden arviointilaitoksen, joka täyttää kyberkestävyysasetuksessa säädetyt vaatimukset.

Nimeämistä koskevassa päätöksessä määritellään ilmoitetun vaatimustenmukaisuuden arviointilaitoksen pätevyysalue, vahvistetaan laitoksen valvontaan liittyvät järjestelyt sekä asetetaan tarvittaessa sellaisia laitoksen toimintaa koskevia vaatimuksia, rajoituksia ja ehtoja, joilla varmistetaan tehtävien asianmukainen suorittaminen.

Nimeämisen rajaamisesta ja peruuttamisesta säädetään kyberkestävyysasetuksen 45 artiklassa.

Ilmoitetun laitoksen sekä sen käyttämän tytäryhtiön ja alihankkijan palveluksessa olevaan henkilöön sovelletaan rikosoikeudellista virkavastuuta koskevia säännöksiä hänen suorittaessaan kyberkestävyysasetuksessa tarkoitettuja tehtäviä. Vahingonkorvausvastuusta säädetään vahingonkorvauslaissa (412/1974).

14 §

Ilmoittavan viranomaisen ja ilmoitetun laitoksen oikeus luovuttaa salassa pidettäviä tietoja

Sen lisäksi, mitä viranomaisten toiminnan julkisuudesta annetussa laissa ja muualla laissa säädetään, ilmoittava viranomainen voi omasta aloitteestaan tai pyynnöstä salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä luovuttaa tai ilmaista vaatimustenmukaisuuden arviointilaitoksen ilmoittamisen perusteita ja muuta sen pätevyyttä koskevan saamansa tai laatimansa asiakirjan tai tiedon Euroopan komissiolle ja toiselle Euroopan unionin jäsenvaltiolle, jos se on tarpeen kyberkestävyysasetuksessa säädetyn ilmoittavan viranomaisen velvoitteen toteuttamiseksi.

Sen lisäksi, mitä viranomaisten toiminnan julkisuudesta annetussa laissa ja muualla laissa säädetään, ilmoitettu laitos voi omasta aloitteestaan tai pyynnöstä salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä luovuttaa tai ilmaista vaatimustenmukaisuuden arviointia ja tarkastuksen tuloksia koskevan saamansa tai laatimansa asiakirjan tai tiedon Euroopan komissiolle, Euroopan unionin jäsenvaltiolle ja toiselle ilmoitetulle laitokselle, jos se on tarpeen kyberkestävyysasetuksessa säädetyn ilmoitetun laitoksen velvoitteen toteuttamiseksi.

4 luku

Markkinavalvonta

15 §

Markkinavalvontaviranomainen

Kyberkestävyysasetuksen 52 artiklassa tarkoitettuna markkinavalvontaviranomaisena toimii Liikenne- ja viestintävirasto.

16 §

Suuririskisen tekoälyjärjestelmän markkinavalvonta

Edellä 15 §:ssä säädetystä poiketen sellaisen tekoälyä koskevista yhdenmukaistetuista säännöistä ja asetusten (EY) N:o 300/2008, (EU) N:o 167/2013, (EU) N:O 168/2013, (EU) 2018/858, (EU) 2018/1139 ja (EU) 2019/2144 sekä direktiivien 2014/90/EU, (EU) 2016/797 ja (EU) 2020/1828 muuttamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2024/1689 (tekoälysäädös) 6 artiklassa tarkoitetun suuririskisen tekoälyjärjestelmän, joka kuuluu kyberkestävyysasetuksen soveltamisalaan, markkinavalvontaviranomaisena toimii eräiden tekoälyjärjestelmien valvonnasta annetun lain 3 §:n nojalla toimivaltainen valvova viranomainen.

17 §

Markkinavalvonnan asiantuntijatuki

Liikenne- ja viestintävirasto voi antaa pyynnöstä kyberkestävyysasetuksen markkinavalvontaa, vaatimustenmukaisuuden arviointia ja kyberturvallisuusriskien arviointia koskevaa asiantuntijatukea 16 §:ssä tarkoitetuille markkinavalvontaviranomaisille sekä sille, jolla on toimivalta määrätä 6 luvussa tarkoitettu seuraamusmaksu. Markkinavalvontaviranomaisten yhteistyöstä säädetään markkinavalvontalaissa.

18 §

Markkinavalvontaviranomaisen oikeus luovuttaa salassa pidettäviä tietoja

Mitä markkinavalvontalain 11 ja 13 §:ssä säädetään oikeudesta luovuttaa tietoja salassapitosäännösten estämättä, sovelletaan myös digitaalisia elementtejä sisältävän tuotteen vaatimustenmukaisuutta, turvajärjestelyjä sekä haavoittuvuutta ja tietoturvaan vaikuttavaa poikkeamaa koskeviin tietoihin. Markkinavalvontaviranomainen voi luovuttaa tietoja omasta aloitteestaan tai pyynnöstä.

Sen lisäksi, mitä viranomaisten toiminnan julkisuudesta annetussa laissa ja muualla laissa säädetään, markkinavalvontaviranomaisella on oikeus omasta aloitteestaan tai pyynnöstä luovuttaa salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto myös:

1) FINAS-akkreditointipalvelulle ja ilmoittavalle viranomaiselle, jos tiedon luovuttaminen on välttämätöntä vaatimustenmukaisuuden arviointilaitoksen pätevyyden arvioimiseksi;

2) 21 §:ssä tarkoitetulle viranomaiselle tai toisen Euroopan unionin jäsenvaltion vastaavalle viranomaiselle, jos tiedon luovuttaminen on välttämätöntä kyseisen viranomaisen valvontatehtävien suorittamiseksi;

3) kyberturvallisuuslain 26 §:ssä ja julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 18 h §:ssä tarkoitetulle valvovalle viranomaiselle, Finanssivalvonnalle tai toisen Euroopan unionin jäsenvaltion vastaavalle viranomaiselle, jos digitaalisia elementtejä sisältävän tuotteen voidaan perustellusti arvioida aiheuttavan merkittävän kyberturvallisuusriskin muiden kuin teknisten riskitekijöiden vuoksi ja tiedon luovuttaminen on välttämätöntä kyberkestävyysasetuksen 54 artiklan 2 kohdassa säädetyn ilmoitusvelvollisuuden täyttämiseksi;

4) Euroopan unionin kyberturvallisuusvirasto ENISAlle ja CSIRT-yksikölle, jos se on välttämätöntä kyberkestävyysasetuksessa 52 artiklan 4 ja 5 kohdassa tai 54 artiklan 1 kohdassa säädetyn yhteistyövelvollisuuden, neuvonnan tai tutkimuksen suorittamiseksi taikka CSIRT-yksikön kyberturvallisuuslaissa säädettyjen tehtävien hoitamista varten;

5) tietosuojavaltuutetulle, jos tiedon luovuttaminen on välttämätöntä sen laissa säädettyjen valvontatehtävien hoitamiseksi;

6) Euroopan komissiolle, Kilpailu- ja kuluttajavirastolle ja toisen Euroopan unionin jäsenvaltion kansalliselle kilpailuviranomaiselle, jos se on välttämätöntä Euroopan unionin kilpailulainsäädännön soveltamisen kannalta merkityksellisen tiedon antamiseksi kyberkestävyysasetuksen 52 artiklan 13 kohdassa säädetyn velvoitteen toteuttamiseksi.

Liikenne- ja viestintävirastolla ja 17 §:ssä tarkoitettua asiantuntijatukea pyytävällä on oikeus salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto toisilleen, jos se on asiantuntijatuen antamiseksi välttämätöntä.

19 §

Markkinavalvontaviranomaisen oikeus tehdä tarkastuksia ja ottaa ohjelmistoja tutkittavaksi

Sen lisäksi, mitä markkinavalvontalain 9 §:n 1 momentissa säädetään, tarkastus voidaan ulottaa myös pysyväisluonteiseen asumiseen käytettäviin tiloihin, joita talouden toimija käyttää elinkeino- tai ammattitoimintaansa liittyviin tarkoituksiin. Tarkastus pysyväisluonteiseen asumiseen käytettävään tilaan saadaan tehdä vain, jos se on välttämätöntä tarkastuksen kohteena olevien seikkojen selvittämiseksi ja on perusteltu ja yksilöity syy epäillä kyberkestävyysasetusta tai sen nojalla annettua säädöstä rikotun tai rikottavan tavalla, josta voi olla seuraamuksena tässä laissa tarkoitettu seuraamusmaksu. Lisäksi edellytyksenä on, että epäillyssä rikkomuksessa on kyse digitaalisen elementin sisältävän tuotteen tai siihen liittyvän prosessin vaatimustenvastaisuudesta tai kyberkestävyysasetuksen 57 artiklassa tarkoitetusta tilanteesta, jossa tuote muutoin aiheuttaa merkittävän kyberturvallisuusriskin.

Markkinavalvontaviranomaisen oikeudesta ottaa tuotteita tutkittavaksi säädetään markkinavalvontalaissa. Ohjelmiston tutkittavaksi ottamisesta ei suoriteta talouden toimijalle korvausta.

20 §

Avoimen lähdekoodin ohjelmistovastaavalle annettava valvontapäätös

Markkinavalvontaviranomainen voi velvoittaa avoimen lähdekoodin ohjelmistovastaavan määräajassa korjaamaan puutteet sen kyberkestävyysasetuksessa säädettyjen velvollisuuksien noudattamisessa.

Markkinavalvontaviranomainen voi asettaa tämän pykälän nojalla antamansa päätöksen tehosteeksi uhkasakon.

5 luku

Kyberturvallisuussertifiointi

21 §

Kansallinen kyberturvallisuussertifioinnin viranomainen

Kyberturvallisuusasetuksen 58 artiklassa tarkoitettuna kansallisena kyberturvallisuussertifioinnin myöntävänä viranomaisena (*kyberturvallisuussertifioinnin viranomainen*) toimii Liikenne- ja viestintävirasto.

Liikenne- ja viestintäviraston eurooppalaisten kyberturvallisuussertifikaattien myöntämiseen liittyvät tehtävät on eriytettävä kyberturvallisuusasetuksen 58 artiklan mukaisesta valvontatoiminnasta ja varmistettava, että nämä toiminnot suoritetaan toisistaan riippumattomasti.

22 §

Vaatimustenmukaisuuden arviointilaitosten ilmoittaminen ja valtuuttaminen kyberturvallissertifiointia varten

Kyberturvallisuussertifioinnin viranomaisen tehtävistä vaatimustenmukaisuuden arviointilaitosten valtuuttamisessa kyberturvallisuussertifiointia varten säädetään kyberturvallisuusasetuksen 60 artiklan 3 kohdassa sekä kyberturvallisuussertifiointia varten akkreditoitujen vaatimustenmukaisuuden arviointilaitosten ilmoittamisesta Euroopan komissiolle kyberturvallisuusasetuksen 61 artiklassa. Jos sovellettava eurooppalainen kyberturvallisuuden sertifiointijärjestelmä sitä edellyttää, on ilmoittamisen edellytyksenä kyberturvallisuussertifioinnin viranomaisen valtuutus. Kyberturvallisuussertifioinnin viranomainen valvoo kyberturvallisuussertifiointia varten ilmoittamiaan vaatimustenmukaisuuden arviointilaitoksia.

Kyberturvallisuussertifiointia varten ilmoittamisen ja valtuuttamisen edellytyksenä on, että vaatimustenmukaisuuden arviointilaitokselle on myönnetty kyberturvallisuusasetuksen 60 artiklan 1 kohdassa tarkoitetusta akkreditoinnista FINAS-akkreditointipalvelun antama akkreditointitodistus siitä, että vaatimustenmukaisuuden arviointilaitos täyttää kyberturvallisuusasetuksessa säädetyt vaatimukset.

23 §

Kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen velvollisuudet

Kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen on suoritettava vaatimustenmukaisuuden arvioinnit kyberturvallisuusasetuksen ja sen nojalla annettujen säädösten mukaisten vaatimustenmukaisuuden arviointimenettelyjen edellyttämällä tavalla. Lisäksi vaatimustenmukaisuuden arviointilaitoksen on suoritettavat muut kyberturvallisuusasetuksessa ja sen nojalla annetuissa säädöksissä säädetyt tehtävät.

Kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen on ilmoitettava kyberturvallisuussertifioinnin viranomaiselle kaikista muutoksista, joilla on vaikutusta ilmoittamisen tai valtuuttamisen edellytysten täyttymiseen.

Kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen sekä sen käyttämän tytäryhtiön ja alihankkijan palveluksessa olevaan henkilöön sovelletaan rikosoikeudellista virkavastuuta koskevia säännöksiä hänen hoitaessaan kyberturvallisuusasetuksessa ja tässä laissa tarkoitettuja tehtäviä. Vahingonkorvausvastuusta säädetään vahingonkorvauslaissa.

24 §

Kyberturvallisuussertifikaatin myöntämiseen liittyvä tehtävien siirtäminen

Kyberturvallisuussertifioinnin viranomainen voi siirtää tietyn eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän osalta kyberturvallisuusasetuksen 52 artiklan 7 kohdassa tarkoitetun korkean varmuustason eurooppalaisen kyberturvallisuussertifikaatin myöntämiseen liittyvän tehtävän kyberturvallisuussertifiointia varten ilmoitetulle vaatimuksenmukaisuuden arviointilaitokselle:

1) kyberturvallisuusasetuksen 56 artiklan 6 kohdan a alakohdassa tarkoitetussa tapauksessa siten, että kyberturvallisuussertifioinnin viranomainen hyväksyy ennalta kunkin kyberturvallisuussertifikaatin myöntämisen; tai

2) kyberturvallisuusasetuksen 56 artiklan 6 kohdan b alakohdassa tarkoitetussa tapauksessa yleisesti siten, että arviointilaitos myöntää kyberturvallisuussertifikaatin ilman kyberturvallisuussertifioinnin viranomaisen erillistä hyväksyntää.

Kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen kanssa tehtävässä sopimuksessa on sovittava ainakin:

1) vaatimustenmukaisuuden arviointilaitoksen tehtävistä;

2) tarpeellisista vaatimustenmukaisuuden arviointilaitoksen pätevyyteen ja sen toiminnan turvallisuuteen kohdistuvista erityisistä vaatimuksista;

3) sopimuskaudesta, toiminnan aloittamisesta ja sopimuksen päättymisestä kesken sopimuskauden;

4) vaatimustenmukaisuuden arviointilaitoksen toimintaan liittyvien asiakirjojen säilyttämisestä ja arkistoinnista;

5) vaatimustenmukaisuuden arviointilaitoksen toiminnan puutteista ja laiminlyönneistä aiheutuvista seuraamuksista.

Kyberturvallisuussertifioinnin viranomainen voi irtisanoa tai purkaa sopimuksen, jos kyberturvallisuussertifiointia varten ilmoitettu vaatimustenmukaisuuden arviointilaitos ei enää täytä vaatimuksia tai jos se olennaisesti laiminlyö sopimuksessa sovittujen tehtävien suorittamisen tai muutoin rikkoo sopimusta tai toimii olennaisesti tai toistuvasti lainvastaisesti.

25 §

Kyberturvallisuussertifioinnin viranomaisen tiedonsaanti- ja tarkastusoikeus

Kyberturvallisuussertifioinnin viranomaisella on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada sen tässä laissa tai kyberturvallisuusasetuksessa säädettyjen tehtävien hoitamiseksi ja kyberturvallisuusasetuksen, sen nojalla annettujen säädösten ja tämän lain noudattamisen valvomiseksi välttämättömät tiedot vaatimustenmukaisuuden arviointilaitokselta, eurooppalaisen kyberturvallisuussertifikaatin haltijalta ja kyberturvallisuusasetuksen 53 artiklan 2 kohdassa tarkoitetulta EU-vaatimustenmukaisuusilmoituksen antajalta. Tiedot on luovutettava ilman aiheetonta viivytystä, viranomaisen pyytämässä muodossa ja maksutta.

Kyberturvallisuussertifioinnin viranomaisella on oikeus tehdä vaatimustenmukaisuuden arviointilaitosta, eurooppalaisen kyberturvallisuussertifikaatin haltijaa tai EU-vaatimustenmukaisuusilmoitusten antajaa koskevia tarkastuksia kyberturvallisuusasetuksen, sen nojalla annettujen säädösten ja tämän lain noudattamisen valvomiseksi. Tarkastuksissa noudatetaan, mitä hallintolain (434/2003) 39 §:ssä säädetään.

Kyberturvallisuussertifioinnin viranomaisella on oikeus teettää tarkastus riippumattomalla asiantuntijalla. Tarkastuksen suorittajalla ja siihen osallistuvalla on oltava sellainen koulutus ja kokemus kuin tarkastuksen suorittamiseksi on tarpeen. Riippumattomaan asiantuntijaan sovelletaan rikosoikeudellista virkavastuuta koskevia säännöksiä hänen suorittaessaan tässä pykälässä tarkoitettuja tehtäviä. Vahingonkorvausvastuusta säädetään vahingonkorvauslaissa.

Tarkastusta suorittavalla kyberturvallisuussertifioinnin viranomaisella ja riippumattomalla asiantuntijalla on oikeus päästä kaikkiin tiloihin, joissa harjoitetaan kyberturvallisuusasetuksessa tarkoitettua toimintaa, sekä kaikkiin tiloihin ja tietojärjestelmiin, joissa säilytetään tai käsitellään valvonnan kannalta merkityksellisiä tietoja. Pysyväisluonteiseen asumiseen käytettäviin tiloihin tarkastuksia ei kuitenkaan saa ulottaa.

26 §

Kyberturvallisuussertifioinnin viranomaisen oikeus luovuttaa salassa pidettäviä tietoja

Sen lisäksi, mitä viranomaisten toiminnan julkisuudesta annetussa laissa ja muualla laissa säädetään, kyberturvallisuussertifioinnin viranomaisella on oikeus omasta aloitteestaan tai pyynnöstä luovuttaa salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä sen tässä laissa tai kyberturvallisuusasetuksessa säädettyjen tehtävien hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettäviä tieto:

1) markkinavalvontalain 4 §:ssä tarkoitetulle markkinavalvontaviranomaiselle, ja Turvallisuus- ja kemikaaliviraston akkreditointiyksikölle tai toisen Euroopan unionin jäsenvaltion kansalliselle akkreditointielimelle, jos tiedon luovuttaminen on välttämätöntä kyseisen viranomaisen tehtävien suorittamisen kannalta;

2) toiselle kansalliselle kyberturvallisuussertifioinnin viranomaiselle ja muulle Euroopan kyberturvallisuuden sertifiointiryhmän jäsenelle, Euroopan unionin kyberturvallisuusvirasto ENISAlle sekä Euroopan komissiolle, jos se on välttämätöntä kyberturvallisuusasetuksessa tai sen nojalla säädetyn kyberturvallisuussertifioinnin viranomaisen velvoitteen toteuttamiseksi;

3) siitä, että tieto- ja viestintätekniikan tuote, palvelu tai prosessi taikka tietoturvapalvelu ei vastaa kyberturvallisuusasetuksessa säädettyjä tai eurooppalaisten kyberturvallisuuden sertifiointijärjestelmän vaatimuksia, samoin kuin tieto tällaista tuotetta, palvelua tai prosessia taikka tietoturvapalvelua koskevasta haavoittuvuudesta kyberturvallisuuslain 26 §:ssä ja julkisen hallinnon tiedonhallinnasta annetun lain 18 h §:ssä tarkoitetulle valvovalle viranomaiselle, Finanssivalvonnalle ja CSIRT-yksikölle, jos se on tarpeen niille säädettyjen tehtävien hoitamista varten.

27 §

Valvontapäätös

Kyberturvallisuussertifioinnin viranomainen voi velvoittaa vaatimustenmukaisuuden arviointilaitoksen, eurooppalaisen kyberturvallisuussertifikaatin haltijan tai EU-vaatimustenmukaisuusilmoitusten antajan määräajassa korjaamaan puutteet sen tässä laissa tai kyberturvallisuusasetuksessa tai sen nojalla säädettyjen velvollisuuksien noudattamisessa.

Kyberturvallisuussertifioinnin viranomainen voi asettaa tämän pykälän nojalla antamansa päätöksen tehosteeksi uhkasakon tai uhan, että velvollisuuksien vastainen toiminta keskeytetään tai tekemättä jätetty toimenpide teetetään vaatimustenmukaisuuden arviointilaitoksen, eurooppalaisen kyberturvallisuussertifikaatin haltijan tai EU-vaatimustenmukaisuusilmoituksen antajan kustannuksella.

28 §

Kyberturvallisuussertifikaatin peruuttaminen

Kyberturvallisuussertifioinnin viranomainen voi peruuttaa myöntämänsä tai kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen kyberturvallisuusasetuksen 56 artiklan 6 kohdan mukaisesti myöntämän eurooppalaisen kyberturvallisuussertifikaatin, jos kyberturvallisuussertifikaatti ei täytä kyberturvallisuusasetuksessa säädettyjä tai kyseisen eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimuksia tai jos kyberturvallisuussertifikaatin haltija ei anna kyberturvallisuussertifioinnin viranomaiselle sen pyytämiä 25 §:n 1 momentissa tarkoitettuja tietoja eikä puutetta tai laiminlyöntiä korjata kohtuullisessa määräajassa.

29 §

Kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen valtuutuksen ja ilmoituksen keskeyttäminen, rajoittaminen tai peruuttaminen

Jollei kyberturvallisuusasetuksen nojalla säädetystä muuta johdu, kyberturvallisuussertifioinnin viranomaisen on tarvittaessa peruutettava tai keskeytettävä vaatimustenmukaisuuden arviointilaitoksen kyberturvallisuusasetuksen 60 artiklan 3 kohdassa tarkoitettu valtuutus tai 61 artiklan 1 kohdassa tarkoitettu ilmoitus tai rajoitettava sitä ja esitettävä kyberturvallisuusasetuksen 61 artiklan 4 kohdassa tarkoitettu pyyntö poistaa arviointilaitos luettelosta, jos kyberturvallisuussertifiointia varten ilmoitettu vaatimustenmukaisuuden arviointilaitos ei ole korjannut toimintaansa 27 §:n nojalla asetetussa määräajassa ja kyseessä on olennainen rikkomus tai laiminlyönti taikka jos arviointilaitos ei täytä sille säädettyjä vaatimuksia tai sen akkreditointia rajoitetaan, akkreditointi peruutetaan tai se keskeytetään.

Jos kyberturvallisuussertifiointia varten ilmoitettu vaatimustenmukaisuuden arviointilaitos on lopettanut toimintansa tai se poistetaan Euroopan komission luettelosta, on kyberturvallisuussertifioinnin viranomaisen ryhdyttävä asianmukaisiin toimenpiteisiin sen varmistamiseksi, että arviointilaitoksen asiakirjat käsittelee toinen kyberturvallisuussertifiointia varten ilmoitettu vaatimustenmukaisuuden arviointilaitos tai että asiakirjat pidetään kyberturvallisuussertifioinnin viranomaisen ja markkinavalvonnasta vastaavien viranomaisten saatavilla.

30 §

Poliisin virka-apu

Poliisi on velvollinen antamaan virka-apua kyberturvallisuussertifioinnin viranomaiselle tässä laissa tai kyberturvallisuusasetuksessa tai sen nojalla säädettyjen velvollisuuksien noudattamisen valvomiseksi ja täytäntöön panemiseksi.

Poliisin antamasta virka-avusta säädetään poliisilaissa (872/2011).

6 luku

Seuraamusmaksut

31 §

Valmistajan seuraamusmaksu

Hallinnollinen seuraamusmaksu voidaan määrätä valmistajalle, joka tahallaan tai huolimattomuudesta:

1) saattaa markkinoille digitaalisia elementtejä sisältävän tuotteen kyberkestävyysasetuksen 13 artiklan 1 kohdan vastaisesti varmistamatta, että tuote on suunniteltu, kehitetty ja tuotettu kyberkestävyysasetuksen liitteessä I olevassa I osassa vahvistettujen olennaisten kyberturvallisuusvaatimusten mukaisesti;

2) laiminlyö kyberkestävyysasetuksen 13 artiklan 2 kohdassa tarkoitetun kyberturvallisuusriskien arvioinnin tai arvioinnin tuloksien huomioon ottamisen;

3) laiminlyö kyberkestävyysasetuksen 13 artiklan 3 kohdassa säädetyn velvollisuuden dokumentoida kyberturvallisuusriskien arviointi tai laiminlyö sen päivittämisen;

4) laiminlyö kyberkestävyysasetuksen 13 artiklan 4 kohdassa säädetyn velvollisuuden sisällyttää teknisiin asiakirjoihin kyberturvallisuusriskien arvioinnin;

5) laiminlyö kyberkestävyysasetuksen 13 artiklan 7 kohdassa säädetyn velvollisuuden dokumentoida kyberturvallisuuteen liittyvät seikat tai laiminlyö päivittää kyberturvallisuusriskien arvioinnin mainitun kohdan mukaisesti;

6) integroi tuotteeseen kolmannelta osapuolelta hankitun komponentin muuten kuin kyberkestävyysasetuksen 13 artiklan 5 kohdassa säädetyllä tavalla taikka laiminlyö kyberkestävyysasetuksen 13 artiklan 6 kohdassa säädetyn velvollisuuden ilmoittaa tuotteeseen integroidun komponentin haavoittuvuudesta komponentin valmistajalle tai ylläpitäjälle, puuttua haavoittuvuuteen tai korjata se tai laiminlyö mainitussa kohdassa säädetyn velvollisuuden jakaa tietoja;

7) määrittää tukiajan kyberkestävyysasetuksen 13 artiklan 8 kohdan vastaisesti tai jättää ilmoittamatta tukiajan päättymisestä 13 artiklan 19 kohdassa säädetyllä tavalla;

8) laiminlyö kyberkestävyysasetuksen 13 artiklan 8 kohdassa säädetyn velvollisuuden käsitellä haavoittuvuuksia tehokkaasti ja kyberkestävyysasetuksen liitteessä I olevassa II osassa vahvistettujen olennaisten kyberturvallisuusvaatimusten mukaisesti tukiajan aikana;

9) laiminlyö pitää tukiaikana käyttäjien saataville asetetun tietoturvapäivityksen saatavilla kyberkestävyysasetuksen 13 artiklan 9 kohdassa säädetyn ajan;

10) varmistaa kyberkestävyysasetuksen 13 artiklan 10 kohdassa tarkoitetun olennaisen kyberturvallisuusvaatimuksen noudattamisen vain viimeksi markkinoille saattamansa version osalta, jos version käyttö ei ole käyttäjille maksutonta tai siitä aiheutuu lisäkustannuksia mainitussa kohdassa säädetyn vastaisesti;

11) laiminlyö laatia kyberkestävyysasetuksen 31 artiklassa tarkoitetut tekniset asiakirjat ennen digitaalisia elementtejä sisältävän tuotteen saattamista markkinoille taikka laatii tekniset asiakirjat mainitun artiklan 1–4 kohdassa tai 33 artiklan 5 kohdassa säädetyn vastaisesti;

12) laiminlyö kyberkestävyysasetuksen 13 artiklan 12 kohdan toisessa alakohdassa säädetyn velvollisuuden suorittaa tai teettää valitsemansa vaatimustenmukaisuuden arviointimenettelyn 32 artiklan 1–5 kohdassa säädetyllä tavalla;

13) laiminlyö laatia EU-vaatimustenmukaisuusvakuutuksen kyberkestävyysasetuksen 28 artiklan mukaisesti taikka laiminlyö kiinnittää tai liittää tuotteeseen CE-merkinnän 30 artiklan mukaisesti silloin, kun vaatimustenmukaisuuden arviointimenettelyllä on osoitettu tuotteen täyttävän kyberkestävyysasetuksen 13 artiklan 12 kohdan kolmannessa alakohdassa tarkoitetut olennaiset kyberturvallisuusvaatimukset;

14) laiminlyö pitää markkinavalvontaviranomaisen saatavilla tuotteen tekniset asiakirjat ja EU-vaatimustenmukaisuusvakuutus kyberkestävyysasetuksen 13 artiklan 13 kohdassa säädetyn ajan;

15) laiminlyö käyttää kyberkestävyysasetuksen 13 artiklan 14 kohdassa tarkoitettuja menettelyitä tai huomioida kohdassa tarkoitettuja muutoksia;

16) laiminlyö liittää tuotteeseen, sen pakkaukseen tai sen mukana seuraavaan asiakirjaan kyberkestävyysasetuksen 13 artiklan 15 kohdassa tarkoitetun tunnisteen, mainitun artiklan 16 kohdassa tarkoitetut tiedot taikka mainitun artiklan 17 kohdan toisessa alakohdassa tarkoitetun tiedon;

17) laiminlyö nimetä kyberkestävyysasetuksen 13 artiklan 17 kohdan ensimmäisessä alakohdassa tarkoitetun keskitetyn yhteyspisteen tai rajaa käyttäjän viestintätavan pelkästään automatisoituihin välineisiin mainitun kohdan kolmannen alakohdan vastaisesti;

18) laiminlyö kyberkestävyysasetuksen 13 artiklan 18 kohdassa säädetyn velvollisuuden varmistaa, että digitaalisia elementtejä sisältävän tuotteen mukana on mainitun säädöksen liitteessä II vahvistetut käyttäjälle annettavat tiedot ja ohjeet ja että ne annetaan mainitussa kohdassa tarkoitetulla tavalla, taikka laiminlyö pitää tiedot ja ohjeet käyttäjien ja markkinavalvontaviranomaisen saatavilla kohdassa säädetyn ajan;

19) laiminlyö kyberkestävyysasetuksen 13 artiklan 20 kohdassa säädetyn velvollisuuden toimittaa EU-vaatimustenmukaisuusvakuutuksen jäljennös tai yksinkertaistettu EU-vaatimustenmukaisuusvakuutus tuotteen mukana;

20) jättää toteuttamatta tarvittavat korjaavat toimenpiteet kyberkestävyysasetuksen 13 artiklan 21 kohdassa tarkoitetussa tilanteessa;

21) laiminlyö kyberkestävyysasetuksen 13 artiklan 22 kohdassa säädetyn velvollisuuden antaa markkinavalvontaviranomaiselle tietoja tai asiakirjoja tai tehdä yhteistyötä;

22) laiminlyö kyberkestävyysasetuksen 13 artiklan 23 kohdassa säädetyn velvollisuuden ilmoittaa toiminnan lopettamisesta;

23) laiminlyö kyberkestävyysasetuksen 14 artiklan 1 kohdassa säädetyn velvollisuuden ilmoittaa digitaalisia elementtejä sisältävään tuotteeseen sisältyvästä aktiivisesti hyödynnetyistä haavoittuvuuksista tai laiminlyö sisällyttää ilmoitukseen tai loppuraporttiin mainitun artiklan 2 kohdan mukaiset tiedot;

24) laiminlyö kyberkestävyysasetuksen 14 artiklan 3 kohdassa säädetyn velvollisuuden ilmoittaa digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavista vakavista poikkeamista tai laiminlyö antaa mainitun artiklan 4 kohdan mukaiset tiedot;

25) laiminlyö toimittaa CSIRT-yksikölle kyberkestävyysasetuksen 14 artiklan 6 kohdassa tarkoitettuja tietoja, kun CSIRT-yksikkö on pyytänyt toimittamaan väliraportin;

26) laiminlyö kyberkestävyysasetuksen 14 artiklan 8 kohdassa säädetyn velvollisuuden tiedottaa aktiivisesti hyödynnetystä haavoittuvuudesta tai digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavasta vakavasta poikkeamasta niitä tuotteen käyttäjiä, joihin vaikutukset kohdistuvat, ja tarvittaessa kaikkia käyttäjiä.

Hallinnollinen seuraamusmaksu voidaan määrätä 1 momentissa säädetyllä perusteella muulle kuin valmistajalle silloin, jos tämä kyberkestävyysasetuksen 21 tai 22 artiklan nojalla vastaa valmistajalle säädetystä velvollisuudesta.

32 §

Valtuutetun edustajan seuraamusmaksu

Hallinnollinen seuraamusmaksu voidaan määrätä valtuutetulle edustajalle, joka tahallaan tai huolimattomuudesta:

1) laiminlyö pitää EU-vaatimustenmukaisuusvakuutuksen ja tekniset asiakirjat markkinavalvontaviranomaisen saatavilla kyberkestävyysasetuksen 18 artiklan 3 kohdan a alakohdassa säädetyn ajan;

2) laiminlyö antaa markkinavalvontaviranomaiselle tämän pyynnöstä kyberkestävyysasetuksen 18 artiklan 3 kohdan johdantokappaleessa tai b alakohdassa tarkoitetut asiakirjat tai tiedot taikka tehdä yhteistyötä mainitun kohdan c alakohdan mukaisesti;

3) muuten kuin 1 tai 2 kohdassa tarkoitetulla tavalla laiminlyö valmistajalta saamaansa toimeksiantoon kuuluvan tehtävän, joka kyberkestävyysasetuksen nojalla kuuluu valmistajan velvollisuuksiin.

33 §

Maahantuojan seuraamusmaksu

Hallinnollinen seuraamusmaksu voidaan määrätä maahantuojalle, joka tahallaan tai huolimattomuudesta:

1) saattaa markkinoille digitaalisia elementtejä sisältävän tuotteen kyberkestävyysasetuksen 19 artiklan 1–3 kohdan vastaisesti;

2) laiminlyö tehdä valmistajalle tai markkinavalvontaviranomaiselle ilmoituksen silloin, kun maahantuoja on siihen kyberkestävyysasetuksen 19 artiklan 3 kohdan nojalla velvollinen;

3) laiminlyö ilmoittaa kyberkestävyysasetuksen 19 artiklan 4 kohdassa tarkoitetut tiedot kohdassa säädetyllä tavalla;

4) laiminlyö toteuttaa kyberkestävyysasetuksen 19 artiklan 5 kohdan ensimmäisessä alakohdassa tarkoitetut toimenpiteet tai laiminlyö antaa mainitun kohdan toisessa alakohdassa tarkoitetun ilmoituksen valmistajalle ja markkinavalvontaviranomaiselle;

5) laiminlyö pitää markkinavalvontaviranomaisen saatavilla EU-vaatimustenmukaisuusvakuutuksen jäljennöksen tai varmistaa, että tekniset asiakirjat voidaan antaa markkinavalvontaviranomaiselle tämän pyynnöstä kyberkestävyysasetuksen 19 artiklan 6 kohdassa säädetyn ajan;

6) laiminlyö antaa markkinavalvontaviranomaiselle tämän pyynnöstä kyberkestävyysasetuksen 19 artiklan 7 kohdassa tarkoitetut tiedot.

34 §

Jakelijan seuraamusmaksu

Hallinnollinen seuraamusmaksu voidaan määrätä jakelijalle, joka tahallaan tai huolimattomuudesta:

1) asettaa digitaalisia elementtejä sisältävän tuotteen saataville markkinoille kyberkestävyysasetuksen 20 artiklan 1–3 kohdan vastaisesti;

2) laiminlyö toteuttaa kyberkestävyysasetuksen 20 artiklan 4 kohdan ensimmäisessä alakohdassa tarkoitetut toimenpiteet tai laiminlyö antaa mainitun kohdan toisessa alakohdassa tarkoitetun ilmoituksen valmistajalle ja markkinavalvontaviranomaiselle;

3) laiminlyö antaa markkinavalvontaviranomaiselle tämän perustellusta pyynnöstä kyberkestävyysasetuksen 20 artiklan 5 kohdassa tarkoitetut tiedot ja asiakirjat;

4) laiminlyö antaa markkinavalvontaviranomaiselle kyberkestävyysasetuksen 20 artiklan 6 kohdassa tarkoitetun ilmoituksen.

35 §

Ilmoitetun laitoksen seuraamusmaksu

Hallinnollinen seuraamusmaksu voidaan määrätä ilmoitetulle laitokselle, joka tahallaan tai huolimattomuudesta:
1) toimii ilmoitetun laitoksen tehtävässä täyttämättä kyberkestävyysasetuksen 39 artiklassa säädettyjä vaatimuksia;
2) käyttää tytäryhtiötä tai teettää tehtäviä alihankintana muuten kuin kyberkestävyysasetuksen 41 artiklan mukaisesti;
3) suorittaa vaatimustenmukaisuuden arvioinnin muuten kuin kyberkestävyysasetuksen 47 artiklassa säädetyn menettelyn mukaisesti taikka muutoin laiminlyö mainitussa artiklassa säädetyn velvollisuuden;
4) laiminlyö tiedottaa kyberkestävyysasetuksen 49 artiklan 1 kohdassa tarkoitetuista seikoista ilmoittamisesta vastaavaa viranomaista tai mainitun artiklan 2 kohdassa tarkoitetuista seikoista mainitun kohdan mukaisesti muita ilmoitettuja laitoksia.

36 §

Muut kyberkestävyysasetukseen liittyvät seuraamusmaksut

Hallinnollinen seuraamusmaksu voidaan määrätä talouden toimijalle, joka tahallaan tai huolimattomuudesta:
1) laiminlyö antaa markkinavalvontaviranomaiselle tämän pyynnöstä kyberkestävyysasetuksen 23 artiklassa tarkoitetut tiedot, kun talouden toimija on tietojen antamiseen velvollinen;
2) kiinnittää tai liittää tuotteeseen CE-merkinnän muuten kuin kyberkestävyysasetuksen 30 artiklassa säädetyllä tavalla;
3) laiminlyö antaa markkinavalvontaviranomaiselle tämän pyynnöstä pääsyn kyberkestävyysasetuksen 53 artiklassa tarkoitettuun tietoon, kun tieto on tarpeen sen arvioimiseksi, täyttävätkö digitaalisia elementtejä sisältävä tuote ja valmistajan käyttöön ottamat prosessit kyberkestävyysasetuksen liitteessä I vahvistetut olennaiset kyberturvallisuusvaatimukset;
4) antaa ilmoitetulle laitokselle tai markkinavalvontaviranomaiselle väärän, puutteellisen tai harhaanjohtavan tiedon, joka on merkityksellinen tässä laissa tai kyberkestävyysasetuksessa tarkoitetun tehtävän hoitamisen kannalta.

37 §

Kyberturvallisuussertifiointia koskeva seuraamusmaksu

Hallinnollinen seuraamusmaksu voidaan määrätä sille, joka tahallaan tai huolimattomuudesta:
1) antaa kyberturvallisuusasetuksen 53 artiklan 2 kohdassa tarkoitetun EU-vaatimustenmukaisuusilmoituksen, vaikka kyseiset tieto- ja viestintätekniikan tuotteet, palvelut tai prosessit taikka tietoturvapalvelut eivät ole kyseisen eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimusten mukaisia;
2) laiminlyö asettaa kyberturvallisuussertifioinnin viranomaisen saataville kyberturvallisuusasetuksen 53 artiklan 3 kohdassa tarkoitetut tiedot tai laiminlyö toimittaa EU-

vaatimustenmukaisuusilmoituksen jäljennöksen kyberturvallisuussertifioinnin viranomaiselle ja Euroopan unionin kyberturvallisuusvirastolle;

3) rikkoo kyberturvallisuusasetuksen 54 artiklan 1 kohdan k alakohdassa tarkoitettuja eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän ehtoja;

4) laiminlyö saattaa julkisesti saataville kyberturvallisuusasetuksen 55 artiklan 1 kohdassa tarkoitetut tiedot mainitun artiklan 2 kohdassa säädetyllä tavalla;

5) antaa kyberturvallisuussertifioinnin viranomaiselle tai kyberturvallisuussertifiointia varten ilmoitetulle vaatimustenmukaisuuden arviointilaitokselle väärän, puutteellisen tai harhaanjohtavan tiedon, joka on merkityksellinen tässä laissa tai kyberturvallisuusasetuksessa tarkoitetun tehtävän hoitamisen kannalta;

6) laiminlyö kyberturvallisuusasetuksen 56 artiklan 8 kohdassa tarkoitetun ilmoituksen tekemisen;

7) käyttää eurooppalaista kyberturvallisuussertifikaattia, joka on peruutettu tai jonka voimassaoloaika on päättynyt.

38 §

Seuraamusmaksun määrä

Edellä 31 §:n 1 momentin nojalla valmistajalle määrättävän seuraamusmaksun enimmäismäärä on 15 000 000 euroa tai kaksi ja puoli prosenttia yrityksen edeltävän tilikauden maailmanlaajuisesta liikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

Edellä 31 §:n 2 momentin nojalla, 32–35 §:n nojalla tai 36 §:n 1–3 kohdan nojalla määrättävän seuraamusmaksun enimmäismäärä on 10 000 000 euroa tai kaksi prosenttia yrityksen edeltävän tilikauden maailmanlaajuisesta liikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

Edellä 36 §:n 4 kohdan nojalla määrättävän seuraamusmaksun enimmäismäärä on 5 000 000 euroa tai yksi prosentti yrityksen edeltävän tilikauden maailmanlaajuisesta liikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

Edellä 37 §:n nojalla määrättävän seuraamusmaksun enimmäismäärä on 100 000 euroa.

Seuraamusmaksun määrä perustuu kokonaisarviointiin. Seuraamusmaksun määrää arvioitaessa on otettava huomioon menettelyn luonne, vakavuus ja kesto sekä sen toistuvuus, rikkomuksen aiheuttama vahinko ja toimijan koko sekä sen mahdolliset aiemmat tämän lain alaan kuuluvat rikkomukset. Kyberkestävyysasetuksen rikkomisen perusteella seuraamusmaksua määrättäessä on lisäksi otettava huomioon, mitä kyberkestävyysasetuksen 64 artiklan 5 kohdassa säädetään.

39 §

Seuraamusmaksun määrääminen

Edellä 31–34 ja 36 §:ssä tarkoitetun hallinnollisen seuraamusmaksun määrää markkinavalvontaviranomainen. Milloin markkinavalvontaviranomaisena toimii eräiden tekoälyjärjestelmien valvonnasta annetun lain 3 §:ssä tarkoitettu markkinavalvontaviranomainen, hallinnollinen seuraamusmaksu määrätään mainitun lain 13 §:ssä säädetyssä järjestyksessä.

Edellä 35 §:ssä tarkoitetun hallinnollisen seuraamusmaksun määrää ilmoittava viranomainen.

Edellä 37 §:ssä tarkoitetun hallinnollisen seuraamusmaksun määrää kyberturvallisuussertifioinnin viranomainen.

Seuraamusmaksun määräävällä viranomaisella on oikeus salassapitosäännösten estämättä saada maksutta talouden toimijalta tai muulta viranomaiselta tiedot, jotka ovat välttämättömiä seuraamusmaksun määräämiseksi tai sen määrän arvioimiseksi.

40 §

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. Kyberturvallisuussertifiointia koskevasta rikkomuksesta ei saa määrätä 37 §:ssä tarkoitettua seuraamusmaksua sille, jolle on määrätty samasta teosta 31–36 §:ssä tarkoitettu seuraamusmaksu.

Seuraamusmaksua ei saa määrätä valtion viranomaisille, valtion liikelaitoksille, hyvinvointialueille tai -yhtymille, kunnallisille viranomaisille, itsenäisille julkisoikeudellisille laitoksille, eduskunnan virastoille, tasavallan presidentin kanslialle eikä Suomen evankelisluterilaiselle kirkolle tai Suomen ortodoksiselle kirkolle eikä niiden seurakunnille, seurakuntayhtymille tai muille elimille.

Valmistajalle, joka on mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä annetussa komission suosituksessa 2003/361/EY tarkoitettu mikro- tai pienyritys, ei saa määrätä seuraamusmaksua sillä perusteella, että yritys on ylittänyt kyberkestävyysasetuksen 14 artiklan 2 kohdan a alakohdassa tai mainitun artiklan 4 kohdan a alakohdassa tarkoitetun määräajan ennakkoilmoitukselle.

Seuraamusmaksua ei saa määrätä avoimen lähdekoodin ohjelmistovastaavalle.

41 §

Seuraamusmaksun täytäntöönpano

Tämän lain nojalla maksettavaksi määrätyn seuraamusmaksun täytäntöönpanosta säädetään sakon täytäntöönpanosta annetussa laissa (672/2002).

7 luku

Erinäiset säännökset

42 §

Oikaisuvaatimus

Ilmoitetun laitoksen antamaan päätökseen, kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen antamaan päätökseen sekä päätökseen, joka koskee

viranomaisen suoritteesta perittävää maksua, saa vaatia oikaisua. Oikaisuvaatimuksesta säädetään hallintolaissa.

43 §

Muutoksenhaku

Muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).

Markkinavalvontaviranomaisen muu kuin seuraamusmaksun määräämistä koskeva päätös voidaan panna täytäntöön muutoksenhausta huolimatta.

Ilmoittava viranomainen voi määrätä, että ilmoitetun laitoksen nimeämistä taikka nimeämisen rajaamista tai peruuttamista koskevaa päätöstä on noudatettava muutoksenhausta huolimatta.

Kyberturvallisuussertifioinnin viranomainen voi muussa kuin seuraamusmaksun määräämistä koskevassa päätöksessä määrätä, että päätöstä on noudatettava muutoksenhausta huolimatta.

Oikaisuvaatimuksesta annetussa ilmoitetun laitoksen tai kyberturvallisuussertifiointia varten ilmoitetun vaatimustenmukaisuuden arviointilaitoksen päätöksessä, joka koskee digitaalisen elementin sisältävän tuotteen valmistajalta tai eurooppalaisen kyberturvallisuussertifikaatin haltijalta vaadittavia korjaavia toimenpiteitä taikka digitaalisen elementin sisältävälle tuotteelle annetun vaatimustenmukaisuustodistuksen tai eurooppalaisen kyberturvallisuussertifikaatin peruuttamista, voidaan määrätä, että päätöstä on noudatettava muutoksenhausta huolimatta.

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

44 §

Maksut

Viranomaisten suoritteiden maksullisuudesta ja suoritteista perittävien maksujen suuruuden yleisistä perusteista sekä maksujen muista perusteista säädetään valtion maksuperustelaissa (150/1992).

45 §

Voimaantulo

Tämä laki tulee voimaan päivänä kuuta 20 .

Tämän lain 3 lukua ja 35 §:ää sovelletaan kuitenkin vasta 11 päivästä kesäkuuta 2026.

Tämän lain 7–9 §:ää ja 31 §:n 1 momentin 23–26 kohtaa sovelletaan kuitenkin vasta 11 päivästä syyskuuta 2026.

Tämän lain 4–6 §:ää, 31 §:n 1 momentin 1–22 kohtaa, 32–34 §:ää ja 36 §:ää sovelletaan kuitenkin vasta 11 päivästä joulukuuta 2027.

———

2.

Laki

eräiden tuotteiden markkinavalvonnasta annetun lain 1 ja 4 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan eräiden tuotteiden markkinavalvonnasta annetun lain (1137/2016) 1 §:n 1 momentin 32 kohta ja 4 §:n 4 momentti,

sellaisina kuin ne ovat, 1 §:n 1 momentin 32 kohta laissa 186/2025 ja 4 §:n 4 momentti laissa 103/2023, sekä

lisätään 1 §:n 1 momenttiin, sellaisena kuin se on laissa 186/2025, uusi 33 kohta seuraavasti:

1 §

Soveltamisala

Tätä lakia sovelletaan seuraavien lakien soveltamisalaan kuuluvien tuotteiden markkinavalvontaan, jollei mainituissa laeissa toisin säädetä:

— —

32) kuluttajatuotteiden turvallisuudesta annettu laki (184/2025);

33) eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista annettu laki (/).

— —

4 §

Valvontaviranomaiset

— —

Poiketen siitä, mitä 1 momentissa säädetään, Liikenne- ja viestintävirasto on tässä laissa tarkoitettu markkinavalvontaviranomainen ilmailulaissa, ajoneuvolaissa, ympäristönsuojelulain 24 a §:n 3 momentissa, huviveneiden turvallisuudesta ja päästövaatimuksista annetussa laissa, sähköisen viestinnän palveluista annetussa laissa, laivavarustelaissa ja eräiden tuotteiden esteettömyysvaatimuksista annetussa laissa tarkoitettujen tuotteiden osalta. Liikenne- ja viestintävirasto on tässä laissa tarkoitettu markkinavalvontaviranomainen myös eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista annetussa laissa tarkoitettujen tuotteiden osalta, ellei mainitussa laissa toisin säädetä.

— —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

3.

Laki

kyberturvallisuuslain 20 ja 28 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan kyberturvallisuuslain (124/2025) 20 §:n 1 momentin 9 kohta ja 28 §:n 4 momentti, sellaisena kuin niistä 28 §:n 4 momentti laissa 369/2025, sekä

lisätään 20 §:n 1 momenttiin uusi 10 kohta seuraavasti:

20 §

CSIRT-yksikön tehtävät

CSIRT-yksikön tehtävänä on:

— —

9) antaa ohjeita ja suosituksia poikkeamien käsittelemisestä, kyberturvallisuuden kriisinhallinnasta ja koordinoidusta haavoittuvuuksien julkistamisesta;

10) vastaanottaa ja käsitellä digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) N:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2024/2847 (kyberkestävyyssäädös) 14 ja 15 artiklassa tarkoitettuja ilmoituksia sekä vastata muista mainitussa asetuksessa sekä eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista annetussa laissa (/) CSIRT-yksikölle säädetyistä tehtävistä.

— —

28 §

Tiedonsaantioikeus

— —

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, CSIRT-yksikölle ja yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 19 §:ssä tarkoitetulle valvovalle viranomaiselle sekä Finanssivalvonnalle, jos se on välttämätöntä tässä laissa tai yhteiskunnan kriittisen infrastruktuurin suojaamisesta annetussa laissa viranomaiselle säädettyä tehtävää varten taikka Finanssivalvonnasta annetun lain (878/2008) 50 p §:n 1 ja 2 momentissa tarkoitettua toimivaltaisen viranomaisen tehtävää varten. Tiedonsaantioikeuden käyttämisellä tai tietojen luovuttamisella ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.

— —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

4.

Laki

sähköisen viestinnän palveluista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan sähköisen viestinnän palveluista annetun lain (917/2014) 304 §:n 1 momentin 14 kohta, sellaisena kuin se on laissa 1211/2022,

muutetaan 3 §:n 35 kohta, 21 luvun otsikko ja 164 §:n 2 momentti, sellaisena kuin niistä on 164 §:n 2 momentti laissa 1003/2018, sekä

lisätään 3 §:ään, sellaisena kuin se on osaksi laeissa 456/2016, 52/2019, 1207/2020, 1211/2022, 105/2023 ja 661/2024, uusi 35 a kohta, 164 §:ään, sellaisena kuin se on laissa 1003/2018, uusi 4 momentti ja lakiin uusi 21 a luku seuraavasti:

3 §

Määritelmät

Tässä laissa tarkoitetaan:

— —

35) *verkkotunnuksella* kirjaimista, numeroista tai muista merkeistä taikka niiden yhdistelmistä muodostuvaa internet-verkossa käytettävää nimimuotoista toisen asteen osoitetietoa;

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

— —

21 luku

Suomen ja Ahvenanmaan verkkotunnukset

164 §

Liikenne- ja viestintäviraston verkkotunnustoiminta ja verkkotunnusten välittäminen

— —

Merkintöjä verkkotunnusrekisteriin voi tehdä vain 165 §:ssä tarkoitetun ilmoituksen tehnyt verkkotunnusvälittäjä. Liikenne- ja viestintävirasto voi kuitenkin merkitä verkkotunnushallinnon tarpeita varten yksimerkkisiä ja muita verkkotunnuksia maksutta. Liikenne- ja viestintävirasto voi tehdä verkkotunnusrekisteriin myös muita tämän lain toteutumisen kannalta tarpeellisia merkintöjä.

— —

Mitä 165 §:ssä, 170 §:n 1 momentin 2 ja 8–11 kohdassa sekä 171 §:ssä säädetään verkkotunnusvälittäjästä, sovelletaan myös verkkotunnusvälittäjän puolesta toimivaan verkkotunnusten rekisteröintipalveluja tarjoavaan tahoon.

21 a luku

Muut verkkotunnukset

172 a §

Luvun soveltamisala

Tätä lukua sovelletaan muihin kuin Suomen tai Ahvenanmaan aluetunnukseen päättyviin verkkotunnuksiin ja niiden välittämiseen.

Tätä lukua sovelletaan sellaiseen aluetunnusrekisterin ylläpitäjään ja verkkotunnusvälittäjään, jonka päätoimipaikka tai Euroopan unioniin nimetty edustaja sijaitsee Suomessa. Jos verkkotunnusvälittäjä ei ole sijoittautunut Euroopan unionin jäsenvaltioon mutta 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. Tätä lukua sovelletaan myös verkkotunnusvälittäjään, joka tarjoaa palveluita Suomessa, ei ole sijoittautunut Euroopan unionin jäsenvaltioon eikä ole asettanut NIS 2 -direktiivin 26 artiklan 3 kohdassa tarkoitettua nimettyä edustajaa.

Mitä tässä luvussa säädetään verkkotunnusvälittäjästä, sovelletaan myös verkkotunnusvälittäjän puolesta toimivaan verkkotunnusten rekisteröintipalveluja tarjoavaan tahoon.

172 b §

Verkkotunnusvälittäjän ilmoitus

Verkkotunnusvälittäjän on ilmoitettava Liikenne- ja viestintävirastolle:

1) nimensä;

2) osoitteensa, sähköpostiosoitteensa, puhelinnumeronsa ja muut ajantasaiset yhteystietonsa;

3) päätoimipaikkansa ja muiden Euroopan unionissa sijaitsevien laillisten toimipaikkojensa osoite, tai, jos verkkotunnusvälittäjä ei ole sijoittautunut Euroopan unioniin, sen Euroopan unioniin nimetyn edustajan osoite, sähköpostiosoite, puhelinnumero ja muut ajantasaiset yhteystiedot;

4) verkkotunnusvälittäjän IP-osoitealueet;

5) luettelo niistä Euroopan unionin jäsenvaltioista, joissa se tarjoaa palveluita.

Verkkotunnusvälittäjän on ilmoitettava Liikenne- ja viestintävirastolle viipymättä muutoksista 1 momentissa tarkoitettuihin tietoihin. Muutoksesta on ilmoitettava Liikenne- ja viestintävirastolle kahden viikon kuluessa muutoshetkestä. Muutoksesta mainitun momentin 3 kohdassa tarkoitettuihin tietoihin on kuitenkin ilmoitettava kolmen kuukauden kuluessa muutoshetkestä. Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä tietojen ilmoittamisesta.

Liikenne- ja viestintäviraston on toimitettava NIS 2 -direktiivin 27 artiklan 4 kohdassa tarkoitetun ilmoituksen tekemiseksi tarpeelliset tiedot verkkotunnusvälittäjien ilmoituksista kyberturvallisuuslain 18 §:ssä tarkoitetulle keskitetylle yhteyspisteelle.

172 c §

Verkkotunnusten rekisteröintitiedot

Aluetunnusrekisterin ylläpitäjän ja verkkotunnusvälittäjän on kerättävä ja ylläpidettävä verkkotunnusten rekisteröintitietoja. Verkkotunnusten rekisteröintitietojen tietokannan tulee sisältää NIS 2 -direktiivin 28 artiklan 2 kohdassa tarkoitetut tiedot verkkotunnuksista.

Aluetunnusrekisterin ylläpitäjällä ja verkkotunnusvälittäjällä on oltava käytössään toimintaperiaatteet ja menettelyt, joilla varmistetaan, että verkkotunnusten rekisteröintitietojen tietokannan tiedot ovat tarkat ja oikeat. Aluetunnusrekisterin ylläpitäjän ja verkkotunnusvälittäjän on asetettava julkisesti saataville käytössään olevat toimintaperiaatteet ja menettelyt.

172 d §

Verkkotunnusten rekisteröintitietojen saatavuus

Aluetunnusrekisterin ylläpitäjän ja verkkotunnusvälittäjän on asetettava julkisesti saataville ilman aiheetonta viivytystä verkkotunnuksen rekisteröinnin jälkeen muut verkkotunnuksen rekisteröintitiedot kuin henkilötiedot.

Aluetunnusrekisterin ylläpitäjän ja verkkotunnusvälittäjän on annettava pääsy muihin kuin 1 momentissa tarkoitettuihin verkkotunnusten rekisteröintitietoihin, jos tietoihin pääsyä oikeutetusti pyytävä esittää lainmukaisen ja asianmukaisesti perustellun pyynnön. Aluetunnusrekisterin ylläpitäjän ja verkkotunnusvälittäjän on vastattava verkkotunnusten rekisteröintitietoihin pääsyä koskevaan pyyntöön ilman aiheetonta viivytystä ja viimeistään 72 tunnin kuluessa pyynnön vastaanottamisesta. Aluetunnusrekisterin ylläpitäjän ja verkkotunnusvälittäjän on asetettava julkisesti saataville käytössään olevat toimintaperiaatteet ja menettelyt verkkotunnusten rekisteröintitietojen luovuttamisesta.

Aluetunnusrekisterin ylläpitäjän ja verkkotunnusvälittäjän on tehtävä yhteistyötä 172 c §:ssä ja tässä pykälässä säädettyjen velvoitteiden toteuttamiseksi ja päällekkäisten rekisteröintitietojen keräämisen välttämiseksi.

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 tietosuojalaissa.

Tämä laki tulee voimaan päivänä kuuta 20 . Lain 304 §:n 1 momentin 14 kohdan kumoaminen tulee kuitenkin voimaan vasta 1 päivänä kesäkuuta 2026.

Verkkotunnusvälittäjän puolesta toimivan verkkotunnusten rekisteröintipalveluja tarjoavan tahon on tehtävä sähköisen viestinnän palveluista annetun lain 165 §:n mukainen ilmoitus kolmen kuukauden kuluessa tämän lain voimaantulosta.

Tämän lain 172 b §:ssä tarkoitettu ilmoitus on tehtävä kolmen kuukauden kuluessa lain voimaantulosta.

Tämän lain 172 c ja 172 d §:ssä tarkoitetut toimintaperiaatteet ja menettelyt on asetettava julkisesti saataville kolmen kuukauden kuluessa lain voimaantulosta.

5.

Laki

sakon täytäntöönpanosta annetun lain 1 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan sakon täytäntöönpanosta annetun lain (672/2002) 1 §:n 2 momentin 60 kohta, sellaisena kuin se on laissa 860/2025, sekä

lisätään 1 §:n 2 momenttiin, sellaisena kuin se on laeissa 416/2025 ja 860/2025, uusi 61 kohta seuraavasti:

1 §

Lain soveltamisala

— —

Tässä laissa säädetään seuraavien rangaistusluonteisten hallinnollisten seuraamusten täytäntöönpanosta:

— —

60) vaarallisten aineiden kuljetuksesta Puolustusvoimissa ja Rajavartiolaitoksessa annetun lain (849/2025) 122 §:ssä tarkoitettu liikennevirhemaksu;

61) eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista annetun lain (/) 31–37 §:ssä tarkoitettu seuraamusmaksu.

— —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

Helsingissä 27.11.2025

Pääministeri

Petteri Orpo

Liikenne- ja viestintäministeri Lulu Ranne

2.

Laki

eräiden tuotteiden markkinavalvonnasta annetun lain 1 ja 4 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan eräiden tuotteiden markkinavalvonnasta annetun lain (1137/2016) 1 §:n 1 momentin 32 kohta ja 4 §:n 4 momentti,

sellaisina kuin ne ovat, 1 §:n 1 momentin 32 kohta laissa 186/2025 ja 4 §:n 4 momentti laissa 103/2023, sekä

lisätään 1 §:n 1 momenttiin, sellaisena kuin se on laissa 186/2025, uusi 33 kohta seuraavasti:

Voimassa oleva laki	*Ehdotus*
1 §	1 §
Soveltamisala	*Soveltamisala*
Tätä lakia sovelletaan seuraavien lakien soveltamisalaan kuuluvien tuotteiden markkinavalvontaan, jollei mainituissa laeissa toisin säädetä:	Tätä lakia sovelletaan seuraavien lakien soveltamisalaan kuuluvien tuotteiden markkinavalvontaan, jollei mainituissa laeissa toisin säädetä:
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
32) kuluttajatuotteiden turvallisuudesta annettu laki (184/2025).	32) kuluttajatuotteiden turvallisuudesta annettu laki (184/2025)*;*
(uusi)	*33) eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista annettu laki (/).*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
4 §	4 §
Valvontaviranomaiset	*Valvontaviranomaiset*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Poiketen siitä, mitä 1 momentissa säädetään, Liikenne- ja viestintävirasto on tässä laissa tarkoitettu markkinavalvontaviranomainen ilmailulaissa, ajoneuvolaissa, ympäristönsuojelulain 24 a §:n 3 momentissa, huviveneiden turvallisuudesta ja päästövaatimuksista annetussa laissa, sähköisen viestinnän	Poiketen siitä, mitä 1 momentissa säädetään, Liikenne- ja viestintävirasto on tässä laissa tarkoitettu markkinavalvontaviranomainen ilmailulaissa, ajoneuvolaissa, ympäristönsuojelulain 24 a §:n 3 momentissa, huviveneiden turvallisuudesta ja päästövaatimuksista annetussa laissa, sähköisen viestinnän

Voimassa oleva laki	*Ehdotus*
palveluista annetussa laissa, laivavarustelaissa ja eräiden tuotteiden esteettömyysvaatimuksista annetussa laissa tarkoitettujen tuotteiden osalta.	palveluista annetussa laissa, laivavarustelaissa ja eräiden tuotteiden esteettömyysvaatimuksista annetussa laissa tarkoitettujen tuotteiden osalta. *Liikenne- ja viestintävirasto on tässä laissa tarkoitettu markkinavalvontaviranomainen myös eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista annetussa laissa tarkoitettujen tuotteiden osalta, ellei mainitussa laissa toisin säädetä.*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

3.

Laki

kyberturvallisuuslain 20 ja 28 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan kyberturvallisuuslain (124/2025) 20 §:n 1 momentin 9 kohta ja 28 §:n 4 momentti, sellaisena kuin niistä 28 §:n 4 momentti laissa 369/2025, sekä
lisätään 20 §:n 1 momenttiin uusi 10 kohta seuraavasti:

Voimassa oleva laki	*Ehdotus*
20 §	20 §
CSIRT-yksikön tehtävät	*CSIRT-yksikön tehtävät*
CSIRT-yksikön tehtävänä on:	CSIRT-yksikön tehtävänä on:
— — — — — — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — — — — — —
9) antaa ohjeita ja suosituksia poikkeamien käsittelemisestä, kyberturvallisuuden kriisinhallinnasta ja koordinoidusta haavoittuvuuksien julkistamisesta.	9) antaa ohjeita ja suosituksia poikkeamien käsittelemisestä, kyberturvallisuuden kriisinhallinnasta ja koordinoidusta haavoittuvuuksien julkistamisesta*;*
(uusi)	*10) vastaanottaa ja käsitellä digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) N:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2024/2847 (kyberkestävyyssäädös) 14 ja 15 artiklassa tarkoitettuja ilmoituksia sekä vastata muista mainitussa asetuksessa sekä eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista annetussa laissa (/) CSIRT-yksikölle säädetyistä tehtävistä.*
— — — — — — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — — — — — —
28 §	28 §
Tiedonsaantioikeus	*Tiedonsaantioikeus*
— — — — — — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — — — — — —
Valvovalla viranomaisella on salassapitosäännösten, 2 momentissa	Valvovalla viranomaisella on salassapitosäännösten, 2 momentissa

Voimassa oleva laki	*Ehdotus*
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, CSIRT-yksikölle ja yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 19 §:ssä tarkoitetulle valvovalle viranomaiselle, jos se on välttämätöntä tässä laissa tai yhteiskunnan kriittisen infrastruktuurin suojaamisesta annetussa laissa viranomaiselle säädettyä tehtävää varten. Tiedonsaantioikeuden käyttämisellä tai tietojen luovuttamisella ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.	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, CSIRT-yksikölle ja yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 19 §:ssä tarkoitetulle valvovalle viranomaiselle *sekä Finanssivalvonnalle*, jos se on välttämätöntä tässä laissa tai yhteiskunnan kriittisen infrastruktuurin suojaamisesta annetussa laissa viranomaiselle säädettyä tehtävää varten *taikka Finanssivalvonnasta annetun lain (878/2008) 50 p §:n 1 ja 2 momentissa tarkoitettua toimivaltaisen viranomaisen tehtävää varten*. Tiedonsaantioikeuden käyttämisellä tai tietojen luovuttamisella ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
	————
	Tämä laki tulee voimaan päivänä kuuta 20 .
	————

4.

Laki

sähköisen viestinnän palveluista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan sähköisen viestinnän palveluista annetun lain (917/2014) 304 §:n 1 momentin 14 kohta, sellaisena kuin se on laissa 1211/2022,

muutetaan 3 §:n 35 kohta, 21 luvun otsikko ja 164 §:n 2 momentti, sellaisena kuin niistä on 164 §:n 2 momentti laissa 1003/2018, sekä

lisätään 3 §:ään, sellaisena kuin se on osaksi laeissa 456/2016, 52/2019, 1207/2020, 1211/2022, 105/2023 ja 661/2024, uusi 35 a kohta, 164 §:ään, sellaisena kuin se on laissa 1003/2018, uusi 4 momentti ja lakiin uusi 21 a luku seuraavasti:

Voimassa oleva laki	*Ehdotus*
3 §	3 §
Määritelmät	*Määritelmät*
Tässä laissa tarkoitetaan:	Tässä laissa tarkoitetaan:
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
35) *verkkotunnuksella* kirjaimista, numeroista tai muista merkeistä taikka niiden yhdistelmistä muodostuvaa internet-verkossa käytettävää *fi-maatunnuksen ja ax-maakuntatunnuksen alaista* nimimuotoista osoitetietoa;	35) *verkkotunnuksella* kirjaimista, numeroista tai muista merkeistä taikka niiden yhdistelmistä muodostuvaa internet-verkossa käytettävää nimimuotoista *toisen asteen* osoitetietoa;
(uusi)	*35 a) aluetunnusrekisterin ylläpitäjällä tahoa, jolle on myönnetty oikeus hallinnoida tiettyä aluetunnusta ja joka sitä hallinnoidessaan vastaa verkkotunnusten rekisteröinnistä sen alle sekä sen teknisestä toiminnasta;*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
21 luku	21 luku
Verkkotunnukset	***Suomen ja Ahvenanmaan verkkotunnukset***
164 §	164 §
Liikenne- ja viestintäviraston verkkotunnustoiminta ja verkkotunnusten välittäminen	*Liikenne- ja viestintäviraston verkkotunnustoiminta ja verkkotunnusten välittäminen*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Merkintöjä verkkotunnusrekisteriin voi tehdä vain 165 §:ssä tarkoitetun	Merkintöjä verkkotunnusrekisteriin voi tehdä vain 165 §:ssä tarkoitetun *ilmoituksen*

Voimassa oleva laki	*Ehdotus*
verkkotunnusvälitysilmoituksen tehnyt toiminnanharjoittaja (verkkotunnusvälittäjä). Liikenne- ja viestintävirasto voi kuitenkin merkitä verkkotunnushallinnon tarpeita varten yksimerkkisiä ja muita verkkotunnuksia maksutta. Liikenne- ja viestintävirasto voi tehdä verkkotunnusrekisteriin myös muita tämän lain toteutumisen kannalta tarpeellisia merkintöjä.	*tehnyt verkkotunnusvälittäjä*. Liikenne- ja viestintävirasto voi kuitenkin merkitä verkkotunnushallinnon tarpeita varten yksimerkkisiä ja muita verkkotunnuksia maksutta. Liikenne- ja viestintävirasto voi tehdä verkkotunnusrekisteriin myös muita tämän lain toteutumisen kannalta tarpeellisia merkintöjä.
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
(uusi)	*Mitä 165 §:ssä, 170 §:n 1 momentin 2 ja 8–11 kohdassa sekä 171 §:ssä säädetään verkkotunnusvälittäjästä, sovelletaan myös verkkotunnusvälittäjän puolesta toimivaan verkkotunnusten rekisteröintipalveluja tarjoavaan tahoon.*
	21 a luku
	Muut verkkotunnukset
	172 a §
	Luvun soveltamisala
(uusi)	*Tätä lukua sovelletaan muihin kuin Suomen tai Ahvenanmaan aluetunnukseen päättyviin verkkotunnuksiin ja niiden välittämiseen.* *Tätä lukua sovelletaan sellaiseen aluetunnusrekisterin ylläpitäjään ja verkkotunnusvälittäjään, jonka päätoimipaikka tai Euroopan unioniin nimetty edustaja sijaitsee Suomessa. Jos verkkotunnusvälittäjä ei ole sijoittautunut Euroopan unionin jäsenvaltioon mutta 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. Tätä lukua sovelletaan myös verkkotunnusvälittäjään, joka tarjoaa palveluita Suomessa, ei ole sijoittautunut Euroopan unionin jäsenvaltioon eikä ole asettanut NIS 2 -direktiivin 26 artiklan 3 kohdassa tarkoitettua nimettyä edustajaa.* *Mitä tässä luvussa säädetään verkkotunnusvälittäjästä, sovelletaan myös*

verkkotunnusvälittäjän puolesta toimivaan verkkotunnusten rekisteröintipalveluja tarjoavaan tahoon.

172 b §

Verkkotunnusvälittäjän ilmoitus

Verkkotunnusvälittäjän on ilmoitettava Liikenne- ja viestintävirastolle:

1) nimensä;

2) osoitteensa, sähköpostiosoitteensa, puhelinnumeronsa ja muut ajantasaiset yhteystietonsa;

3) päätoimipaikkansa ja muiden Euroopan unionissa sijaitsevien laillisten toimipaikkojensa osoite, tai, jos verkkotunnusvälittäjä ei ole sijoittautunut Euroopan unioniin, sen Euroopan unioniin nimetyn edustajan osoite, sähköpostiosoite, puhelinnumero ja muut ajantasaiset yhteystiedot;

4) verkkotunnusvälittäjän IP-osoitealueet;

5) luettelo niistä Euroopan unionin jäsenvaltioista, joissa se tarjoaa palveluita.

Verkkotunnusvälittäjän on ilmoitettava Liikenne- ja viestintävirastolle viipymättä muutoksista 1 momentissa tarkoitettuihin tietoihin. Muutoksesta on ilmoitettava Liikenne- ja viestintävirastolle kahden viikon kuluessa muutoshetkestä. Muutoksesta mainitun momentin 3 kohdassa tarkoitettuihin tietoihin on kuitenkin ilmoitettava kolmen kuukauden kuluessa muutoshetkestä. Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä tietojen ilmoittamisesta.

Liikenne- ja viestintäviraston on toimitettava NIS 2 -direktiivin 27 artiklan 4 kohdassa tarkoitetun ilmoituksen tekemiseksi tarpeelliset tiedot verkkotunnusvälittäjien ilmoituksista kyberturvallisuuslain 18 §:ssä tarkoitetulle keskitetylle yhteyspisteelle.

172 c §

Verkkotunnusten rekisteröintitiedot

Voimassa oleva laki *Ehdotus*

Aluetunnusrekisterin ylläpitäjän ja verkkotunnusvälittäjän on kerättävä ja ylläpidettävä verkkotunnusten rekisteröintitietoja. Verkkotunnusten rekisteröintitietojen tietokannan tulee sisältää NIS 2 -direktiivin 28 artiklan 2 kohdassa tarkoitetut tiedot verkkotunnuksista.

Aluetunnusrekisterin ylläpitäjällä ja verkkotunnusvälittäjällä on oltava käytössään toimintaperiaatteet ja menettelyt, joilla varmistetaan, että verkkotunnusten rekisteröintitietojen tietokannan tiedot ovat tarkat ja oikeat. Aluetunnusrekisterin ylläpitäjän ja verkkotunnusvälittäjän on asetettava julkisesti saataville käytössään olevat toimintaperiaatteet ja menettelyt.

172 d §

Verkkotunnusten rekisteröintitietojen saatavuus

Aluetunnusrekisterin ylläpitäjän ja verkkotunnusvälittäjän on asetettava julkisesti saataville ilman aiheetonta viivytystä verkkotunnuksen rekisteröinnin jälkeen muut verkkotunnuksen rekisteröintitiedot kuin henkilötiedot.

Aluetunnusrekisterin ylläpitäjän ja verkkotunnusvälittäjän on annettava pääsy muihin kuin 1 momentissa tarkoitettuihin verkkotunnusten rekisteröintitietoihin, jos tietoihin pääsyä oikeutetusti pyytävä esittää lainmukaisen ja asianmukaisesti perustellun pyynnön. Aluetunnusrekisterin ylläpitäjän ja verkkotunnusvälittäjän on vastattava verkkotunnusten rekisteröintitietoihin pääsyä koskevaan pyyntöön ilman aiheetonta viivytystä ja viimeistään 72 tunnin kuluessa pyynnön vastaanottamisesta. Aluetunnusrekisterin ylläpitäjän ja verkkotunnusvälittäjän on asetettava julkisesti saataville käytössään olevat toimintaperiaatteet ja menettelyt verkkotunnusten rekisteröintitietojen luovuttamisesta.

Aluetunnusrekisterin ylläpitäjän ja verkkotunnusvälittäjän on tehtävä yhteistyötä 172 c §:ssä ja tässä pykälässä säädettyjen

Voimassa oleva laki	*Ehdotus*
	velvoitteiden toteuttamiseksi ja päällekkäisten rekisteröintitietojen keräämisen välttämiseksi. *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 tietosuojalaissa.*
304 §	304 §
Liikenne- ja viestintäviraston erityiset tehtävät	*Liikenne- ja viestintäviraston erityiset tehtävät*
Sen lisäksi, mitä muualla tässä laissa säädetään, Liikenne- ja viestintäviraston tehtävänä on:	Sen lisäksi, mitä muualla tässä laissa säädetään, Liikenne- ja viestintäviraston tehtävänä on:
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
14) toimia Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus) annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 mukaisena kansallisena kyberturvallisuussertifioinnin viranomaisena;	(kumotaan)
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
	——— *Tämä laki tulee voimaan päivänä kuuta 20 . Lain 304 §:n 1 momentin 14 kohdan kumoaminen tulee kuitenkin voimaan vasta 1 päivänä kesäkuuta 2026.* *Verkkotunnusvälittäjän puolesta toimivan verkkotunnusten rekisteröintipalveluja tarjoavan tahon on tehtävä sähköisen viestinnän palveluista annetun lain 165 §:n mukainen ilmoitus kolmen kuukauden kuluessa tämän lain voimaantulosta.* *Tämän lain 172 b §:ssä tarkoitettu ilmoitus on tehtävä kolmen kuukauden kuluessa lain voimaantulosta.* *Tämän lain 172 c ja 172 d §:ssä tarkoitetut toimintaperiaatteet ja menettelyt on*

Voimassa oleva laki	*Ehdotus*
	asetettava julkisesti saataville kolmen kuukauden kuluessa lain voimaantulosta.

5.

Laki

sakon täytäntöönpanosta annetun lain 1 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan sakon täytäntöönpanosta annetun lain (672/2002) 1 §:n 2 momentin 60 kohta, sellaisena kuin se on laissa 860/2025, sekä

lisätään 1 §:n 2 momenttiin, sellaisena kuin se on laeissa 416/2025 ja 860/2025, uusi 61 kohta seuraavasti:

Voimassa oleva laki	*Ehdotus*
1 §	1 §
Lain soveltamisala	*Lain soveltamisala*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Tässä laissa säädetään seuraavien rangaistusluonteisten hallinnollisten seuraamusten täytäntöönpanosta:	Tässä laissa säädetään seuraavien rangaistusluonteisten hallinnollisten seuraamusten täytäntöönpanosta:
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
60) vaarallisten aineiden kuljetuksesta Puolustusvoimissa ja Rajavartiolaitoksessa annetun lain (849/2025) 122 §:ssä tarkoitettu liikennevirhemaksu.	60) vaarallisten aineiden kuljetuksesta Puolustusvoimissa ja Rajavartiolaitoksessa annetun lain (849/2025) 122 §:ssä tarkoitettu liikennevirhemaksu*;*
(uusi)	*61) eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista annetun lain (/) 31–37 §:ssä tarkoitettu seuraamusmaksu.*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———