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;

HE 179/2025 vp
LiVM 6/2026 vp
EV 55/2026 vp

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 (1377/2025).

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 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 ohjelmistovastaavan valvonta

Markkinavalvontaviranomainen voi ohjeistaa avoimen lähdekoodin ohjelmistovastaavaa kyberkestävyysasetuksessa säädetyistä velvollisuuksista sekä ehdottaa käytännöllisiä parannuksia ohjelmistovastaavan ylläpitämän avoimen lähdekoodin ohjelmistoprojektin sisältöön tai toimintatapoihin.

Markkinavalvontaviranomainen voi velvoittaa avoimen lähdekoodin ohjelmistovastaavan korjaamaan kohtuullisessa määräajassa havaitsemansa puutteet kyberkestävyysasetuksessa säädettyjen velvollisuuksien noudattamisessa. Markkinavalvontaviranomainen voi julkaista tietoja havaitsemistaan puutteista tai tiedottaa asiasta, mikäli havaittuja puutteita ei korjata kohtuullisessa määräajassa.

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 suoritettava 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 1 päivänä kesäkuuta 2026.

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.

Helsingissä 29.5.2026

Tasavallan Presidentti

Alexander Stubb

Liikenne- ja viestintäministeri Lulu Ranne