EUROOPAN
KOMISSIO

Bryssel 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS

digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvavaatimuksista ja asetuksen (EU) 2019/1020 muuttamisesta

(ETA:n kannalta merkityksellinen teksti)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

PERUSTELUT

1. EHDOTUKSEN TAUSTA

• Ehdotuksen perustelut ja tavoitteet

Laitteisto- ja ohjelmistotuotteisiin kohdistuu enenevässä määrin onnistuneita kyberhyökkäyksiä. Kyberrikollisuuden arvioidut maailmanlaajuiset vuotuiset kokonaiskustannukset olivat vuoteen 2021 mennessä nousseet jo 5,5 biljoonaan euroon. Tällaisiin tuotteisiin liittyy kaksi merkittävää ongelmaa, jotka aiheuttavat käyttäjille ja yhteiskunnalle lisäkustannuksia: 1) kyberturvallisuuden alhainen taso, joka johtuu laajalle levinneistä haavoittuvuuksista ja niiden korjaamiseksi tarvittavien tietoturvapäivitysten riittämättömästä ja epäjohdonmukaisesta tarjonnasta ja 2) käyttäjien riittämätön ymmärrys ja tiedonsaanti, mikä estää valitsemasta tuotteita, joilla on riittävät kyberturvaominaisuudet, tai estää käyttämästä tuotteita tietoturvallisesti. Verkotetussa ympäristössä yhden tuotteen kyberturvapoikkeama voi vaikuttaa kokonaiseen organisaatioon tai koko toimitusketjuun, ja se leviää sisämarkkinoilla rajojen yli usein minuuteissa. Tämä voi johtaa taloudellisen ja sosiaalisen toiminnan vakaviin häiriöihin tai jopa hengenvaaraan.

Digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuudella on vahva rajat ylittävä ulottuvuus, sillä yhdessä maassa valmistettuja tuotteita käytetään usein monissa muissa maissa sisämarkkinoilla. Lisäksi tietoturvapoikkeamat, jotka vaikuttavat alun perin yhteen toimijaan tai yhteen jäsenvaltioon, leviävät usein minuuteissa koko sisämarkkinoille.

Vaikka nykyistä sisämarkkinalainsäädäntöä sovelletaan tiettyihin digitaalisia elementtejä sisältäviin tuotteisiin, suurin osa laitteisto- ja ohjelmistotuotteista ei tällä hetkellä kuulu minkään kyberturvallisuutta koskevan EU-lainsäädännön piiriin. Nykyisessä EU:n oikeudellisessa kehyksessä ei käsitellä sulauttamattomien ohjelmistojen kyberturvallisuutta, vaikka tällaisten tuotteiden haavoittuvuuksiin kohdistuu yhä enemmän kyberhyökkäyksiä, mikä aiheuttaa merkittäviä yhteiskunnallisia ja taloudellisia kustannuksia. On olemassa lukuisia esimerkkejä merkittävistä kyberhyökkäyksistä, jotka ovat seurausta tuotteiden epäoptimaalisesta tietoturvasta, kuten WannaCry-kiristysohjelma, joka hyödynsi Windows-käyttöjärjestelmän haavoittuvuutta. Se saastutti 200 000 tietokonetta 150 maassa vuonna 2017 ja aiheutti miljardien Yhdysvaltain dollarien vahingot. Kaseya VSA -toimitusketjuhyökkäyksessä hyökättiin Kaseyan verkonhallintaohjelmiston avulla yli tuhanteen yritykseen ja muun muassa pakotettiin ruotsalainen valintamyymäläketju sulkemaan kaikki 500 myymäläänsä eri puolilla Ruotsia. On myös lukuisia tapauksia, joissa pankkisovelluksia on hakkeroitu rahan varastamiseksi kuluttajilta.

Sisämarkkinoiden moitteettoman toiminnan varmistamiseksi asetettiin kaksi päätavoitetta: 1) luodaan edellytykset digitaalisia elementtejä sisältävien tietoturvallisten tuotteiden kehittämiselle varmistamalla, että laitteisto- ja ohjelmistotuotteet saatetaan markkinoille vähemmin haavoittuvuuksin ja että valmistajat suhtautuvat tietoturvaan vakavasti tuotteen koko elinkaaren ajan ja 2) luodaan olosuhteet, joissa käyttäjät voivat ottaa kyberturvan huomioon valitessaan ja käyttäessään digitaalisia elementtejä sisältäviä tuotteita. Lisäksi asetettiin neljä erityistavoitetta: i) varmistetaan, että valmistajat parantavat digitaalisia elementtejä sisältävien tuotteiden tietoturvaa suunnittelu- ja kehitysvaiheesta lähtien ja koko elinkaaren ajan, ii) luodaan johdonmukaiset kyberturvapuitteet, joissa laite- ja ohjelmistovalmistajien on helpompi noudattaa vaatimuksia, iii) lisätään läpinäkyvyyttä digitaalisia elementtejä sisältävien tuotteiden tietoturvaominaisuuksien suhteen ja iv) luodaan yrityksille ja kuluttajille edellytyksiä käyttää digitaalisia elementtejä sisältäviä tuotteita tietoturvallisesti.

Kyberturvallisuuden selkeästi rajat ylittävä luonne ja lisääntyvät poikkeamat, joilla on heijastusvaikutuksia yli maiden, toimialojen ja tuotteiden rajojen, merkitsevät, että jäsenvaltiot eivät voi saavuttaa tavoitteita tuloksellisesti yksin. Koska digitaalisia elementtejä sisältävien tuotteiden markkinat ovat maailmanlaajuiset, jäsenvaltiot kohtaavat kaikki alueellaan samoja riskejä samojen tuotteiden osalta. Kehittymässä oleva hajanainen, mahdollisesti toisistaan poikkeavista kansallisista säännöistä syntyvä ympäristö saattaa myös haitata digitaalisia elementtejä sisältävien tuotteiden avoimia ja kilpailukykyisiä sisämarkkinoita. Näin ollen tarvitaan EU:n tason yhteisiä toimia käyttäjien luottamuksen lisäämiseksi ja digitaalisia elementtejä sisältävien EU-lähtöisten tuotteiden houkuttelevuuden lisäämiseksi. Tämä hyödyttäisi myös sisämarkkinoita tarjoamalla oikeusvarmuutta ja luomalla tasapuoliset toimintaedellytykset digitaalisia elementtejä sisältävien tuotteiden toimittajille, mitä korostetaan myös Euroopan tulevaisuuskonferenssin loppuraportissa, jossa kansalaiset vaativat EU:lta vahvempaa roolia kyberuhkien torjunnassa.

- **Vuorovaikutus muiden alaa koskevien politiikkojen säännösten kanssa**

EU-kehys sisältää useita horisontaalisia säädöksiä, jotka kattavat tiettyjä kyberturvallisuuteen eri näkökulmista liittyviä seikkoja (tuotteet, palvelut, kriisinhallinta ja rikollisuus). Tietojärjestelmiin kohdistuvista hyökkäyksistä annettu direktiivi[1], jolla yhdenmukaistettiin useiden tietojärjestelmiin kohdistuvien rikosten kriminalisointi ja niistä määrättävät seuraamukset, tuli voimaan vuonna 2013. Elokuussa 2016 tuli voimaan verkko- ja tietojärjestelmien turvallisuudesta annettu direktiivi (EU) 2016/1148[2] (ns. NIS-direktiivi), joka on ensimmäinen EU:n laajuinen kyberturvallisuutta koskeva säädös. Direktiivin tarkistus, joka johti direktiiviin [direktiivi XXX/XXXX, ns. NIS2-direktiivi], nostaa EU:n yhteistä tavoitetasoa. Vuonna 2019 tuli voimaan EU:n kyberturvasäädös[3], jolla pyritään parantamaan tieto- ja viestintäteknisten tuotteiden, palvelujen ja prosessien tietoturvaa ottamalla käyttöön vapaaehtoinen eurooppalainen kyberturvallisuuden sertifiointikehys[4].

Koko toimitusketjun kyberturvallisuus voidaan varmistaa vain, jos kaikki sen osatekijät ovat kyberturvallisia. Edellä mainitussa EU:n lainsäädännössä on kuitenkin tältä osin huomattavia aukkoja, koska se ei sisällä digitaalisia elementtejä sisältävien tuotteiden tietoturvaa koskevia pakollisia vaatimuksia.

Ehdotettu kyberkestävyyssäädös kattaa markkinoille saatetut digitaalisia elementtejä sisältävät tuotteet, kun taas direktiivillä [direktiivi XXX/XXX (NIS2)] pyritään varmistamaan keskeisten ja tärkeiden toimijoiden tarjoamien palvelujen korkeatasoinen kyberturvallisuus. Direktiivin XXX/XXXX (NIS2) mukaan jäsenvaltioiden on varmistettava, että sen soveltamisalaan kuuluvat keskeiset ja tärkeät toimijat, kuten terveydenhuollon tai pilvipalvelujen tarjoajat ja julkishallinnon toimijat, toteuttavat asianmukaiset ja oikeasuhteiset

---

1 Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU, annettu 12 päivänä elokuuta 2013, tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta (EUVL L 218, 14.8.2013, s. 8).

2 Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa (EUVL L 194, 19.7.2016, s. 1).

3 Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvasäädös) (EUVL L 151, 7.6.2019, s. 15).

4 Kyberturvasäädös mahdollistaa tuoteryhmäkohtaisten sertifiointijärjestelmien kehittämisen. Kussakin järjestelmässä viitataan asiaa koskeviin standardeihin, teknisiin eritelmiin tai muihin järjestelmässä määriteltyihin kyberturvavaatimuksiin. Päätös luoda tietty kyberturvallisuuden sertifiointijärjestelmä perustuu riskinarviointiin.

tekniset, operatiiviset ja organisatoriset kyberturvatoimenpiteet. Tähän sisältyy muun muassa vaatimus varmistaa tietoturva verkko- ja tietojärjestelmien hankinnoissa, kehittämisessä ja ylläpidossa, mukaan lukien haavoittuvuuksien käsittely ja niistä tiedottaminen. Direktiivin [direktiivi XXX/XXXX (NIS2)] mukaan komissio hyväksyy täytäntöönpanosäädökset, joissa vahvistetaan tietyntyyppisten toimijoiden, kuten pilvipalveluntarjoajien, osalta kyseisiin toimenpiteisiin liittyvät tekniset ja menetelmävaatimukset, 21 kuukauden kuluessa direktiivin voimaantulopäivästä. Kaikkien muiden toimijoiden osalta komissio voi hyväksyä täytäntöönpanosäädöksiä, joissa vahvistetaan teknisiä ja menetelmävaatimuksia, sekä asettaa alakohtaisia vaatimuksia. Tällä kehyksellä varmistetaan, että myös palveluna tarjottavien ohjelmistojen (*Software-as-a-Service*) suunnittelua, kehittämistä ja haavoittuvuuksien käsittelyä varten on olemassa tekniset eritelmät ja vaatimukset, jotka vastaavat kyberkestävyyssäädöksen olennaisia kyberturvavaatimuksia. Tämä voisi olla keino varmistaa korkea kyberturvataso esimerkiksi sähköisissä terveystietojärjestelmissä, myös silloin, kun ne toimitetaan palveluna tarjottavien ohjelmistojen muodossa tai niitä kehitetään terveydenhuollon yksiköiden sisäisesti ehdotetun [eurooppalaisesta terveysdata-avaruudesta annetun asetuksen] mukaisesti.

Vuorovaikutus unionin muiden politiikkojen kanssa

Kuten tiedonannossa ”Euroopan digitaalista tulevaisuutta rakentamassa”[5] todetaan, on ratkaisevan tärkeää, että EU hyödyntää kaikki digiajan edut ja vahvistaa teollista ja innovointikapasiteettiaan turvallisten ja eettisten rajojen puitteissa. Euroopan datastrategiassa esitetään neljä pilaria – tietosuoja, perusoikeudet, turvallisuus ja kyberturvallisuus – datavetoisen yhteiskunnan olennaisina edellytyksinä.

Tuotteisiin, joihin voi sisältyä myös digitaalisia elementtejä, sovellettava EU:n nykyinen kehys[6] sisältää useita säädöksiä, kuten tiettyjä tuotteita koskevan EU:n lainsäädännön, joka kattaa turvallisuuteen liittyviä näkökohtia, ja tuotevastuuta koskevan yleisen lainsäädännön. Nyt käsillä oleva ehdotus on johdonmukainen nykyisen tuotteisiin liittyvän EU:n sääntelykehyksen sekä viimeaikaisten lainsäädäntöehdotusten, kuten komission asetusehdotuksen[7] [tekoälyasetus] kanssa.

Ehdotettua asetusta sovellettaisiin kaikkiin komission delegoidun asetuksen (EU) 2022/30 soveltamisalaan kuuluviin radiolaitteisiin. Lisäksi tässä asetuksessa säädetyt vaatimukset sisältävät kaikki direktiivin 2014/53/EU 3 artiklan 3 kohdan d, e ja f alakohdassa tarkoitettujen olennaisten vaatimusten osat, mukaan lukien kyseisen delegoidun asetuksen perusteella annetussa [Euroopan standardointijärjestöille esitetystä standardointipyynnöstä annetussa komission täytäntöönpanopäätöksessä XXX/2022] vahvistetut keskeiset osat. Sääntelyn päällekkäisyyden välttämiseksi komissio aikoo kumota delegoidun asetuksen tai muuttaa sitä ehdotetun asetuksen soveltamisalaan kuuluvien radiolaitteiden osalta siten, että niihin sovelletaan viimeksi mainittua asetusta, kun asetuksen soveltaminen alkaa.

---

5 Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle – *Euroopan digitaalista tulevaisuutta rakentamassa*, COM(2020) 67 final, 19.2.2020.

6 Pääasiassa ns. uuden lainsäädäntökehyksen (*New Legislative Framework*, NLF) mukaista lainsäädäntöä.

7 Ehdotus Euroopan parlamentin ja neuvoston asetukseksi tekoälyä koskevista yhdenmukaistetuista säännöistä (tekoälysäädös) ja tiettyjen unionin säädösten muuttamisesta, COM(2021) 206 final, 21.4.2021.

Päällekkäisen työn välttämiseksi komission ja eurooppalaisten standardointijärjestöjen on tarkoitus ottaa huomioon standardointityö, joka on tehty RED-direktiivin mukaista delegoitua asetusta 2022/30 koskevasta standardointipyynnöstä annetun komission täytäntöönpanopäätöksen C(2022) 5637 yhteydessä, kun yhdenmukaistettuja standardeja valmistellaan ja kehitetään asetuksen täytäntöönpanon helpottamiseksi.

2. OIKEUSPERUSTA, TOISSIJAISUUSPERIAATE JA SUHTEELLISUUSPERIAATE

• Oikeusperusta

Tämän ehdotuksen oikeusperusta on Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 114 artikla, jossa määrätään toimenpiteistä sisämarkkinoiden toteuttamisen ja toiminnan varmistamiseksi. Ehdotuksen tarkoituksena on yhdenmukaistaa digitaalisia elementtejä sisältävien tuotteiden kyberturvavaatimukset kaikissa jäsenvaltioissa ja poistaa esteitä tavaroiden vapaalta liikkuvuudelta.

SEUT-sopimuksen 114 artiklaa voidaan käyttää oikeusperustana tällaisten esteiden esiintymisen estämiseksi, kun esteet johtuisivat erilaisista kansallisista laeista ja lähestymistavoista, jotka koskevat nykyisten oikeudellisten kehysten oikeudellisen epävarmuuden poistamista ja aukkojen paikkaamista.[8] Lisäksi unionin tuomioistuin on todennut, että epäyhtenäisten teknisten vaatimusten soveltaminen voi olla pätevä peruste SEUT-sopimuksen 114 artiklan soveltamiselle.[9]

Digitaalisia elementtejä sisältäviin tuotteisiin sovellettava EU:n nykyinen lainsäädäntökehys perustuu SEUT-sopimuksen 114 artiklaan ja sisältää useita säädöksiä, kuten tiettyjä tuotteita koskevan EU:n lainsäädännön, joka kattaa turvallisuuteen liittyviä näkökohtia, ja tuotevastuuta koskevan yleisen lainsäädännön. Se kattaa kuitenkin vain tietyt näkökohdat, jotka liittyvät aineellisten digitaalisten tuotteiden ja näihin tuotteisiin sulautettujen ohjelmistojen kyberturvallisuuteen. Jäsenvaltiot ovat alkaneet toteuttaa kansallisia toimenpiteitä, joissa edellytetään, että digitaalisten tuotteiden toimittajat parantavat tuotteidensa kyberturvallisuutta.[10] Samalla digitaalisten tuotteiden kyberturvallisuudella on kuitenkin erityisen vahva rajat ylittävä ulottuvuus, sillä yhdessä maassa valmistettuja tuotteita käyttävät usein organisaatiot ja kuluttajat monissa muissa maissa koko sisämarkkinoilla. Poikkeamat, jotka koskevat alun perin yhtä toimijaa tai jäsenvaltiota, leviävät usein minuuteissa organisaatioiden, toimialojen ja jäsenvaltioiden rajojen yli.

EU:n ja kansallisella tasolla tähän mennessä käyttöön otetuilla eri säädöksillä ja aloitteilla puututaan havaittuihin ongelmiin vain osittain ja vaarana on, että sisämarkkinoilla syntyy lainsäädännön hajanaisuutta, mikä lisää sekä näiden tuotteiden toimittajien että käyttäjien oikeudellista epävarmuutta ja aiheuttaa yrityksille tarpeetonta rasitetta, kun ne joutuvat noudattamaan samantyyppisten tuotteiden osalta toisistaan eriäviä vaatimuksia.

Ehdotetulla asetuksella yhdenmukaistettaisiin ja virtaviivaistettaisiin EU:n sääntely-ympäristöä ottamalla käyttöön yhteiset kyberturvavaatimukset digitaalisia elementtejä

---

8 Unionin tuomioistuimen tuomio (suuri jaosto) 3.12.2019, *Tšekin tasavalta* v. *Euroopan parlamentti ja Euroopan unionin neuvosto*, asia C-482/17, 35 kohta.

9 Unionin tuomioistuimen tuomio (suuri jaosto) 2.5.2006, *Ison-Britannian ja Pohjois-Irlannin Yhdistynyt kuningaskunta* v. *Euroopan parlamentti ja Euroopan unionin neuvosto*, asia C-217/04, 62–63 kohta.

10 Esimerkiksi vuonna 2019 Suomessa luotiin ETSIn standardeihin perustuva merkintäjärjestelmä esineiden internetin piiriin kuuluville laitteille, kuten älytelevisioille, älypuhelimille ja leluille. Saksassa on hiljattain otettu käyttöön kuluttajille suunnattu tietoturvamerkintä laajakaistareitittimille, älytelevisioille, kameroille, kaiuttimille, leluille sekä robottiruohonleikkureille ja -imureille.

sisältäville tuotteille, ja vältettäisiin eri säädöksistä johtuvat päällekkäiset vaatimukset. Tämä lisäisi oikeusvarmuutta toimijoiden ja käyttäjien näkökulmasta kaikkialla unionissa, yhdenmukaistaisi Euroopan sisämarkkinoita ja loisi suotuisammat olosuhteet toimijoille, jotka pyrkivät EU:n markkinoille.

Toissijaisuusperiaate (jaetun toimivallan osalta)

Kyberturvallisuuden ylipäätään selkeästi rajat ylittävä luonne ja lisääntyvät riskit ja poikkeamat, joilla on heijastusvaikutuksia yli maiden, toimialojen ja tuotteiden rajojen, merkitsevät, että jäsenvaltiot eivät voi saavuttaa nyt tarkasteltavana olevan intervention tavoitteita tuloksellisesti yksin. Kansalliset lähestymistavat ongelmien ratkaisemiseen ja erityisesti lähestymistavat, joilla otetaan käyttöön pakollisia vaatimuksia, lisäävät oikeudellista epävarmuutta ja oikeudellisia esteitä. Tämä voisi estää yrityksiä laajentamasta toimintaansa saumattomasti muihin jäsenvaltioihin, ja käyttäjät eivät pääsisi hyötymään niiden tuotteista.

Näin ollen tarvitaan EU:n tason yhteisiä toimia käyttäjien luottamuksen lisäämiseksi ja digitaalisia elementtejä sisältävien EU-lähtöisten tuotteiden houkuttelevuuden lisäämiseksi. Tämä hyödyttäisi myös digitaalisia sisämarkkinoita ja sisämarkkinoita yleensä tarjoamalla oikeusvarmuutta ja luomalla tasapuoliset toimintaedellytykset digitaalisia elementtejä sisältävien tuotteiden valmistajille.

Olennaista on myös todeta, että Euroopan unionin kybertoimien kehittämisestä 23. toukokuuta 2022 annetuissa neuvoston päätelmissä kehotetaan komissiota ehdottamaan vuoden 2022 loppuun mennessä verkkoon liitettyjä laitteita koskevia yhteisiä kyberturvavaatimuksia.

Suhteellisuusperiaate

Ehdotetun asetuksen oikeasuhteisuuden osalta voidaan todeta, että tarkasteltuihin toimintavaihtoehtoihin sisältyvät toimenpiteet eivät menisi pidemmälle kuin on tarpeen yleisten ja erityisten tavoitteiden saavuttamiseksi eivätkä aiheuttaisi suhteettomia kustannuksia. Tarkemmin sanoen tarkasteltavalla interventiolla varmistettaisiin, että digitaalisia elementtejä sisältävät tuotteet olisivat tietoturvallisia koko niiden elinkaaren ajan. Tähän päästäisiin objektiivisilla ja teknologianeutraaleilla, riskeihin oikein suhteutetuilla vaatimuksilla, jotka pysyvät kohtuullisella tasolla ja ovat yleisesti ottaen asianomaisten toimijoiden etujen mukaisia.

Ehdotuksen keskeiset kyberturvavaatimukset perustuvat laajalti käytettyihin standardeihin, ja tulevassa standardointiprosessissa otettaisiin huomioon tuotteiden tekniset erityispiirteet. Tämä tarkoittaa, että jos tietty riskitaso sitä edellyttäisi, tietoturvavalvontaa mukautettaisiin tarvittavalla tavalla. Lisäksi kaavailluissa horisontaalisissa säännöissä vaadittaisiin kolmannen osapuolen suorittamaa arviointia vain kriittisille tuotteille. Tämä koskisi siis vain pientä osaa digitaalisia elementtejä sisältävien tuotteiden markkinoista. Vaikutus pk-yrityksiin riippuisi niiden läsnäolosta näiden tiettyjen tuoteluokkien markkinoilla.

Vaatimustenmukaisuuden arvioinnista aiheutuvien kustannusten oikeasuhteisuuden osalta voidaan todeta, että ilmoitetut laitokset, jotka suorittavat arviointeja kolmansina osapuolina, ottaisivat yrityksen koon huomioon maksuja määrittäessään. Lisäksi säädettäisiin kohtuullisesta 24 kuukauden siirtymäajasta täytäntöönpanon valmistelemiseksi, jotta asianomaisilla markkinoilla olisi aikaa valmistautua, ja samalla annettaisiin selkeä suunta T&K-investoinneille. Yrityksille säännösten noudattamisesta mahdollisesti aiheutuvat kustannukset kompensoituisivat hyödyillä, joita saadaan digitaalisia elementtejä sisältävien tuotteiden tietoturvan paranemisesta ja viime kädessä käyttäjien näitä tuotteita kohtaan tunteman luottamuksen lisääntymisestä.

- **Toimintatavan valinta**

Sääntelyllinen interventio edellyttäisi asetusta direktiivin sijaan. Tämä johtuu siitä, että tämäntyyppisen tuotelainsäädännön tapauksessa asetuksella puututtaisiin havaittuihin ongelmiin tuloksellisemmin ja saavutettaisiin asetetut tavoitteet, koska kyseessä on interventio, jolla asetetaan ehtoja hyvin laajan tuoteluokan saattamiselle sisämarkkinoille. Direktiivin saattaminen osaksi kansallista lainsäädäntöä voisi jättää liikaa harkintavaltaa kansalliselle tasolle, mikä saattaisi johtaa tiettyjen olennaisten kyberturvavaatimusten epäyhdenmukaisuuteen, oikeudelliseen epävarmuuteen, suurempaan hajanaisuuteen tai jopa syrjintään rajat ylittävissä tilanteissa, varsinkin kun otetaan huomioon, että soveltamisalaan kuuluvilla tuotteilla voi olla useita käyttötarkoituksia tai -kohteita ja että valmistajat voivat tuottaa useita tällaisten tuotteiden luokkia.

3. JÄLKIARVIOINTIEN, SIDOSRYHMIEN KUULEMISTEN JA VAIKUTUSTENARVIOINTIEN TULOKSET

- **Sidosryhmien kuuleminen**

Komissio on kuullut laajasti erilaisia sidosryhmiä. Jäsenvaltioita ja sidosryhmiä pyydettiin osallistumaan avoimeen julkiseen kuulemiseen sekä kyselyihin ja työpajoihin, joita järjestettiin komission vaikutustenarvioinnin valmistelutyötä tukevan konsortion tekemän tutkimuksen yhteydessä. Konsortioon kuuluivat Wavestone, Centre for European Policy Studies (CEPS) ja ICF. Kuultuihin sidosryhmiin kuului kansallisia markkinavalvontaviranomaisia, kyberturvallisuutta käsitteleviä unionin elimiä, laitteistojen ja ohjelmistojen valmistajia, laitteistojen ja ohjelmistojen maahantuojia ja jakelijoita, toimialajärjestöjä, kuluttajajärjestöjä ja digitaalisia elementtejä sisältävien tuotteiden käyttäjiä sekä yksittäisiä kansalaisia, tutkijoita ja tiedeyhteisön edustajia, ilmoitettuja laitoksia ja akkreditointilaitoksia sekä kyberturvallisuusalan ammattilaisia.

Kuulemistoimiin sisältyivät:

- Alustava selvitys[11], jonka toteuttivat ICF, Wavestone, Carsa ja CEPS ja joka julkaistiin joulukuussa 2021. Tutkimuksessa havaittiin useita markkinoiden toimintapuutteita ja arvioitiin mahdollisia sääntelytoimia.
- Avoin julkinen kuuleminen, joka oli suunnattu kansalaisille, sidosryhmille ja kyberturvallisuuden asiantuntijoille. Vastauksia saatiin 176. Kuuleminen auttoi kokoamaan erilaisia mielipiteitä ja kokemuksia kaikentyyppisiltä sidosryhmiltä.
- Komission kyberkestävyyssäädöksen valmistelutyötä tukevan selvityksen yhteydessä järjestettyihin työpajoihin osallistui noin 100 eri sidosryhmien edustajaa kaikista 27 jäsenvaltiosta.
- Lisäksi tehtiin asiantuntijahaastatteluja, jotta saataisiin syvällisempi käsitys digitaalisia elementtejä sisältäviin tuotteisiin liittyvistä nykyisistä kyberturvahaasteista ja joissa keskusteltiin toimintavaihtoehdoista mahdollisia sääntelytoimia silmällä pitäen.

[11] *Study on the need of Cybersecurity requirements for ICT products* – No. 2020-0715, Final Study Report, saatavilla osoitteessa https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products.

- Kansallisten kyberturvallisuusviranomaisten, yksityisen sektorin ja kuluttajajärjestöjen kanssa käytiin kahdenvälisiä keskusteluja.
- Yhteyttä pidettiin myös alan keskeisiin pk-yrityksiin.

- **Asiantuntijatiedon keruu ja käyttö**

Kuulemistoimilla pyrittiin saamaan palautetta viidestä keskeisestä arviointikriteeristä, jotka perustuvat EU:n paremman sääntelyn suuntaviivoihin (vaikuttavuus, tehokkuus, relevanssi, johdonmukaisuus, EU:n tason lisäarvo), sekä mahdollisten toimintavaihtoehtojen potentiaalisista vaikutuksista. Sen lisäksi, että selvityksen toimeksisaaja on ollut yhteydessä sidosryhmiin, joihin ehdotettu asetus vaikuttaisi suoraan, se on kuullut myös lukuisia kyberturvallisuuden asiantuntijoita.

- **Vaikutustenarviointi**

Komissio teki ehdotuksesta vaikutustenarvioinnin, joka toimitettiin komission sääntelyntarkastelulautakunnan käsiteltäväksi. Lautakunnan kanssa pidettiin kokous 6. heinäkuuta 2022, minkä jälkeen se antoi myönteisen lausunnon. Vaikutustenarviointia kuitenkin mukautettiin sääntelyntarkastelulautakunnan suositusten ja huomautusten huomioon ottamiseksi.

Komissio tarkasteli erilaisia toimintavaihtoehtoja, joilla ehdotuksen yleiset tavoitteet voitaisiin saavuttaa:

- Ei-sitova lähestymistapa ja vapaaehtoiset toimenpiteet (vaihtoehto 1): Tässä vaihtoehdossa ei tehtäisi sitovaa sääntelyllistä interventiota. Sen sijaan komissio antaisi tiedonantoja, ohjeistusta, suosituksia ja mahdollisesti käytännesääntöjä vapaaehtoisten toimenpiteiden edistämiseksi. Vapaaehtoisia tai pakollisia kansallisia järjestelmiä kehitettäisiin edelleen EU:n horisontaalisten sääntöjen puuttumisen kompensoimiseksi.
- Tapauskohtaiset interventiot, jotka koskisivat digitaalisia elementtejä sisältävien aineellisten tuotteiden ja niihin sulautettujen ohjelmistojen kyberturvallisuutta (vaihtoehto 2): Tämä vaihtoehto sisältäisi tapaus- ja tuotekohtaisen intervention, joka rajoittuisi kyberturvavaatimusten täydentämiseen ja/tai muuttamiseen jo voimassa olevassa lainsäädännössä tai uuden lainsäädännön antamiseen uusien riskien ilmetessä, mukaan lukien mahdollisesti sulauttamattomien ohjelmistojen osalta.

Vaihtoehdot 3 ja 4 edellyttäisivät tietyn laajuista horisontaalista interventiota, joka vastaisi suurelta osin tuotteiden kaupan pitämistä koskevaa uutta lainsäädäntökehystä (*New Legislative Framework,* NLF). Kehyksessä asetetaan olennaisten vaatimusten täyttyminen edellytykseksi tiettyjen tuotteiden sisämarkkinoille saattamiselle. Kehyksessä säädetään yleensä myös vaatimustenmukaisuuden arvioinnista, jonka valmistaja suorittaa sen osoittamiseksi, täyttyvätkö kyseiset tuotteelle asetetut vaatimukset.

- Yhdistetty lähestymistapa, johon kuuluisivat digitaalisia elementtejä sisältävien aineellisten tuotteiden ja niihin sulautettujen ohjelmistojen kyberturvallisuutta koskevat horisontaaliset pakolliset säännöt sekä sulauttamattomia ohjelmistoja koskeva porrastettu lähestymistapa (vaihtoehto 3): Tähän vaihtoehtoon sisältyisi asetus, jolla otettaisiin käyttöön horisontaaliset kyberturvavaatimukset kaikille digitaalisia elementtejä sisältäville aineellisille tuotteille ja niihin sulautetuille ohjelmistoille edellytyksenä markkinoille saattamiselle, ja siihen sisältyisi kaksi alavaihtoehtoa, joissa joko

edellytettäisiin tai ei edellytettäisi pakollista kolmannen osapuolen tekemää arviointia (alavaihtoehdot 3i ja 3ii). Sulauttamattomia ohjelmistoja ei säänneltäisi.

- Horisontaalinen sääntelytoimi, jolla otetaan käyttöön kyberturvallisuusvaatimuksia laajalle joukolle digitaalisia elementtejä sisältäviä aineellisia ja aineettomia tuotteita, mukaan lukien sulauttamattomat ohjelmistot (vaihtoehto 4): Tämä vaihtoehto muistuttaa soveltamisalaa lukuun ottamatta vaihtoehtoa 3. Vaihtoehdossa 4 mahdollinen asetus kattaisi sulauttamattomat ohjelmistot (kaksi alavaihtoehtoa, joista toinen kattaa vain kriittiset ohjelmistot (alavaihtoehto 4a) ja toinen kaikki ohjelmistot (alavaihtoehto 4b)). Kunkin alavaihtoehdon osalta harkittaisiin samoja vaatimustenmukaisuuden arviointiin liittyviä alavaihtoehtoja kuin vaihtoehdossa 3.

Vaihtoehto 4 (alavaihtoehdolla, joka kattaa kaikki ohjelmistot ja edellyttää kriittisten tuotteiden pakollista kolmannen osapuolen arviointia) nousi parhaaksi vaihtoehdoksi, kun arvioitiin tuloksellisuutta suhteessa erityistavoitteisiin ja kustannustehokkuutta verrattuna hyötyihin. Tällä vaihtoehdolla varmistettaisiin horisontaalisten kyberturvavaatimusten asettaminen kaikille digitaalisia elementtejä sisältäville tuotteille, jotka asetetaan saataville sisämarkkinoilla, ja se olisi ainoa vaihtoehto, joka kattaisi koko digitaalisen toimitusketjun. Tällainen interventio kattaisi myös sulauttamattomat ohjelmistot, jotka ovat usein alttiita haavoittuvuuksille. Näin varmistettaisiin johdonmukainen lähestymistapa digitaalisia elementtejä sisältäviä kaikkia tuotteita varten, sekä eri talouden toimijoiden selkeä vastuunjako.

Tämä toimintavaihtoehto tuo lisäarvoa myös, koska se kattaa huolellisuusvelvoitteeseen ja koko elinkaareen liittyvät näkökohdat sen jälkeen, kun digitaalisia elementtejä sisältävä tuote on saatettu markkinoille, jotta varmistetaan muun muassa asianmukainen tiedottaminen tietoturvatuesta ja tietoturvapäivitysten tarjoamisesta. Tämä toimintavaihtoehto täydentäisi myös tuloksellisimmin verkko- ja tietoturvakehyksen (NIS) hiljattain tehtyä tarkistusta luomalla edellytykset vahvemmalle koko toimitusketjun tietoturvalle.

Parhaaksi arvioidusta vaihtoehdosta koituisi merkittäviä hyötyjä eri sidosryhmille. Yritysten kannalta se estäisi sen, että digitaalisia elementtejä sisältäviin tuotteisiin alettaisiin soveltaa toisistaan poikkeavia tietoturvasääntöjä. Se vähentäisi myös asiaan liittyvän kyberturvalainsäädännön noudattamisesta aiheutuvia kustannuksia. Se vähentäisi kyberturvapoikkeamien määrää, poikkeamien käsittelykustannuksia ja mainehaittaa. Arvion mukaan aloite voisi koko EU:ssa alentaa yrityksiä haittaavista poikkeamista aiheutuvia kustannuksia noin 180–290 miljardilla eurolla vuodessa. Se kasvattaisi liikevaihtoa, kun digitaalisia elementtejä sisältävien tuotteiden käyttö lisääntyisi. Se parantaisi eurooppalaisten yritysten mainetta maailmalla ja johtaisi myös EU:n ulkopuolelta tulevan kysynnän kasvuun. Käyttäjien kannalta taas parhaaksi arvioitu vaihtoehto lisäisi läpinäkyvyyttä tietoturvaominaisuuksien suhteen ja helpottaisi digitaalisia elementtejä sisältävien tuotteiden käyttöä. Myös kuluttajien ja kansalaisten perusoikeudet, kuten yksityisyyden suoja ja tietosuoja, turvattaisiin paremmin.

Kun julkisen kuulemisen vastaajia pyydettiin arvioimaan eri toimintatapojen tuloksellisuutta, vastaajat olivat yhtä mieltä siitä, että vaihtoehto 4 olisi vaikuttavin toimenpide (4,08 asteikolla 1–5). Tätä mieltä olivat kuluttajajärjestöt (5,00), käyttäjiksi itsensä ilmoittaneet vastaajat (4,22), ilmoitetut laitokset (4,17), markkinavalvontaviranomaiset (5,00) ja digitaalisia elementtejä sisältävien tuotteiden valmistajat (3,85), mukaan lukien pienet ja keskisuuret valmistajat (4,05).

- **Sääntelyn toimivuus ja yksinkertaistaminen**

Tässä ehdotuksessa asetetaan vaatimuksia ohjelmistojen ja laitteistojen valmistajille. On tarpeen varmistaa oikeusvarmuus ja välttää tuotteisiin liittyvien kyberturvavaatimusten hajanaistuminen entisestään sisämarkkinoilla. Tästä tarpeesta on osoituksena eri sidosryhmien laaja tuki horisontaaliselle interventiolle. Ehdotuksella minimoidaan useista tuoteturvallisuussäädöksistä valmistajille aiheutuva sääntelytaakka. Koska ehdotus on sovitettu yhteen tuotteiden kaupan pitämistä koskevan uuden lainsäädäntökehyksen kanssa, intervention toimivuus paranee ja sen toimintaa on helpompi valvoa. Ehdotuksella virtaviivaistetaan varmistusmenettelyjä ottamalla valmistajat ja jäsenvaltiot niihin mukaan ennen komissiolle ilmoittamista. Suuri osa ehdotuksen soveltamisalaan kuuluvista valmistajista tuntee jo tuotteiden kaupan pitämistä koskevan uuden lainsäädäntökehyksen toiminnan, mikä helpottaa ehdotuksen ymmärtämistä ja täytäntöönpanoa. Kuluttajien ja yritysten kannalta ehdotuksella lisätään luottamusta digitaalisia elementtejä sisältäviä tuotteita kohtaan.

- **Perusoikeudet**

Kaikkien toimintavaihtoehtojen odotetaan jossain määrin tehostavan perusoikeuksien ja -vapauksien suojaa, kuten yksityisyyden ja henkilötietojen suojaa, elinkeinovapautta sekä omaisuuden tai henkilökohtaisen ihmisarvon ja koskemattomuuden suojaa. Erityisesti parhaaksi arvioitu toimintavaihtoehto 4, joka koostuu horisontaalisista interventioista ja laajasta soveltamisalasta, olisi tältä osin tuloksellisin, koska se todennäköisesti auttaisi vähentämään poikkeamien, myös henkilötietoturvaloukkausten, määrää ja vakavuusastetta. Se myös parantaisi oikeusvarmuutta ja loisi talouden toimijoille tasapuoliset toimintaedellytykset, lisäisi käyttäjien luottamusta ja lisäisi digitaalisia elementtejä sisältävien EU-tuotteiden houkuttelevuutta kokonaisuudessaan. Näin suojeltaisiin talouden toimijoiden omaisuutta ja parannettaisiin niiden liiketoimintaedellytyksiä.

Horisontaaliset kyberturvavaatimukset edistäisivät henkilötietoturvaa suojaamalla tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä digitaalisia elementtejä sisältävissä tuotteissa. Näiden vaatimusten täyttäminen edesauttaa yleisen tietosuoja-asetuksen (EU) 2016/679[12] (GDPR) mukaisen henkilötietojen käsittelyn tietoturvaa koskevan vaatimuksen täyttymistä. Ehdotuksella lisättäisiin läpinäkyvyyttä ja tiedottamista käyttäjille, myös sellaisille käyttäjille, joiden kyberturvaosaaminen voi olla vähäisempää. Käyttäjät saisivat myös paremmin tietoa digitaalisia elementtejä sisältävien tuotteiden riskeistä, toiminnoista ja rajoituksista, mikä antaisi heille paremmat mahdollisuudet ennaltaehkäistä ja lieventää jäljelle jääviä riskejä.

4. TALOUSARVIOVAIKUTUKSET

Voidakseen hoitaa sille tällä asetuksella osoitetut tehtävät Euroopan unionin kyberturvallisuusviraston (ENISA) on kohdennettava uudelleen noin 4,5 kokoaikaisen työntekijän verran resursseja. Komission olisi kohdennettava uudelleen 7 kokoaikaisen työntekijän verran resursseja tämän asetuksen täytäntöönpanoon liittyvien velvollisuuksiensa täyttämiseksi.

Yksityiskohtainen erittely kustannuksista esitetään tähän ehdotukseen liittyvässä rahoitusselvityksessä.

[12] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (EUVL L 119, 4.5.2016, s. 1).

5. LISÄTIEDOT

• Toteuttamissuunnitelmat, seuranta, arviointi ja raportointijärjestelyt

Komissio seuraa näiden uusien säännösten täytäntöönpanoa, soveltamista ja noudattamista niiden vaikuttavuuden arvioinnin näkökulmasta. Asetuksessa pyydetään komissiolta asetuksen arviointia ja uudelleentarkastelua ja kehotetaan komissiota toimittamaan asiaa käsittelevä julkinen kertomus Euroopan parlamentille ja neuvostolle viimeistään 36 kuukauden kuluttua soveltamispäivästä ja sen jälkeen neljän vuoden välein.

• Ehdotukseen sisältyvien säännösten yksityiskohtaiset selitykset

Yleiset säännökset (I luku)

Asetusehdotuksessa vahvistetaan a) säännöt digitaalisia elementtejä sisältävien tuotteiden markkinoille saattamiselle niiden kyberturvallisuuden varmistamiseksi, b) digitaalisia elementtejä sisältävien tuotteiden suunnittelua, kehittämistä ja tuotantoa koskevat olennaiset vaatimukset ja näihin tuotteisiin liittyvät talouden toimijoiden kyberturvavelvoitteet, c) olennaiset vaatimukset haavoittuvuuksien käsittelyprosesseille, joita valmistajat ovat ottaneet käyttöön varmistaakseen digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuuden koko niiden elinkaaren ajan, sekä näihin prosesseihin liittyvät talouden toimijoiden velvoitteet ja d) markkinavalvontaa ja edellä mainittujen sääntöjen ja vaatimusten noudattamisen valvontaa koskevat säännöt.

Ehdotettua asetusta sovelletaan kaikkiin digitaalisia elementtejä sisältäviin tuotteisiin, joiden aiottu ja kohtuudella ennakoitavissa oleva käyttö sisältää suoran tai epäsuoran loogisen tai fyysisen datayhteyden johonkin laitteeseen tai verkkoon.

Ehdotettua asetusta ei sovelleta digitaalisia elementtejä sisältäviin tuotteisiin, jotka kuuluvat asetuksen (EU) 2017/745 [ihmisille tarkoitetut lääkinnälliset laitteet ja tällaisten laitteiden lisälaitteet] ja asetuksen (EU) 2017/746 [ihmisten käyttöön tarkoitetut in vitro -diagnostiikkaan tarkoitetut lääkinnälliset laitteet ja tällaisten laitteiden lisälaitteet] soveltamisalaan, koska näihin molempiin asetuksiin sisältyy laitteita, ohjelmistot mukaan lukien, koskevia vaatimuksia, tuotteiden koko elinkaaren kattavia valmistajien yleisiä velvoitteita sekä vaatimustenmukaisuuden arviointimenettelyjä koskevia vaatimuksia. Tätä asetusta ei sovelleta digitaalisia elementtejä sisältäviin tuotteisiin, jotka on sertifioitu asetuksen 2018/1139 [korkea ja yhdenmukainen siviili-ilmailun turvallisuustaso] mukaisesti, eikä tuotteisiin, joihin sovelletaan [moottoriajoneuvojen ja niiden perävaunujen tyyppihyväksyntävaatimuksista sekä tällaisiin ajoneuvoihin tarkoitetuista järjestelmistä, komponenteista ja erillisistä teknisistä yksiköistä annettua] asetusta (EU) 2019/2144.

Digitaalisia elementtejä sisältäviin kriittisiin tuotteisiin sovelletaan erityisiä vaatimustenmukaisuuden arviointimenettelyjä, ja ne jaetaan luokkiin I ja II liitteen III mukaisesti kyberturvariskitason mukaisesti siten, että luokka II edustaa suurempaa riskiä. Digitaalisia elementtejä sisältävää tuotetta pidetään kriittisenä ja sen vuoksi se sisällytetään liitteeseen III sen potentiaalisten kyberhaavoittuvuuksien vaikutusten perusteella. Kyberturvariskin määrittämisessä otetaan huomioon muun muassa digitaalisia elementtejä sisältävän tuotteen kyberturvallisuuteen liittyvä toiminnallisuus ja käyttötarkoitus herkissä ympäristöissä, kuten teollisessa käytössä.

Komissiolle siirretään myös valta antaa delegoituja säädöksiä, joilla täydennetään tätä asetusta määrittämällä sellaiset erittäin kriittiset digitaalisia elementtejä sisältävät tuoteryhmät, joiden osalta valmistajien on hankittava eurooppalainen kyberturvasertifikaatti eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti sen osoittamiseksi, että tuotteet ovat

liitteessä I vahvistettujen olennaisten vaatimusten tai niiden osien mukaisia. Määrittäessään tällaisia, digitaalisia elementtejä sisältäviä erittäin kriittisiä tuoteryhmiä komissio ottaa huomioon digitaalisia elementtejä sisältävään tuoteryhmään liittyvän kyberturvariskin tason tarkastellen yhtä tai useampaa digitaalisia elementtejä sisältävien kriittisten tuotteiden luetteloinnissa liitteessä III vahvistettua kriteeriä, sekä sitä, käyttävätkö tai hyödyntävätkö direktiivin [direktiivin XXX/XXXX (NIS2) liitteessä [liitteessä I] tarkoitetut keskeiset toimijat kyseistä tuoteryhmää tai onko sillä mahdollisesti tulevaisuudessa merkitystä näiden toimijoiden toiminnan kannalta tai ovatko ne merkityksellisiä digitaalisia elementtejä sisältävien tuotteiden koko toimitusketjun häiriönsietokyvyn kannalta.

Talouden toimijoiden velvollisuudet (II luku)

Ehdotukseen sisältyy valmistajia, maahantuojia ja jakelijoita koskevia velvollisuuksia, jotka perustuvat päätöksen 768/2008/EY viitesäännöksiin. Olennaisissa kyberturvavaatimuksissa ja -velvoitteissa määrätään, että digitaalisia elementtejä sisältäviä tuotteita voidaan asettaa saataville markkinoilla vain, jos ne asianmukaisesti toimitettuina, asennettuina, huollettuina ja käytettyinä käyttötarkoituksensa mukaisesti tai kohtuudella ennakoitavissa olosuhteissa täyttävät tässä asetuksessa vahvistetut olennaiset kyberturvavaatimukset.

Olennaisilla vaatimuksilla ja velvoitteilla asetettaisiin valmistajille velvollisuus ottaa kyberturvallisuus huomioon digitaalisia elementtejä sisältävien tuotteiden suunnittelussa, kehittämisessä ja tuotannossa, noudattaa tietoturvaan liittyen asianmukaista huolellisuutta tuotteidensa suunnittelussa ja kehittämisessä, tiedottaa avoimesti kyberturvanäkökohdista, jotka on saatettava asiakkaiden tietoon, varmistaa oikeasuhteisella tavalla tietoturvatuki (päivitykset) ja noudattaa haavoittuvuuksien käsittelyä koskevia vaatimuksia.

Talouden toimijoille valmistajista aina jakelijoihin ja maahantuojiin saakka asetettaisiin digitaalisia elementtejä sisältävien tuotteiden markkinoille saattamista koskevia velvoitteita sen mukaan, mikä on niiden rooli ja vastuu toimitusketjussa.

Digitaalisia elementtejä sisältävän tuotteen vaatimustenmukaisuus (III luku)

Yhdenmukaistettujen standardien tai niiden osien, joiden viitetiedot on julkaistu *Euroopan unionin virallisessa lehdessä*, mukaisen digitaalisia elementtejä sisältävän tuotteen katsotaan täyttävän tämän asetusehdotuksen olennaiset vaatimukset. Jos yhdenmukaistettuja standardeja ei ole tai ne ovat riittämättömiä tai jos standardointimenettely viivästyy kohtuuttomasti tai jos eurooppalaiset standardointiorganisaatiot eivät ole hyväksyneet komission pyyntöä, komissio voi täytäntöönpanosäädöksillä hyväksyä yhteisiä eritelmiä.

Lisäksi digitaalisia elementtejä sisältävien tuotteiden, jotka on sertifioitu tai joille on annettu EU-vaatimustenmukaisuusvakuutus tai sertifikaatti asetuksen (EU) 2019/881 mukaisen eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti ja joiden osalta komissio on täytäntöönpanosäädöksellä vahvistanut, että tämä muodostaa vaatimustenmukaisuusolettaman tämän asetuksen vaatimusten suhteen, oletetaan olevan tämän asetuksen tai sen osien olennaisten vaatimusten mukaisia siltä osin kuin EU-vaatimustenmukaisuusvakuutus tai kyberturvasertifikaatti tai sen osa kattaa kyseiset vaatimukset.

Lisäksi valmistajien tarpeettoman hallinnollisen taakan välttämiseksi komission olisi tarvittaessa täsmennettävä, poistaako tällaisen eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti myönnetty kyberturvasertifikaatti valmistajilta velvoitteen teettää kolmansilla osapuolilla tässä asetuksessa säädetty vaatimustenmukaisuuden arviointi vastaavien vaatimusten osalta.

Valmistajan on suoritettava digitaalisia elementtejä sisältävän tuotteen ja haavoittuvuuksien käsittelyprosessiensa vaatimustenmukaisuuden arviointi osoittaakseen, että liitteessä I

vahvistetut olennaiset vaatimukset täyttyvät, noudattamalla jotakin liitteessä VI vahvistettua menettelyä. Luokkaan I ja II kuuluvien kriittisten tuotteiden valmistajien on käytettävä vaatimustenmukaisuuden osoittamiseen luokkiin sovellettavia moduuleja. Luokkaan II kuuluvien kriittisten tuotteiden valmistajien on otettava vaatimustenmukaisuuden arviointiin mukaan kolmas osapuoli.

Vaatimustenmukaisuuden arviointilaitosten ilmoittaminen (IV luku)

Ilmoitettujen laitosten moitteeton toiminta on olennainen edellytys sille, että korkeatasoinen kyberturvallisuus ja kaikkien sidosryhmien luottamus uuden lähestymistavan mukaiseen järjestelmään saadaan varmistettua. Sen vuoksi ehdotuksessa vahvistetaan päätöksen 768/2008/EY mukaisesti vaatimukset, joita sovelletaan vaatimustenmukaisuuden arviointilaitoksista (ilmoitetuista laitoksista) vastaaviin kansallisiin viranomaisiin. Ehdotuksen mukaan jäsenvaltiot vastaavat viime kädessä ilmoitettujen laitosten nimeämisestä ja valvonnasta. Jäsenvaltioiden on nimettävä ilmoittava viranomainen, joka on vastuussa vaatimustenmukaisuuden arviointilaitosten arviointiin ja ilmoittamiseen ja ilmoitettujen laitosten valvontaan liittyvien tarvittavien menettelyjen perustamisesta ja suorittamisesta.

Markkinavalvonta ja täytäntöönpano (V luku)

Asetuksen (EU) 2019/1020 mukaisesti kansalliset markkinavalvontaviranomaiset toteuttavat markkinavalvontaa kyseisen jäsenvaltion alueella. Jäsenvaltiot voivat nimetä minkä tahansa olemassa olevan tai uuden viranomaisen, mukaan lukien [direktiivin XXX/XXXX (NIS2) XXX artiklassa tarkoitetut kansalliset toimivaltaiset viranomaiset] tai asetuksen (EU) 2019/881 58 artiklassa tarkoitetut nimetyt kansalliset kyberturvasertifiointiviranomaiset, toimimaan markkinavalvontaviranomaisena. Talouden toimijoita pyydetään tekemään täysimääräistä yhteistyötä markkinavalvontaviranomaisten ja muiden toimivaltaisten viranomaisten kanssa.

Säädösvallan siirtäminen ja komiteamenettelyt (VI luku)

Sen varmistamiseksi, että sääntelykehystä voidaan tarvittaessa mukauttaa, komissiolle siirretään valta hyväksyä Euroopan unionin toiminnasta tehdyn sopimuksen 290 artiklan mukaisesti säädösvallan siirron nojalla annettavia delegoituja säädöksiä, joilla päivitetään luokkaan I ja II kuuluvien kriittisten tuotteiden luetteloa ja esitetään näiden tuotteiden määritelmät; täsmennetään, onko rajoitus tai poissulkeminen tarpeen sellaisten digitaalisia elementtejä sisältävien tuotteiden osalta, jotka kuuluvat muiden sellaisten unionin sääntöjen soveltamisalaan, joissa vahvistetaan vaatimukset, joilla saavutetaan sama suojelun taso kuin tässä asetuksessa; säädetään tässä asetuksessa vahvistettujen kriteerien perusteella pakolliseksi tiettyjen erittäin kriittisten digitaalisia elementtejä sisältävien tuotteiden sertifiointi; täsmennetään EU-vaatimustenmukaisuusvakuutuksen vähimmäissisältö ja täydennetään teknisiin asiakirjoihin sisällytettäviä tietoelementtejä.

Lisäksi komissiolle siirretään valta antaa täytäntöönpanosäädöksiä, joilla: täsmennetään raportointivelvoitteiden ja ohjelmistosisältöluettelon muoto tai osatekijät; yksilöidään eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät, joita voidaan käyttää osoittamaan tässä asetuksessa säädettyjen olennaisten vaatimusten tai niiden osien täyttyminen; hyväksytään yhteisiä eritelmiä; säädetään teknisistä eritelmistä CE-merkinnän sijoittamista varten; hyväksytään unionin tasolla korjaavia tai rajoittavia toimenpiteitä poikkeuksellisissa olosuhteissa, jotka oikeuttavat välittömiin toimiin sisämarkkinoiden moitteettoman toiminnan suojaamiseksi.

Luottamuksellisuus ja seuraamukset (VII luku)

Kaikkien tätä asetusta soveltavien osapuolten on kunnioitettava tehtäviään suorittaessaan ja toimintaansa harjoittaessaan saamiensa tietojen luottamuksellisuutta.

Tässä asetuksessa säädettyjen velvoitteiden tuloksellisen täytäntöönpanon varmistamiseksi kullakin markkinavalvontaviranomaisella olisi oltava valtuudet määrätä hallinnollisia sakkoja tai pyytää niiden määräämistä. Näin ollen tässä asetuksessa vahvistetaan tämän asetuksen velvoitteiden laiminlyömisestä perittävien hallinnollisten sakkojen enimmäismäärät, joista olisi säädettävä kansallisessa lainsäädännössä.

Siirtymä- ja loppusäännökset (VIII luku)

Jotta valmistajilla, ilmoitetuilla laitoksilla ja jäsenvaltioilla olisi aikaa sopeutua uusiin vaatimuksiin, ehdotettua asetusta aletaan soveltaa [24] kuukauden kuluttua sen voimaantulosta, lukuun ottamatta valmistajia koskevaa raportointivelvollisuutta, jota sovellettaisiin [12 kuukauden] kuluttua voimaantulosta.

2022/0272 (COD)

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS

digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvavaatimuksista ja asetuksen (EU) 2019/1020 muuttamisesta

(ETA:n kannalta merkityksellinen teksti)

EUROOPAN PARLAMENTTI JA EUROOPAN UNIONIN NEUVOSTO, jotka

ottavat huomioon Euroopan unionin toiminnasta tehdyn sopimuksen ja erityisesti sen 114 artiklan,

ottavat huomioon Euroopan komission ehdotuksen,

sen jälkeen, kun esitys lainsäätämisjärjestyksessä hyväksyttäväksi säädökseksi on toimitettu kansallisille parlamenteille,

ottavat huomioon Euroopan talous- ja sosiaalikomitean lausunnon[1],

ottavat huomioon alueiden komitean lausunnon[2],

noudattavat tavallista lainsäätämisjärjestystä,

sekä katsovat seuraavaa:

(1) Sisämarkkinoiden toimintaa on tarpeen parantaa vahvistamalla yhtenäinen oikeudellinen kehys olennaisille kyberturvavaatimuksille, joita sovelletaan digitaalisia elementtejä sisältävien tuotteiden saattamiseen unionin markkinoille. Olisi puututtava kahteen merkittävään ongelmaan, joista aiheutuu kustannuksia käyttäjille ja yhteiskunnalle: digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuuden alhainen taso, josta ovat osoituksena laajalle levinneet haavoittuvuudet ja niiden korjaamiseksi tarvittavien tietoturvapäivitysten riittämätön ja epäjohdonmukainen tarjonta ja käyttäjien riittämätön ymmärrys ja tiedonsaanti, mikä estää valitsemasta tuotteita, joilla on riittävät kyberturvaominaisuudet, tai estää käyttämästä tuotteita tietoturvallisesti.

(2) Tämän asetuksen tavoitteena on luoda edellytykset digitaalisia elementtejä sisältävien tietoturvallisten tuotteiden kehittämiselle varmistamalla, että laitteisto- ja ohjelmistotuotteet saatetaan markkinoille vähemmin haavoittuvuuksin ja että valmistajat suhtautuvat tietoturvaan vakavasti tuotteen koko elinkaaren ajan. Sillä pyritään myös luomaan olosuhteet, joissa käyttäjät voivat ottaa kyberturvallisuuden huomioon valitessaan ja käyttäessään digitaalisia elementtejä sisältäviä tuotteita.

(3) Tällä hetkellä voimassa oleva asiaa koskeva unionin lainsäädäntö sisältää useita horisontaalisia säännöstöjä, joissa käsitellään tiettyjä kyberturvatekijöitä eri näkökulmista, mukaan lukien toimenpiteet digitaalisen toimitusketjun tietoturvan

[1] EUVL C […], […], s. […].
[2] EUVL C […], […], s. […].

parantamiseksi. Kyberturvallisuuteen liittyvä voimassa oleva unionin lainsäädäntö, mukaan lukien [direktiivi XXX/XXXX (NIS2)] ja Euroopan parlamentin ja neuvoston asetus (EU) 2019/881[3], ei kuitenkaan suoraan kata digitaalisia elementtejä sisältävien tuotteiden tietoturvaa koskevia pakollisia vaatimuksia.

(4) Voimassa olevaa unionin lainsäädäntöä sovelletaan tiettyihin digitaalisia elementtejä sisältäviin tuotteisiin, mutta ei ole olemassa horisontaalista unionin sääntelykehystä, jossa vahvistettaisiin kattavat kyberturvavaatimukset kaikille digitaalisia elementtejä sisältäville tuotteille. Unionin ja kansallisella tasolla tähän mennessä käyttöön otetuilla eri säädöksillä ja aloitteilla puututaan havaittuihin kyberturvaongelmiin vain osittain ja vaarana on, että sisämarkkinoilla syntyy lainsäädännön hajanaisuutta, mikä lisää sekä näiden tuotteiden valmistajien että käyttäjien oikeudellista epävarmuutta ja luo yrityksille tarpeetonta rasitetta, kun ne joutuvat noudattamaan samantyyppisten tuotteiden osalta toisistaan eriäviä vaatimuksia. Näiden tuotteiden kyberturvallisuudella on kuitenkin erityisen vahva rajat ylittävä ulottuvuus, sillä yhdessä maassa valmistettuja tuotteita käyttävät usein organisaatiot ja kuluttajat monissa muissa maissa koko sisämarkkinoilla. Tämän vuoksi alaa on tarpeen säännellä unionin tasolla. Unionin sääntely-ympäristö olisi yhdenmukaistettava asettamalla digitaalisia elementtejä sisältäville tuotteille kyberturvavaatimukset. Lisäksi olisi parannettava oikeusvarmuutta toimijoiden ja käyttäjien näkökulmasta kaikkialla unionissa ja yhdenmukaistettava sisämarkkinoita luoden samalla suotuisammat olosuhteet toimijoille, jotka pyrkivät unionin markkinoille.

(5) Unionin tasolla erilaisissa ohjelmakohtaisissa ja poliittisissa asiakirjoissa, kuten EU:n kyberturvallisuusstrategiassa digitaaliselle vuosikymmenelle[4], 2 päivänä joulukuuta 2020 ja 23 päivänä toukokuuta 2022 annetuissa neuvoston päätelmissä ja Euroopan parlamentin 10 päivänä kesäkuuta 2021 antamassa päätöslauselmassa[5], peräänkuulutetaan erityisiä unionin kyberturvavaatimuksia digitaalisille tai verkotetuille tuotteille, ja useat maat eri puolilla maailmaa ovat ottaneet oma-aloitteisesti käyttöön sääntelyä asian ratkaisemiseksi. Euroopan tulevaisuuskonferenssin loppuraportissa[6] kansalaiset kehottivat vahvistamaan EU:n roolia kyberturvauhkien torjunnassa.

(6) Kaikkien sisämarkkinoille saatettujen digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuuden yleisen tason nostamiseksi on tarpeen ottaa käyttöön näille tuotteille horisontaalisesti sovellettavat objektiiviset ja teknologianeutraalit olennaiset kyberturvavaatimukset.

(7) Tietyissä olosuhteissa kaikki digitaalisia elementtejä sisältävät tuotteet, jotka ovat laajempaan sähköiseen tietojärjestelmään integroituja tai liitettyjä, voivat päätyä vihamielisten toimijoiden hyökkäyskanaviksi. Tämän johdosta myös vähemmän kriittisinä pidetyt laitteistot ja ohjelmistot voivat helpottaa laitteen tai verkon ensi

---

3 Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus) (EUVL L 151, 7.6.2019, s. 15).

4 JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/FI/ALL/?uri=JOIN:2020:18:FIN.

5 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_FI.html.

6 Euroopan tulevaisuuskonferenssi – raportti konferenssin lopullisista tuloksista, toukokuu 2022, ehdotus 28(2). Konferenssi järjestettiin huhtikuun 2021 ja toukokuun 2022 välisenä aikana. Se edusti ainutlaatuista kansalaisjohtoista keskustelevaa demokratiaa yleiseurooppalaisella tasolla, ja siihen osallistui tuhansia Euroopan kansalaisia sekä poliittisia toimijoita, työmarkkinaosapuolia, kansalaisyhteiskunnan edustajia ja keskeisiä sidosryhmiä.

vaiheen vaarantumista, jolloin vihamieliset toimijat voivat saada luvattoman pääsyn järjestelmään tai siirtyä samantasoisten järjestelmien välillä. Tästä syystä valmistajien olisi varmistettava, että kaikki liitettävissä olevat digitaalisia elementtejä sisältävät tuotteet suunnitellaan ja tuotetaan tässä asetuksessa säädettyjen olennaisten vaatimusten mukaisesti. Tämä koskee sekä tuotteita, jotka voidaan liittää fyysisesti laitteistorajapintojen kautta, että tuotteita, jotka voidaan liittää loogisesti, kuten verkkorajapintojen, pipe-ratkaisujen, tiedostojen, sovellusrajapintojen tai muiden ohjelmistorajapintojen kautta. Koska kyberturvauhat voivat edetä erilaisten digitaalisia elementtejä sisältävien tuotteiden kautta ennen tietyn kohteen saavuttamista, esimerkiksi ketjuttamalla yhteen useita haavoittuvuuksia, valmistajien olisi varmistettava myös sellaisten tuotteiden kyberturvallisuus, jotka on liitetty muihin laitteisiin tai verkkoihin vain välillisesti.

(8) Asettamalla kyberturvavaatimuksia digitaalisia elementtejä sisältävien tuotteiden markkinoille saattamiselle parannetaan näiden tuotteiden kyberturvallisuutta sekä kuluttajien että yritysten kannalta. Tämä pätee myös vaatimuksiin, jotka koskevat haavoittuvassa asemassa oleville kuluttajille tarkoitettujen digitaalisia elementtejä sisältävien kulutustuotteiden, kuten lelujen ja itkuhälyttimien, saattamista markkinoille.

(9) Tällä asetuksella varmistetaan digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuuden korkea taso. Sillä ei säännellä palveluja, kuten ohjelmistopalveluja (*Software-as-a-Service*, SaaS), lukuun ottamatta digitaalisia elementtejä sisältävään tuotteeseen liittyvää datan etäkäsittelyä, jolla tarkoitetaan kaikkea etäkäsittelyä, jota varten kyseinen ohjelmisto on suunniteltu ja kehitetty kyseisen tuotteen valmistajan toimesta tai kyseisen valmistajan vastuulla ja jonka puuttuminen estäisi digitaalisia elementtejä sisältävää tuotetta suorittamasta jotakin toimintoaan. Direktiivillä [XXX/XXXX (NIS2)] asetetaan kyberturvallisuutta ja poikkeamien raportointia koskevia vaatimuksia olennaisille ja tärkeille toimijoille, kuten kriittisen infrastruktuurin ylläpitäjille, jotta voidaan parantaa niiden tarjoamien palvelujen häiriönsietokykyä. [Direktiiviä XXX/XXXX (NIS2)] sovelletaan pilvipalveluihin ja pilvipalvelumalleihin, kuten SaaS-palveluihin. Kaikki pilvipalveluja unionissa tarjoavat toimijat, jotka täyttävät tai ylittävät keskisuuria yrityksiä koskevan kynnysarvon, kuuluvat kyseisen direktiivin soveltamisalaan.

(10) Jotta ei haitattaisi innovointia tai tutkimusta, tämän asetuksen ei pitäisi kattaa vapaasti käytettävissä olevia ja avoimen lähdekoodin ohjelmistoja, jotka on luotu tai asetettu käytettäviksi kaupallisen toiminnan ulkopuolella. Tämä koskee erityisesti ohjelmistoja, mukaan lukien niiden lähdekoodi ja muunnellut versiot, jotka ovat avoimesti jaettuja ja vapaasti saatavilla, käytettävissä, muunneltavissa ja uudelleen jaeltavissa. Ohjelmistojen yhteydessä toiminnan kaupallisuudesta voi olla merkkinä paitsi tuotteen käytöstä laskuttaminen myös hinnan periminen teknisistä tukipalveluista, muita vastikkeellisia palveluja edellyttävän ohjelmistoalustan tarjoaminen tai henkilötietojen vaatiminen muista syistä kuin yksinomaan ohjelmiston tietoturvan, yhteensopivuuden tai yhteentoimivuuden parantamiseksi.

(11) Internetin tietoturvallisuus on välttämätön edellytys kriittisten infrastruktuurien toiminnalle ja koko yhteiskunnalle. [Direktiivin XXX/XXXX (NIS2)] tavoitteena on varmistaa keskeisten ja tärkeiden toimijoiden tarjoamien palvelujen korkea kyberturvataso, mukaan lukien digitaalisen infrastruktuurin tarjoajat, jotka tukevat avoimen internetin ydintoimintoja ja varmistavat pääsyn internetiin ja sen palveluihin. Sen vuoksi on tärkeää, että digitaalisen infrastruktuurin tarjoajien tarvitsemat digitaalisia elementtejä sisältävät tuotteet on kehitetty tietoturvallisiksi ja että ne ovat

vakiintuneiden internetin tietoturvastandardien mukaisia. Tämän asetuksen, jota sovelletaan kaikkiin liitettävissä oleviin laitteisto- ja ohjelmistotuotteisiin, tavoitteena on myös auttaa digitaalisen infrastruktuurin tarjoajia noudattamaan [direktiivin XXX/XXXX (NIS2)] mukaisia toimitusketjua koskevia vaatimuksia varmistamalla, että digitaalisia elementtejä sisältävät tuotteet, joita ne käyttävät palvelujensa tarjoamiseen, kehitetään tietoturvallisiksi ja että infrastruktuurin tarjoajien saatavilla on oikea-aikaisesti tällaisten tuotteiden tietoturvapäivityksiä.

(12) Euroopan parlamentin ja neuvoston asetuksessa (EU) 2017/745[7] vahvistetaan lääkinnällisiä laitteita koskevat säännöt ja Euroopan parlamentin ja neuvoston asetuksessa (EU) 2017/746[8] *in vitro* -diagnostiikkaan tarkoitettuja lääkinnällisiä laitteita koskevat säännöt. Molemmissa asetuksissa käsitellään kyberturvallisuusriskejä ja noudatetaan tiettyjä lähestymistapoja, jotka sisältyvät myös tähän asetukseen. Asetuksissa (EU) 2017/745 ja (EU) 2017/746 vahvistetaan olennaiset vaatimukset lääkinnällisille laitteille, jotka toimivat sähköisen järjestelmän kautta tai jotka ovat itsessään ohjelmistoja. Asetukset kattavat myös tietyt sulauttamattomat ohjelmistot ja niissä noudatetaan koko elinkaareen perustuvaa lähestymistapaa. Näissä vaatimuksissa edellytetään, että valmistajat kehittävät ja toteuttavat tuotteensa soveltaen riskinhallintaperiaatteita ja täyttäen tietoturvatoimenpiteitä koskevat vaatimukset sekä käyden läpi vastaavat vaatimustenmukaisuuden arviointimenettelyt. Lisäksi lääkinnällisten laitteiden kyberturvallisuudesta on annettu joulukuussa 2019 erityisohjeistusta[9], jossa lääkinnällisten laitteiden, myös *in vitro* -diagnostiikkaan tarkoitettujen laitteiden, valmistajille annetaan ohjeita siitä, miten täyttää kaikki kyseisten asetusten liitteissä I vahvistetut kyberturvallisuutta koskevat olennaiset vaatimukset. Sen vuoksi tätä asetusta ei pitäisi soveltaa digitaalisia elementtejä sisältäviin tuotteisiin, jotka kuuluvat jommankumman edellä mainitun asetuksen soveltamisalaan.

(13) Euroopan parlamentin ja neuvoston asetuksessa (EU) 2019/2144[10] vahvistetaan ajoneuvojen sekä niiden järjestelmien ja komponenttien tyyppihyväksyntää koskevat vaatimukset, joihin kuuluu myös tiettyjä kyberturvavaatimuksia, mukaan lukien sertifioidun kyberturvahallintajärjestelmän toiminta ja ohjelmistopäivitykset, jotka kattavat ajoneuvojen, laitteiden ja palvelujen koko elinkaareen liittyviä kyberriskejä koskevat toimintaperiaatteet ja prosessit sovellettavien teknisiä eritelmiä ja

---

7 Euroopan parlamentin ja neuvoston asetus (EU) 2017/745, annettu 5 päivänä huhtikuuta 2017, lääkinnällisistä laitteista, direktiivin 2001/83/EY, asetuksen (EY) N:o 178/2002 ja asetuksen (EY) N:o 1223/2009 muuttamisesta sekä neuvoston direktiivien 90/385/ETY ja 93/42/ETY kumoamisesta (EUVL L 117, 5.5.2017, s. 1).

8 Euroopan parlamentin ja neuvoston asetus (EU) 2017/746, annettu 5 päivänä huhtikuuta 2017, *in vitro* -diagnostiikkaan tarkoitetuista lääkinnällisistä laitteista sekä direktiivin 98/79/EY ja komission päätöksen 2010/227/EU kumoamisesta (EUVL L 117, 5.5.2017, s. 176).

9 Asetuksen (EU) 2017/745 103 artiklalla perustetun lääkinnällisten laitteiden koordinointiryhmän (MDCG) hyväksymä asiakirja MDCG 2019-16.

10 Euroopan parlamentin ja neuvoston asetus (EU) 2019/2144, annettu 27 päivänä marraskuuta 2019, moottoriajoneuvojen ja niiden perävaunujen sekä näihin ajoneuvoihin tarkoitettujen järjestelmien, komponenttien ja erillisten teknisten yksiköiden tyyppihyväksyntävaatimuksista niiden yleisen turvallisuuden ja ajoneuvon matkustajien ja loukkaantumiselle alttiiden tienkäyttäjien suojelun osalta, Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/858 muuttamisesta ja asetusten (EY) N:o 78/2009, (EY) N:o 79/2009 ja (EY) N:o 661/2009 sekä komission asetusten (EY) N:o 631/2009, (EU) N:o 406/2010, (EU) N:o 672/2010, (EU) N:o 1003/2010, (EU) N:o 1005/2010, (EU) N:o 1008/2010, (EU) N:o 1009/2010, (EU) N:o 19/2011, (EU) N:o 109/2011, (EU) N:o 458/2011, (EU) N:o 65/2012, (EU) N:o 130/2012, (EU) N:o 347/2012, (EU) N:o 351/2012, (EU) N:o 1230/2012 ja (EU) 2015/166 kumoamisesta (EUVL L 325, 16.12.2019, s. 1).

kyberturvallisuutta koskevien Yhdistyneiden kansakuntien sääntöjen[11] mukaisesti. Kyseisessä asetuksessa säädetään myös erityisistä vaatimustenmukaisuuden arviointimenettelyistä. Euroopan parlamentin ja neuvoston asetuksessa (EU) 2018/1139[12] on päätavoitteena siviili-ilmailun yhtenäisen ja korkean turvallisuustason luominen ja ylläpitäminen unionissa. Sillä luodaan puitteet ilmailualan tuotteiden, osien ja varusteiden, ohjelmistot mukaan lukien, olennaisille lentokelpoisuusvaatimuksille, joissa otetaan huomioon tietoturvauhkilta suojautumista koskevat velvoitteet. Digitaalisia elementtejä sisältäviin tuotteisiin, joihin sovelletaan asetusta (EU) 2019/2144, ja kyseisiin tuotteisiin, jotka on sertifioitu asetuksen (EU) 2018/1139 mukaisesti, ei sen vuoksi sovelleta tässä asetuksessa säädettyjä olennaisia vaatimuksia ja vaatimustenmukaisuuden arviointimenettelyjä. Asetuksen (EU) 2018/1139 mukaisella sertifiointimenettelyllä varmistetaan tässä asetuksessa tavoiteltu varmuustaso.

(14) Tässä asetuksessa vahvistetaan horisontaalisia kyberturvasääntöjä, jotka eivät koske pelkästään tiettyjä toimialoja tai tiettyjä digitaalisia elementtejä sisältäviä tuotteita. On kuitenkin mahdollista, että vahvistetaan alakohtaisia tai tuotekohtaisia unionin sääntöjä, joilla puututaan kaikkiin tai joihinkin tässä asetuksessa säädettyjen olennaisten vaatimusten kattamiin riskeihin. Tällaisissa tapauksissa tämän asetuksen soveltamista digitaalisia elementtejä sisältäviin tuotteisiin, joihin sovelletaan muita unionin sääntöjä ja niissä vahvistettuja vaatimuksia, jotka koskevat kaikkia tai joitakin tämän asetuksen liitteen I olennaisten vaatimusten kattamista riskeistä, voidaan rajoittaa tai se voidaan sulkea pois, jos tällainen rajoittaminen tai poissulkeminen on johdonmukaista kyseisiin tuotteisiin sovellettavan yleisen sääntelykehyksen kanssa ja jos alakohtaisilla säännöillä saavutetaan sama suojelun taso kuin tässä asetuksessa säädetään. Komissiolle olisi siirrettävä valta antaa delegoituja säädöksiä tämän asetuksen muuttamiseksi yksilöimällä tällaiset tuotteet ja säännöt. Sellaisen voimassa olevan unionin lainsäädännön osalta, jonka suhteen tällaisia rajoituksia tai poissulkemisia olisi sovellettava, tämä asetus sisältää säännöksiä, joilla selvennetään sen suhdetta kyseiseen unionin lainsäädäntöön.

(15) Delegoidussa asetuksessa (EU) 2022/30 todetaan, että tiettyihin radiolaitteisiin sovelletaan olennaisia vaatimuksia, joista säädetään direktiivin 2014/53/EU 3 artiklan 3 kohdan d alakohdassa (verkon vahingoittaminen ja verkkoresurssien väärinkäyttö), e alakohdassa (henkilötiedot ja yksityisyys) ja f alakohdassa (petokset). [Euroopan standardointijärjestöille esitetystä standardointipyynnöstä tehdyssä komission täytäntöönpanopäätöksessä XXX/2022] vahvistetaan vaatimukset, joiden mukaisesti on laadittava tietyt standardit sen täsmentämiseksi, miten nämä kolme olennaista vaatimusta olisi täytettävä. Tässä asetuksessa säädetyt vaatimukset kattavat kaikki direktiivin 2014/53/EU 3 artiklan 3 kohdan d, e ja f alakohdassa tarkoitettujen olennaisten vaatimusten osatekijät. Lisäksi tässä asetuksessa säädetyt olennaiset vaatimukset ovat linjassa kyseiseen standardointipyyntöön sisältyvien tiettyjä standardeja koskevien vaatimusten tavoitteiden kanssa. Näin ollen jos komissio

[11] E-sääntö nro 155 – Yhdenmukaiset vaatimukset, jotka koskevat ajoneuvojen hyväksyntää kyberturvallisuuden ja sen hallintajärjestelmän osalta [2021/387].

[12] Euroopan parlamentin ja neuvoston asetus (EU) 2018/1139, annettu 4 päivänä heinäkuuta 2018, yhteisistä siviili-ilmailua koskevista säännöistä ja Euroopan unionin lentoturvallisuusviraston perustamisesta, Euroopan parlamentin ja neuvoston asetusten (EY) N:o 2111/2005, (EY) N:o 1008/2008, (EU) N:o 996/2010, (EU) N:o 376/2014 ja direktiivien 2014/30/EU ja 2014/53/EU muuttamisesta sekä Euroopan parlamentin ja neuvoston asetusten (EY) N:o 552/2004, (EY) N:o 216/2008 ja neuvoston asetuksen (ETY) N:o 3922/91 kumoamisesta (EUVL L 212, 22.8.2018, s. 1).

kumoaa delegoidun asetuksen (EU) 2022/30 tai muuttaa sitä niin, että sitä ei enää sovelleta tiettyihin tämän asetuksen soveltamisalaan kuuluviin tuotteisiin, komission ja eurooppalaisten standardointijärjestöjen olisi otettava huomioon standardointityö, joka on tehty radiolaitedirektiivin mukaista delegoitua asetusta 2022/30 koskevasta standardointipyynnöstä annetun komission täytäntöönpanopäätöksen C(2022) 5637 yhteydessä, kun yhdenmukaistettuja standardeja valmistellaan ja kehitetään tämän asetuksen täytäntöönpanon helpottamiseksi.

(16) Direktiivi 85/374/ETY[13] täydentää tätä asetusta. Kyseisessä direktiivissä vahvistetaan tuotevastuusäännöt, joiden mukaisesti vahinkoa kärsineet voivat vaatia korvausta, jos vahinko on aiheutunut tuoteviasta. Siinä vahvistetaan periaate, jonka mukaan tuotteen valmistaja on tuottamuksellisuudesta riippumatta vastuussa tuotteen puutteellisesta turvallisuudesta johtuvista vahingoista (ns. ankara vastuu). Jos tällainen turvallisuuspuute johtuu siitä, että tuotteen markkinoille saattamisen jälkeen ei ole tehty tietoturvapäivityksiä ja tämä aiheuttaa vahinkoa, valmistaja voi joutua vastuuseen. Valmistajien velvollisuudet, jotka koskevat tällaisten tietoturvapäivitysten tarjoamista, olisi vahvistettava tässä asetuksessa.

(17) Tämä asetus ei saisi vaikuttaa Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679[14] soveltamiseen, mukaan lukien säännökset, jotka koskevat tietosuojaa koskevien sertifiointimekanismien ja tietosuojasinettien ja -merkkien käyttöönottoa sen osoittamiseksi, että rekisterinpitäjät ja henkilötietojen käsittelijät noudattavat tietojenkäsittelytoimissaan kyseistä asetusta. Digitaalisia elementtejä sisältävässä tuotteessa voi olla sulautettuna tällaisia tietojenkäsittelytoimia. Sisäänrakennettu ja oletusarvoinen tietosuoja sekä kyberturvallisuus yleensä ovat asetuksen (EU) 2016/679 keskeisiä osatekijöitä. Tässä asetuksessa säädetyillä olennaisilla kyberturvavaatimuksilla suojataan kuluttajia ja organisaatioita kyberturvariskeiltä, joten niillä pyritään myös osaltaan parantamaan henkilötietojen ja yksityisyyden suojaa. Kyberturvanäkökohtien standardoinnin ja sertifioinnin synergioihin olisi pyrittävä yhteistyössä komission, eurooppalaisten standardointiorganisaatioiden, Euroopan unionin kyberturvallisuusviraston (ENISA), asetuksella (EU) 2016/679 perustetun Euroopan tietosuojaneuvoston (EDPB) ja kansallisten tietosuojaviranomaisten välillä. Tämän asetuksen ja unionin tietosuojalainsäädännön välisiä synergioita olisi luotava myös markkinavalvonnan ja täytäntöönpanon alalla. Tätä varten tämän asetuksen nojalla nimettyjen kansallisten markkinavalvontaviranomaisten olisi tehtävä yhteistyötä unionin tietosuojalainsäädännön noudattamista valvovien viranomaisten kanssa. Viimeksi mainituilla olisi myös oltava pääsy tehtäviensä suorittamisen kannalta merkityksellisiin tietoihin.

(18) Siltä osin kuin niiden tuotteet kuuluvat tämän asetuksen soveltamisalaan, [asetuksen (EU) N:o 910/2014, sellaisena kuin se on muutettuna ehdotuksella asetukseksi asetuksen (EU) N:o 910/2014 muuttamisesta eurooppalaisen digitaalisen identiteetin kehyksen osalta] 6 a artiklan 2 kohdassa tarkoitettujen eurooppalaisten digitaalisen identiteetin lompakoiden liikkeeseenlaskijoiden olisi noudatettava sekä tässä

[13] Neuvoston direktiivi 85/374/ETY, annettu 25 päivänä heinäkuuta 1985, tuotevastuuta koskevien jäsenvaltioiden lakien, asetusten ja hallinnollisten määräysten lähentämisestä (EYVL L 210, 7.8.1985).

[14] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (EUVL L 119, 4.5.2016, s. 1).

asetuksessa vahvistettuja horisontaalisia olennaisia vaatimuksia että [asetuksen (EU) N:o 910/2014 6 a artiklassa, sellaisena kuin se on muutettuna ehdotuksella asetukseksi asetuksen (EU) N:o 910/2014 muuttamisesta eurooppalaisen digitaalisen identiteetin kehyksen osalta] vahvistettuja tietoturvavaatimuksia. Vaatimusten noudattamisen helpottamiseksi lompakkojen liikkeeseenlaskijoiden olisi voitava osoittaa, että eurooppalaiset digitaalisen identiteetin lompakot ovat molempien säädösten vaatimusten mukaisia, sertifioimalla tuotteensa sellaisen asetuksella (EU) 2019/881 perustetun eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti, jonka osalta komissio on täytäntöönpanosäädöksellä määrittänyt vaatimustenmukaisuusolettaman tämän asetuksen suhteen, siltä osin kuin sertifikaatti tai sen osat kattavat kyseiset vaatimukset.

(19) Tietyt tässä asetuksessa säädetyt tehtävät olisi asetuksen (EU) 2019/881 3 artiklan 2 kohdan mukaisesti annettava ENISAlle. ENISAn olisi erityisesti saatava valmistajilta ilmoitukset aktiivisesti hyödynnetyistä digitaalisia elementtejä sisältäviin tuotteisiin sisältyvistä haavoittuvuuksista sekä poikkeamista, jotka vaikuttavat kyseisten tuotteiden tietoturvaan. ENISAn olisi myös toimitettava nämä ilmoitukset edelleen asiaan liittyville tietoturvaloukkauksiin reagoiville ryhmille (CSIRT-toimijat) tai direktiivin [direktiivin XXX/XXXX (NIS2)] [X artiklan] mukaisesti nimetyille jäsenvaltioiden keskitetyille yhteyspisteille ja ilmoitettava haavoittuvuudesta asianomaisille markkinavalvontaviranomaisille. ENISAn olisi keräämiensä tietojen perusteella laadittava joka toinen vuosi tekninen raportti digitaalisia elementtejä sisältävien tuotteiden kyberriskien uusista suuntauksista ja toimitettava se direktiivissä [direktiivi XXX/XXXX (NIS2)] tarkoitetulle yhteistyöryhmälle]. Lisäksi ENISAn olisi asiantuntemuksensa ja toimeksiantonsa vuoksi voitava tukea tämän asetuksen täytäntöönpanoprosessia. Sen olisi erityisesti voitava ehdottaa markkinavalvontaviranomaisten yhteisiä toimia saatuaan tietoa digitaalisia elementtejä sisältävien tuotteiden mahdollisista tämän asetuksen vastaisuuksista, joita ilmenee useissa jäsenvaltioissa, tai määrittää tuoteluokkia, joiden osalta olisi järjestettävä samanaikaisia koordinoituja valvontatoimia. Poikkeuksellisissa olosuhteissa ENISAn olisi komission pyynnöstä voitava tehdä arviointeja tietyistä digitaalisia elementtejä sisältävistä tuotteista, jotka aiheuttavat merkittävän kyberturvariskin, jos sisämarkkinoiden moitteettoman toiminnan säilyttämiseksi tarvitaan välittömiä toimia.

(20) Digitaalisia elementtejä sisältävissä tuotteissa olisi oltava CE-merkintä, joka osoittaa niiden olevan tämän asetuksen mukaisia, jotta ne voivat liikkua vapaasti sisämarkkinoilla. Jäsenvaltiot eivät saisi perusteettomasti asettaa esteitä sellaisten digitaalisia elementtejä sisältävien tuotteiden markkinoille saattamiselle, jotka ovat tässä asetuksessa vahvistettujen vaatimusten mukaisia ja joissa on CE-merkintä.

(21) Sen varmistamiseksi, että valmistajat voivat julkaista ohjelmistoja testaustarkoituksiin ennen tuotteidensa vaatimustenmukaisuuden arviointia, jäsenvaltioiden ei pitäisi estää keskeneräisten ohjelmistojen, kuten alfaversioiden, beetaversioiden tai julkaisuehdokkaiden, asettamista saataville edellyttäen, että versio on saatavilla vain niin kauan kuin on tarpeen sen testaamiseksi ja palautteen keräämiseksi. Valmistajien olisi varmistettava, että näiden edellytysten mukaisesti saataville asetettavat ohjelmistot julkaistaan vasta riskinarvioinnin jälkeen ja että ne täyttävät mahdollisimman suuressa määrin tässä asetuksessa säädetyt digitaalisia elementtejä sisältävien tuotteiden ominaisuuksiin liittyvät tietoturvavaatimukset. Valmistajien olisi mahdollisimman suuressa määrin täytettävä myös haavoittuvuuksien käsittelyä koskevat vaatimukset. Valmistajien ei pitäisi pakottaa käyttäjiä päivittämään ohjelmistojaan versioihin, jotka on julkaistu ainoastaan testaustarkoituksiin.

(22) Sen varmistamiseksi, että digitaalisia elementtejä sisältävät tuotteet eivät markkinoille saatettaessa aiheuta kyberturvariskejä yksityishenkilöille ja organisaatioille, tällaisille tuotteille olisi vahvistettava olennaiset vaatimukset. Jos tuotteita myöhemmin muutetaan joko fyysisesti tai digitaalisesti tavalla, jota valmistaja ei ole ennakoinut ja jonka johdosta ne eivät mahdollisesti enää täytä niitä koskevia olennaisia vaatimuksia, muutos olisi katsottava merkittäväksi. Esimerkiksi ohjelmistopäivitykset tai -korjaukset voitaisiin rinnastaa ylläpitotoimiin edellyttäen, että niillä ei muuteta jo markkinoille saatettua tuotetta siten, että se voi vaikuttaa sovellettavien vaatimusten täyttymiseen tai muuttaa käyttötarkoitusta, jota varten tuote on arvioitu. Kuten fyysisten korjausten tai muutosten tapauksessa, digitaalisia elementtejä sisältävän tuotteen olisi katsottava olevan merkittävästi muutettu ohjelmistomuokkauksella, jos ohjelmistopäivitys muuttaa tuotteen alkuperäisiä tarkoitettuja toimintoja, tuotteen tyyppiä tai tuotteen suorituskykyä eikä näitä muutoksia ole otettu huomioon alkuperäisessä riskinarvioinnissa tai vaaran luonne on muuttunut tai riskitaso noussut ohjelmistopäivityksen vuoksi.

(23) Unionin yhdenmukaistamislainsäädännön soveltamisalaan kuuluvien tuotteiden osalta yleisesti vahvistetun merkittävän muutoksen käsitteen mukaisesti aina, kun tapahtuu merkittävä muutos, joka voi vaikuttaa siihen, onko tuote tämän asetuksen mukainen, tai kun tuotteen käyttötarkoitus muuttuu, on asianmukaista, että digitaalisia elementtejä sisältävän tuotteen vaatimustenmukaisuus todennetaan ja että sille tehdään tarvittaessa uusi vaatimustenmukaisuuden arviointi. Jos valmistaja suorittaa vaatimustenmukaisuuden arvioinnin, johon osallistuu kolmas osapuoli, muutoksista, jotka voivat johtaa merkittävään muutokseen, olisi ilmoitettava kolmannelle osapuolelle.

(24) Digitaalisia elementtejä sisältävän tuotteen asetuksessa [ekologista suunnittelua koskeva asetus] määritelty kunnostaminen, ylläpito ja korjaaminen ei välttämättä johda tuotteen merkittävään muutokseen esimerkiksi kun aiottu käyttötarkoitus ja toiminnallisuus ei muutu eikä riskitasoon kohdistu vaikutusta. Valmistajan suorittama tuoteparannus voi kuitenkin johtaa muutoksiin tuotteen rakenteessa ja toteuttamistavassa ja siten vaikuttaa aiottuun käyttötarkoitukseen ja siihen, onko tuote tässä asetuksessa säädettyjen vaatimusten mukainen.

(25) Digitaalisia elementtejä sisältävää tuotetta olisi pidettävä kriittisenä, jos tuotteen mahdollisten kyberturvahaavoittuvuuksien hyödyntämisen kielteinen vaikutus voi olla vakava esimerkiksi kyberturvallisuuteen liittyvän toiminnon tai aiotun käyttötarkoituksen perusteella. Erityisesti sellaisten digitaalisia elementtejä sisältävien tuotteiden haavoittuvuudet, joissa on kyberturvallisuuteen liittyviä toimintoja, kuten suojattuja elementtejä, voivat johtaa tietoturvaongelmien leviämiseen koko toimitusketjussa. Kyberturvapoikkeaman vaikutusten vakavuus voi lisääntyä myös, kun otetaan huomioon tuotteen aiottu käyttötarkoitus, kuten käyttö teollisessa ympäristössä tai [direktiivin XXX/XXXX (NIS2)] liitteessä [liite I] tarkoitetun keskeisen toimijan toiminnassa, tai kun on kyse kriittisten tai arkaluonteisten toimintojen, kuten henkilötietojen käsittelyn, suorittamisesta.

(26) Digitaalisia elementtejä sisältäviin kriittisiin tuotteisiin olisi sovellettava tiukempia vaatimustenmukaisuuden arviointimenettelyjä, mutta kuitenkin oikeasuhteisesti. Tätä varten digitaalisia elementtejä sisältävät kriittiset tuotteet olisi jaettava kahteen luokkaan, jotka kuvastavat näihin tuoteluokkiin liittyvän kyberturvariskin tasoa. Luokan II tuotteisiin liittyvä mahdollinen kyberturvapoikkeama voisi johtaa suurempiin kielteisiin vaikutuksiin kuin luokan I tuotteisiin liittyvä poikkeama esimerkiksi niiden kyberturvallisuuteen liittyvän toiminnan luonteen tai

arkaluontoisissa ympäristöissä suunnitellun käytön vuoksi, ja siksi ne olisi alistettava tiukempaan vaatimustenmukaisuuden arviointimenettelyyn.

(27) Tämän asetuksen liitteessä III tarkoitetut digitaalisia elementtejä sisältävien kriittisten tuotteiden luokat olisi ymmärrettävä sellaisten tuotteiden luokiksi, joilla on jokin tämän asetuksen liitteessä III luetellun tyyppinen ydintoiminto. Tämän asetuksen liitteessä III luetellaan esimerkiksi tuotteet, jotka määritellään ydintoiminnoillaan luokkaan II kuuluviksi yleiskäyttöön tarkoitetuiksi mikroprosessoreiksi. Tästä seuraa, että yleiskäyttöisille mikroprosessoreille on tehtävä pakollinen kolmannen osapuolen suorittama vaatimustenmukaisuuden arviointi. Tämä ei koske muita tuotteita, joita ei nimenomaisesti mainita tämän asetuksen liitteessä III, mutta joihin voi sisältyä yleiskäyttöön tarkoitettu mikroprosessori. Komission olisi annettava [12 kuukauden kuluessa tämän asetuksen voimaantulosta] delegoituja säädöksiä, joissa täsmennetään liitteessä III esitetyt I ja II luokkaan kuuluvien tuoteryhmien määritelmät.

(28) Tällä asetuksella puututaan kohdennetusti kyberturvallisuusriskeihin. Digitaalisia elementtejä sisältävät tuotteet voivat kuitenkin aiheuttaa muita turvallisuusriskejä, jotka eivät liity kyberturvallisuuteen. Näitä riskejä olisi edelleen säänneltävä muulla asiaa koskevalla unionin tuotelainsäädännöllä. Jos muuta unionin yhdenmukaistamislainsäädäntöä ei voida soveltaa, niihin olisi sovellettava asetusta [yleinen tuoteturvallisuusasetus]. Kun otetaan huomioon tämän asetuksen kohdennettu luonne, poiketen siitä, mitä asetuksen [yleinen tuoteturvallisuusasetus] 2 artiklan 1 kohdan kolmannen alakohdan b alakohdassa säädetään, asetuksen [yleinen tuoteturvallisuusasetus] III luvun 1 jakson V ja VII lukua sekä IX-XI lukua olisi sen vuoksi sovellettava digitaalisia elementtejä sisältäviin tuotteisiin tämän asetuksen soveltamisalaan kuulumattomien turvallisuusriskien osalta, jos kyseisiin tuotteisiin ei sovelleta [yleisen tuoteturvallisuusasetuksen 3 artiklan 25 kohdassa] tarkoitettuja unionin muussa yhdenmukaistamislainsäädännössä asetettuja erityisvaatimuksia.

(29) Asetuksen XXX[15] [tekoälyasetus] 6 artiklan mukaisesti suuririskisiksi tekoälyjärjestelmiksi luokiteltujen digitaalisia elementtejä sisältävien tuotteiden, jotka kuuluvat tämän asetuksen soveltamisalaan, olisi täytettävä tässä asetuksessa vahvistetut olennaiset vaatimukset. Kun kyseiset suuririskiset tekoälyjärjestelmät täyttävät tämän asetuksen olennaiset vaatimukset, niiden olisi katsottava olevan asetuksen [tekoälyasetus] [15 artiklassa] vahvistettujen kyberturvavaatimusten mukaisia siltä osin kuin kyseiset vaatimukset kuuluvat tämän asetuksen nojalla annetun EU-vaatimustenmukaisuusvakuutuksen tai sen osien piiriin. Tämän asetuksen soveltamisalaan kuuluvan digitaalisia elementtejä sisältävän ja suuririskiseksi tekoälyjärjestelmäksi luokitellun tuotteen olennaisiin kyberturvavaatimuksiin liittyvien vaatimustenmukaisuuden arviointimenettelyjen osalta olisi sovellettava pääsääntöisesti asetuksen [tekoälyasetus] 43 artiklan asiaankuuluvia säännöksiä tämän asetuksen vastaavien säännösten sijasta. Tämä pääsääntö ei kuitenkaan saisi johtaa tämän asetuksen soveltamisalaan kuuluvien digitaalisia elementtejä sisältävien kriittisten tuotteiden tarvittavan varmuustason alenemiseen. Sen vuoksi tästä pääsäännöstä poiketen suuririskisiin tekoälyjärjestelmiin, jotka kuuluvat asetuksen [tekoälyasetus] soveltamisalaan ja jotka luokitellaan myös tämän asetuksen mukaisiksi digitaalisia elementtejä sisältäviksi kriittisiksi tuotteiksi ja joihin sovelletaan asetuksen [tekoälyasetus] liitteessä VI tarkoitettua sisäiseen valvontaan perustuvaa vaatimustenmukaisuuden arviointimenettelyä, olisi sovellettava tämän asetuksen

[15] Asetus (tekoälyasetus).

vaatimustenmukaisuuden arviointia koskevia säännöksiä siltä osin kuin kyse on tämän asetuksen olennaisista vaatimuksista. Tässä tapauksessa kaikkiin muihin asetuksen [tekoälyasetus] kattamiin näkökohtiin olisi sovellettava asetuksen [tekoälyasetus] liitteessä VI vahvistettuja sisäiseen valvontaan perustuvaa vaatimustenmukaisuuden arviointia koskevia säännöksiä.

(30) Asetuksen [koneasetusehdotus] soveltamisalaan kuuluvien konetuotteiden, jotka ovat tässä asetuksessa tarkoitettuja digitaalisia elementtejä sisältäviä tuotteita ja joille on annettu vaatimustenmukaisuusvakuutus tämän asetuksen pohjalta, olisi katsottava olevan asetuksen [koneasetusehdotus] [liitteessä III olevassa 1.1.9 ja 1.2.1 kohdassa] vahvistettujen olennaisten terveys- ja turvallisuusvaatimusten mukaisia korruptoitumiselta suojautumisen sekä ohjausjärjestelmien turvallisuuden ja luotettavuuden osalta, jos näiden vaatimusten täyttyminen osoitetaan tämän asetuksen nojalla annetulla EU-vaatimustenmukaisuusvakuutuksella.

(31) Asetus [ehdotus eurooppalaista terveysdata-avaruutta koskevaksi asetukseksi] täydentää tässä asetuksessa säädettyjä olennaisia vaatimuksia. Asetuksen [eurooppalaista terveysdata-avaruutta koskeva asetusehdotus] soveltamisalaan kuuluvien sähköisten potilaskertomusjärjestelmien, jäljempänä ’sähköiset potilastietojärjestelmät’, jotka ovat tässä asetuksessa tarkoitettuja digitaalisia elementtejä sisältäviä tuotteita, olisi sen vuoksi täytettävä myös tässä asetuksessa säädetyt olennaiset vaatimukset. Niiden valmistajien olisi osoitettava vaatimustenmukaisuus asetuksen [ehdotus eurooppalaisesta terveysdata-avaruudesta] mukaisesti. Vaatimusten noudattamisen helpottamiseksi valmistajat voivat laatia yksittäisen teknisen dokumentaation, joka sisältää molemmissa säädöksissä vaaditut tiedot. Koska tämä asetus ei kata palveluna tarjottavia ohjelmistoja (SaaS) sellaisenaan, SaaS-lisenssillä tarjottavat sähköiset potilastietojärjestelmät eivät kuulu tämän asetuksen soveltamisalaan. Vastaavasti organisaation sisäisesti kehitetyt ja käytettävät sähköiset potilastietojärjestelmät eivät kuulu tämän asetuksen soveltamisalaan, koska niitä ei saateta markkinoille.

(32) Sen varmistamiseksi, että digitaalisia elementtejä sisältävät tuotteet ovat tietoturvallisia sekä niiden markkinoille saattamisen ajankohtana että koko niiden elinkaaren ajan, on tarpeen vahvistaa haavoittuvuuksien käsittelyä koskevat olennaiset vaatimukset ja digitaalisia elementtejä sisältävien tuotteiden ominaisuuksiin liittyvät olennaiset kyberturvavaatimukset. Valmistajien olisi täytettävä kaikki haavoittuvuuksien käsittelyn olennaiset vaatimukset ja varmistettava, että kaikki niiden tuotteet toimitetaan ilman tiedossa olevia hyödynnettävissä olevia haavoittuvuuksia, mutta niiden olisi myös määritettävä, mitkä muut tuotteen ominaisuuksiin liittyvät olennaiset vaatimukset ovat merkityksellisiä kyseisen tuotetyypin kannalta. Tätä varten valmistajien olisi suoritettava digitaalisia elementtejä sisältävään tuotteeseen liittyvien kyberturvariskien arviointi kyseeseen tulevien riskien ja olennaisten vaatimusten tunnistamiseksi, jotta ne voisivat käyttää asianmukaisia yhdenmukaistettuja standardeja tai yhteisiä eritelmiä.

(33) Sisämarkkinoille saatettavien digitaalisia elementtejä sisältävien tuotteiden tietoturvan parantamiseksi on tarpeen vahvistaa olennaiset vaatimukset. Nämä olennaiset vaatimukset eivät saisi vaikuttaa [direktiivin XXX/XXXX(NIS2)][16] [XX artiklalla]

[16] Euroopan parlamentin ja neuvoston direktiivi XXX, annettu [päivämäärä], toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta (EUVL L xx, päivämäärä, s. x).

perustettuihin kriittisiä toimitusketjuja koskeviin koordinoituihin EU:n riskinarviointeihin, joissa otetaan huomioon sekä tekniset että tarvittaessa muut kuin tekniset riskitekijät, kuten kolmannen maan asiaton vaikuttaminen laitteisto- ja ohjelmistotoimittajiin. Lisäksi se ei saisi rajoittaa jäsenvaltioiden oikeuksia asettaa lisävaatimuksia, joissa otetaan häiriönsietokyvyn parantamiseksi huomioon muita kuin teknisiä tekijöitä, mukaan lukien suosituksessa (EU) 2019/534, 5G-verkkojen tietoturvaa koskevassa unionin laajuisessa koordinoidussa riskinarvioinnissa ja [direktiivissä XXX/XXXX (NIS2)] tarkoitetun verkko- ja tietoturva-alan yhteistyöryhmän hyväksymässä 5G-kyberturvallisuutta koskevassa EU:n välineistössä määritellyt tekijät.

(34) Jotta kansalliset CSIRT-yksiköt ja direktiivin [direktiivin XX/XXXX (NIS2) [X artiklan] mukaisesti nimetyt keskitetyt yhteyspisteet saavat tehtäviensä suorittamiseksi ja keskeisten ja tärkeiden toimijoiden kyberturvan yleisen tason nostamiseksi tarvitsemansa tiedot ja jotta varmistettaisiin markkinavalvontaviranomaisten toiminnan tuloksellisuus, digitaalisia elementtejä sisältävien tuotteiden valmistajien olisi ilmoitettava ENISAlle aktiivisesti hyödynnetyistä haavoittuvuuksista. Koska useimpia digitaalisia elementtejä sisältäviä tuotteita markkinoidaan koko sisämarkkinoilla, jokainen digitaalisia elementtejä sisältävien tuotteiden hyväksikäytetty haavoittuvuus olisi katsottava uhkaksi sisämarkkinoiden toiminnalle. Valmistajien olisi myös harkittava korjattujen haavoittuvuuksien ilmoittamista direktiivin [direktiivi XX/XXXX (NIS2)] nojalla perustettuun Euroopan haavoittuvuustietokantaan, jota hallinnoi ENISA, tai johonkin muuhun yleisesti saatavilla olevaan haavoittuvuustietokantaan.

(35) Valmistajien olisi myös ilmoitettava ENISAlle kaikista poikkeamista, jotka vaikuttavat digitaalisia elementtejä sisältävän tuotteen tietoturvaan. Sen estämättä, mitä direktiivissä [direktiivissä XXX/XXXX (NIS2)] säädetään poikkeamien raportointivelvoitteista keskeisten ja tärkeiden toimijoiden osalta, on ratkaisevan tärkeää, että ENISA, jäsenvaltioiden direktiivin XXX/XXXX (NIS2) [X artiklan] mukaisesti nimeämät keskitetyt yhteyspisteet ja markkinavalvontaviranomaiset saavat digitaalisia elementtejä sisältävien tuotteiden valmistajilta tiedot, joiden avulla ne voivat arvioida näiden tuotteiden tietoturvallisuuden. Jotta käyttäjät voisivat reagoida nopeasti digitaalisia elementtejä sisältävien tuotteiden tietoturvaan vaikuttaviin poikkeamiin, valmistajien olisi ilmoitettava poikkeamista ja tarvittaessa mahdollisista korjaavista toimenpiteistä, joita käyttäjät voivat toteuttaa poikkeaman vaikutusten lieventämiseksi, myös käyttäjilleen, esimerkiksi julkaisemalla asiaankuuluvat tiedot verkkosivustoillaan tai, jos valmistajalla on yhteys käyttäjiin ja jos se on riskien vuoksi perusteltua, ottamalla käyttäjiin suoraan yhteyttä.

(36) Digitaalisia elementtejä sisältävien tuotteiden valmistajien olisi otettava käyttöön koordinoidut haavoittuvuuksien ilmoittamisperiaatteet, jotka auttaisivat yksityishenkilöitä ja eri toimijoita raportoimaan haavoittuvuuksista. Koordinoiduissa haavoittuvuuksien ilmoittamisperiaatteissa määritellään jäsennelty prosessi, jonka avulla haavoittuvuuksista ilmoitetaan valmistajalle siten, että se voi diagnosoida haavoittuvuuden ja korjata sen ennen kuin yksityiskohtaisia tietoja haavoittuvuudesta paljastetaan kolmansille osapuolille tai yleisölle. Kun otetaan huomioon, että tietoa laajalti käytettyjen digitaalisia elementtejä sisältävien tuotteiden hyväksikäytettävissä olevista haavoittuvuuksista saatetaan myydä korkean hintaan pimeillä markkinoilla, tällaisten tuotteiden valmistajien olisi voitava käyttää osana koordinoituja haavoittuvuuksien ilmoittamisperiaatteitaan erityisiä ohjelmia, joilla luodaan kannustimia haavoittuvuuksista ilmoittamiseen varmistamalla, että yksityishenkilöt ja

eri toimijat saavat tunnustusta ja korvauksen ilmoituksistaan (ns. *bug bounty* -ohjelmat).

(37) Haavoittuvuusanalyysin helpottamiseksi valmistajien olisi yksilöitävä ja dokumentoitava digitaalisia elementtejä sisältävien tuotteidensa komponentit muun muassa laatimalla ohjelmistosisältöluettelo. Ohjelmistosisältöluettelosta ohjelmistojen valmistajat, ostajat ja käyttäjät voivat saada tietoja, jotka parantavat heidän ymmärrystään toimitusketjusta, mistä koituu monia hyötyjä, varsinkin kun se auttaa valmistajia ja käyttäjiä jäljittämään ilmaantuneita uusia haavoittuvuuksia ja riskejä. Valmistajille on erityisen tärkeää varmistaa, että niiden tuotteet eivät sisällä kolmansien osapuolten kehittämiä haavoittuvia komponentteja.

(38) Jotta tässä asetuksessa säädettyjen vaatimusten täyttymisen arviointi olisi helpompaa, olisi oltava olemassa vaatimustenmukaisuusolettama niiden digitaalisten elementtien osalta, jotka ovat sellaisten yhdenmukaistettujen standardien mukaisia, jotka muuntavat tämän asetuksen olennaiset vaatimukset yksityiskohtaisiksi teknisiksi eritelmiksi ja jotka on hyväksytty Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1025/2012[17] mukaisesti. Asetuksessa (EU) N:o 1025/2012 säädetään yhdenmukaistetuista standardeista esitettäviä vastalauseita koskevasta menettelystä tapauksissa, joissa kyseiset standardit eivät kokonaan täytä tämän asetuksen vaatimuksia.

(39) Asetuksella (EU) 2019/881 perustetaan vapaaehtoinen eurooppalainen kyberturvallisuuden sertifiointikehys tieto- ja viestintäteknisille tuotteille, prosesseille ja palveluille. Eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät voivat kattaa tämän asetuksen soveltamisalaan kuuluvia, digitaalisia elementtejä sisältäviä tuotteita. Tällä asetuksella olisi luotava synergioita asetuksen (EU) 2019/881 kanssa. Jotta tässä asetuksessa säädettyjen vaatimusten täyttymisen arviointi olisi helpompaa, digitaalisia elementtejä sisältävien tuotteiden, jotka on sertifioitu tai joista on annettu vaatimustenmukaisuusvakuutus asetuksen (EU) 2019/881 mukaisessa ja komission täytäntöönpanosäädöksellä yksilöimässä kyberturvajärjestelmässä, katsotaan olevan tämän asetuksen olennaisten vaatimusten mukaisia siltä osin kuin kyberturvasertifikaatti tai vaatimustenmukaisuusvakuutus tai niiden osat kattavat kyseiset vaatimukset. Digitaalisia elementtejä sisältävien tuotteiden uusien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien tarvetta olisi arvioitava tämän asetuksen valossa. Mahdollisissa tulevissa eurooppalaisissa kyberturvallisuuden sertifiointijärjestelmissä, jotka kattavat digitaalisia elementtejä sisältäviä tuotteita, olisi otettava huomioon tässä asetuksessa vahvistetut olennaiset vaatimukset ja helpotettava tämän asetuksen noudattamista. Komissiolle olisi siirrettävä valta määritellä täytäntöönpanosäädöksillä eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät, joita voidaan käyttää osoittamaan tässä asetuksessa säädettyjen olennaisten vaatimusten täyttyminen. Lisäksi valmistajien tarpeettoman hallinnollisen taakan välttämiseksi komission olisi tarvittaessa täsmennettävä, poistaako tällaisen eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti myönnetty

[17] Euroopan parlamentin ja neuvoston asetus (EU) N:o 1025/2012, annettu 25 päivänä lokakuuta 2012, eurooppalaisesta standardoinnista, neuvoston direktiivien 89/686/ETY ja 93/15/ETY sekä Euroopan parlamentin ja neuvoston direktiivien 94/9/EY, 94/25/EY, 95/16/EY, 97/23/EY, 98/34/EY, 2004/22/EY, 2007/23/EY, 2009/23/EY ja 2009/105/EY muuttamisesta ja neuvoston päätöksen 87/95/ETY ja Euroopan parlamentin ja neuvoston päätöksen N:o 1673/2006/EY kumoamisesta (EUVL L 316, 14.11.2012, s. 12).

sertifikaatti valmistajilta velvoitteen teettää vastaavien vaatimusten osalta tässä asetuksessa säädetty vaatimustenmukaisuuden arviointi kolmansilla osapuolilla.

(40) Kun [yhteisiin kriteereihin perustuvasta eurooppalaisesta kyberturvallisuuden sertifiointijärjestelmästä annettu komission täytäntöönpanoasetus XXX (EU) N:o.../...] (EUCC), joka koskee tämän asetuksen soveltamisalaan kuuluvia laitteistotuotteita, kuten laiteteknisiä turvamoduuleja ja mikroprosessoreja, tulee voimaan, komissio voi täytäntöönpanosäädöksellä täsmentää, miten EUCC luo olettaman tämän asetuksen liitteessä I tarkoitettujen olennaisten vaatimusten tai niiden osien täyttymisestä. Lisäksi tällaisessa täytäntöönpanosäädöksessä voidaan täsmentää, miten EUCC:n mukainen sertifiointi poistaa valmistajilta velvoitteen teettää vastaavien vaatimusten osalta tässä asetuksessa säädetty vaatimustenmukaisuuden arviointi kolmansilla osapuolilla.

(41) Jos yhdenmukaistettuja standardeja ei ole tai jos niissä ei oteta riittävästi huomioon tämän asetuksen olennaisia vaatimuksia, komission olisi voitava hyväksyä täytäntöönpanosäädöksillä yhteisiä eritelmiä. Syitä tällaisten yhteisten eritelmien laatimiseen yhdenmukaistettujen standardien sijaan voisivat olla eurooppalaisten standardointiorganisaatioiden kieltäytyminen standardointipyynnöstä, aiheettomat viivästykset asianmukaisten yhdenmukaistettujen standardien laatimisessa tai se, että kehitetyt standardit eivät ole tämän asetuksen vaatimusten tai komission pyynnön mukaisia. Tässä asetuksessa säädettyjen olennaisten vaatimusten täyttymisen arvioinnin helpottamiseksi olisi voitava olettaa, että digitaalisia elementtejä sisältävät tuotteet, jotka ovat sellaisten yhteisten eritelmien mukaisia, jotka komissio on tämän asetuksen mukaisesti hyväksynyt kyseisten vaatimusten yksityiskohtaisten teknisten eritelmien ilmaisemiseksi, täyttävät tässä asetuksessa säädetyt olennaiset vaatimukset.

(42) Valmistajien olisi laadittava EU-vaatimustenmukaisuusvakuutus, jossa annetaan tässä asetuksessa edellytetyt tiedot siitä, että digitaalisia elementtejä sisältävä tuote on tämän asetuksen olennaisten vaatimusten sekä soveltuvin osin unionin muun asiaankuuluvan yhdenmukaistamislainsäädännön, jonka piiriin tuote kuuluu, mukainen. Valmistajilta saatetaan edellyttää EU-vaatimustenmukaisuusvakuutuksen laatimista myös muun unionin lainsäädännön nojalla. Jotta voidaan varmistaa tosiasiallinen tiedonsaanti markkinavalvontaa varten, kaikkien asiaan kuuluvien unionin säädösten vaatimusten täyttymisen osalta olisi laadittava yksi ainoa EU-vaatimustenmukaisuusvakuutus. Talouden toimijoiden hallinnollisen rasitteen vähentämiseksi tällaisen kattavan EU-vaatimustenmukaisuusvakuutuksen olisi voitava olla kooste, joka koostuu tuotetta koskevista erillisistä vaatimustenmukaisuusvakuutuksista.

(43) CE-merkintä osoittaa tuotteen vaatimustenmukaisuuden ja on näkyvä osoitus vaatimustenmukaisuuden arvioinnin koko prosessista sen laajassa merkityksessä. CE-merkinnän yleisistä periaatteista säädetään Euroopan parlamentin ja neuvoston asetuksessa (EY) N:o 765/2008[18]. CE-merkinnän kiinnittämistä digitaalisia elementtejä sisältäviin tuotteisiin koskevat säännöt olisi annettava tässä asetuksessa. CE-merkinnän olisi oltava ainoa merkintä, joka takaa, että digitaalisia elementtejä sisältävät tuotteet ovat tämän asetuksen vaatimusten mukaisia.

(44) Jotta talouden toimijat voivat osoittaa tässä asetuksessa säädettyjen olennaisten vaatimusten täyttymisen ja jotta markkinavalvontaviranomaiset voivat varmistaa, että

[18] Euroopan parlamentin ja neuvoston asetus (EY) N:o 765/2008, annettu 9 päivänä heinäkuuta 2008, akkreditoinnin vaatimusten vahvistamisesta ja asetuksen (ETY) N:o 339/93 kumoamisesta (EUVL L 218, 13.8.2008, s. 30).

markkinoilla saataville asetetut digitaalisia elementtejä sisältävät tuotteet ovat näiden vaatimusten mukaisia, on tarpeen säätää vaatimustenmukaisuuden arviointimenettelyistä. Euroopan parlamentin ja neuvoston päätöksessä N:o 768/2008/EY[19] vahvistetaan vaatimustenmukaisuuden arviointimenettelyjen moduulit suhteessa riskitasoon ja vaadittuun turvallisuustasoon. Eri toimialojen välisen johdonmukaisuuden varmistamiseksi ja tapauskohtaisten muunnosten välttämiseksi vaatimustenmukaisuuden arviointimenettelyjen, jotka riittävät sen todentamiseen, että digitaalisia elementtejä sisältävät tuotteet täyttävät tässä asetuksessa vahvistetut olennaiset vaatimukset, olisi perustuttava kyseisiin moduuleihin. Vaatimustenmukaisuuden arviointimenettelyissä olisi tutkittava ja todennettava sekä tuotteisiin että prosesseihin liittyvät ominaisuudet digitaalisia elementtejä sisältävien tuotteiden koko elinkaaren pituudelta, mukaan lukien tuotteen suunnittelu, rakenne, kehittäminen/tuotanto, testaus ja ylläpito.

(45) Pääsääntöisesti valmistajan olisi suoritettava digitaalisia elementtejä sisältävien tuotteiden vaatimustenmukaisuuden arviointi omalla vastuullaan noudattaen päätöksen 768/2008/EY moduuliin A perustuvaa menettelyä. Valmistajan olisi joustavasti voitava valita tiukempi vaatimustenmukaisuuden arviointimenettely, johon osallistuu kolmas osapuoli. Jos tuote on luokiteltu luokan I kriittiseksi tuotteeksi, tarvitaan lisätakeita sen osoittamiseksi, että tuote täyttää tässä asetuksessa säädetyt olennaiset vaatimukset. Jos valmistaja haluaa suorittaa vaatimustenmukaisuuden arvioinnin omalla vastuullaan (moduuli A), sen olisi sovellettava asetuksen (EU) 2019/881 mukaisia yhdenmukaistettuja standardeja, yhteisiä eritelmiä tai kyberturvallisuuden sertifiointijärjestelmiä, jotka komissio on yksilöinyt täytäntöönpanosäädöksessä. Jos valmistaja ei sovella tällaisia yhdenmukaistettuja standardeja, yhteisiä eritelmiä tai kyberturvallisuuden sertifiointijärjestelmiä, valmistajan olisi tehtävä vaatimustenmukaisuuden arviointi, johon osallistuu kolmas osapuoli. Kun otetaan huomioon valmistajille aiheutuva hallinnollinen rasite ja se, että kyberturvallisuudella on tärkeä rooli digitaalisia elementtejä sisältävien aineellisten ja aineettomien tuotteiden suunnittelu- ja kehitysvaiheessa, päätöksen 768/2008/EY moduuliin B+C tai moduuliin H perustuvat vaatimustenmukaisuuden arviointimenettelyt on valittu oikeasuhteisuuden ja tuloksellisuuden näkökulmasta sopivimmiksi tavoiksi arvioida digitaalisia elementtejä sisältävien kriittisten tuotteiden vaatimustenmukaisuus. Valmistaja, joka käyttää kolmannen osapuolen suorittamaa vaatimustenmukaisuuden arviointia, voi valita suunnittelu- ja tuotantoprosessiinsa parhaiten soveltuvan menettelyn. Koska luokan II kriittisiksi tuotteiksi luokiteltujen tuotteiden käyttöön liittyy vieläkin suurempi kyberturvariski, vaatimustenmukaisuuden arvioinnissa olisi aina oltava mukana kolmas osapuoli.

(46) Digitaalisia elementtejä sisältävien aineellisten tuotteiden luominen edellyttää yleensä valmistajilta huomattavia panostuksia koko suunnittelu-, kehitys- ja tuotantovaiheen ajan, kun taas ohjelmistomuotoisten digitaalisia elementtejä sisältävien tuotteiden luominen painottuu lähes yksinomaan suunnitteluun ja kehittämiseen, ja tuotantovaiheella on vähäisempi merkitys. Monissa tapauksissa ohjelmistotuotteet on kuitenkin vielä koottava, koostettava, pakattava, asetettava saataville ladattavaksi tai kopioitava fyysiselle tallennusvälineelle ennen markkinoille saattamista. Nämä toimet olisi katsottava tuotantoa vastaaviksi toimiksi, kun sovelletaan asiaankuuluvia

[19] Euroopan parlamentin ja neuvoston päätös N:o 768/2008/EY, tehty 9 päivänä heinäkuuta 2008, tuotteiden kaupan pitämiseen liittyvistä yhteisistä puitteista ja päätöksen 93/465/ETY kumoamisesta (EUVL L 218, 13.8.2008, s. 82).

vaatimustenmukaisuuden arviointimoduuleja sen todentamiseksi, että tuote on tämän asetuksen olennaisten vaatimusten mukainen kaikissa suunnittelu-, kehitys- ja tuotantovaiheissa.

(47) Jotta voidaan käyttää kolmannen osapuolen suorittamia, digitaalisia elementtejä sisältävien tuotteiden vaatimustenmukaisuuden arviointeja, kansallisten ilmoittavien viranomaisten olisi ilmoitettava vaatimustenmukaisuuden arviointilaitokset komissiolle ja muille jäsenvaltioille edellyttäen, että laitokset täyttävät tietyt vaatimukset erityisesti riippumattomuuden, pätevyyden ja eturistiriitojen suhteen.

(48) Jotta varmistetaan yhtenäinen laatutaso digitaalisia elementtejä sisältävien tuotteiden vaatimustenmukaisuuden arvioinnissa, on tarpeen vahvistaa myös ilmoittavia viranomaisia sekä muita ilmoitettujen laitosten arvioinnissa, ilmoittamisessa ja valvonnassa mukana olevia elimiä koskevat vaatimukset. Tässä asetuksessa käyttöön otettua järjestelmää olisi täydennettävä akkreditointijärjestelmällä, josta säädetään asetuksessa (EY) N:o 765/2008. Koska akkreditointi on olennainen keino tarkastaa vaatimustenmukaisuuden arviointilaitosten pätevyys, sitä olisi käytettävä myös ilmoittamistarkoituksia varten.

(49) Kansallisten viranomaisten olisi kaikkialla unionissa pidettävä asetuksen (EY) N:o 765/2008 mukaista avointa akkreditointia, jolla varmistetaan tarvittava luottamuksen taso vaatimustenmukaisuustodistuksissa, ensisijaisena keinona osoittaa vaatimustenmukaisuuden arviointilaitosten tekninen pätevyys. Kansalliset viranomaiset voivat kuitenkin katsoa, että niillä on käytettävissään asianmukaiset keinot suorittaa tämä arviointi itse. Tällaisessa tapauksessa, jotta voidaan varmistaa muiden kansallisten viranomaisten tekemän arvioinnin uskottavuuden asianmukainen taso, niiden olisi toimitettava komissiolle ja muille jäsenvaltioille tarvittava asiakirja-aineisto, jolla osoitetaan, että arvioidut vaatimustenmukaisuuden arviointilaitokset täyttävät asian kannalta merkitykselliset lainsäädännölliset vaatimukset.

(50) Vaatimustenmukaisuuden arviointilaitokset teettävät usein osia vaatimustenmukaisuuden arviointiin liittyvistä toimistaan alihankintana tai käyttävät tytäryhtiötä. Digitaalisia elementtejä sisältävän tuotteen saattaminen markkinoille edellyttää suojauksen tasoa, jonka turvaamiseksi on olennaista, että vaatimustenmukaisuuden arviointitehtävien suorittamista varten alihankkijat ja tytäryhtiöt täyttävät samat vaatimukset kuin ilmoitetut laitokset.

(51) Ilmoittavan viranomaisen olisi lähetettävä vaatimustenmukaisuuden arviointilaitosta koskeva ilmoitus komissiolle ja muille jäsenvaltioille uuden lähestymistavan mukaisen ilmoitettujen ja nimettyjen organisaatioiden tietojärjestelmän (NANDO) kautta. NANDO on komission kehittämä ja hallinnoima sähköinen ilmoitusväline, joka sisältää luettelon kaikista ilmoitetuista laitoksista.

(52) Koska ilmoitetut laitokset voivat tarjota palvelujaan koko unionin alueella, on tarkoituksenmukaista antaa muille jäsenvaltioille ja komissiolle mahdollisuus esittää vastalauseita ilmoitetun laitoksen osalta. Sen vuoksi on tärkeää säätää ajanjaksosta, jonka aikana voidaan selvittää mahdolliset epäilykset tai huolenaiheet vaatimustenmukaisuuden arviointilaitosten pätevyyden suhteen, ennen kuin ne alkavat toimia ilmoitettuina laitoksina.

(53) Kilpailukyvyn vuoksi on oleellista, että ilmoitetut laitokset soveltavat vaatimustenmukaisuuden arviointimenettelyjä aiheuttamatta kohtuutonta rasitetta talouden toimijoille. Samasta syystä ja talouden toimijoiden yhdenvertaisen kohtelun takaamiseksi olisi varmistettava vaatimustenmukaisuuden arviointimenettelyiden

tekninen johdonmukaisuus. Tämä voitaisiin saavuttaa parhaiten asianmukaisella koordinoinnilla ja yhteistyöllä ilmoitettujen laitosten välillä.

(54) Markkinavalvonta on keskeinen keino unionin lainsäädännön asianmukaisen ja yhdenmukaisen soveltamisen varmistamiseksi. Sen vuoksi on aiheellista luoda oikeudelliset puitteet, joita noudattamalla markkinavalvontaa voidaan toteuttaa tarkoituksenmukaisesti. Tämän asetuksen soveltamisalaan kuuluviin digitaalisia elementtejä sisältäviin tuotteisiin sovelletaan Euroopan parlamentin ja neuvoston asetuksessa (EU) 2019/1020[20] säädettyjä unionin markkinavalvontaa ja unionin markkinoille tuleville tuotteille tehtäviä tarkastuksia koskevia sääntöjä.

(55) Asetuksen (EU) 2019/1020 mukaisesti markkinavalvontaviranomaiset toteuttavat markkinavalvontaa kyseisen jäsenvaltion alueella. Tämä asetus ei saisi estää jäsenvaltioita valitsemasta toimivaltaisia viranomaisia, jotka suorittavat kyseiset tehtävät. Jokaisen jäsenvaltion olisi nimettävä alueelleen yksi tai useampi markkinavalvontaviranomainen. Jäsenvaltiot voivat nimetä minkä tahansa olemassa olevan tai uuden viranomaisen, mukaan lukien [direktiivin XXX/XXXX (NIS2) X artiklassa] tarkoitetut kansalliset toimivaltaiset viranomaiset tai asetuksen (EU) 2019/881 58 artiklassa tarkoitetut nimetyt kansalliset kyberturvasertifiointiviranomaiset, toimimaan markkinavalvontaviranomaisena. Talouden toimijoiden olisi tehtävä täysimääräistä yhteistyötä markkinavalvontaviranomaisten ja muiden toimivaltaisten viranomaisten kanssa. Kunkin jäsenvaltion olisi ilmoitettava komissiolle ja muille jäsenvaltioille markkinavalvontaviranomaisensa ja kunkin viranomaisen toimivaltaan kuuluvat alat sekä varmistettava, että käytössä on tarvittavat resurssit ja tarvittava asiantuntemus tähän asetukseen liittyvien valvontatehtävien suorittamiseksi. Asetuksen (EU) 2019/1020 10 artiklan 2 ja 3 kohdan mukaisesti kunkin jäsenvaltion olisi nimettävä yhteysvirasto, jonka olisi vastattava muun muassa markkinavalvontaviranomaisten koordinoidun kannan edustamisesta ja eri jäsenvaltioiden markkinavalvontaviranomaisten välisen yhteistyön sujuvoittamisesta.

(56) Tämän asetuksen yhdenmukaista soveltamista varten olisi perustettava erityinen hallinnollisen yhteistyön ryhmä asetuksen (EU) 2019/1020 30 artiklan 2 kohdan mukaisesti. Hallinnollisen yhteistyön ryhmän olisi koostuttava nimettyjen markkinavalvontaviranomaisten edustajista ja tarvittaessa yhteysvirastojen edustajista. Komission olisi tuettava ja edistettävä markkinavalvontaviranomaisten välistä yhteistyötä asetuksen (EU) 2019/1020 29 artiklan nojalla perustetussa tuotteiden vaatimustenmukaisuutta käsittelevässä unionin verkostossa, joka koostuu kunkin jäsenvaltion edustajista, mukaan lukien kunkin asetuksen (EU) 2019/1020 10 artiklassa tarkoitetun yhteysviraston edustaja ja valinnainen kansallinen asiantuntija, hallinnollisen yhteistyön ryhmien puheenjohtajat ja komission edustajat. Komission olisi osallistuttava verkoston, sen alaryhmien ja tämän asetuksen mukaisen hallinnollisen yhteistyön ryhmän kokouksiin. Sen olisi myös avustettava tämän asetuksen mukaista hallinnollisen yhteistyön ryhmää sihteeristöllä, joka tarjoaa teknistä ja logistista tukea.

(57) Jotta voidaan varmistaa oikea-aikaiset, oikeasuhteiset ja tulokselliset toimenpiteet sellaisten tuotteiden osalta, joihin liittyy merkittävä kyberturvariski, olisi säädettävä

[20] Euroopan parlamentin ja neuvoston asetus (EU) 2019/1020, annettu 20 päivänä kesäkuuta 2019, markkinavalvonnasta ja tuotteiden vaatimustenmukaisuudesta sekä direktiivin 2004/42/EY ja asetusten (EY) N:o 765/2008 ja (EU) N:o 305/2011 muuttamisesta (EUVL L 169, 25.6.2019, s. 1).

unionin suojamenettelystä, jonka mukaisesti asianomaisille osapuolille ilmoitetaan toimenpiteistä, joita aiotaan toteuttaa tällaisten tuotteiden suhteen. Tämän olisi myös annettava markkinavalvontaviranomaisille mahdollisuus toimia tarvittaessa varhaisemmassa vaiheessa yhteistyössä asianomaisten talouden toimijoiden kanssa. Silloin kun jäsenvaltiot ja komissio ovat yhtä mieltä jäsenvaltion toteuttaman toimenpiteen oikeutuksesta, komissiolta ei pitäisi edellyttää jatkotoimia, paitsi jos vaatimustenvastaisuuden voidaan katsoa johtuvan yhdenmukaistetun standardin puutteista.

(58) Tietyissä tapauksissa tämän asetuksen mukainen digitaalisia elementtejä sisältävä tuote voi kuitenkin aiheuttaa merkittävän kyberturvariskin tai riskin ihmisten terveydelle tai turvallisuudelle, unionin oikeuteen tai kansalliseen oikeuteen pohjautuvien perusoikeuksien suojaamiseen tähtäävien velvoitteiden täyttymiselle, [direktiivin XXX/XXXX (NIS2) liitteessä I] tarkoitettujen keskeisten toimijoiden sähköisen tietojärjestelmän avulla tarjoamien palvelujen saatavuudelle, aitoudelle, eheydelle tai luottamuksellisuudelle tai muille yleisen edun suojeluun liittyville näkökohdille. Sen vuoksi on tarpeen vahvistaa säännöt, joilla torjutaan näitä riskejä. Tämän vuoksi markkinavalvontaviranomaisten olisi toteutettava toimenpiteitä, joilla talouden toimijaa vaaditaan varmistamaan, että tuote ei enää aiheuta kyseistä riskiä, tai järjestämään sitä koskeva palautusmenettely tai poistamaan se markkinoilta, riskistä riippuen. Heti kun markkinavalvontaviranomainen rajoittaa tuotteen vapaata liikkuvuutta tai kieltää sen tällä tavalla, jäsenvaltion on ilmoitettava väliaikaisista toimenpiteistä viipymättä komissiolle ja muille jäsenvaltioille ja esitettävä päätöksen syyt ja perustelut. Jos markkinavalvontaviranomainen toteuttaa tällaisia toimenpiteitä riskin aiheuttavia tuotteita vastaan, komission olisi viipymättä kuultava jäsenvaltioita ja asianomaisia talouden toimijoita ja arvioitava kansallinen toimenpide. Komission tulisi päättää tämän arvioinnin tulosten perusteella, onko kansallinen toimenpide oikeutettu vai ei. Komission olisi osoitettava päätöksensä kaikille jäsenvaltioille ja annettava se välittömästi tiedoksi niille ja asianomaisille talouden toimijoille. Jos toimenpide katsotaan perustelluksi, komissio voi myös harkita ehdotusten esittämistä vastaavan unionilainsäädännön tarkistamiseksi.

(59) Merkittävän kyberturvariskin aiheuttavien digitaalisia elementtejä sisältävien tuotteiden osalta ja kun on syytä epäillä, että ne eivät ole tämän asetuksen mukaisia, tai sellaisten tuotteiden osalta, jotka ovat tämän asetuksen mukaisia, mutta joihin liittyy muita merkittäviä riskejä, kuten riskejä ihmisten terveydelle tai turvallisuudelle, perusoikeuksille tai [direktiivin XXX/XXXX (NIS2) liitteessä I] tarkoitettujen keskeisten toimijoiden tarjoamille palveluille, komissio voi pyytää ENISAa suorittamaan arvioinnin. Tämän arvioinnin perusteella komissio voi hyväksyä täytäntöönpanosäädöksillä korjaavia tai rajoittavia toimenpiteitä unionin tasolla, mukaan lukien asianomaisten tuotteiden markkinoiltaveto tai palautusmenettely kohtuullisen ajan kuluessa ja oikeassa suhteessa riskin luonteeseen. Komissio voi turvautua tällaiseen interventioon ainoastaan poikkeuksellisissa olosuhteissa, jotka oikeuttavat välittömät toimet sisämarkkinoiden moitteettoman toiminnan säilyttämiseksi, ja ainoastaan, jos valvontaviranomaiset eivät ole toteuttaneet tuloksellisia toimenpiteitä tilanteen korjaamiseksi. Tällaiset poikkeukselliset olosuhteet voivat olla hätätilanteita, joissa valmistaja esimerkiksi asettaa vaatimustenvastaisen tuotteen laajalti saataville useissa jäsenvaltioissa, tuotetta käyttävät myös [direktiivin XXX/XXXX (NIS2)] soveltamisalaan kuuluvat toimijat keskeisillä aloilla ja tuote sisältää tunnettuja haavoittuvuuksia, joita pahantahtoiset toimijat hyödyntävät ja joita varten valmistaja ei tarjoa korjaavia päivityksiä. Komissio voi puuttua tällaisiin hätätilanteisiin vain poikkeuksellisten olosuhteiden

keston ajan ja jos tämän asetuksen vastaisuudet tai niihin liittyvät merkittävät riskit jatkuvat.

(60) Tapauksissa, joissa on viitteitä tämän asetuksen vastaisuuksista useissa jäsenvaltioissa, markkinavalvontaviranomaisten olisi voitava toteuttaa yhteistoimia muiden viranomaisten kanssa vaatimusten täyttymisen todentamiseksi ja digitaalisia elementtejä sisältävien tuotteiden kyberturvariskien tunnistamiseksi.

(61) Samanaikaiset koordinoidut valvontatoimet (’tehotarkastukset’) ovat markkinavalvontaviranomaisten erityistoimenpiteitä, joilla voidaan edelleen parantaa tuoteturvallisuutta. Tehotarkastuksia olisi tehtävä erityisesti silloin, kun markkinasuuntaukset, kuluttajavalitukset tai muut merkit viittaavat siihen, että tietyt tuoteluokat aiheuttavat usein vakavan riskin. ENISAn olisi muun muassa tuotteiden haavoittuvuuksista ja poikkeamista saamiensa ilmoitusten perusteella esitettävä markkinavalvontaviranomaisille ehdotuksia tuoteluokista, joiden osalta voitaisiin järjestää tehotarkastuksia.

(62) Jotta sääntelykehystä voitaisiin tarvittaessa mukauttaa, komissiolle olisi siirrettävä valta hyväksyä perussopimuksen 290 artiklan mukaisesti delegoituja säädöksiä, joilla päivitetään liitteen III kriittisten tuotteiden luetteloa ja esitetään näiden tuoteluokkien tarkemmat määritelmät. Komissiolle olisi siirrettävä valta hyväksyä kyseisen artiklan mukaisesti delegoituja säädöksiä niiden digitaalisia elementtejä sisältävien tuotteiden yksilöimiseksi, jotka kuuluvat sellaisten muiden unionin sääntöjen soveltamisalaan, joilla saavutetaan sama suojelun taso kuin tällä asetuksella, ja sen täsmentämiseksi, olisiko joitain tuotteita tarpeen jättää kokonaan tai osittain tämän asetuksen soveltamisalan ulkopuolelle ja jos olisi, miltä osin. Komissiolle olisi myös siirrettävä valta hyväksyä kyseisen artiklan mukaisesti delegoituja säädöksiä, jotka koskevat mahdollisuutta edellyttää tämän asetuksen kriittisyyskriteerien pohjalta tiettyjen digitaalisia elementtejä sisältävien erittäin kriittisten tuotteiden sertifiointia ja joilla täsmennetään EU-vaatimustenmukaisuusvakuutuksen vähimmäissisältöä ja täydennetään teknisiin asiakirjoihin sisällytettäviä tekijöitä. On erityisen tärkeää, että komissio asiaa valmistellessaan toteuttaa asianmukaiset kuulemiset, myös asiantuntijatasolla, ja että nämä kuulemiset toteutetaan paremmasta lainsäädännöstä 13 päivänä huhtikuuta 2016 tehdyssä toimielinten välisessä sopimuksessa[21] vahvistettujen periaatteiden mukaisesti. Jotta voitaisiin erityisesti varmistaa tasavertainen osallistuminen delegoitujen säädösten valmisteluun, Euroopan parlamentille ja neuvostolle toimitetaan kaikki asiakirjat samaan aikaan kuin jäsenvaltioiden asiantuntijoille, ja Euroopan parlamentin ja neuvoston asiantuntijoilla on järjestelmällisesti oikeus osallistua komission asiantuntijaryhmien kokouksiin, joissa valmistellaan delegoituja säädöksiä.

(63) Jotta voidaan varmistaa tämän asetuksen yhdenmukainen täytäntöönpano, komissiolle olisi siirrettävä täytäntöönpanovaltaa täsmentää ohjelmistosisältöluettelon muoto ja osatekijät, täsmentää valmistajien ENISAlle toimittamien, aktiivisesti hyödynnettyjä haavoittuvuuksia ja poikkeamia koskevien ilmoitusten tietotyypit, muoto ja menettelysäännöt, yksilöidä asetuksen (EU) 2019/881 nojalla hyväksytyt eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät, joita voidaan käyttää osoittamaan tämän asetuksen liitteessä I esitettyjen olennaisten vaatimusten tai niiden osien täyttyminen, hyväksyä yhteisiä eritelmiä liitteessä I esitettyjen olennaisten vaatimusten osalta, vahvistaa teknisiä eritelmiä kuvasymboleille tai muille merkeille,

[21] EUVL L 123, 12.5.2016, s. 1.

jotka liittyvät digitaalisia elementtejä sisältävien tuotteiden tietoturvaan, ja luoda mekanismeja niiden käytön edistämiseksi sekä päättää unionin tason korjaavista tai rajoittavista toimenpiteistä poikkeuksellisissa olosuhteissa, jotka oikeuttavat välittömiin toimiin sisämarkkinoiden moitteettoman toiminnan säilyttämiseksi. Tätä valtaa olisi käytettävä Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 182/2011[22] mukaisesti.

(64) Jotta voidaan varmistaa markkinavalvontaviranomaisten luotettava ja rakentava yhteistyö unionin tasolla ja kansallisella tasolla, kaikkien tämän asetuksen soveltamiseen osallistuvien osapuolten olisi kunnioitettava tehtäviään suorittaessaan saamiensa tietojen ja data-aineistojen luottamuksellisuutta.

(65) Tässä asetuksessa säädettyjen velvoitteiden tuloksellisen täytäntöönpanon varmistamiseksi kullakin markkinavalvontaviranomaisella olisi oltava valtuudet määrätä hallinnollisia sakkoja tai pyytää niiden määräämistä. Sen vuoksi olisi vahvistettava tämän asetuksen velvoitteiden laiminlyönnistä johtuvien hallinnollisten sakkojen enimmäismäärät, joista voidaan säätää kansallisessa lainsäädännössä. Päätettäessä hallinnollisen sakon määrästä kussakin yksittäistapauksessa olisi otettava huomioon kaikki kyseiseen tilanteeseen liittyvät merkitykselliset olosuhteet ja vähintään ne, jotka on nimenomaisesti vahvistettu tässä asetuksessa, mukaan lukien se, ovatko muut markkinavalvontaviranomaiset jo määränneet hallinnollisia sakkoja samalle toimijalle samankaltaisista rikkomisista. Tällaiset olosuhteet voivat olla joko raskauttavia, kun saman toimijan rikkomus jatkuu muiden jäsenvaltioiden alueella kuin siinä, jossa on jo asetettu hallinnollinen sakko, tai lieventäviä siten, että toisen markkinavalvontaviranomaisen harkitsemassa mahdollisessa muussa hallinnollisessa sakossa saman talouden toimijan tai samantyyppisen rikkomisen osalta otetaan jo yhdessä muiden merkityksellisten erityisolosuhteiden kanssa huomioon toisessa jäsenvaltioissa määrätty seuraamus ja sen määrä. Kaikissa tällaisissa tapauksissa kumulatiivisen hallinnollisen sakon, joka koostuu useiden jäsenvaltioiden markkinavalvontaviranomaisten sakoista samalle talouden toimijalle samantyyppisestä rikkomisesta, olisi noudatettava suhteellisuusperiaatetta.

(66) Jos hallinnollisia sakkoja määrätään henkilöille, jotka eivät ole yrityksiä, toimivaltaisen viranomaisen olisi sakon sopivan määrän harkinnassa otettava huomioon jäsenvaltion yleinen tulotaso ja henkilön taloudellinen tilanne. Jäsenvaltioilla olisi oltava vastuu määritellä onko viranomaisille määrättävä hallinnollisia sakkoja ja missä määrin.

(67) Suhteissaan kolmansiin maihin EU pyrkii edistämään säänneltyjen tuotteiden kansainvälistä kauppaa. Kaupan helpottamiseen voidaan käyttää monenlaisia keinoja, muun muassa useita oikeudellisia välineitä, kuten kahdenvälisiä (hallitusten välisiä) vastavuoroista tunnustamista koskevia sopimuksia säänneltyjen tuotteiden vaatimustenmukaisuuden arvioimiseksi ja merkitsemiseksi. Sopimuksia vastavuoroisesta tunnustamisesta tehdään unionin ja sellaisten kolmansien maiden välillä, joiden tekninen kehitys on samalla tasolla ja joiden lähestymistapa vaatimustenmukaisuuden arviointiin on yhteensopiva. Tällaiset sopimukset perustuvat sopimuspuolten vaatimustenmukaisuuden arviointilaitosten toisen sopimuspuolen lainsäädännön mukaisesti antamien todistusten, vaatimustenmukaisuusmerkintöjen ja

[22] Euroopan parlamentin ja neuvoston asetus (EU) N:o 182/2011, annettu 16 päivänä helmikuuta 2011, yleisistä säännöistä ja periaatteista, joiden mukaisesti jäsenvaltiot valvovat komission täytäntöönpanovallan käyttöä (EUVL L 55, 28.2.2011, s. 13).

testiraporttien vastavuoroiseen hyväksymiseen. Tällä hetkellä vastavuoroista tunnustamista koskevia sopimuksia on olemassa useiden maiden kanssa. Sopimuksia on tehty useilla erityisaloilla, jotka voivat vaihdella maittain. Kaupan helpottamiseksi edelleen ja koska digitaalisia elementtejä sisältävien tuotteiden toimitusketjut ovat maailmanlaajuisia, tämän asetuksen nojalla säänneltyjen tuotteiden osalta voidaan SEUT-sopimuksen 218 artiklan mukaisesti tehdä vaatimustenmukaisuuden arviointia koskevia sopimuksia vastavuoroisesta tunnustamisesta. Yhteistyö kumppanimaiden kanssa on tärkeää myös kyberkestävyyden vahvistamiseksi maailmanlaajuisesti, sillä pitkällä aikavälillä se edistää kyberturvakehyksen vahvistumista sekä EU:ssa että sen ulkopuolella.

(68) Komission olisi tarkasteltava tätä asetusta säännöllisin väliajoin uudelleen asianomaisia osapuolia kuullen, erityisesti yhteiskunnan, politiikan, tekniikan ja markkinaolojen kehitykseen perustuvien muutostarpeiden selvittämiseksi.

(69) Talouden toimijoille olisi annettava riittävästi aikaa mukautua tämän asetuksen vaatimuksiin. Tätä asetusta olisi sovellettava [24 kuukauden] kuluttua sen voimaantulosta, lukuun ottamatta aktiivisesti hyödynnettyjä haavoittuvuuksia ja poikkeamia koskevia raportointivelvoitteita, joita olisi sovellettava [12 kuukauden] kuluttua tämän asetuksen voimaantulosta.

(70) Jäsenvaltiot eivät voi riittävällä tavalla saavuttaa tämän asetuksen tavoitteita, vaan ne voidaan toiminnan laajuuden ja vaikutusten vuoksi saavuttaa paremmin unionin tasolla, joten unioni voi toteuttaa toimenpiteitä Euroopan unionista tehdyn sopimuksen 5 artiklassa vahvistetun toissijaisuusperiaatteen mukaisesti. Mainitussa artiklassa vahvistetun suhteellisuusperiaatteen mukaisesti tässä asetuksessa ei ylitetä sitä, mikä on tarpeen tämän tavoitteen saavuttamiseksi.

(71) Euroopan tietosuojavaltuutettua on kuultu Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 2018/1725[23] 42 artiklan 1 kohdan mukaisesti, ja hän on antanut lausuntonsa [...],

OVAT HYVÄKSYNEET TÄMÄN ASETUKSEN:

I LUKU

YLEISET SÄÄNNÖKSET

1 artikla

Kohde

Tässä asetuksessa vahvistetaan

a) säännöt digitaalisia elementtejä sisältävien tuotteiden markkinoille saattamiselle niiden kyberturvallisuuden varmistamiseksi,

[23] Euroopan parlamentin ja neuvoston asetus (EU) 2018/1725, annettu 23 päivänä lokakuuta 2018, luonnollisten henkilöiden suojelusta unionin toimielinten, elinten ja laitosten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta sekä asetuksen (EY) N:o 45/2001 ja päätöksen N:o 1247/2002/EY kumoamisesta (EUVL L 295, 21.11.2018, s. 39).

b) digitaalisia elementtejä sisältävien tuotteiden suunnittelua, kehittämistä ja tuotantoa koskevat olennaiset vaatimukset ja näihin tuotteisiin liittyvät talouden toimijoiden kyberturvavelvoitteet,

c) olennaiset vaatimukset haavoittuvuuksien käsittelyprosesseille, joita valmistajat ovat ottaneet käyttöön varmistaakseen digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuuden koko niiden elinkaaren ajan, sekä näihin prosesseihin liittyvät talouden toimijoiden velvoitteet ja

d) markkinavalvontaa ja edellä mainittujen sääntöjen ja vaatimusten noudattamisen valvontaa koskevat säännökset.

2 artikla

Soveltamisala

1. Tätä asetusta sovelletaan kaikkiin digitaalisia elementtejä sisältäviin tuotteisiin, joiden aiottu tai kohtuudella ennakoitavissa oleva käyttö sisältää suoran tai epäsuoran loogisen tai fyysisen datayhteyden johonkin laitteeseen tai verkkoon.

2. Tätä asetusta ei sovelleta digitaalisia elementtejä sisältäviin tuotteisiin, joihin sovelletaan seuraavia unionin säädöksiä:

   a) asetus (EU) 2017/745;

   b) asetus (EU) 2017/746;

   c) asetus (EU) 2019/2144.

3. Tätä asetusta ei sovelleta digitaalisia elementtejä sisältäviin tuotteisiin, jotka on sertifioitu asetuksen (EU) 2018/1139 mukaisesti.

4. Tämän asetuksen soveltamista sellaisiin digitaalisia elementtejä sisältäviin tuotteisiin, joihin sovellettavien muiden unionin sääntöjen vaatimuksilla puututaan kaikkiin tai osaan liitteessä I vahvistettujen olennaistenvaatimusten kattamista riskeistä, voidaan rajoittaa tai se voidaan sulkea pois, jos

   a) tällainen rajoitus tai poissulkeminen on johdonmukainen kyseisiin tuotteisiin sovellettavan yleisen sääntelykehyksen kanssa ja

   b) alakohtaisilla säännöillä saavutetaan sama suojelun taso kuin tällä asetuksella.

   Siirretään komissiolle valta antaa 50 artiklan mukaisesti delegoituja säädöksiä, joilla muutetaan tätä asetusta ja täsmennetään, onko tällainen rajoitus tai poissulkeminen tarpeen, vahvistetaan asianomaiset tuotteet ja säännöt sekä määritellään tarvittaessa rajoituksen soveltamisala.

5. Tätä asetusta ei sovelleta digitaalisia elementtejä sisältäviin tuotteisiin, jotka on kehitetty yksinomaan kansallisiin turvallisuus- tai sotilastarkoituksiin, eikä tuotteisiin, jotka on erityisesti suunniteltu turvallisuusluokiteltujen tietojen käsittelyä varten.

3 artikla

Määritelmät

Tässä asetuksessa tarkoitetaan

1) ’digitaalisia elementtejä sisältävällä tuotteella’ ohjelmisto- tai laitteistotuotetta ja siihen sisältyviä datan etäkäsittelyratkaisuja, mukaan lukien toisistaan erillään markkinoille saatettavat ohjelmisto- tai laitteistokomponentit;

2) ’datan etäkäsittelyllä’ etäältä tapahtuvaa datan käsittelyä, jota varten on suunniteltu ja kehitetty ohjemisto valmistajan toimesta tai valmistajan vastuulla ja jota ilman digitaalisia elementtejä sisältävä tuote ei kykenisi suorittamaan jotakin toimintoaan;

3) ’digitaalisia elementtejä sisältävällä kriittisellä tuotteella’ digitaalisia elementtejä sisältävää tuotetta, joka muodostaa 6 artiklan 2 kohdassa vahvistettujen kriteerien perusteella kyberturvariskin ja jonka ydintoiminto esitetään liitteessä III;

4) ’digitaalisia elementtejä sisältävällä erittäin kriittisellä tuotteella’ digitaalisia elementtejä sisältävää tuotetta, joka muodostaa 6 artiklan 5 kohdassa vahvistettujen kriteerien perusteella kyberturvariskin;

5) ’operatiivisella teknologialla’ ohjelmoitavia digitaalisia järjestelmiä tai laitteita, jotka ovat vuorovaikutuksessa fyysisen ympäristön kanssa tai ohjaavat fyysisen ympäristön kanssa vuorovaikutuksessa olevia laitteita;

6) ’ohjelmistolla’ sitä sähköisen tietojärjestelmän osaa, joka koostuu tietokonekoodista;

7) ’laitteistolla’ fyysistä sähköistä tietojärjestelmää tai sen osia, jotka kykenevät käsittelemään, tallentamaan tai lähettämään digitaalista dataa;

8) ’komponentilla’ ohjelmistoa tai laitteistoa, joka on tarkoitettu integroitavaksi sähköiseen tietojärjestelmään;

9) ’sähköisellä tietojärjestelmällä’ mitä tahansa järjestelmää, mukaan lukien sähköiset tai elektroniset laitteet, joka kykenee käsittelemään, tallentamaan tai lähettämään digitaalista dataa;

10) ’loogisella yhteydellä’ ohjelmistorajapinnan kautta toteutetun dataliitännän virtuaalista representaatiota;

11) ’fyysisellä yhteydellä’ sähköisten tietojärjestelmien tai komponenttien välistä liitäntää, joka toteutetaan fyysisin keinoin, kuten elektronisten tai mekaanisten rajapintojen, johtimien tai radioaaltojen välityksellä;

12) ’epäsuoralla yhteydellä’ laitteeseen tai verkkoon luotua yhteyttä, joka ei toimi suoraan vaan pikemminkin osana laajempaa järjestelmää, joka voidaan liittää suoraan kyseiseen laitteeseen tai verkkoon;

13) ’etuoikeudella’ tietyille käyttäjille tai ohjelmille myönnettyä oikeutta suorittaa tietoturvan kannalta merkityksellisiä toimintoja sähköisessä tietojärjestelmässä;

14) ’korkean tason etuoikeudella’ tietyille käyttäjille tai ohjelmille myönnettyä oikeutta suorittaa sähköisessä tietojärjestelmässä laajasti tietoturvan kannalta merkityksellisiä toimintoja, joiden väärinkäyttö tai vaarantuminen voisi antaa pahantahtoiselle toimijalle laajemman pääsyn järjestelmän tai organisaation resursseihin;

15) ’päätepisteellä’ laitetta, joka on liitetty verkkoon ja joka toimii porttina kyseiseen verkkoon;

16) ’verkko- tai laskentaresurssilla’ data-, laitteisto- tai ohjelmistotoiminnallisuutta, joka on saatavilla joko paikallisesti tai verkon tai muun siihen liitetyn laitteen kautta;

17) ’talouden toimijalla’ valmistajaa, valtuutettua edustajaa, maahantuojaa, jakelijaa tai muuta luonnollista tai oikeushenkilöä, joka kuuluu tässä asetuksessa säädettyjen velvoitteiden piiriin;

18) ’valmistajalla’ luonnollista tai oikeushenkilöä, joka kehittää tai valmistaa digitaalisia elementtejä sisältäviä tuotteita tai suunnitteluttaa, kehityttää tai valmistuttaa digitaalisia elementtejä sisältäviä tuotteita ja markkinoi niitä omalla nimellään tai tuotemerkillään joko maksua vastaan tai maksutta;

19) ’valtuutetulla edustajalla’ unioniin sijoittautunutta luonnollista henkilöä tai oikeushenkilöä, jolla on valmistajan antama kirjallinen toimeksianto hoitaa valmistajan puolesta tietyt tehtävät;

20) ’maahantuojalla’ unioniin sijoittautunutta luonnollista tai oikeushenkilöä, joka saattaa markkinoille digitaalisia elementtejä sisältävän tuotteen, jolla on unionin ulkopuolelle sijoittautuneen luonnollisen tai oikeushenkilön nimi tai tavaramerkki;

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

22) ’markkinoille saattamisella’ digitaalisia elementtejä sisältävän tuotteen asettamista ensimmäistä kertaa saataville unionin markkinoilla;

23) ’asettamisella saataville markkinoilla’ digitaalisia elementtejä sisältävän tuotteen toimittamista unionin markkinoille liiketoiminnan yhteydessä jakelua tai käyttöä varten joko maksua vastaan tai maksutta;

24) ’käyttötarkoituksella’ käyttöä, johon valmistaja on tarkoittanut digitaalisia elementtejä sisältävän tuotteen, mukaan lukien erityinen käyttöyhteys ja erityiset käyttöolosuhteet, siten kuin ne on määritelty tiedoissa, jotka valmistaja on antanut käyttöohjeissa, markkinointi- tai myyntimateriaaleissa ja -ilmoituksissa sekä teknisessä dokumentaatiossa;

25) ’kohtuudella ennakoitavissa olevalla käytöllä’ käyttöä, joka ei välttämättä ole valmistajan käyttöohjeissa, markkinointi- tai myyntimateriaaleissa ja -ilmoituksissa sekä teknisessä dokumentaatiossa ilmoittama käyttötarkoitus, mutta joka voi todennäköisesti seurata kohtuudella ennakoitavissa olevasta ihmisen käyttäytymisestä tai teknisistä toimenpiteistä tai vuorovaikutussuhteista;

26) ’kohtuudella ennakoitavissa olevalla väärinkäytöllä’ digitaalisia elementtejä sisältävän tuotteen käyttöä tavalla, joka ei ole sen käyttötarkoituksen mukainen, mutta joka voi olla seurausta kohtuudella ennakoitavissa olevasta ihmisen käyttäytymisestä tai järjestelmän vuorovaikutuksesta muiden järjestelmien kanssa;

27) ’ilmoittavalla viranomaisella’ kansallista viranomaista, joka vastaa vaatimustenmukaisuuden arviointilaitosten arviointiin, nimeämiseen ja ilmoittamiseen sekä niiden seurantaan tarvittavien menettelyjen perustamisesta ja toteuttamisesta;

28) ’vaatimustenmukaisuuden arvioinnilla’ prosessia, jossa selvitetään, ovatko liitteessä I esitetyt olennaiset vaatimukset täyttyneet;

29) ’vaatimustenmukaisuuden arviointilaitoksella’ asetuksen (EU) N:o 765/2008 2 artiklan 13 alakohdassa määriteltyä laitosta;

30) ’ilmoitetulla laitoksella’ vaatimustenmukaisuuden arviointilaitosta, joka on nimetty tämän asetuksen 33 artiklan ja unionin muun asiaankuuluvan yhdenmukaistamislainsäädännön mukaisesti;

31) ’merkittävällä muutoksella’ digitaalisia elementtejä sisältävään tuotteeseen sen markkinoille saattamisen jälkeen tehtyä muutosta, joka vaikuttaa siihen, täyttääkö

digitaalisia elementtejä sisältävä tuote liitteessä I olevassa 1 jaksossa vahvistetut olennaiset vaatimukset, tai muuttaa käyttötarkoitusta, jota varten digitaalisia elementtejä sisältävä tuote on arvioitu;

32) ’CE-merkinnällä’ merkintää, jolla valmistaja osoittaa, että digitaalisia elementtejä sisältävä tuote ja valmistajan käyttöön ottamat prosessit ovat liitteessä I esitettyjen olennaisten vaatimusten ja muussa sovellettavassa unionin lainsäädännössä, jolla yhdenmukaistetaan tuotteiden kaupan pitämisen ehtoja (’unionin yhdenmukaistamislainsäädäntö’) ja jossa säädetään merkinnän kiinnittämisestä, mukaisia;

33) ’markkinavalvontaviranomaisella’ asetuksen (EU) 2019/1020 3 artiklan 4 alakohdassa määriteltyä viranomaista;

34) ’yhdenmukaistetulla standardilla’ asetuksen (EU) N:o 1025/2012 2 artiklan 1 kohdan c alakohdassa määriteltyä yhdenmukaistettua standardia;

35) ’kyberturvariskillä’ direktiivin [direktiivin XXX/XXXX (NIS2) X artiklassa] määriteltyä riskiä;

36) ’merkittävällä kyberturvariskillä’ kyberturvallisuusriskiä, jonka voidaan teknisten ominaispiirteidensä perusteella suurella todennäköisyydellä olettaa aiheuttavan poikkeaman, jolla voisi olla vakavia kielteisiä vaikutuksia muun muassa aiheuttamalla huomattavia aineellisia tai aineettomia menetyksiä tai häiriöitä;

37) ’ohjelmistosisältöluettelolla’ muodollista selitettä, jossa esitetään digitaalisia elementtejä sisältävän tuotteen ohjelmistoelementteihin sisältyvien komponenttien yksityiskohtaiset tiedot ja toimitusketjusuhteet;

38) ’haavoittuvuudella’ direktiivin [direktiivin XXX/XXXX (NIS2) X artiklassa] määriteltyä haavoittuvuutta;

39) ’aktiivisesti hyödynnetyllä haavoittuvuudella’ haavoittuvuutta, jonka osalta on luotettavaa näyttöä siitä, että jokin toimija on ajanut tietyssä järjestelmässä haitallista koodia ilman järjestelmän omistajan lupaa;

40) ’henkilötiedoilla’ asetuksen (EU) 2016/679 4 artiklan 1 kohdassa määriteltyjä tietoja.

4 artikla

Vapaa liikkuvuus

1. Jäsenvaltiot eivät saa tämän asetuksen soveltamisalaan kuuluvien seikkojen osalta estää tämän asetuksen mukaisten digitaalisia elementtejä sisältävien tuotteiden asettamista saataville markkinoilla.

2. Jäsenvaltiot eivät saa estää digitaalisia elementtejä sisältävien tuotteiden, jotka eivät ole tämän asetuksen mukaisia, esittelyä ja käyttöä messuilla, näyttelyissä ja esittelytilaisuuksissa tai vastaavissa tapahtumissa.

3. Jäsenvaltiot eivät saa estää sellaisten keskeneräisten ohjelmistojen asettamista saataville, jotka eivät ole tämän asetuksen mukaisia, edellyttäen, että ohjelmisto asetetaan saataville vain rajoitetuksi ajaksi, joka on tarpeen testausta varten, ja että näkyvästä merkinnästä käy selvästi ilmi, että ohjelmisto ei ole tämän asetuksen mukainen ja että se ei ole saatavilla markkinoilla muita tarkoituksia kuin testausta varten.

5 artikla

Digitaalisia elementtejä sisältäviä tuotteita koskevat vaatimukset

Digitaalisia elementtejä sisältäviä tuotteita saa asettaa saataville markkinoilla ainoastaan seuraavin edellytyksin:

1) ne täyttävät liitteessä I olevassa 1 jaksossa vahvistetut olennaiset vaatimukset ja niitä käytetään asianmukaisesti asennettuina ja huollettuina käyttötarkoituksensa mukaisesti tai kohtuudella ennakoitavissa olosuhteissa ja tarvittaessa päivitettyinä ja

2) valmistajan käyttämät prosessit täyttävät liitteessä I olevassa 2 jaksossa vahvistetut olennaiset vaatimukset.

6 artikla

Digitaalisia elementtejä sisältävät kriittiset tuotteet

1. Liitteessä III lueteltuun tuoteryhmään kuuluvia, digitaalisia elementtejä sisältäviä tuotteita on pidettävä digitaalisia elementtejä sisältävinä kriittisinä tuotteina. Tuotteiden, joiden ydintoiminto kuuluu tämän asetuksen liitteessä III lueteltuun tuoteryhmään, katsotaan kuuluvan kyseiseen tuoteryhmään. Digitaalisia elementtejä sisältävät kriittiset tuoteryhmät jaetaan liitteen III mukaisesti kyberturvariskin tason perusteella luokkiin I ja II.

2. Siirretään komissiolle valta antaa 50 artiklan mukaisesti delegoituja säädöksiä, joilla muutetaan liitettä III sisällyttämällä digitaalisia elementtejä sisältävien kriittisten tuoteryhmien luetteloon uusi tuoteryhmä tai poistamalla siitä tietty tuoteryhmä. Arvioidessaan tarvetta muuttaa liitteessä III olevaa luetteloa komissio ottaa huomioon digitaalisia elementtejä sisältävien tuoteryhmien kyberturvariskin tason. Kyberturvariskin tasoa määritettäessä on otettava huomioon yksi tai useampi seuraavista kriteereistä:

   a) digitaalisia elementtejä sisältävän tuotteen kyberturvallisuuteen liittyvä toiminnallisuus ja se, onko digitaalisia elementtejä sisältävällä tuotteella vähintään yksi seuraavista ominaisuuksista:

      i) se on suunniteltu toimimaan korkean tason etuoikeuksin tai hallinnoimaan oikeuksia;

      ii) sillä on suora tai etuoikeutettu pääsy verkko- tai laskentaresursseihin;

      iii) se on suunniteltu valvomaan datan tai operatiivisen teknologian käyttöoikeuksia;

      iv) se suorittaa luotettavuuden kannalta kriittisiä toimintoja, erityisesti tietoturvatoimintoja, kuten verkon valvonta, päätepisteen tietoturva ja verkon suojaus;

   b) tuotteen aiottu käyttötarkoitus herkissä ympäristöissä, kuten teollisuusympäristöissä tai direktiivin [direktiivin XXX/XXXX (NIS2)] liitteessä [liitteessä I] tarkoitettujen keskeisten toimijoiden toimesta;

   c) tuotteen aiottu käyttötarkoitus kriittisten tai herkkien toimintojen, kuten henkilötietojen käsittelyn, suorittamisessa;

   d) haitallisen vaikutuksen mahdollinen laajuus, erityisesti sen voimakkuus ja kyky vaikuttaa lukuisiin henkilöihin;

e) se, missä määrin kyseisten digitaalisia elementtejä sisältävien tuotteiden käyttö on jo aiheuttanut aineellisia tai aineettomia menetyksiä tai häiriöitä tai aiheuttanut huomattavaa huolta haitallisen vaikutuksen toteutumisesta.

3. Siirretään komissiolle valta antaa 50 artiklan mukaisesti delegoitu säädös, jolla täydennetään tätä asetusta täsmentämällä liitteessä III esitetyt luokkiin I ja II kuuluvien tuoteryhmien määritelmät. Delegoitu säädös annetaan [12 kuukauden kuluessa tämän asetuksen voimaantulosta].

4. Digitaalisia elementtejä sisältävien kriittisten tuotteiden on läpikäytävä 24 artiklan 2 ja 3 kohdassa tarkoitettu vaatimustenmukaisuuden arviointimenettely.

5. Siirretään komissiolle valta antaa 50 artiklan mukaisesti delegoituja säädöksiä, joilla täydennetään tätä asetusta määrittämällä sellaisten digitaalisia elementtejä sisältävien erittäin kriittisten tuotteiden ryhmät, joiden osalta valmistajien on asetuksen (EU) 2019/881 nojalla hankittava eurooppalainen kyberturvasertifikaatti eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti sen osoittamiseksi, että ne ovat liitteessä I vahvistettujen olennaisten vaatimusten tai niiden osien mukaisia. Määrittäessään tällaisia digitaalisia elementtejä sisältäviä erittäin kriittisiä tuoteryhmiä komissio ottaa huomioon tuoteryhmään liittyvän kyberturvariskin tason yhden tai useamman 2 kohdassa luetellun kriteerin perusteella sekä sen perusteella, päteekö tuoteryhmään jompi kumpi seuraavista:

a) käyttävätkö tai hyödyntävätkö tuoteryhmää direktiivin [direktiivi XXX/XXXX (NIS2)] liitteessä [liite I] tarkoitetun tyyppiset keskeiset toimijat tai onko tuoteryhmällä mahdollisesti tulevaisuudessa merkitystä näiden toimijoiden toiminnan kannalta tai

b) onko tuoteryhmällä merkitystä digitaalisia elementtejä sisältävien tuotteiden koko toimitusketjun häiriönsietokyvyn kannalta.

7 artikla

Yleinen tuoteturvallisuus

Poiketen siitä, mitä säädetään asetuksen [yleisestä tuoteturvallisuudesta annettu asetus] 2 artiklan 1 kohdan kolmannen alakohdan b alakohdassa, jos digitaalisia elementtejä sisältäviin tuotteisiin ei sovelleta unionin muussa yhdenmukaistamislainsäädännössä säädettyjä [yleisestä tuoteturvallisuudesta annetun asetuksen 3 artiklan 25 kohdassa] tarkoitettuja erityisvaatimuksia, kyseisiin tuotteisiin sovelletaan tämän asetuksen soveltamisalaan kuulumattomien turvallisuusriskien osalta asetuksen [yleisestä tuoteturvallisuudesta annettu asetus] III luvun 1 jakson V ja VII lukua ja IX-XI lukua.

8 artikla

Suuririskiset tekoälyjärjestelmät

1. Asetuksen [tekoälyasetus] [6 artiklan] mukaisesti suuririskisiksi tekoälyjärjestelmiksi luokiteltujen digitaalisia elementtejä sisältävien tuotteiden, jotka kuuluvat tämän asetuksen soveltamisalaan ja täyttävät tämän asetuksen liitteessä I olevassa 1 jaksossa vahvistetut olennaiset vaatimukset ja jos valmistajan käyttöön ottamat prosessit täyttävät liitteessä I olevassa 2 jaksossa vahvistetut olennaiset vaatimukset, katsotaan täyttävän asetuksen [tekoälyasetus] [15 artiklassa] vahvistetut kyberturvallisuuteen liittyvät vaatimukset, sanotun kuitenkaan vaikuttamatta edellä mainittuun artiklaan sisältyviin muihin, tarkkuuteen ja luotettavuuteen liittyviin

vaatimuksiin ja siltä osin kuin kyseisillä vaatimuksilla edellytettävä suojan taso osoitetaan tämän asetuksen nojalla annetulla EU-vaatimustenmukaisuusvakuutuksella.

2. Edellä 1 kohdassa tarkoitettuihin tuotteisiin ja kyberturvavaatimuksiin sovelletaan asetuksen [tekoälyasetus] [43 artiklassa] edellytettyä asiaankuuluvaa vaatimustenmukaisuuden arviointimenettelyä. Tätä arviointia varten niillä ilmoitetuilla laitoksilla, joilla on oikeus valvoa suuririskisten tekoälyjärjestelmien vaatimustenmukaisuutta asetuksen [tekoälyasetus] nojalla, on myös oikeus valvoa, että tämän asetuksen soveltamisalaan kuuluvat suuririskiset tekoälyjärjestelmät täyttävät tämän asetuksen liitteessä I vahvistetut vaatimukset, edellyttäen että se, että kyseiset ilmoitetut laitokset täyttävät tämän asetuksen 29 artiklassa säädetyt vaatimukset, on arvioitu asetuksen [tekoälyasetus] mukaisen ilmoitusmenettelyn yhteydessä.

3. Poiketen siitä, mitä 2 kohdassa säädetään, tämän asetuksen liitteessä III lueteltujen digitaalisia elementtejä sisältävien kriittisten tuotteiden, joiden on läpikäytävä tämän asetuksen 24 artiklan 2 kohdan a ja b alakohdassa ja 24 artiklan 3 kohdan a ja b alakohdassa tarkoitetut vaatimustenmukaisuuden arviointimenettelyt ja jotka luokitellaan myös asetuksen [tekoälyasetus] [6 artiklan] mukaisiksi suuririskisiksi tekoälyjärjestelmiksi, joiden on läpikäytävä asetuksen [tekoälyasetus] liitteessä [liite VI] tarkoitettu sisäiseen valvontaan perustuva vaatimustenmukaisuuden arviointimenettely, on läpikäytävä tässä asetuksessa edellytetyt vaatimustenmukaisuuden arviointimenettelyt siltä osin kuin on kyse tämän asetuksen olennaisten vaatimusten täyttymisestä.

9 artikla

Konetuotteet

Asetuksen [koneasetusehdotus] soveltamisalaan kuuluvien konetuotteiden, jotka ovat tässä asetuksessa tarkoitettuja digitaalisia elementtejä sisältäviä tuotteita ja joille on annettu EU-vaatimustenmukaisuusvakuutus tämän asetuksen nojalla, katsotaan olevan asetuksen [koneasetusehdotus] liitteessä [liitteessä III olevassa 1.1.9 ja 1.2.1 kohdassa] vahvistettujen olennaisten terveys- ja turvallisuusvaatimusten mukaisia korruptoitumiselta suojautumisen sekä ohjausjärjestelmien turvallisuuden ja luotettavuuden osalta siltä osin kuin kyseisillä vaatimuksilla edellytettävä suojan taso osoitetaan tämän asetuksen nojalla annetulla EU-vaatimustenmukaisuusvakuutuksella.

II LUKU

TALOUDEN TOIMIJOIDEN VELVOLLISUUDET

10 artikla

Valmistajien velvollisuudet

1. Saattaessaan digitaalisia elementtejä sisältävää tuotetta markkinoille valmistajien on varmistettava, että se on suunniteltu, kehitetty ja tuotettu liitteessä I olevassa 1 jaksossa vahvistettujen olennaisten vaatimusten mukaisesti.

2. Edellä 1 kohdassa säädetyn velvoitteen noudattamiseksi valmistajien on arvioitava digitaalisia elementtejä sisältävän tuotteen kyberturvariskit ja otettava arvioinnin

tulokset huomioon digitaalisia elementtejä sisältävän tuotteen suunnittelu-, kehitys-, tuotanto-, toimitus- ja ylläpitovaiheissa kyberturvariskien minimoimiseksi, tietoturvapoikkeamien ehkäisemiseksi ja tällaisten poikkeamien vaikutusten minimoimiseksi, myös käyttäjien terveyden ja turvallisuuden osalta.

3. Saattaessaan markkinoille digitaalisia elementtejä sisältävää tuotetta valmistajan on sisällytettävä teknisiin asiakirjoihin 23 artiklan ja liitteen V mukaisesti arvio kyberturvariskeistä. Tämän asetuksen 8 artiklassa ja 24 artiklan 4 kohdassa tarkoitettujen digitaalisia elementtejä sisältävien tuotteiden, joihin sovelletaan myös muita unionin säädöksiä, osalta kyberturvariskien arviointi voi olla osa kyseisissä unionin muissa säädöksissä edellytettyä riskinarviointia. Jos tietyt olennaiset vaatimukset eivät sovellu tiettyyn digitaalisia elementtejä sisältävään markkinoituun tuotteeseen, valmistajan on perusteltava tämä selkeästi kyseisissä asiakirjoissa.

4. Edellä 1 kohdassa säädetyn velvoitteen täyttämiseksi valmistajien on noudatettava asianmukaista huolellisuutta, kun ne integroivat digitaalisia elementtejä sisältäviin tuotteisiin kolmansilta osapuolilta hankittuja komponentteja. Niiden on varmistettava, että tällaiset komponentit eivät vaaranna digitaalisia elementtejä sisältävän tuotteen tietoturvaa.

5. Valmistajan on oikeassa suhteessa kyberturvariskin suuruuteen ja luonteeseen nähden järjestelmällisesti dokumentoitava digitaalisia elementtejä sisältävän tuotteen asiaankuuluvat kyberturvallisuusnäkökohdat, mukaan lukien tietoonsa tulleet haavoittuvuudet ja kaikki kolmansien osapuolten toimittamat merkitykselliset tiedot, ja tarvittaessa päivitettävä tuotteen riskinarviointi.

6. Saattaessaan markkinoille digitaalisia elementtejä sisältävää tuotetta ja tuotteen odotetun käyttöiän ajan tai viiden vuoden ajan tuotteen markkinoille saattamisesta sen mukaan, kumpi näistä on lyhyempi ajanjakso, valmistajien on varmistettava, että kyseisen tuotteen haavoittuvuudet käsitellään tehokkaasti ja liitteessä I olevassa 2 jaksossa vahvistettujen olennaisten vaatimusten mukaisesti.

   Valmistajilla on oltava asianmukaiset toimintatavat ja menettelyt, mukaan lukien liitteessä I olevan 2 jakson 5 kohdassa tarkoitetut koordinoidut haavoittuvuuksien ilmoittamisperiaatteet ja -menettelyt, joilla käsitellään ja korjataan sisäisten tai ulkoisten lähteiden raportoimat digitaalisia elementtejä sisältävän tuotteen mahdolliset haavoittuvuudet.

7. Ennen digitaalisia elementtejä sisältävän tuotteen saattamista markkinoille valmistajien on laadittava 23 artiklassa tarkoitetut tekniset asiakirjat.

   Niiden on suoritettava tai teetettävä valitsemansa 24 artiklassa tarkoitetut vaatimustenmukaisuuden arviointimenettelyt.

   Jos kyseisellä vaatimustenmukaisuuden arviointimenettelyllä on osoitettu, että tuote täyttää liitteessä I olevassa 1 jaksossa vahvistetut olennaiset vaatimukset ja että valmistajan prosessit täyttävät liitteessä I olevassa 2 jaksossa vahvistetut olennaiset vaatimukset, valmistajan on laadittava EU-vaatimustenmukaisuusvakuutus 20 artiklan mukaisesti ja kiinnitettävä CE-merkintä 22 artiklan mukaisesti.

8. Valmistajien on pidettävä tekniset asiakirjat ja tarvittaessa EU-vaatimustenmukaisuusvakuutus markkinavalvontaviranomaisten saatavilla kymmenen vuoden ajan sen jälkeen, kun digitaalisia elementtejä sisältävä tuote on saatettu markkinoille.

9. Valmistajien on huolehdittava siitä, että käytössä on menettelyt, joiden avulla sarjatuotantoon kuuluvat digitaalisia elementtejä sisältävät tuotteet edelleenkin täyttävät vaatimukset. Valmistajan on otettava asianmukaisesti huomioon muutokset kehitys- ja tuotantoprosessissa tai digitaalisia elementtejä sisältävän tuotteen rakenteessa tai ominaisuuksissa sekä muutokset yhdenmukaistetuissa standardeissa, eurooppalaisissa kyberturvallisuuden sertifiointijärjestelmissä tai 19 artiklassa tarkoitetuissa yhteisissä eritelmissä, joihin viitaten digitaalisia elementtejä sisältävän tuotteen vaatimustenmukaisuus ilmoitetaan tai joiden perusteella tuotteen vaatimustenmukaisuus todennetaan.

10. Valmistajien on varmistettava, että digitaalisia elementtejä sisältävien tuotteiden mukana on sähköisessä tai fyysisessä muodossa liitteessä II esitetyt tiedot ja ohjeet. Näiden tietojen ja ohjeiden on oltava kielellä, jota käyttäjät helposti ymmärtävät. Niiden on oltava selkeitä, ymmärrettäviä, sisäistettäviä ja luettavia. Niiden on mahdollistettava digitaalisia elementtejä sisältävien tuotteiden tietoturvallinen asentaminen, ylläpito ja käyttö.

11. Valmistajien on joko toimitettava EU-vaatimustenmukaisuusvakuutus digitaalisia elementtejä sisältävän tuotteen mukana tai sisällytettävä liitteessä II tarkoitettuihin käyttöohjeisiin ja tietoihin verkko-osoite, jossa EU-vaatimustenmukaisuusvakuutus on saatavilla.

12. Digitaalisia elementtejä sisältävän tuotteen markkinoille saattamisesta alkaen ja tuotteen odotetun käyttöiän ajan tai viiden vuoden ajan markkinoille saattamisesta sen mukaan, kumpi näistä on lyhyempi ajanjakso, valmistajien, jotka tietävät tai joilla on syytä uskoa, että digitaalisia elementtejä sisältävä tuote tai niiden käyttämät prosessit eivät täytä liitteessä I vahvistettuja olennaisia vaatimuksia, on välittömästi toteutettava tarvittavat korjaavat toimenpiteet digitaalisia elementtejä sisältävien tuotteiden tai prosessiensa saattamiseksi vaatimusten mukaisiksi tai tapauksen mukaan tuotteen poistamiseksi markkinoilta tai sitä koskevan palautusmenettelyn järjestämiseksi.

13. Valmistajien on markkinavalvontaviranomaisen perustellusta pyynnöstä annettava kyseiselle viranomaiselle sen helposti ymmärtämällä kielellä kaikki paperilla tai sähköisessä muodossa olevat tiedot ja asiakirjat, jotka ovat tarpeen sen osoittamiseksi, että digitaalisia elementtejä sisältävä tuote ja valmistajan prosessit täyttävät liitteessä I vahvistetut olennaiset vaatimukset. Valmistajien on tehtävä kyseisen viranomaisen kanssa tämän pyynnöstä yhteistyötä kaikissa toimenpiteissä, joita toteutetaan niiden markkinoille saattamien digitaalisia elementtejä sisältävien tuotteiden aiheuttamien kyberturvariskien poistamiseksi.

14. Valmistajan, joka lopettaa toimintansa eikä sen vuoksi pysty noudattamaan tässä asetuksessa säädettyjä velvoitteitaan, on ennen toiminnan loppumista ilmoitettava tilanteesta asianomaisille markkinavalvontaviranomaisille sekä kaikin käytettävissä olevin keinoin ja mahdollisuuksien mukaan markkinoille saatettujen digitaalisia elementtejä sisältävien tuotteiden käyttäjille.

15. Komissio voi täytäntöönpanosäädöksillä täsmentää liitteessä I olevan 2 jakson 1 kohdassa tarkoitetun ohjelmistosisältöluettelon muodon ja osatekijät. Nämä täytäntöönpanosäädökset hyväksytään 51 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

11 artikla

Valmistajien raportointivelvoitteet

1. Valmistajan on ilman aiheetonta viivytystä ja joka tapauksessa 24 tunnin kuluessa siitä, kun se on tullut asiasta tietoiseksi, ilmoitettava ENISAlle kaikista digitaalisia elementtejä sisältävän tuotteen sisältämistä aktiivisesti hyödynnetyistä haavoittuvuuksista. Ilmoituksessa on oltava yksityiskohtaiset tiedot kyseisestä haavoittuvuudesta ja korjaavista tai lieventävistä toimenpiteistä, jos sellaisiin on ryhdytty. ENISAn on ilman aiheetonta viivytystä, paitsi kyberturvariskeihin liittyvistä perustelluista syistä, välitettävä ilmoitus asianomaisten jäsenvaltioiden koordinoidusta haavoittuvuuksien ilmoittamisesta [direktiivin XXX/XXXX (NIS2) X artiklan] mukaisesti vastaavalle CSIRT-yksikölle ja tiedotettava ilmoitetusta haavoittuvuudesta markkinavalvontaviranomaiselle.

2. Valmistajan on ilman aiheetonta viivytystä ja joka tapauksessa 24 tunnin kuluessa siitä, kun se on tullut asiasta tietoiseksi, ilmoitettava ENISAlle kaikista digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavista poikkeamista. ENISAn on ilman aiheetonta viivytystä, paitsi kyberturvariskeihin liittyvistä perustelluista syistä, välitettävä ilmoitukset asianomaisten jäsenvaltioiden [direktiivin XXX/XXXX (NIS2) X artiklan] mukaisesti nimetyille keskitetyille yhteysvirastoille ja tiedotettava ilmoitetuista poikkeamista markkinavalvontaviranomaiselle. Poikkeamailmoituksessa on oltava tiedot poikkeaman vakavuudesta ja vaikutuksista ja tarvittaessa tieto siitä, epäileekö valmistaja poikkeaman johtuvan laittomista tai haitan aiheuttamiseen tähtäävistä pyrkimyksistä tai katsooko se sillä olevan rajat ylittäviä vaikutuksia.

3. ENISAn on toimitettava 1 ja 2 kohdan mukaiset tiedot [direktiivin XXX/XXXX (NIS2) X artiklalla] perustetulle Euroopan kyberkriisiyhteysorganisaatioiden verkostolle (EU-CyCLONe), jos tiedot ovat operatiivisella tasolla tarpeen laajamittaisten kyberturvapoikkeamien ja -kriisien koordinoidun hallinnan kannalta.

4. Valmistajan on ilman aiheetonta viivytystä ja tultuaan asiasta tietoiseksi tiedotettava digitaalisia elementtejä sisältävän tuotteen käyttäjille poikkeamasta ja mahdollisista korjaavista toimenpiteistä, joita käyttäjä voi tehdä poikkeaman vaikutusten lieventämiseksi.

5. Komissio voi täytäntöönpanosäädöksin täsmentää 1 ja 2 kohdan nojalla toimitettavien ilmoitusten tietosisältöä, muotoa ja toimitustapaa. Tällaiset täytäntöönpanosäädökset hyväksytään 51 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

6. ENISAn on 1 ja 2 kohdan nojalla saamiensa ilmoitusten perusteella laadittava joka toinen vuosi tekninen raportti digitaalisia elementtejä sisältävien tuotteiden kyberturvariskien uusista suuntauksista ja toimitettava se direktiivissä [direktiivi XXX/XXXX (NIS2)] tarkoitetulle yhteistyöryhmälle. Ensimmäinen tällainen raportti on toimitettava 24 kuukauden kuluessa siitä, kun 1 ja 2 kohdassa säädettyjä velvoitteita on alettu soveltaa.

7. Valmistajan on digitaalisia elementtejä sisältävään tuotteeseen integroidun komponentin, myös avoimen lähdekoodin komponentin, haavoittuvuuden todettuaan raportoitava haavoittuvuudesta komponenttia ylläpitävälle henkilölle tai taholle.

12 artikla

Valtuutetut edustajat

1. Valmistaja voi nimittää valtuutetun edustajan kirjallisella toimeksiannolla.

2. Edellä 10 artiklan 1–6 kohdassa, 7 kohdan ensimmäisessä alakohdassa ja 9 kohdassa säädetyt velvollisuudet eivät saa kuulua osana valtuutetun edustajan toimeksiantoon.

3. Valtuutetun edustajan on suoritettava valmistajalta saadussa toimeksiannossa eritellyt tehtävät. Toimeksiannon perusteella valtuutetun edustajan on voitava suorittaa ainakin seuraavat tehtävät:

   a) edustajan on pidettävä 20 artiklassa tarkoitettu EU-vaatimustenmukaisuusvakuutus ja 23 artiklassa tarkoitetut tekniset asiakirjat markkinavalvontaviranomaisten saatavilla kymmenen vuoden ajan sen jälkeen, kun digitaalisia elementtejä sisältävä tuote on saatettu markkinoille;

   b) edustajan on annettava markkinaviranomaisen perustellusta pyynnöstä kyseiselle viranomaiselle kaikki tiedot ja asiakirjat, jotka ovat tarpeen digitaalisia elementtejä sisältävän tuotteen vaatimustenmukaisuuden osoittamiseksi;

   c) edustajan on tehtävä markkinavalvontaviranomaisten kanssa näiden pyynnöstä yhteistyötä toimissa, joilla pyritään poistamaan valtuutetun edustajan toimeksiannon piiriin kuuluvien digitaalisia elementtejä sisältävien tuotteiden aiheuttamat riskit.

13 artikla

Maahantuojien velvollisuudet

1. Maahantuojat saavat saattaa markkinoille ainoastaan digitaalisia elementtejä sisältäviä tuotteita, jotka täyttävät liitteessä I olevassa 1 jaksossa vahvistetut olennaiset vaatimukset ja joiden osalta valmistajan prosessit täyttävät liitteessä I olevassa 2 jaksossa vahvistetut olennaiset vaatimukset.

2. Ennen digitaalisia elementtejä sisältävän tuotteen saattamista markkinoille maahantuojien on varmistettava, että

   a) valmistaja on suorittanut 24 artiklassa tarkoitetut asianmukaiset vaatimustenmukaisuuden arviointimenettelyt;

   b) valmistaja on laatinut tekniset asiakirjat;

   c) digitaalisia elementtejä sisältävässä tuotteessa on 22 artiklassa tarkoitettu CE-merkintä, ja sen mukana on liitteessä II esitetyt tiedot ja käyttöohjeet.

3. Jos maahantuoja katsoo tai sillä on syytä uskoa, että digitaalisia elementtejä sisältävät tuotteet tai valmistajan prosessit eivät täytä liitteessä I vahvistettuja olennaisia vaatimuksia, maahantuoja ei saa saattaa tuotetta markkinoille ennen kuin kyseiset tuotteet tai valmistajan prosessit on saatettu liitteessä I vahvistettujen olennaisten vaatimusten mukaisiksi. Lisäksi jos digitaalisia elementtejä sisältävä tuote aiheuttaa merkittävän kyberturvariskin, maahantuojan on ilmoitettava asiasta valmistajalle ja markkinavalvontaviranomaisille.

4. Maahantuojien on ilmoitettava nimensä, rekisteröity tuotenimensä tai rekisteröity tavaramerkkinsä, postiosoitteensa sekä sähköpostiosoitteensa, joista heihin saa yhteyden, joko digitaalisia elementtejä sisältävässä tuotteessa tai, mikäli se ei ole

mahdollista, digitaalisia elementtejä sisältävän tuotteen pakkauksessa tai sen mukana seuraavassa asiakirjassa. Yhteystiedot on annettava käyttäjien ja markkinavalvontaviranomaisten helposti ymmärtämällä kielellä.

5. Maahantuojien on varmistettava, että digitaalisia elementtejä sisältävään tuotteeseen liitetään liitteessä II esitetyt ohjeet ja tiedot käyttäjien helposti ymmärtämällä kielellä.

6. Maahantuojien, jotka tietävät tai joilla on syytä uskoa, että digitaalisia elementtejä sisältävä tuote, jonka ne ovat saattaneet markkinoille, tai sen valmistajan prosessit eivät täytä liitteessä I vahvistettuja olennaisia vaatimuksia, on välittömästi toteutettava tarvittavat korjaavat toimenpiteet kyseisen digitaalisia elementtejä sisältävän tuotteen tai sen valmistajan prosessien saattamiseksi liitteessä I vahvistettujen olennaisten vaatimusten mukaisiksi tai tarvittaessa tuotteen poistamiseksi markkinoilta tai sitä koskevan palautusmenettelyn järjestämiseksi.

   Kun maahantuojat havaitsevat digitaalisia elementtejä sisältävässä tuotteessa haavoittuvuuden, niiden on ilman aiheetonta viivytystä ilmoitettava siitä valmistajalle. Jos digitaalisia elementtejä sisältävä tuote aiheuttaa merkittävän kyberturvariskin, maahantuojien on lisäksi välittömästi tiedotettava asiasta niiden jäsenvaltioiden markkinavalvontaviranomaisille, joissa ne ovat asettaneet digitaalisia elementtejä sisältävän tuotteen saataville markkinoilla, ja ilmoitettava yksityiskohtaiset tiedot erityisesti vaatimustenvastaisuudesta ja mahdollisesti toteutetuista korjaavista toimenpiteistä.

7. Maahantuojien on 10 vuoden ajan sen jälkeen, kun digitaalisia elementtejä sisältävä tuote on saatettu markkinoille, pidettävä EU-vaatimustenmukaisuusvakuutuksen jäljennös markkinavalvontaviranomaisten saatavilla ja varmistettava, että tekniset asiakirjat voidaan antaa pyynnöstä kyseisten viranomaisten saataville.

8. Maahantuojien on markkinavalvontaviranomaisen perustellusta pyynnöstä annettava kyseiselle viranomaiselle sen helposti ymmärtämällä kielellä paperiversiona tai sähköisessä muodossa kaikki tiedot ja asiakirjat, jotka ovat tarpeen sen osoittamiseksi, että digitaalisia elementtejä sisältävä tuote täyttää liitteessä I olevassa 1 kohdassa vahvistetut olennaiset vaatimukset ja valmistajan prosessit täyttävät liitteessä I olevassa 2 kohdassa vahvistetut olennaiset vaatimukset. Niiden on tehtävä kyseisen viranomaisen kanssa tämän pyynnöstä yhteistyötä toimissa, joilla pyritään poistamaan niiden markkinoille saattamien digitaalisia elementtejä sisältävien tuotteiden aiheuttamat kyberturvallisuusriskit.

9. Kun digitaalisia elementtejä sisältävän tuotteen maahantuoja tulee tietoiseksi siitä, että tuotteen valmistaja on lopettanut toimintansa eikä sen vuoksi pysty noudattamaan tässä asetuksessa säädettyjä velvoitteitaan, maahantuojan on ilmoitettava tilanteesta asianomaisille markkinavalvontaviranomaisille sekä kaikin käytettävissä olevin keinoin ja mahdollisuuksien mukaan markkinoille saatettujen digitaalisia elementtejä sisältävien tuotteiden käyttäjille.

14 artikla

Jakelijoiden velvollisuudet

1. Kun jakelijat asettavat digitaalisia elementtejä sisältävän tuotteen saataville markkinoilla, niiden on toimittava noudattaen asiaankuuluvaa huolellisuutta tämän asetuksen vaatimusten suhteen.

2. Ennen digitaalisia elementtejä sisältävän tuotteen asettamista saataville markkinoilla jakelijoiden on tarkastettava, että

   a) digitaalisia elementtejä sisältävässä tuotteessa on CE-merkintä;

   b) valmistaja ja maahantuoja ovat täyttäneet 10 artiklan 10 ja 11 kohdassa ja 13 artiklan 4 kohdassa säädetyt velvollisuutensa.

3. Jos jakelija katsoo tai sillä on syytä uskoa, että digitaalisia elementtejä sisältävät tuotteet tai valmistajan prosessit eivät täytä liitteessä I vahvistettuja olennaisia vaatimuksia, jakelija ei saa asettaa digitaalisia elementtejä sisältävää tuotetta saataville markkinoilla ennen kuin kyseiset tuotteet tai valmistajan prosessit on saatettu vaatimusten mukaisiksi. Lisäksi jos digitaalisia elementtejä sisältävä tuote aiheuttaa merkittävän kyberturvariskin, jakelijan on ilmoitettava siitä valmistajalle ja markkinavalvontaviranomaisille.

4. Jakelijoiden, jotka tietävät tai joilla on syytä uskoa, että digitaalisia elementtejä sisältävä tuote, jonka ne ovat saattaneet markkinoille, tai sen valmistajan prosessit eivät täytä liitteessä I vahvistettuja olennaisia vaatimuksia, on varmistettava, että toteutetaan tarvittavat korjaavat toimenpiteet kyseisen digitaalisia elementtejä sisältävän tuotteen tai sen valmistajan prosessien saattamiseksi vaatimusten mukaisiksi tai tarvittaessa tuotteen poistamiseksi markkinoilta tai sitä koskevan palautusmenettelyn järjestämiseksi.

   Kun jakelijat havaitsevat digitaalisia elementtejä sisältävässä tuotteessa haavoittuvuuden, niiden on ilman aiheetonta viivytystä ilmoitettava siitä valmistajalle. Jos digitaalisia elementtejä sisältävä tuote aiheuttaa merkittävän kyberturvariskin, jakelijoiden on lisäksi välittömästi tiedotettava asiasta niiden jäsenvaltioiden markkinavalvontaviranomaisille, joissa ne ovat asettaneet digitaalisia elementtejä sisältävän tuotteen saataville markkinoilla, ja ilmoitettava yksityiskohtaiset tiedot erityisesti vaatimustenvastaisuudesta ja mahdollisesti toteutetuista korjaavista toimenpiteistä.

5. Jakelijoiden on markkinavalvontaviranomaisen perustellusta pyynnöstä annettava kyseiselle viranomaiselle sen helposti ymmärtämällä kielellä paperiversiona tai sähköisessä muodossa kaikki tiedot ja asiakirjat, jotka ovat tarpeen sen osoittamiseksi, että digitaalisia elementtejä sisältävät tuotteet ja valmistajan prosessit täyttävät liitteessä I vahvistetut olennaiset vaatimukset. Niiden on tehtävä kyseisen viranomaisen kanssa tämän pyynnöstä yhteistyötä toimissa, joilla pyritään poistamaan niiden markkinoille saattamien digitaalisia elementtejä sisältävien tuotteiden aiheuttamat kyberturvariskit.

6. Kun digitaalisia elementtejä sisältävän tuotteen jakelija tulee tietoiseksi siitä, että tuotteen valmistaja on lopettanut toimintansa eikä sen vuoksi pysty noudattamaan tässä asetuksessa säädettyjä velvoitteitaan, jakelijan on ilmoitettava tilanteesta asianomaisille markkinavalvontaviranomaisille sekä kaikin käytettävissä olevin keinoin ja mahdollisuuksien mukaan markkinoille saatettujen digitaalisia elementtejä sisältävien tuotteiden käyttäjille.

15 artikla

Tapaukset, joissa valmistajien velvoitteita sovelletaan maahantuojiin ja jakelijoihin

Maahantuojaa tai jakelijaa on pidettävä tämän asetuksen mukaisesti valmistajana ja sitä koskevat 10 artiklassa ja 11 artiklan 1, 2, 4 ja 7 kohdassa säädetyt valmistajan velvollisuudet

silloin, kun kyseinen maahantuoja tai jakelija saattaa digitaalisia elementtejä sisältävän tuotteen markkinoille omalla nimellään tai tavaramerkillään tai tekee merkittävän muutoksen jo markkinoille saatettuun digitaalisia elementtejä sisältävään tuotteeseen.

16 artikla

Muut tapaukset, joissa sovelletaan valmistajien velvollisuuksia

Muuta luonnollista tai oikeushenkilöä kuin valmistajaa, maahantuojaa tai jakelijaa, joka tekee digitaalisia elementtejä sisältävään tuotteeseen merkittävän muutoksen, pidetään tätä asetusta sovellettaessa valmistajana.

Kyseiseen henkilöön sovelletaan 10 artiklassa ja 11 artiklan 1, 2, 4 ja 7 kohdassa säädettyjä valmistajan velvoitteita tuotteen sen osan osalta, johon merkittävä muutos vaikuttaa, tai jos merkittävä muutos vaikuttaa digitaalisia elementtejä sisältävän tuotteen kyberturvallisuuteen kokonaisuudessaan, koko tuotteen osalta.

17 artikla

Talouden toimijoiden yksilöiminen

1. Talouden toimijoiden on pyynnöstä ja jos tiedot ovat saatavilla, toimitettava markkinavalvontaviranomaisille seuraavat tiedot:

   a) sen talouden toimijan nimi ja osoite, joka on toimittanut digitaalisia elementtejä sisältävän tuotteen;

   b) sen talouden toimijan nimi ja osoite, jolle digitaalisia elementtejä sisältävä tuote on toimitettu.

2. Talouden toimijoiden on voitava esittää 1 kohdassa tarkoitetut tiedot kymmenen vuoden ajan sen jälkeen, kun digitaalisia elementtejä sisältävä tuote on toimitettu niille, ja kymmenen vuoden ajan sen jälkeen, kun ne ovat toimittaneet digitaalisia elementtejä sisältävän tuotteen.

III LUKU

DIGITAALISIA ELEMENTTEJÄ SISÄLTÄVÄN TUOTTEEN VAATIMUSTENMUKAISUUS

18 artikla

Vaatimustenmukaisuusolettama

1. Digitaalisia elementtejä sisältävien tuotteiden ja valmistajan prosessien, jotka ovat yhdenmukaistettujen standardien tai niiden osien, joiden viitetiedot on julkaistu *Euroopan unionin virallisessa lehdessä*, mukaisia, katsotaan olevan kyseisten standardien tai niiden osien kattamien, liitteessä I säädettyjen olennaisten vaatimusten mukaisia.

2. Digitaalisia elementtejä sisältävien tuotteiden ja valmistajan prosessien, jotka ovat 19 artiklassa tarkoitettujen yhteisten eritelmien mukaisia, katsotaan olevan liitteessä I vahvistettujen olennaisten vaatimusten mukaisia siltä osin kuin kyseiset yhteiset eritelmät kattavat kyseiset vaatimukset.

3. Digitaalisia elementtejä sisältävien tuotteiden ja valmistajan prosessien, joille on annettu EU-vaatimustenmukaisuusvakuutus tai asetuksen (EU) 2019/881 mukaisesti hyväksytyn ja 4 kohdan mukaisesti yksilöidyn eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukainen sertifikaatti, katsotaan olevan liitteessä I vahvistettujen keskeisten vaatimusten mukaisia, jos EU-vaatimustenmukaisuusvakuutus tai kyberturvasertifikaatti tai niiden osat kattavat kyseiset vaatimukset.

4. Siirretään komissiolle valta yksilöidä täytäntöönpanosäädöksillä ne asetuksen (EU) 2019/881 nojalla hyväksytyt eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät, joita voidaan käyttää osoittamaan liitteessä I vahvistettujen olennaisten vaatimusten tai niiden osien täyttyminen. Lisäksi komissio täsmentää tarvittaessa, poistaako tällaisten järjestelmien mukaisesti myönnetty kyberturvasertifikaatti valmistajan velvoitteen teettää 24 artiklan 2 kohdan a ja b alakohdassa sekä 3 kohdan a ja b alakohdassa säädettyjen vaatimusten osalta vaatimustenmukaisuuden arviointi kolmannella osapuolella. Tällaiset täytäntöönpanosäädökset hyväksytään 51 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

19 artikla

Yhteiset eritelmät

Jos 18 artiklassa tarkoitettuja yhdenmukaistettuja standardeja ei ole tai jos komissio katsoo, että ne eivät riitä täyttämään tämän asetuksen vaatimuksia tai komission standardointipyyntöä, tai jos standardointimenettely viivästyy kohtuuttomasti tai eurooppalaiset standardointiorganisaatiot eivät ole hyväksyneet komission esittämää yhdenmukaistettuja standardeja koskevaa pyyntöä, komissiolle siirretään valta hyväksyä täytäntöönpanosäädöksillä yhteisiä eritelmiä liitteessä I vahvistettujen olennaisten vaatimusten osalta. Nämä täytäntöönpanosäädökset hyväksytään 51 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

20 artikla

EU-vaatimustenmukaisuusvakuutus

1. Valmistajien on laadittava EU-vaatimustenmukaisuusvakuutus 10 artiklan 7 kohdan mukaisesti, ja siinä on mainittava, että liitteessä I vahvistettujen sovellettavien olennaisten vaatimusten täyttyminen on osoitettu.

2. EU-vaatimustenmukaisuusvakuutuksen on oltava rakenteeltaan liitteessä IV vahvistetun mallin mukainen, ja sen on sisällettävä liitteessä VI vahvistetuissa asiaankuuluvissa vaatimustenmukaisuuden arviointimenettelyissä eritellyt tekijät. Tällaista vakuutusta on jatkuvasti päivitettävä. Se on asetettava saataville sen jäsenvaltion vaatimalla yhdellä tai useammalla kielellä, jossa digitaalisia elementtejä sisältävä tuote saatetaan markkinoille tai asetetaan saataville.

3. Jos digitaalisia elementtejä sisältävään tuotteeseen sovelletaan useampia unionin säädöksiä, joissa edellytetään EU-vaatimustenmukaisuusvakuutusta, kaikkien kyseisten unionin säädösten osalta laaditaan yksi ainoa EU-vaatimustenmukaisuusvakuutus. Tällaisessa vakuutuksessa on mainittava kyseisten unionin säädösten tunnistetiedot, niiden julkaisuviitteet mukaan luettuina.

4. Laatimalla EU-vaatimustenmukaisuusvakuutuksen valmistaja ottaa vastuun tuotteen vaatimustenmukaisuudesta.

5. Siirretään komissiolle valta antaa delegoituja säädöksiä 50 artiklan mukaisesti tämän asetuksen täydentämiseksi lisäämällä teknologian kehittymisen perusteella elementtejä liitteessä IV vahvistetun EU-vaatimustenmukaisuusvakuutuksen vähimmäissisältöön.

21 artikla

CE-merkintää koskevat yleiset periaatteet

Tämän asetuksen 3 artiklan 32 alakohdassa määriteltyä CE-merkintää koskevat asetuksen (EY) N:o 765/2008 30 artiklassa säädetyt yleiset periaatteet.

22 artikla

CE-merkinnän kiinnittämistä koskevat säännöt ja ehdot

1. CE-merkintä on liitettävä digitaalisia elementtejä sisältävään tuotteeseen näkyvästi, helposti luettavasti ja pysyvästi. Jos tämä ei ole mahdollista tai perusteltua digitaalisia elementtejä sisältävän tuotteen luonteen vuoksi, merkintä on liitettävä tuotteen pakkaukseen ja 20 artiklassa tarkoitettuun sen mukana toimitettavaan EU-vaatimustenmukaisuusvakuutukseen. Ohjelmistomuotoisiin digitaalisia elementtejä sisältäviin tuotteisiin CE-merkintä on liitettävä joko 20 artiklassa tarkoitettuun EU-vaatimustenmukaisuusvakuutukseen tai esitettävä ohjelmistotuotteen verkkosivustolla.

2. Jos digitaalisia elementtejä sisältävän tuotteen luonne sitä vaatii, CE-merkinnän korkeus voi olla alle 5 mm, kunhan merkintä on edelleen näkyvä ja luettavissa.

3. CE-merkintä on liitettävä tuotteeseen ennen sen markkinoille saattamista. Sen yhteyteen voidaan liittää 6 kohdassa tarkoitetuissa täytäntöönpanosäädöksissä vahvistettu erityistä riskiä tai käyttötapaa osoittava kuva- tai muu merkki.

4. CE-merkinnän yhteydessä on esitettävä ilmoitetun laitoksen tunnusnumero, jos kyseinen laitos on osallistunut 24 artiklassa tarkoitettuun täydelliseen laadunvarmistukseen perustuvaan vaatimustenmukaisuuden arviointimenettelyyn (perustuen moduuliin H).

   Ilmoitetun laitoksen tunnusnumeron kiinnittää laitos itse tai sen ohjeiden mukaisesti valmistaja tai valmistajan valtuutettu edustaja.

5. Jäsenvaltioiden on nykyisiä mekanismeja hyödyntämällä varmistettava CE-merkintää koskevan järjestelmän moitteeton soveltaminen ja ryhdyttävä tarkoituksenmukaisiin toimiin, jos tätä merkintää käytetään sääntöjenvastaisesti. Jos digitaalisia elementtejä sisältävät tuotteet kuuluvat unionin muun sellaisen lainsäädännön soveltamisalaan, jossa myös säädetään CE-merkinnän kiinnittämisestä, CE-merkinnän on osoitettava, että tuotteet täyttävät myös kyseisessä muussa lainsäädännössä vahvistetut vaatimukset.

6. Komissio voi täytäntöönpanosäädöksillä vahvistaa teknisiä eritelmiä, jotka koskevat digitaalisia elementtejä sisältävien tuotteiden tietoturvaan liittyviä kuvamerkkejä tai muita merkkejä, sekä mekanismeja, joilla edistetään merkkien käyttöä. Tällaiset täytäntöönpanosäädökset hyväksytään 51 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

23 artikla

Tekniset asiakirjat

1. Teknisten asiakirjojen on sisällettävä kaikki asiaankuuluvat tiedot tai kuvaukset keinoista, joilla valmistaja on varmistanut, että digitaalisia elementtejä sisältävä tuote ja valmistajan prosessit täyttävät liitteessä I vahvistetut olennaiset vaatimukset. Asiakirjojen on sisällettävä vähintään liitteessä V vahvistetut osatekijät.

2. Tekniset asiakirjat on laadittava ennen digitaalisia elementtejä sisältävän tuotteen saattamista markkinoille, ja niitä on tarvittaessa päivitettävä jatkuvasti tuotteen odotetun käyttöiän ajan tai viiden vuoden ajan tuotteen markkinoille saattamisen jälkeen sen mukaan, kumpi näistä ajanjaksoista on lyhyempi.

3. Sellaisten 8 artiklassa ja 24 artiklan 4 kohdassa tarkoitettujen digitaalisia elementtejä sisältävien tuotteiden osalta, joihin sovelletaan myös muita unionin säädöksiä, on laadittava kootusti tekniset asiakirjat, jotka sisältävät tämän asetuksen liitteessä V tarkoitetut tiedot ja kyseisissä unionin muissa säädöksissä vaaditut tiedot.

4. Vaatimustenmukaisuuden arviointimenettelyyn liittyvät tekniset asiakirjat ja kirjeenvaihto on laadittava sen jäsenvaltion virallisella kielellä, johon ilmoitettu laitos on sijoittautunut, tai muulla laitoksen hyväksymällä kielellä.

5. Siirretään komissiolle valta antaa 50 artiklan mukaisesti delegoituja säädöksiä, joilla täydennetään tätä asetusta liitteessä V vahvistettuihin teknisiin asiakirjoihin sisällytettävillä osilla, jotta voidaan ottaa huomioon teknologian kehitys sekä tämän asetuksen täytäntöönpanoprosessissa havaittu kehitys.

24 artikla

Digitaalisia elementtejä sisältävien tuotteiden vaatimustenmukaisuuden arviointimenettelyt

1. Valmistajan on suoritettava digitaalisia elementtejä sisältävän tuotteen ja prosessiensa vaatimustenmukaisuuden arviointi selvittääkseen, täyttävätkö ne liitteessä I vahvistetut olennaiset vaatimukset. Valmistajan tai valmistajan valtuutetun edustajan on osoitettava olennaisten vaatimusten täyttyminen jollakin seuraavista menettelyistä:

   a) liitteessä VI esitetty sisäisen valvonnan menettely (perustuen moduuliin A) tai

   b) liitteessä VI esitetty EU-tyyppitarkastusmenettely (perustuen moduuliin B), jota seuraa liitteessä VI esitetty sisäiseen tuotannonvalvontaan perustuva EU-tyypinmukaisuus (perustuen moduuliin C) tai

   c) liitteessä VI esitetty täydelliseen laadunvarmistukseen perustuva vaatimustenmukaisuusarviointi (perustuen moduuliin H).

2. Jos valmistaja tai valmistajan valtuutettu edustaja ei ole käyttänyt tai on käyttänyt vain osittain 18 artiklassa tarkoitettuja yhdenmukaistettuja standardeja, yhteisiä eritelmiä tai eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä tai jos tällaisia yhdenmukaistettuja standardeja, yhteisiä eritelmiä tai eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä ei ole ja kyseessä on liitteessä III esitetyn mukainen luokkaan I kuuluva digitaalisia elementtejä sisältävä kriittinen tuote, tuote ja valmistajan prosessit on alistettava jompaankumpaan seuraavista menettelyistä, jotta voidaan arvioida, täyttävätkö ne liitteessä I vahvistetut olennaiset vaatimukset:

a) liitteessä VI esitetty EU-tyyppitarkastusmenettely (perustuen moduuliin B), jota seuraa liitteessä VI esitetty sisäiseen tuotannonvalvontaan perustuva EU-tyypinmukaisuus (perustuen moduuliin C) tai

b) liitteessä VI esitetty täydelliseen laadunvarmistukseen perustuva vaatimustenmukaisuusarviointi (perustuen moduuliin H).

3. Jos tuote on liitteessä III esitetyn mukainen luokkaan II kuuluva digitaalisia elementtejä sisältävä kriittinen tuote, valmistajan tai valmistajan valtuutetun edustajan on osoitettava, että tuote on täyttää liitteessä I vahvistetut olennaiset vaatimukset käyttäen jompaa kumpaa seuraavista menettelyistä:

a) liitteessä VI esitetty EU-tyyppitarkastusmenettely (perustuen moduuliin B), jota seuraa liitteessä VI esitetty sisäiseen tuotannonvalvontaan perustuva EU-tyypinmukaisuus (perustuen moduuliin C) tai

b) liitteessä VI esitetty täydelliseen laadunvarmistukseen perustuva vaatimustenmukaisuusarviointi (perustuen moduuliin H).

4. Asetuksen [eurooppalaisesta terveysdata-avaruudesta annettu asetus] soveltamisalaan kuuluviksi sähköisiksi potilastietojärjestelmiksi luokiteltujen digitaalisia elementtejä sisältävien tuotteiden valmistajien on osoitettava, että ne täyttävät tämän asetuksen liitteessä I vahvistetut olennaiset vaatimukset, käyttäen asiaankuuluvaa vaatimustenmukaisuuden arviointimenettelyä, jota edellytetään asetuksessa [eurooppalaisesta terveysdata-avaruudesta annetun asetuksen III luku].

5. Ilmoitettujen laitosten on otettava huomioon pienten ja keskisuurten yritysten (pk-yritysten) intressit ja tarpeet vaatimustenmukaisuuden arviointimenettelyistä perittäviä maksuja vahvistettaessa ja alennettava näitä maksuja suhteessa näiden yritysten intresseihin ja tarpeisiin.

IV LUKU

VAATIMUSTENMUKAISUUDEN ARVIOINTILAITOSTEN ILMOITTAMINEN

25 artikla

Ilmoittaminen

Jäsenvaltioiden on ilmoitettava komissiolle ja muille jäsenvaltioille vaatimustenmukaisuuden arviointilaitokset, joille on annettu lupa suorittaa vaatimustenmukaisuuden arviointeja tämän asetuksen mukaisesti.

26 artikla

Ilmoittavat viranomaiset

1. Jäsenvaltioiden on nimettävä ilmoittava viranomainen, joka vastaa vaatimustenmukaisuuden arviointilaitosten arviointiin ja ilmoittamiseen sekä ilmoitettujen laitosten valvontaan liittyvien tarvittavien menettelyjen perustamisesta ja toteuttamisesta, myös 31 artiklan noudattamisen osalta.

2. Jäsenvaltiot voivat päättää, että 1 kohdassa tarkoitetun arvioinnin ja valvonnan suorittaa asetuksen (EY) N:o 765/2008 mukaisesti mainitussa asetuksessa tarkoitettu kansallinen akkreditointielin.

27 artikla

Ilmoittavia viranomaisia koskevat vaatimukset

1. Ilmoittavan viranomaisen on oltava sillä tavoin perustettu, ettei synny eturistiriitaa vaatimustenmukaisuuden arviointilaitosten kanssa.

2. Ilmoittavan viranomaisen on oltava organisaatioltaan ja toiminnaltaan sellainen, että sen toiminnan objektiivisuus ja puolueettomuus on turvattu.

3. Ilmoittava viranomainen on organisoitava siten, että kunkin vaatimustenmukaisuuden arviointilaitoksen ilmoittamista koskevan päätöksen tekee eri toimivaltainen henkilöstö kuin arvioinnit suorittava henkilöstö.

4. Ilmoittava viranomainen ei saa tarjota eikä suorittaa mitään toimintoja, joita vaatimustenmukaisuuden arviointilaitokset tai konsultointipalvelut suorittavat kaupallisin tai kilpailullisin perustein.

5. Ilmoittavan viranomaisen on turvattava saamiensa tietojen luottamuksellisuus.

6. Ilmoittavalla viranomaisella on oltava käytössään riittävä määrä pätevää henkilöstöä tehtäviensä asianmukaista hoitamista varten.

28 artikla

Ilmoittavien viranomaisten tiedotusvelvoite

1. Jäsenvaltioiden on tiedotettava komissiolle menettelyistään, jotka koskevat vaatimustenmukaisuuden arviointilaitosten arviointia ja ilmoittamista sekä ilmoitettujen laitosten valvontaa, sekä mahdollisista muutoksista niihin.

2. Komissio asettaa kyseiset tiedot julkisesti saataville.

29 artikla

Ilmoitettuja laitoksia koskevat vaatimukset

1. Jotta vaatimustenmukaisuuden arviointilaitos voidaan ilmoittaa, sen on täytettävä 2–12 kohdassa säädetyt vaatimukset.

2. Vaatimustenmukaisuuden arviointilaitos on perustettava kansallisen lainsäädännön mukaisesti, ja sen on oltava oikeushenkilö.

3. Vaatimustenmukaisuuden arviointilaitoksen on oltava arvioimastaan organisaatiosta tai tuotteesta riippumaton kolmas osapuoli.

   Laitosta, joka kuuluu yrittäjäjärjestöön tai ammattialajärjestöön, joka edustaa yrityksiä, jotka ovat osallisina laitoksen arvioimien digitaalisia elementtejä sisältävien tuotteiden suunnittelussa, kehittämisessä, tuotannossa, toimittamisessa, asentamisessa, käytössä tai ylläpidossa, voidaan pitää tällaisena laitoksena sillä ehdolla, että osoitetaan sen riippumattomuus ja välttyminen eturistiriidoilta.

4. Vaatimustenmukaisuuden arviointilaitos, sen ylin johto ja vaatimustenarviointitehtävien suorittamisesta vastaava henkilöstö eivät saa olla arvioimiensa digitaalisia elementtejä sisältävien tuotteiden suunnittelija, kehittäjä, valmistaja, toimittaja, asentaja, ostaja, omistaja, käyttäjä tai ylläpitäjä eikä minkään tällaisen osapuolen valtuutettu edustaja. Tämä ei sulje pois sellaisten arvioitujen tuotteiden käyttöä, jotka ovat vaatimustenmukaisuuden arviointilaitoksen toimien kannalta tarpeellisia, tai sellaisten tuotteiden käyttöä henkilökohtaisiin tarkoituksiin.

Vaatimustenmukaisuuden arviointilaitos, sen ylin johto ja vaatimustenmukaisuuden arviointitehtävien suorittamisesta vastaava henkilöstö eivät myöskään saa olla suoranaisesti mukana näiden tuotteiden suunnittelussa, kehittämisessä tai tuotannossa, markkinoinnissa, asentamisessa, käytössä tai ylläpidossa eivätkä edustaa näissä toiminnoissa mukana olevia osapuolia. Ne eivät saa osallistua mihinkään toimintaan, joka voi olla ristiriidassa sen kanssa, että ne ovat arvioissaan riippumattomia, tai joka voi vaarantaa niiden riippumattomuuden niissä vaatimuksenmukaisuuden arviointitoimissa, joita varten ne on ilmoitettu. Tämä koskee erityisesti konsultointipalveluja.

Vaatimustenmukaisuuden arviointilaitosten on varmistettava, että niiden tytäryhtiöiden tai alihankkijoiden toimet eivät vaikuta niiden vaatimustenmukaisuuden arviointitoimien luottamuksellisuuteen, objektiivisuuteen tai puolueettomuuteen.

5. Vaatimustenmukaisuuden arviointilaitosten ja niiden henkilöstön on suoritettava vaatimustenmukaisuuden arviointitoimet mahdollisimman suurta ammatillista luotettavuutta ja kyseisellä erityisalalla vaadittavaa teknistä pätevyyttä noudattaen ja oltava vapaat kaikesta, erityisesti taloudellisesta, painostuksesta ja houkuttelusta, joka saattaisi vaikuttaa niiden harkintaan tai vaatimustenmukaisuuden arviointitoimien tuloksiin, erityisesti sellaisten henkilöiden tai henkilöryhmien taholta, joille näiden toimien tuloksilla on merkitystä.

6. Vaatimustenmukaisuuden arviointilaitoksen on kyettävä suorittamaan kaikki vaatimustenmukaisuuden arviointitehtävät, joita tarkoitetaan liitteessä VI ja joita varten se on ilmoitettu, riippumatta siitä, suorittaako vaatimustenmukaisuuden arviointilaitos kyseiset tehtävät itse vai suoritetaanko ne sen puolesta ja sen vastuulla.

Vaatimustenmukaisuuden arviointilaitoksella on kaikissa tapauksissa ja kunkin sellaisen vaatimustenmukaisuuden arviointimenettelyn ja tuotetyypin tai -ryhmän osalta, jota varten se on ilmoitettu, oltava käytössään

a) tarvittava henkilöstö, jolla on tekninen tietämys sekä riittävä ja soveltuva kokemus vaatimustenmukaisuuden arviointitehtävien suorittamiseksi;

b) tarvittavat kuvaukset menettelyistä, joiden mukaisesti vaatimustenmukaisuuden arviointi suoritetaan, siten, että varmistetaan näiden menettelyiden läpinäkyvyys ja toistettavuus. Sillä on oltava käytössään asianmukaiset toimintatavat ja menettelyt, joissa erotetaan toisistaan ilmoitettuna laitoksena suoritetut tehtävät ja muu toiminta;

c) tarvittavat menettelyt, joiden mukaisesti se hoitaa tehtäviään siten, että yritysten koko, toimiala ja rakenne, tuotteissa käytettävän teknologian monimutkaisuus sekä tuotannon luonne massa- tai sarjatuotantona otetaan asianmukaisesti huomioon.

Sillä on oltava käytössään tarvittavat keinot niiden teknisten ja hallinnollisten tehtävien suorittamiseen, joita vaatimustenmukaisuuden arviointitoimien asianmukainen hoitaminen edellyttää, ja sillä on oltava mahdollisuus käyttää kaikkia tarvittavia laitteita tai välineitä.

7. Vaatimustenmukaisuuden arviointitoimien suorittamisesta vastaavalla henkilöstöllä on oltava:

a) vankka tekninen ja ammatillinen koulutus, joka kattaa kaikki ne vaatimustenmukaisuuden arviointitoimet, joita varten vaatimustenmukaisuuden arviointilaitos on ilmoitettu;

b) riittävät tiedot suoritettavia arviointeja koskevista vaatimuksista ja riittävät valtuudet tällaisten arviointien suorittamiseen;

c) asianmukaiset tiedot ja ymmärrys olennaisista vaatimuksista, sovellettavista yhdenmukaistetuista standardeista ja asiaa koskevista unionin yhdenmukaistamislainsäädännön säännöksistä ja täytäntöönpanosäädöksistä;

d) kyky laatia todistuksia, asiakirjoja ja raportteja, joilla osoitetaan, että arvioinnit on suoritettu.

8. Vaatimustenmukaisuuden arviointilaitosten, niiden ylimmän johdon ja arviointihenkilöstön puolueettomuus on taattava.

Vaatimustenmukaisuuden arviointilaitoksen ylimmän johdon ja arviointihenkilöstön palkkiot eivät saa olla riippuvaisia suoritettujen arviointien määrästä eivätkä mainittujen arviointien tuloksista.

9. Vaatimustenmukaisuuden arviointilaitosten on otettava vastuuvakuutus, jollei tällainen vastuu kuulu valtiolle kansallisen lainsäädännön perusteella tai jollei jäsenvaltio itse ole suoraan vastuussa vaatimustenmukaisuuden arvioinnista.

10. Vaatimustenmukaisuuden arviointilaitosten henkilöstöllä on vaitiolovelvollisuus kaikkien niiden tietojen suhteen, jotka se saa suorittaessaan tehtäviään liitteen VI tai sen täytäntöönpanemiseksi annetun kansallisen lainsäädännön säännösten mukaisesti, paitsi sen jäsenvaltion markkinavalvontaviranomaisiin nähden, jossa laitosten toimet suoritetaan. Omistusoikeudet on suojattava. Vaatimustenmukaisuuden arviointilaitoksella on oltava dokumentoidut menettelyt, joilla varmistetaan tämän kohdan mukaisuus.

11. Vaatimustenmukaisuuden arviointilaitosten on osallistuttava asiaankuuluviin standardointitoimiin ja 40 artiklan nojalla perustetun ilmoitettujen laitosten koordinointiryhmän toimiin tai varmistettava, että niiden arviointihenkilöstö saa niistä tiedon, ja sovellettava yleisinä ohjeina kyseisen ryhmän työn tuloksena saatuja hallinnollisia päätöksiä ja asiakirjoja.

12. Vaatimustenmukaisuuden arviointilaitosten on toimittava johdonmukaisilla, oikeudenmukaisilla ja kohtuullisilla ehdoilla ja edellytyksillä ja otettava erityisesti huomioon maksuihin liittyvät pk-yritysten intressit.

30 artikla

Ilmoitettujen laitosten vaatimustenmukaisuusolettama

Jos vaatimustenmukaisuuden arviointilaitos voi osoittaa olevansa sellaisissa asianomaisissa yhdenmukaistetuissa standardeissa tai niiden osissa vahvistettujen edellytysten mukainen, joiden viitetiedot on julkaistu *Euroopan unionin virallisessa lehdessä*, sen oletetaan täyttävän 29 artiklassa säädetyt vaatimukset siltä osin kuin sovellettavat yhdenmukaistetut standardit kattavat nämä vaatimukset.

31 artikla

Ilmoitettujen laitosten tytäryhtiöt ja alihankinta

1. Jos ilmoitettu laitos teettää tiettyjä vaatimustenmukaisuuden arviointiin liittyviä tehtäviä alihankintana tai käyttää tytäryhtiötä, sen on varmistettava, että alihankkija tai tytäryhtiö täyttää 29 artiklassa säädetyt vaatimukset, ja tiedotettava asiasta ilmoittavalle viranomaiselle.

2. Ilmoitettujen laitosten on otettava täysi vastuu alihankkijoiden tai tytäryhtiöiden suorittamista tehtävistä riippumatta siitä, mihin nämä ovat sijoittautuneet.

3. Toimia voidaan teettää alihankintana tai tytäryhtiöllä ainoastaan, jos siitä on sovittu valmistajan kanssa.

4. Ilmoitettujen laitosten on pidettävä ilmoittavan viranomaisen saatavilla asiakirjat, jotka koskevat alihankkijan tai tytäryhtiön pätevyyden arviointia sekä työtä, jonka nämä ovat suorittaneet tämän asetuksen nojalla.

32 artikla

Ilmoittamista koskeva hakemus

1. Vaatimustenmukaisuuden arviointilaitoksen on toimitettava ilmoittamista koskeva hakemus sen jäsenvaltion ilmoittavalle viranomaiselle, johon se on sijoittautunut.

2. Hakemukseen on liitettävä kuvaus vaatimustenmukaisuuden arviointitoimista, vaatimustenmukaisuuden arviointimenettelyistä ja tuotteista, joiden osalta laitos katsoo olevansa pätevä, sekä mahdollinen akkreditointitodistus, jonka kansallinen akkreditointielin on antanut ja jossa todistetaan, että vaatimustenmukaisuuden arviointilaitos täyttää 29 artiklassa säädetyt vaatimukset.

3. Jos asianomainen vaatimustenmukaisuuden arviointilaitos ei voi toimittaa akkreditointitodistusta, sen on toimitettava ilmoittavalle viranomaiselle kaikki tarpeelliset asiakirjatodisteet, joiden avulla voidaan todentaa, tunnustaa ja säännöllisesti valvoa, että se täyttää 29 artiklassa säädetyt vaatimukset.

33 artikla

Ilmoitusmenettely

1. Ilmoittavat viranomaiset voivat ilmoittaa ainoastaan sellaiset vaatimustenmukaisuuden arviointilaitokset, jotka ovat täyttäneet 29 artiklassa säädetyt vaatimukset.

2. Ilmoittavan viranomaisen on ilmoitettava asiasta komissiolle ja muille jäsenvaltioille käyttäen komission kehittämää ja hallinnoimaa uuden lähestymistavan mukaista ilmoitettujen ja nimettyjen organisaatioiden tietojärjestelmää (NANDO).

3. Ilmoituksen on sisällettävä täydelliset tiedot vaatimustenmukaisuuden arviointitoimista, vaatimustenmukaisuuden arviointimoduuleista ja kyseessä olevista tuotteista sekä asiaankuuluva todistus pätevyydestä.

4. Jos ilmoitus ei perustu 32 artiklan 2 kohdassa tarkoitettuun akkreditointitodistukseen, ilmoittavan viranomaisen on toimitettava komissiolle ja muille jäsenvaltioille asiakirjatodisteet, joiden avulla voidaan todistaa vaatimustenmukaisuuden arviointilaitoksen pätevyys ja toteutetut järjestelyt, joilla varmistetaan, että laitosta valvotaan säännöllisesti ja että se täyttää edelleen 29 artiklassa säädetyt vaatimukset.

5. Asianomainen laitos voi suorittaa ilmoitetun laitoksen tehtäviä ainoastaan, jos komissio ja muut jäsenvaltiot eivät esitä vastalauseita kahden viikon kuluessa

ilmoittamisesta siinä tapauksessa, että on käytetty akkreditointitodistusta, tai kahden kuukauden kuluessa ilmoituksesta siinä tapauksessa, että akkreditointia ei käytetä.

Ainoastaan tällaista laitosta pidetään tässä asetuksessa tarkoitettuna ilmoitettuna laitoksena.

6. Komissiolle ja muille jäsenvaltioille on ilmoitettava myöhemmistä muutoksista kyseiseen ilmoitukseen.

34 artikla

Ilmoitettujen laitosten tunnusnumerot ja luettelot

1. Komissio antaa ilmoitetulle laitokselle tunnusnumeron.

Se antaa vain yhden tällaisen numeron myös silloin, kun laitos ilmoitetaan usean unionin säädöksen nojalla.

2. Komissio asettaa julkisesti saataville luettelon laitoksista, jotka on ilmoitettu tämän asetuksen nojalla, mukaan luettuna tunnusnumerot, jotka niille on annettu ja toimet, joita varten ne on ilmoitettu.

Komissio huolehtii luettelon pitämisestä ajan tasalla.

35 artikla

Muutokset ilmoituksiin

1. Jos ilmoittava viranomainen on todennut tai saanut tietää, ettei ilmoitettu laitos enää täytä 29 artiklassa säädettyjä vaatimuksia tai ettei se noudata velvoitteitaan, ilmoittavan viranomaisen on tarpeen mukaan rajoitettava ilmoitusta taikka peruutettava se toistaiseksi tai kokonaan, riippuen vaatimusten täyttämättä jättämisen tai velvoitteiden noudattamatta jättämisen vakavuudesta. Sen on ilmoitettava asiasta välittömästi komissiolle ja muille jäsenvaltioille.

2. Jos ilmoitusta rajoitetaan tai se peruutetaan toistaiseksi tai kokonaan tai jos ilmoitettu laitos on lopettanut toimintansa, ilmoittaneen jäsenvaltion on toteutettava asianmukaiset toimenpiteet varmistaakseen, että kyseisen laitoksen asiakirja-aineiston joko käsittelee toinen ilmoitettu laitos tai se pidetään ilmoittavan viranomaisen ja markkinavalvontaviranomaisten pyynnöstä niiden saatavilla.

36 artikla

Ilmoitettujen laitosten pätevyyden riitauttaminen

1. Komissio tutkii kaikki tapaukset, joissa sillä itsellään on tai sen tietoon saatetaan epäilyksiä, jotka koskevat ilmoitetun laitoksen pätevyyttä tai sitä, täyttääkö ilmoitettu laitos edelleen sitä koskevat vaatimukset ja velvollisuudet.

2. Ilmoituksen tehneen jäsenvaltion on toimitettava pyynnöstä komissiolle kaikki tiedot, jotka liittyvät ilmoituksen perusteisiin tai asianomaisen laitoksen pätevyyden ylläpitoon.

3. Komissio varmistaa, että kaikkia sen tutkimusten yhteydessä saatuja arkaluonteisia tietoja käsitellään luottamuksellisesti.

4. Jos komissio toteaa, että ilmoitettu laitos ei täytä tai ei enää täytä sen ilmoittamiselle asetettuja vaatimuksia, se ilmoittaa asiasta ilmoituksen tehneelle jäsenvaltiolle ja

pyytää sitä ryhtymään tarvittaviin korjaaviin toimenpiteisiin, mukaan luettuna ilmoituksen peruuttaminen tarvittaessa.

37 artikla

Ilmoitettujen laitosten toimintaan liittyvät velvollisuudet

1. Ilmoitettujen laitosten on suoritettava vaatimustenmukaisuuden arvioinnit 24 artiklassa ja liitteessä VI säädettyjen vaatimustenmukaisuuden arviointimenettelyjen mukaisesti.

2. Vaatimustenmukaisuuden arvioinnit on suoritettava oikeasuhteisesti siten, ettei talouden toimijoille aiheuteta tarpeetonta taakkaa. Vaatimustenmukaisuuden arviointilaitosten on tehtäviään hoitaessaan otettava asianmukaisesti huomioon yrityksen koko, toimiala ja rakenne, tuotteissa käytettävän teknologian monimutkaisuus sekä tuotannon luonne massa- tai sarjatuotantona.

3. Ilmoitettujen laitosten on kuitenkin noudatettava sellaista tarkkuutta ja suojelun tasoa, jota tuotteiden vaatimustenmukaisuudelta edellytetään tämän asetuksen säännösten mukaisesti.

4. Jos ilmoitettu laitos katsoo, että valmistaja ei ole täyttänyt vaatimuksia, joista säädetään liitteessä tai vastaavissa yhdenmukaistetuissa standardeissa tai 19 artiklassa tarkoitetuissa yhteisissä eritelmissä, sen on vaadittava valmistajaa ryhtymään tarvittaviin korjaaviin toimenpiteisiin eikä se saa antaa vaatimustenmukaisuustodistusta.

5. Jos ilmoitettu laitos katsoo todistuksen antamisen jälkeen suoritettavan vaatimustenmukaisuuden valvonnan yhteydessä, ettei tuote enää täytä tässä asetuksessa säädettyjä vaatimuksia, sen on vaadittava valmistajaa ryhtymään tarvittaviin korjaaviin toimenpiteisiin ja tarvittaessa peruutettava todistus toistaiseksi tai kokonaan.

6. Jos korjaavia toimenpiteitä ei toteuteta tai niillä ei ole vaadittua vaikutusta, ilmoitetun laitoksen on tarpeen mukaan rajoitettava myöntämiään todistuksia tai peruutettava ne toistaiseksi tai kokonaan.

38 artikla

Ilmoitettujen laitosten tiedotusvelvoite

1. Ilmoitettujen laitosten on tiedotettava ilmoittavalle viranomaiselle seuraavista seikoista:

   a) todistusten epäämiset, rajoittamiset tai peruuttamiset väliaikaisesti tai kokonaan;

   b) olosuhteet, jotka vaikuttavat ilmoituksen soveltamisalaan ja ehtoihin;

   c) vaatimustenmukaisuuden arviointitoimia koskevat tietopyynnöt, jotka ne ovat saaneet markkinavalvontaviranomaisilta;

   d) pyynnöstä vaatimustenmukaisuuden arviointitoimet, jotka on suoritettu niitä koskevan ilmoituksen puitteissa, ja mahdollisesti suoritetut muut toimet, mukaan lukien rajat ylittävät toimet ja alihankinta.

2. Ilmoitettujen laitosten on toimitettava tämän asetuksen nojalla ilmoitetuille muille laitoksille, jotka suorittavat samanlaisia samat tuotteet kattavia

vaatimustenmukaisuuden arviointitoimia, asiaankuuluvat tiedot kysymyksistä, jotka liittyvät vaatimustenmukaisuuden arvioinnin kielteisiin tuloksiin ja pyynnöstä myös myönteisiin tuloksiin.

39 artikla

Kokemusten vaihto

Komissio huolehtii kokemusten vaihdon järjestämisestä niiden kansallisten viranomaisten välillä, jotka vastaavat ilmoittamista koskevista jäsenvaltioiden toimintatavoista.

40 artikla

Ilmoitettujen laitosten koordinointi

1. Komissio varmistaa, että ilmoitettujen laitosten välillä tapahtuu asianmukaista yhteensovittamista ja yhteistyötä ilmoitettujen laitosten monialaisessa ryhmässä.

2. Jäsenvaltioiden on varmistettava, että niiden ilmoittamat laitokset osallistuvat kyseisen ryhmän työhön suoraan tai nimettyjen edustajien välityksellä.

V LUKU

MARKKINAVALVONTA JA TÄYTÄNTÖÖNPANO

41 artikla

Markkinavalvonta ja digitaalisia elementtejä sisältäville tuotteille unionin markkinoilla tehtävät tarkastukset

1. Tämän asetuksen soveltamisalaan kuuluviin digitaalisia elementtejä sisältäviin tuotteisiin sovelletaan asetusta (EU) 2019/1020.

2. Kunkin jäsenvaltion on nimettävä yksi tai useampi markkinavalvontaviranomainen tämän asetuksen tosiasiallisen täytäntöönpanon varmistamiseksi. Jäsenvaltiot voivat nimetä tätä asetusta varten markkinavalvontaviranomaiseksi jo olemassa olevan tai uuden viranomaisen.

3. Markkinavalvontaviranomaisten on tarvittaessa tehtävä yhteistyötä asetuksen (EU) 2019/881 58 artiklan mukaisesti nimettyjen kansallisten kyberturvasertifiointiviranomaisten kanssa ja vaihdettava säännöllisesti niiden kanssa tietoja. Tämän asetuksen 11 artiklan mukaisten raportointivelvoitteiden noudattamisen valvonnan osalta nimettyjen markkinavalvontaviranomaisten on tehtävä yhteistyötä ENISAn kanssa.

4. Markkinavalvontaviranomaisten on tarvittaessa tehtävä yhteistyötä muiden muita tuotteita koskevan unionin yhdenmukaistamislainsäädännön perusteella nimettyjen markkinavalvontaviranomaisten kanssa ja vaihdettava säännöllisesti niiden kanssa tietoja.

5. Markkinavalvontaviranomaisten on tarvittaessa tehtävä yhteistyötä unionin tietosuojalainsäädäntöä valvovien viranomaisten kanssa. Tällaiseen yhteistyöhön sisältyy tiedottaminen kyseisille viranomaisille niiden toimivaltuuksien kannalta merkityksellisistä havainnoista, myös silloin, kun annetaan ohjeistusta ja neuvoja

tämän artiklan 8 kohdan mukaisesti, jos ohjeistot ja neuvot koskevat henkilötietojen käsittelyä.

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 suorittamiseksi. Niiden on ilmoitettava tällaisesta pyynnöstä asianomaisen jäsenvaltion nimetyille markkinavalvontaviranomaisille.

6. Jäsenvaltioiden on varmistettava, että nimetyille markkinavalvontaviranomaisille annetaan riittävät taloudelliset ja henkilöstöresurssit, jotta ne voivat hoitaa tämän asetuksen mukaiset tehtävänsä.

7. Komissio helpottaa kokemusten vaihtoa nimettyjen markkinavalvontaviranomaisten välillä.

8. Markkinavalvontaviranomaiset voivat komission tuella antaa talouden toimijoille ohjeita ja neuvoja tämän asetuksen täytäntöönpanosta.

9. Markkinavalvontaviranomaisten on raportoitava vuosittain komissiolle asiaankuuluvien markkinavalvontatoimien tuloksista. Nimettyjen markkinavalvontaviranomaisten on ilmoitettava viipymättä komissiolle ja asianomaisille kansallisille kilpailuviranomaisille kaikki markkinavalvontatoimien yhteydessä esiin tulleet tiedot, joilla voi olla merkitystä unionin kilpailuoikeuden soveltamisen kannalta.

10. Kun on kyse tämän asetuksen soveltamisalaan kuuluvista digitaalisia elementtejä sisältävistä tuotteista, jotka on luokiteltu suuririskisiksi tekoälyjärjestelmiksi asetuksen [tekoälyasetus] [6 artiklan] mukaisesti, asetusta [tekoälyasetus] varten nimetyt markkinavalvontaviranomaiset vastaavat myös tämän asetuksen nojalla vaadituista markkinavalvontatoimista. Asetuksen [tekoälyasetus] nojalla nimettyjen markkinavalvontaviranomaisten on tarvittaessa tehtävä yhteistyötä tämän asetuksen nojalla nimettyjen markkinavalvontaviranomaisten kanssa ja 11 artiklan mukaisten raportointivelvoitteiden noudattamisen valvonnan osalta ENISAn kanssa. Asetuksen [tekoälyasetus] nojalla nimettyjen markkinavalvontaviranomaisten on ilmoitettava tämän asetuksen nojalla nimetyille markkinavalvontaviranomaisille kaikista havainnoista, joilla on merkitystä niiden tämän asetuksen täytäntöönpanoon liittyvien tehtävien hoitamisessa.

11. Tämän asetuksen yhdenmukaista soveltamista varten perustetaan erityinen hallinnollisen yhteistyön ryhmä asetuksen (EU) 2019/1020 30 artiklan 2 kohdan mukaisesti. Hallinnollisen yhteistyön ryhmä koostuu nimettyjen markkinavalvontaviranomaisten edustajista ja tarvittaessa yhteysvirastojen edustajista.

42 artikla

Tietojen ja dokumentaation saatavuus

Jos se on tarpeen sen arvioimiseksi, täyttävätkö digitaalisia elementtejä sisältävät tuotteet ja valmistajien prosessit liitteessä I vahvistetut olennaiset vaatimukset, markkinavalvontaviranomaisille on myönnettävä perustellusta pyynnöstä pääsy tietoihin, joita tarvitaan tällaisten tuotteiden suunnittelun, kehittämisen, tuotannon ja haavoittuvuuskäsittelyn arvioimiseksi, mukaan lukien asianomaisen talouden toimijan asiaan liittyvä sisäinen dokumentaatio.

43 artikla

Kansallisen tason menettely merkittävän kyberturvariskin aiheuttavia tuotteita varten

1. Jos jäsenvaltion markkinavalvontaviranomaisella on riittävät perusteet katsoa, että digitaalisia elementtejä sisältävä tuote, mukaan lukien sen haavoittuvuuskäsittely, aiheuttaa merkittävän kyberturvariskin, sen on arvioitava, täyttääkö tuote kaikki tässä asetuksessa säädetyt vaatimukset. Asianomaisten talouden toimijoiden on tehtävä tarpeen mukaan yhteistyötä markkinavalvontaviranomaisen kanssa.

   Kun markkinavalvontaviranomainen havaitsee arvioinnin yhteydessä, että digitaalisia elementtejä sisältävä tuote ei täytä tässä asetuksessa säädettyjä vaatimuksia, sen on vaadittava viipymättä asianomaista toimijaa ryhtymään kaikkiin tarvittaviin korjaaviin toimenpiteisiin tuotteen saattamiseksi vastaamaan kyseisiä vaatimuksia tai sen poistamiseksi markkinoilta tai sen palauttamisen järjestämiseksi sellaisen määrittelemänsä kohtuullisen ajanjakson kuluessa, joka on oikeassa suhteessa riskin laatuun.

   Markkinavalvontaviranomaisten on ilmoitettava tästä asianomaiselle ilmoitetulle laitokselle. Asianmukaisiin korjaaviin toimenpiteisiin sovelletaan asetuksen (EU) 2019/1020 18 artiklaa.

2. Kun markkinavalvontaviranomainen katsoo, että vaatimustenvastaisuus ei rajoitu sen kansalliselle alueelle, sen on ilmoitettava komissiolle ja muille jäsenvaltioille arvioinnin tuloksista ja toimenpiteistä, jotka se on vaatinut toimijaa toteuttamaan.

3. Valmistajan on varmistettava, että kaikki asianmukaiset korjaavat toimenpiteet toteutetaan kaikkien digitaalisia elementtejä sisältävien tuotteiden osalta, jotka se on asettanut saataville markkinoilla unionin alueella.

4. Jos digitaalisia elementtejä sisältävän tuotteen valmistaja ei 1 kohdan toisessa alakohdassa tarkoitetun ajanjakson kuluessa toteuta riittäviä korjaavia toimenpiteitä, markkinavalvontaviranomaisen on toteutettava kaikki tarvittavat väliaikaiset toimenpiteet, joilla kielletään kyseisen tuotteen asettaminen saataville kansallisilla markkinoilla tai rajoitetaan sitä tai joilla tuote poistetaan kyseisiltä markkinoilta tai järjestetään sitä koskeva palautusmenettely.

   Viranomaisen on viipymättä ilmoitettava komissiolle ja muille jäsenvaltioille näistä toimenpiteistä.

5. Edellä 4 kohdassa tarkoitettuun ilmoitukseen on sisällyttävä kaikki saatavilla olevat yksityiskohdat, erityisesti ne, jotka ovat tarpeen vaatimustenvastaisen digitaalisia elementtejä sisältävän tuotteen tunnistamista ja tuotteen alkuperän, siihen liittyvän väitetyn vaatimustenvastaisuuden ja riskin luonteen ja toteutettujen kansallisten toimenpiteiden luonteen ja keston määrittämistä varten, sekä asianomaisen toimijan esittämät perustelut. Markkinavalvontaviranomaisen on erityisesti ilmoitettava, johtuuko vaatimustenvastaisuus yhdestä tai useammasta seuraavista:

   a) tuotteet tai valmistajan prosessit eivät täytä liitteessä I vahvistettuja olennaisia vaatimuksia;

   b) yhdenmukaistetuissa standardeissa, kyberturvallisuuden sertifiointijärjestelmissä tai 18 artiklassa tarkoitetuissa yhteisissä eritelmissä on puutteita.

6. Muiden jäsenvaltioiden markkinavalvontaviranomaisten kuin menettelyn aloittaneen jäsenvaltion markkinavalvontaviranomaisen on viipymättä ilmoitettava komissiolle

ja muille jäsenvaltioille kaikki toteutetut toimenpiteet ja kaikki niiden hallussa olevat lisätiedot, jotka liittyvät asianomaisen tuotteen vaatimustenvastaisuuteen, sekä vastalauseensa siinä tapauksessa, että ilmoitetusta kansallisesta toimenpiteestä on erimielisyyttä.

7. Jos mikään jäsenvaltio tai komissio ei ole kolmen kuukauden kuluessa 4 kohdassa tarkoitetun ilmoituksen vastaanottamisesta esittänyt vastalausetta jonkin jäsenvaltion toteuttamaa väliaikaista toimenpidettä kohtaan, toimenpiteen katsotaan olevan oikeutettu. Tämä ei rajoita asianomaisen toimijan asetuksen (EU) 2019/1020 18 artiklan mukaisia menettelyllisiä oikeuksia.

8. Kaikkien jäsenvaltioiden markkinavalvontaviranomaisten on varmistettava, että kyseistä tuotetta koskevat asianmukaiset rajoittavat toimenpiteet, kuten tuotteen vetäminen pois markkinoilta, toteutetaan viipymättä.

44 artikla

Unionin suojamenettely

1. Mikäli kolmen kuukauden kuluessa 43 artiklan 4 kohdassa tarkoitetun ilmoituksen vastaanottamisesta jokin jäsenvaltio esittää vastalauseen toisen jäsenvaltion toteuttamasta toimenpiteestä tai mikäli komissio pitää toimenpidettä unionin lainsäädännön vastaisena, komissio kuulee viipymättä asianomaista jäsenvaltiota ja talouden toimijaa ja arvioi kansallisen toimenpiteen. Komissio päättää arvioinnin tulosten perusteella, onko kansallinen toimenpide perusteltu, yhdeksän kuukauden kuluessa 43 artiklan 4 kohdassa tarkoitetusta ilmoituksesta, ja ilmoittaa tällaisesta päätöksestä asianomaiselle jäsenvaltiolle.

2. Jos kansallisen toimenpiteen katsotaan olevan perusteltu, kaikkien jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että vaatimustenvastainen digitaalisia elementtejä sisältävä tuote vedetään pois markkinoilta, ja niiden on ilmoitettava asiasta komissiolle. Jos kansallista toimenpidettä pidetään perusteettomana, asianomaisen jäsenvaltion on peruutettava toimenpide.

3. Jos kansallinen toimenpide katsotaan perustelluksi ja digitaalisia elementtejä sisältävän tuotteen vaatimustenvastaisuuden katsotaan johtuvan puutteista yhdenmukaistetuissa standardeissa, komissio soveltaa asetuksen (EU) N:o 1025/2012 10 artiklassa säädettyä menettelyä.

4. Jos kansallinen toimenpide katsotaan perustelluksi ja digitaalisia elementtejä sisältävän tuotteen vaatimustenvastaisuuden katsotaan johtuvan puutteista 18 artiklassa tarkoitetussa eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä, komissio harkitsee, muutetaanko tai kumotaanko 18 artiklan 4 kohdassa tarkoitettu täytäntöönpanosäädös, jossa vahvistetaan kyseistä sertifiointijärjestelmää koskeva vaatimustenmukaisuusolettama.

5. Jos kansallinen toimenpide katsotaan perustelluksi ja digitaalisia elementtejä sisältävän tuotteen vaatimustenvastaisuuden katsotaan johtuvan puutteista 19 artiklassa tarkoitetuissa yhteisissä eritelmissä, komissio harkitsee, muutetaanko tai kumotaanko 19 artiklassa tarkoitettu täytäntöönpanosäädös, jossa vahvistetaan kyseiset yhteiset eritelmät.

45 artikla

EU:n tason menettely merkittävän kyberturvariskin aiheuttavia tuotteita varten

1. Jos komissiolla on riittävät perusteet katsoa, myös ENISAn toimittamien tietojen perusteella, että digitaalisia elementtejä sisältävä merkittävän kyberturvallisuusriskin aiheuttava tuote ei täytä tässä asetuksessa säädettyjä vaatimuksia, se voi pyytää asianomaisia markkinavalvontaviranomaisia suorittamaan vaatimustenmukaisuuden arvioinnin ja noudattamaan 43 artiklassa tarkoitettuja menettelyjä.

2. Poikkeuksellisissa olosuhteissa, joissa on perusteltua ryhtyä välittömiin toimiin sisämarkkinoiden moitteettoman toiminnan säilyttämiseksi, ja jos komissiolla on riittävät perusteet katsoa, että 1 kohdassa tarkoitettu tuote ei edelleenkään täytä tässä asetuksessa säädettyjä vaatimuksia, eivätkä asianomaiset markkinavalvontaviranomaiset ole toteuttaneet tuloksellisia toimenpiteitä, komissio voi pyytää ENISAa suorittamaan vaatimustenmukaisuuden arvioinnin. Komissio ilmoittaa asiasta asianomaisille markkinavalvontaviranomaisille. Asianomaisten talouden toimijoiden on tehtävä tarpeen mukaan yhteistyötä ENISAn kanssa.

3. ENISAn arvioinnin perusteella komissio voi päättää, että unionin tasolla tarvitaan korjaava tai rajoittava toimenpide. Tätä varten sen on viipymättä kuultava asianomaisia jäsenvaltioita ja asianomaisia talouden toimijoita.

4. Edellä 3 kohdassa tarkoitetun kuulemisen perusteella komissio voi hyväksyä täytäntöönpanosäädöksillä korjaavia tai rajoittavia toimenpiteitä unionin tasolla, mukaan lukien markkinoiltaveto tai palautusmenettely kohtuullisen ajan kuluessa ja oikeassa suhteessa riskin luonteeseen. Tällaiset täytäntöönpanosäädökset hyväksytään 51 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

5. Komissio antaa 4 kohdassa tarkoitetun päätöksen viipymättä tiedoksi asiaankuuluville talouden toimijoille. Jäsenvaltioiden on pantava 4 kohdassa tarkoitetut säädökset täytäntöön viipymättä ja tiedotettava tästä komissiolle.

6. Edellä olevaa 2–5 kohtaa sovelletaan komission toimenpiteen perusteena olleen poikkeuksellisen tilanteen keston ajan ja niin kauan kuin kyseistä tuotetta ei ole saatettu tämän asetuksen mukaiseksi.

46 artikla

Digitaalisia elementtejä sisältävät merkittävän kyberturvariskin aiheuttavat vaatimustenmukaiset tuotteet

1. Jos jäsenvaltion markkinavalvontaviranomainen toteaa 43 artiklan mukaisen arvioinnin suoritettuaan, että vaikka digitaalisia elementtejä sisältävät tuotteet ja valmistajan prosessit täyttävät tämän asetuksen vaatimukset, ne aiheuttavat merkittävän kyberturvariskin ja lisäksi riskin ihmisten terveydelle tai turvallisuudelle, perusoikeuksien suojaamiseen tarkoitetun unionin tai kansallisen lainsäädännön mukaisten velvoitteiden täyttymiselle, [direktiivin XXX/XXXX (NIS2) liitteessä I] tarkoitettujen keskeisten toimijoiden sähköisen tietojärjestelmän avulla tarjoamien palvelujen saatavuudelle, aitoudelle, eheydelle tai luottamuksellisuudelle tai muille yleisen edun suojaan liittyville näkökohdille, sen on vaadittava asianomaista toimijaa toteuttamaan kaikki asianmukaiset toimenpiteet sen varmistamiseksi, että digitaalisia elementtejä sisältävät tuotteet ja kyseisen valmistajan prosessit eivät enää aiheuta kyseistä riskiä, digitaalisia elementtejä sisältävä tuote poistetaan markkinoilta tai järjestetään palautusmenettely kohtuullisessa ajassa ja oikeassa suhteessa riskin luonteeseen.

2. Valmistajan tai muiden asiaankuuluvien toimijoiden on varmistettava, että korjaavat toimenpiteet toteutetaan kaikkien asianomaisten digitaalisia elementtejä sisältävien

tuotteiden osalta, jotka ne ovat asettaneet saataville markkinoilla unionin alueella, edellä 1 kohdassa tarkoitetun jäsenvaltion markkinavalvontaviranomaisen asettamassa määräajassa.

3. Jäsenvaltion on välittömästi ilmoitettava komissiolle ja muille jäsenvaltioille 1 kohdan nojalla toteutetuista toimenpiteistä. Ilmoitukseen on sisällyttävä kaikki saatavilla olevat yksityiskohtaiset tiedot, erityisesti ne, jotka ovat tarpeen asianomaisten digitaalisia elementtejä sisältävien tuotteiden tunnistamista sekä niiden alkuperän ja toimitusketjun, riskin luonteen sekä toteutettujen kansallisten toimenpiteiden luonteen ja keston määrittämistä varten.

4. Komissio ryhtyy viipymättä kuulemaan jäsenvaltioita ja asianomaisia talouden toimijoita ja arvioi toteutetut kansalliset toimenpiteet. Komissio tekee tämän arvioinnin tulosten perusteella päätöksen siitä, onko toimenpide perusteltu vai ei, ja ehdottaa tarvittaessa soveltuvia toimenpiteitä.

5. Komissio osoittaa päätöksensä jäsenvaltioille.

6. Jos komissiolla on riittävät perusteet katsoa, myös ENISAn toimittamien tietojen perusteella, että vaikka digitaalisia elementtejä sisältävä tuote täyttää tämän asetuksen vaatimukset, se aiheuttaa 1 kohdassa tarkoitettuja riskejä, komissio voi pyytää asianomaisia markkinavalvontaviranomaisia suorittamaan vaatimustenmukaisuuden arvioinnin ja noudattamaan 43 artiklassa ja tämän artiklan 1, 2 ja 3 kohdassa tarkoitettuja menettelyjä.

7. Poikkeuksellisissa olosuhteissa, joissa on perusteltua ryhtyä välittömiin toimiin sisämarkkinoiden moitteettoman toiminnan säilyttämiseksi, ja jos komissiolla on riittävät perusteet katsoa, että 6 kohdassa tarkoitettu tuote aiheuttaa edelleen 1 kohdassa tarkoitettuja riskejä, eivätkä asianomaiset kansalliset markkinavalvontaviranomaiset ole toteuttaneet tuloksellisia toimenpiteitä, komissio voi pyytää ENISAa arvioimaan tuotteen aiheuttamat riskit ja ilmoittaa tästä asianomaisille markkinavalvontaviranomaisille. Asianomaisten talouden toimijoiden on tehtävä tarpeen mukaan yhteistyötä ENISAn kanssa.

8. Edellä 7 kohdassa tarkoitetun ENISAn arvioinnin perusteella komissio voi päättää, että unionin tasolla tarvitaan korjaava tai rajoittava toimenpide. Tätä varten sen on viipymättä kuultava asianomaisia jäsenvaltioita ja asianomaisia toimijoita.

9. Edellä 8 kohdassa tarkoitetun kuulemisen perusteella komissio voi hyväksyä täytäntöönpanosäädöksillä korjaavia tai rajoittavia toimenpiteitä unionin tasolla, mukaan lukien markkinoiltaveto tai palautusmenettely kohtuullisen ajan kuluessa ja oikeassa suhteessa riskin luonteeseen. Tällaiset täytäntöönpanosäädökset hyväksytään 51 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

10. Komissio antaa 9 kohdassa tarkoitetun päätöksen viipymättä tiedoksi asianomaisille toimijoille. Jäsenvaltioiden on pantava tällaiset säädökset täytäntöön viipymättä ja tiedotettava tästä komissiolle.

11. Edellä olevaa 6–10 kohtaa sovelletaan komission toimenpiteen perusteena olleen poikkeuksellisen tilanteen keston ajan ja niin kauan kuin kyseinen tuote aiheuttaa 1 kohdassa tarkoitettuja riskejä.

47 artikla

Muodollinen vaatimustenvastaisuus

1. Jos jäsenvaltion markkinavalvontaviranomainen tekee jonkin seuraavista havainnoista, sen on vaadittava asianomaista valmistajaa korjaamaan kyseinen vaatimustenvastaisuus:

   a) vaatimustenmukaisuusmerkintä on kiinnitetty 21 ja 22 artiklan vastaisesti;

   b) vaatimustenmukaisuusmerkintää ei ole kiinnitetty;

   c) EU:n vaatimustenmukaisuusvakuutusta ei ole laadittu;

   d) EU:n vaatimustenmukaisuusvakuutusta ei ole laadittu oikein;

   e) vaatimustenmukaisuuden arviointimenettelyyn osallistuvan ilmoitetun laitoksen tunnusnumeroa ei ole kiinnitetty, jos sitä vaaditaan;

   f) teknisiä asiakirjoja ei ole saatavilla tai ne ovat epätäydelliset.

2. Jos 1 kohdassa tarkoitettu vaatimustenvastaisuus jatkuu, asianomaisen jäsenvaltion on ryhdyttävä kaikkiin tarvittaviin toimenpiteisiin digitaalisia elementtejä sisältävän tuotteen markkinoilla saataville asettamisen rajoittamiseksi tai kieltämiseksi tai sen varmistamiseksi, että järjestetään sitä koskeva palautusmenettely tai se poistetaan markkinoilta.

48 artikla

Markkinavalvontaviranomaisten yhteistoimet

1. Markkinavalvontaviranomaiset voivat sopia muiden asiaan liittyvien viranomaisten kanssa yhteistoimista, joilla pyritään varmistamaan kyberturvallisuus ja kuluttajien suojelu tiettyjen markkinoille saatettujen tai markkinoilla saataville asetettujen digitaalisia elementtejä sisältävien tuotteiden osalta, erityisesti sellaisten tuotteiden osalta, joiden havaitaan usein aiheuttavan kyberturvariskejä.

2. Komissio tai ENISA voi ehdottaa yhteistoimia, joilla markkinavalvontaviranomaiset tarkastavat tämän asetuksen vaatimusten täyttymisen, kun on viitteitä tai tietoja siitä, että tämän asetuksen soveltamisalaan kuuluvat tuotteet eivät mahdollisesti useissa jäsenvaltioissa täytä tämän asetuksen vaatimuksia.

3. Markkinavalvontaviranomaisten ja tarvittavilta osin komission on varmistettava, että sopimus yhteistoimien toteuttamisesta ei johda epäreiluun kilpailuun talouden toimijoiden välillä ja että se ei kielteisesti vaikuta sopimuksen osapuolten objektiivisuuteen, riippumattomuuteen ja puolueettomuuteen.

4. Markkinavalvontaviranomainen voi käyttää toimien tuloksena saatuja tietoja missä tahansa tutkinnassaan.

5. Kyseisen markkinavalvontaviranomaisen ja tarvittaessa komission on saatettava yhteistoimia koskeva sopimus, mukaan lukien asianomaisten osapuolten nimet, julkisesti saataville.

49 artikla

Tehotarkastukset

1. Markkinavalvontaviranomaiset voivat päättää tehdä tiettyjen digitaalisia elementtejä sisältävien tuotteiden ja tuoteryhmien samanaikaisia, koordinoituja valvontatoimia (’tehotarkastuksia’), joilla ne tarkastavat, onko tämän asetuksen säännöksiä noudatettu tai onko niitä rikottu.

2. Ellei asianomaisten markkinavalvontaviranomaisten kanssa sovita toisin, komissio vastaa tehotarkastusten koordinoinnista. Tehotarkastuksen koordinoija voi tarvittaessa julkaista yhteistulokset.

3. ENISA voi tehtäviään suorittaessaan, myös 11 artiklan 1 ja 2 kohdan mukaisesti vastaanotettujen ilmoitusten perusteella, yksilöidä tuoteryhmät, joille voidaan tehdä tehotarkastuksia. Tehotarkastuksia koskeva ehdotus on toimitettava 2 kohdassa tarkoitetulle mahdolliselle koordinaattorille markkinavalvontaviranomaisten tarkasteltavaksi.

4. Markkinavalvontaviranomaiset voivat tehotarkastuksia tehdessään käyttää 41–47 artiklassa vahvistettuja tutkintavaltuuksia ja kaikkia muita niille kansallisen oikeuden nojalla kuuluvia valtuuksia.

5. Markkinavalvontaviranomaiset voivat kutsua komission virkamiehiä ja muita komission valtuuttamia henkilöitä mukaan tehotarkastuksiin.

VI LUKU

SÄÄDÖSVALLAN SIIRTÄMINEN JA KOMITEAMENETTELY

50 artikla

Siirretyn säädösvallan käyttäminen

1. Komissiolle siirrettyä valtaa antaa delegoituja säädöksiä koskevat tässä artiklassa säädetyt edellytykset.

2. Siirretään komissiolle valta antaa 2 artiklan 4 kohdassa, 6 artiklan 2 kohdassa, 6 artiklan 3 kohdassa, 6 artiklan 5 kohdassa, 20 artiklan 5 kohdassa ja 23 artiklan 5 kohdassa tarkoitettuja delegoituja säädöksiä.

3. Euroopan parlamentti tai neuvosto voi milloin tahansa peruuttaa 2 artiklan 4 kohdassa, 6 artiklan 2 kohdassa, 6 artiklan 3 kohdassa, 6 artiklan 5 kohdassa, 20 artiklan 5 kohdassa ja 23 artiklan 5 kohdassa tarkoitetun säädösvallan siirron. Peruuttamispäätöksellä lopetetaan tuossa päätöksessä mainittu säädösvallan siirto. Peruuttaminen tulee voimaan sitä päivää seuraavana päivänä, jona sitä koskeva päätös julkaistaan *Euroopan unionin virallisessa lehdessä*, tai jonakin myöhempänä, kyseisessä päätöksessä mainittuna päivänä. Peruuttamispäätös ei vaikuta jo voimassa olevien delegoitujen säädösten pätevyyteen.

4. Ennen kuin komissio hyväksyy delegoidun säädöksen, se kuulee kunkin jäsenvaltion nimeämiä asiantuntijoita paremmasta lainsäädännöstä 13 päivänä huhtikuuta 2016 tehdyssä toimielinten välisessä sopimuksessa vahvistettujen periaatteiden mukaisesti.

5. Heti kun komissio on antanut delegoidun säädöksen, komissio antaa sen tiedoksi yhtäaikaisesti Euroopan parlamentille ja neuvostolle.

6. Edellä olevien 2 artiklan 4 kohdan, 6 artiklan 2 kohdan, 6 artiklan 3 kohdan, 6 artiklan 5 kohdan, 20 artiklan 5 kohdan ja 23 artiklan 5 kohdan nojalla annettu delegoitu säädös tulee voimaan ainoastaan, jos Euroopan parlamentti tai neuvosto ei ole kahden kuukauden kuluessa siitä, kun asianomainen säädös on annettu tiedoksi Euroopan parlamentille ja neuvostolle, ilmaissut vastustavansa sitä tai jos sekä Euroopan parlamentti että neuvosto ovat ennen mainitun määräajan päättymistä

ilmoittaneet komissiolle, että ne eivät vastusta säädöstä. Euroopan parlamentin tai neuvoston aloitteesta tätä määräaikaa jatketaan kahdella kuukaudella.

51 artikla

Komiteamenettely

1. Komissiota avustaa komitea. Tämä komitea on asetuksessa (EU) N:o 182/2011 tarkoitettu komitea.
2. Kun viitataan tähän kohtaan, sovelletaan asetuksen (EU) N:o 182/2011 5 artiklaa.
3. Kun komitean lausunto on tarkoitus hankkia kirjallista menettelyä noudattaen, tämä menettely päätetään tuloksettomana, jos komitean puheenjohtaja lausunnon antamiselle asetetussa määräajassa niin päättää tai komitean jäsen sitä pyytää.

VII LUKU

LUOTTAMUKSELLISUUS JA SEURAAMUKSET

52 artikla

Luottamuksellisuus

1. Kaikkien tämän asetuksen soveltamiseen osallistuvien osapuolten on noudatettava tehtäviään ja toimiaan suorittaessaan saamiensa tietojen ja datan luottamuksellisuutta siten, että suojellaan erityisesti
   a) teollis- ja tekijänoikeuksia ja luonnollisen henkilön tai oikeushenkilön luottamuksellisia liiketoimintatietoja tai liikesalaisuuksia, lähdekoodi mukaan lukien, lukuun ottamatta Euroopan parlamentin ja neuvoston direktiivin 2016/943[24] 5 artiklassa tarkoitettuja tapauksia;
   b) tämän asetuksen tosiasiallista täytäntöönpanoa, etenkin tarkastusten, tutkinnan ja auditointien yhteydessä;
   c) yleisiä ja kansallisia turvallisuusetuja;
   d) rikosoikeudellisten tai hallinnollisten menettelyjen luotettavuutta.
2. Markkinavalvontaviranomaisten kesken tai markkinavalvontaviranomaisten ja komission välillä luottamuksellisesti vaihdettuja tietoja ei saa paljastaa ilman tiedot luovuttaneen markkinavalvontaviranomaisen etukäteen antamaa suostumusta, sanotun kuitenkaan rajoittamatta 1 kohdan soveltamista.
3. Edellä oleva 1 ja 2 kohta eivät vaikuta komission, jäsenvaltioiden ja ilmoitettujen laitosten tiedonvaihtoa ja varoitusten antamista koskeviin oikeuksiin ja velvollisuuksiin eivätkä asianomaisten henkilöiden tiedonantovelvollisuuteen jäsenvaltioiden rikosoikeuden mukaisesti.
4. Komissio ja jäsenvaltiot voivat tarvittaessa vaihtaa arkaluonteisia tietoja sellaisten kolmansien maiden asiaan liittyvien viranomaisten kanssa, joiden kanssa ne ovat

[24] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/943, annettu 8 päivänä kesäkuuta 2016, julkistamattoman taitotiedon ja liiketoimintatiedon (liikesalaisuuksien) suojaamisesta laittomalta hankinnalta, käytöltä ja ilmaisemiselta (EUVL L 157, 15.6.2016, s. 1).

tehneet kahdenvälisiä tai monenvälisiä luottamuksellisuutta suojaavia järjestelyjä, joilla taataan riittävä suojan taso.

53 artikla

Seuraamukset

1. Jäsenvaltioiden on säädettävä seuraamuksista, joita sovelletaan, jos talouden toimijat rikkovat tämän asetuksen säännöksiä, ja toteutettava kaikki tarvittavat toimenpiteet sen varmistamiseksi, että ne pannaan täytäntöön. Seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia.

2. Jäsenvaltioiden on ilmoitettava nämä säännökset ja toimenpiteet komissiolle viipymättä, ja jäsenvaltioiden on ilmoitettava komissiolle kaikki niitä koskevat myöhemmät muutokset viipymättä.

3. Liitteessä I vahvistettujen olennaisten kyberturvavaatimusten ja 10 ja 11 artiklassa säädettyjen velvoitteiden täyttämättä jättämisestä on määrättävä hallinnollinen sakko, joka on enimmillään 15 000 000 euroa tai, jos rikkomiseen syyllistynyt on yritys, enimmillään 2,5 prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

4. Tämän asetuksen mukaisten muiden velvoitteiden laiminlyönnistä on määrättävä hallinnollinen sakko, joka on enimmillään 10 000 000 euroa tai, jos rikkomiseen syyllistynyt on yritys, enimmillään 2 prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

5. Virheellisten, puutteellisten tai harhaanjohtavien tietojen toimittamisesta vastauksena ilmoitettujen laitosten ja markkinavalvontaviranomaisten pyyntöön on määrättävä hallinnollinen sakko, joka on enimmillään 5 000 000 euroa tai, jos rikkomiseen syyllistynyt on yritys, enimmillään 1 prosentti sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

6. 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 muut markkinavalvontaviranomaiset jo määränneet hallinnollisia sakkoja samalle toimijalle samankaltaisesta rikkomisesta;

   c) rikkomiseen syyllistyneen toimijan koko ja markkinaosuus.

7. Hallinnollisia sakkoja määräävien markkinavalvontaviranomaisten on jaettava nämä tiedot muiden jäsenvaltioiden markkinavalvontaviranomaisten kanssa asetuksen (EU) 2019/1020 34 artiklassa tarkoitetun tieto- ja viestintäjärjestelmän kautta.

8. Kunkin jäsenvaltion on vahvistettava säännöt siitä, voidaanko viranomaisille tai julkishallinnon elimille määrätä kyseisessä jäsenvaltiossa hallinnollisia sakkoja ja missä määrin.

9. Jäsenvaltion oikeusjärjestelmästä riippuen hallinnollisia sakkoja koskevia sääntöjä voidaan soveltaa siten, että sakkojen määräämisestä vastaavat toimivaltaiset kansalliset tuomioistuimet tai muut elimet kansallisella tasolla kyseisissä

jäsenvaltioissa säädettyjen toimivaltuuksien mukaisesti. Tällaisten sääntöjen soveltamisella näissä jäsenvaltioissa on oltava vastaava vaikutus.

10. Hallinnollisia sakkoja voidaan määrätä kunkin yksittäisen tapauksen olosuhteista riippuen niiden muiden korjaavien tai rajoittavien toimenpiteiden lisäksi, joita markkinavalvontaviranomaiset toteuttavat saman rikkomisen johdosta.

VIII LUKU

SIIRTYMÄSÄÄNNÖKSET JA LOPPUSÄÄNNÖKSET

54 artikla

Asetuksen (EU) N:o 2019/1020 muuttaminen

Lisätään asetuksen (EU) 2019/1020 liitteeseen I kohta seuraavasti:

’71. [Asetus XXX][kyberkestävyyssäädös]’.

55 artikla

Siirtymäsäännökset

1. EU-tyyppitarkastustodistukset ja hyväksymispäätökset, jotka on annettu digitaalisia elementtejä sisältävien tuotteiden, joihin sovelletaan muuta unionin yhdenmukaistamislainsäädäntöä, kyberturvavaatimuksista, pysyvät voimassa [42 kuukautta tämän asetuksen voimaantulopäivästä], paitsi jos niiden voimassaolo päättyy ennen kyseistä ajankohtaa tai jollei muussa unionin lainsäädännössä toisin säädetä, jolloin ne pysyvät voimassa kyseisessä unionin lainsäädännössä tarkoitetulla tavalla.

2. Ennen [57 artiklassa tarkoitettu tämän asetuksen soveltamispäivä] markkinoille saatettuihin digitaalisia elementtejä sisältäviin tuotteisiin sovelletaan tämän asetuksen vaatimuksia ainoastaan, jos kyseisten tuotteiden rakenteeseen tai käyttötarkoitukseen tehdään kyseisen ajankohdan jälkeen merkittäviä muutoksia.

3. Poiketen siitä, mitä 2 kohdassa säädetään, 11 artiklassa säädettyjä velvoitteita sovelletaan kaikkiin tämän asetuksen soveltamisalaan kuuluviin digitaalisia elementtejä sisältäviin tuotteisiin, jotka on saatettu markkinoille ennen [57 artiklassa tarkoitettu tämän asetuksen soveltamispäivä].

56 artikla

Arviointi ja uudelleentarkastelu

Viimeistään [36 kuukauden kuluttua tämän asetuksen soveltamispäivästä] ja sen jälkeen joka neljäs vuosi komissio toimittaa Euroopan parlamentille ja neuvostolle kertomuksen tämän asetuksen arvioinnista ja uudelleentarkastelusta. Kertomukset julkistetaan.

57 artikla

Voimaantulo ja soveltaminen

Tämä asetus tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

Sitä sovelletaan [24 kuukauden kuluttua tämän asetuksen voimaantulosta]. Asetuksen 11 artiklaa sovelletaan kuitenkin [12 kuukauden kuluttua tämän asetuksen voimaantulopäivästä].

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

Tehty Brysselissä

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puhemies	*Puheenjohtaja*

SÄÄDÖSEHDOTUKSEEN LIITTYVÄ RAHOITUSSELVITYS

1. PERUSTIEDOT EHDOTUKSESTA/ALOITTEESTA

1.1. Ehdotuksen/aloitteen nimi

1.2. Toimintalohko(t)

1.3. Ehdotus/aloite liittyy

1.4. Tavoite (Tavoitteet)

1.4.1. Yleistavoite (Yleistavoitteet)

1.4.2. Erityistavoite (Erityistavoitteet)

1.4.3. Odotettavissa olevat tulokset ja vaikutukset

1.4.4. Tulosindikaattorit

1.5. Ehdotuksen/aloitteen perustelut

1.5.1. Tarpeet, joihin ehdotuksella/aloitteella vastataan lyhyellä tai pitkällä aikavälillä sekä aloitteen yksityiskohtainen toteutusaikataulu

1.5.2. EU:n osallistumisesta saatava lisäarvo (joka voi olla seurausta eri tekijöistä, kuten koordinoinnin paranemisesta, oikeusvarmuudesta tai toiminnan vaikuttavuuden tai täydentävyyden paranemisesta). EU:n osallistumisesta saatavalla lisäarvolla tarkoitetaan tässä kohdassa arvoa, jonka EU:n osallistuminen tuottaa sen arvon lisäksi, joka olisi saatu aikaan pelkillä jäsenvaltioiden toimilla.

1.5.3. Vastaavista toimista saadut kokemukset

1.5.4. Yhteensopivuus monivuotisen rahoituskehyksen kanssa ja mahdolliset synergiaedut suhteessa muihin kyseeseen tuleviin välineisiin

1.5.5. Arvio käytettävissä olevista rahoitusvaihtoehdoista, mukaan lukien mahdollisuudet määrärahojen uudelleenkohdentamiseen

1.6. Ehdotetun toimen/aloitteen kesto ja rahoitusvaikutukset

1.7. Hallinnointitapa (Hallinnointitavat)

2. HALLINNOINTI

2.1. Seuranta- ja raportointisäännöt

2.2. Hallinnointi- ja valvontajärjestelmä(t)

2.2.1. Perustelut ehdotetu(i)lle hallinnointitavalle(/-tavoille), rahoituksen toteutusmekanismille(/-mekanismeille), maksujärjestelyille sekä valvontastrategialle

2.2.2. Tiedot todetuista riskeistä ja niiden vähentämiseksi käyttöön otetuista sisäisistä valvontajärjestelmistä

2.2.3. Valvonnan kustannustehokkuutta (valvontakustannusten suhde hallinnoitujen varojen arvoon) koskevat arviot ja perustelut sekä arviot maksujen suoritusajankohdan ja toimen päättämisajankohdan odotetuista virheriskitasoista

2.3. Toimenpiteet petosten ja sääntöjenvastaisuuksien ehkäisemiseksi

3. EHDOTUKSEN/ALOITTEEN ARVIOIDUT RAHOITUSVAIKUTUKSET

3.1. Kyseeseen tulevat monivuotisen rahoituskehyksen otsakkeet ja menopuolen budjettikohdat

3.2. Arvioidut vaikutukset määrärahoihin

3.2.1. Yhteenveto arvioiduista vaikutuksista toimintamäärärahoihin

3.2.2. Arvioidut toimintamäärärahoista rahoitetut tuotokset

3.2.3. Yhteenveto arvioiduista vaikutuksista hallintomäärärahoihin

3.2.4. Yhteensopivuus nykyisen monivuotisen rahoituskehyksen kanssa

3.2.5. Ulkopuolisten tahojen rahoitusosuudet

3.3. Arvioidut vaikutukset tuloihin

SÄÄDÖSEHDOTUKSEEN LIITTYVÄ RAHOITUSSELVITYS

1. PERUSTIEDOT EHDOTUKSESTA/ALOITTEESTA

1.1. Ehdotuksen/aloitteen nimi

Ehdotus asetukseksi digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvavaatimuksista (kyberkestävyyssäädös)

1.2. Toimintalohko(t)

Viestintäverkot, sisällöt ja teknologia

1.3. Ehdotus/aloite liittyy

× **uuteen toimeen**

☐ **uuteen toimeen, joka perustuu pilottihankkeeseen tai valmistelutoimeen**[37]

☐ **käynnissä olevan toimen jatkamiseen**

☐ **yhden tai useamman toimen sulauttamiseen tai uudelleen suuntaamiseen johonkin toiseen/uuteen toimeen**

1.4. Tavoite (Tavoitteet)

1.4.1. Yleistavoite (Yleistavoitteet)

Sisämarkkinoiden moitteettoman toiminnan varmistamiseksi ehdotuksella on kaksi päätavoitetta: 1) **luodaan edellytykset digitaalisia elementtejä sisältävien tietoturvallisten tuotteiden kehittämiselle** varmistamalla, että laitteisto- ja ohjelmistotuotteet saatetaan markkinoille vähemmin haavoittuvuuksin ja että valmistajat suhtautuvat tietoturvaan vakavasti tuotteen koko elinkaaren ajan ja 2) **luodaan olosuhteet, joissa käyttäjät voivat ottaa kyberturvan huomioon valitessaan ja käyttäessään digitaalisia elementtejä sisältäviä tuotteita**.

1.4.2. Erityistavoite (Erityistavoitteet)

Ehdotukselle asetettiin **neljä erityistavoitetta**: i) varmistetaan, että valmistajat parantavat digitaalisia elementtejä sisältävien tuotteiden tietoturvaa suunnittelu- ja kehitysvaiheesta lähtien ja koko elinkaaren ajan, ii) luodaan johdonmukaiset kyberturvapuitteet, joissa laite- ja ohjelmistovalmistajien on helpompi noudattaa vaatimuksia, iii) lisätään läpinäkyvyyttä digitaalisia elementtejä sisältävien tuotteiden tietoturvaominaisuuksien suhteen ja iv) luodaan yrityksille ja kuluttajille edellytyksiä käyttää digitaalisia elementtejä sisältäviä tuotteita tietoturvallisesti.

Odotettavissa olevat tulokset ja vaikutukset

Selvitys siitä, miten ehdotuksella/aloitteella on tarkoitus vaikuttaa edunsaajien/kohderyhmän tilanteeseen

Ehdotuksesta koituisi merkittäviä hyötyjä eri sidosryhmille. Yritysten kannalta se estäisi sen, että digitaalisia elementtejä sisältäviin tuotteisiin alettaisiin soveltaa toisistaan poikkeavia tietoturvasääntöjä. Se vähentäisi myös asiaan liittyvän kyberturvalainsäädännön noudattamisesta aiheutuvia kustannuksia. Se vähentäisi

[37] Sellaisina kuin nämä on määritelty varainhoitoasetuksen 58 artiklan 2 kohdan a ja b alakohdassa.

kyberturvapoikkeamien määrää, poikkeamien käsittelykustannuksia ja mainehaittaa. Arvion mukaan aloite voisi koko EU:ssa alentaa yrityksiä haittaavista poikkeamista aiheutuvia kustannuksia noin 180–290 miljardilla eurolla vuodessa.[38] Se kasvattaisi liikevaihtoa, kun digitaalisia elementtejä sisältävien tuotteiden käyttö lisääntyisi. Se parantaisi eurooppalaisten yritysten mainetta maailmalla ja johtaisi myös EU:n ulkopuolelta tulevan kysynnän kasvuun. Käyttäjien kannalta parhaaksi arvioitu vaihtoehto lisäisi läpinäkyvyyttä tietoturvaominaisuuksien suhteen ja helpottaisi digitaalisia elementtejä sisältävien tuotteiden käyttöä. Myös kuluttajien ja kansalaisten perusoikeudet, kuten yksityisyyden suoja ja tietosuoja, turvattaisiin paremmin.

Samalla ehdotuksella kuitenkin lisättäisiin yrityksille, ilmoitetuille laitoksille ja viranomaisille, kuten akkreditointi- ja markkinavalvontaviranomaisille, vaatimusten noudattamisen valvonnasta ja säännösten täytäntöönpanosta aiheutuvia kustannuksia. Ohjelmistokehittäjien ja laitevalmistajien näkökulmasta ehdotus lisäisi uusien tietoturvavaatimusten sekä vaatimustenmukaisuuden arviointi-, dokumentointi- ja raportointivelvoitteiden noudattamisesta aiheutuvia suoria kustannuksia, jotka ovat yhteensä noin 29 miljardia euroa, kun arvioitu liikevaihdossa laskettu markkina-arvo on 1485 miljardia euroa.[39] Käyttäjät, kuten yrityskäyttäjät, kuluttajat ja kansalaiset, saattaisivat joutua maksamaan korkeampia hintoja digitaalisia elementtejä sisältävistä tuotteista. Tätä olisi kuitenkin tarkasteltava edellä kuvattujen merkittävien hyötyjen valossa.

1.4.3. Tulosindikaattorit

Selvitys siitä, millaisin indikaattorein ehdotuksen/aloitteen etenemistä ja tuloksia seurataan.

Sen testaamiseksi, parantavatko valmistajat digitaalisia elementtejä sisältävien tuotteidensa tietoturvaa suunnittelu- ja kehitysvaiheesta lähtien ja koko elinkaaren ajan, voitaisiin ottaa huomioon useita indikaattoreita. Näitä voisivat olla haavoittuvuuksista johtuvien merkittävien poikkeamien määrä unionissa, sellaisten laite- ja ohjelmistovalmistajien osuus, jotka käyttävät kehittämisessä koko elinkaaren kattavaa järjestelmällistä tietoturvallista lähestymistapaa, digitaalisia elementtejä sisältävien tuotteiden tietoturvan laadullinen analyysi, haavoittuvuustietokantojen määrällinen ja laadullinen analysointi, valmistajien saataville asettamien tietoturvapäivitysten tiheys tai keskimääräinen päivien lukumäärä haavoittuvuuden havaitsemisen ja tietoturvapäivitysten tarjoamisen välillä.

Kyberturvakehyksen johdonmukaisuuden indikaattori voisi olla se, että voimassa ei olisi kohdennettua tuotekohtaista kansallista kyberturvalainsäädäntöä.

Digitaalisia elementtejä sisältävien tuotteiden tietoturvaominaisuuksien läpinäkyvyyden lisääntymisen indikaattori voisi olla sellaisten digitaalisia elementtejä sisältävien tuotteiden osuus, joiden mukana toimitetaan tiedot myös tietoturvaominaisuuksista. Lisäksi sellaisten digitaalisia elementtejä sisältävien tuotteiden osuutta, jotka toimitetaan tietoturvallista käyttöä koskevien ohjeiden kanssa, voitaisiin käyttää indikaattorina siitä, annetaanko organisaatioille ja kuluttajille riittävästi edellytyksiä käyttää digitaalisia elementtejä sisältäviä tuotteita tietoturvallisesti.

38 Ks. [komission yksiköiden valmisteluasiakirja vaikutustenarviointiraportista, joka liittyy digitaalisia elementtejä sisältävien tuotteiden horisontaalisia kyberturvavaatimuksia koskevaan asetukseen].

39 Ks. [komission yksiköiden valmisteluasiakirja vaikutustenarviointiraportista, joka liittyy digitaalisia elementtejä sisältävien tuotteiden horisontaalisia kyberturvavaatimuksia koskevaan asetukseen].

Asetuksen vaikutusten seurantaa varten otettaisiin käyttöön tiettyjä indikaattoreita, joita komissio arvioisi tarvittaessa ENISAn tuella. Operatiivisesta tavoitteesta riippuen seurantaindikaattoreita, joiden perusteella horisontaalisten kyberturvavaatimusten toimivuutta arvioitaisiin, olisivat muun muassa seuraavat:

Digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuuden tason arvioinnin osalta:

- Digitaalisia elementtejä sisältäviin tuotteisiin vaikuttavien poikkeamien ja niiden käsittelyn tilastollinen ja laadullinen analyysi. Nämä tiedot voisi koota ja arvioida komissio ENISAn tuella.

- Kirjaukset tunnetuista haavoittuvuuksista ja analyysit niiden käsittelystä. Tällaisia analyysejä voisi tehdä ENISA [direktiivin XXX/XXXX (NIS2) nojalla perustetun] Euroopan haavoittuvuustietokannan pohjalta.

- Laitteistojen ja ohjelmistojen valmistajille suunnatut kyselyt edistymisen seuraamiseksi.

Tietoturvaominaisuuksia, tietoturvatukea, käyttöiän loppuvaiheen käsittelyä ja huolenpitovelvollisuutta koskevan tiedotuksen tason arvioinnin osalta: tulokset kyselyistä, joita komissio toteuttaa ENISAn tuella sekä käyttäjille että yrityksille.

Täytäntöönpanon arvioinnin osalta komissio pyrkisi varmistamaan, että vaatimustenmukaisuuden arvioinnit suoritetaan tuloksellisesti. Tätä varten esitetään standardointipyyntö ja seurataan sen toteutumista. Komissio todentaa myös ilmoitettujen laitosten ja tarvittaessa sertifiointielinten valmiudet.

Soveltamisen osalta komissio tarkastaa jäsenvaltioiden raporttien perusteella, että kansalliset aloitteet eivät koske asetuksen kattamia näkökohtia.

1.5. Ehdotuksen/aloitteen perustelut

1.5.1. Tarpeet, joihin ehdotuksella/aloitteella vastataan lyhyellä tai pitkällä aikavälillä sekä aloitteen yksityiskohtainen toteutusaikataulu

Asetusta on määrä soveltaa täysimääräisesti 24 kuukauden kuluttua sen voimaantulosta. Hallintorakenteen osatekijöiden olisi kuitenkin oltava käytössä jo ennen sitä. Jäsenvaltioiden on varsinkin nimettävä jo olemassa olevat viranomaiset ja/tai perustettava uudet viranomaistahot hoitamaan lainsäädännössä säädettyjä tehtäviä.

1.5.2. EU:n osallistumisesta saatava lisäarvo (joka voi olla seurausta eri tekijöistä, kuten koordinoinnin paranemisesta, oikeusvarmuudesta tai toiminnan vaikuttavuuden tai täydentävyyden paranemisesta). EU:n osallistumisesta saatavalla lisäarvolla tarkoitetaan tässä kohdassa arvoa, jonka EU:n osallistuminen tuottaa sen arvon lisäksi, joka olisi saatu aikaan pelkillä jäsenvaltioiden toimilla.

Kyberturvallisuuden selkeästi rajat ylittävä luonne ja lisääntyvät poikkeamat, joilla on heijastusvaikutuksia yli maiden, toimialojen ja tuotteiden rajojen, merkitsevät, että jäsenvaltiot eivät voi saavuttaa tavoitteita tuloksellisesti yksin. Koska digitaalisia elementtejä sisältävien tuotteiden markkinat ovat maailmanlaajuiset, jäsenvaltiot kohtaavat kaikki alueellaan samoja riskejä samojen digitaalisia elementtejä sisältävien tuotteiden osalta. Kehittymässä oleva hajanainen, mahdollisesti toisistaan poikkeavista kansallisista säännöistä syntyvä ympäristö saattaa myös haitata

digitaalisia elementtejä sisältävien tuotteiden avoimia ja kilpailtuja sisämarkkinoita. Näin ollen tarvitaan EU:n tason yhteisiä toimia käyttäjien luottamuksen lisäämiseksi ja digitaalisia elementtejä sisältävien EU-lähtöisten tuotteiden houkuttelevuuden lisäämiseksi. Tämä hyödyttäisi myös sisämarkkinoita tarjoamalla oikeusvarmuutta ja luomalla tasapuoliset toimintaedellytykset digitaalisia elementtejä sisältävien tuotteiden myyjille.

1.5.3. Vastaavista toimista saadut kokemukset

Kyberkestävyyssäädös on laatuaan ensimmäinen säädös, jolla asetetaan kyberturvavaatimuksia digitaalisia elementtejä sisältävien tuotteiden markkinoille saattamiselle. Se perustuu kuitenkin uuteen lainsäädäntökehykseen (*New Legislative Framework*, NLF) ja eri tuotteita koskevan voimassa olevan unionin yhdenmukaistamislainsäädännön täytäntöönpanosta saatuihin kokemuksiin, erityisesti täytäntöönpanon valmistelun osalta, mukaan lukien yhdenmukaistettujen standardien valmistelun kaltaiset näkökohdat.

1.5.4. Yhteensopivuus monivuotisen rahoituskehyksen kanssa ja mahdolliset synergiaedut suhteessa muihin kyseeseen tuleviin välineisiin

Digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvavaatimuksista annettavassa asetuksessa määritellään kaikille EU:n markkinoille saatetuille digitaalisia elementtejä sisältäville tuotteille uudet kyberturvavaatimukset, jotka menevät voimassa olevassa lainsäädännössä säädettyjä vaatimuksia pidemmälle. Samalla ehdotus perustuu uutta lainsäädäntökehystä noudattavaan nykyiseen lainsäädäntöön. Sen vuoksi se perustuisi olemassa oleviin uuden lainsäädäntökehyksen rakenteisiin ja menettelyihin, kuten ilmoitettujen laitosten yhteistyöhön ja markkinavalvontaan, vaatimustenmukaisuuden arviointimoduuleihin ja yhdenmukaistettujen standardien kehittämiseen. Uusi ehdotus perustuisi myös joihinkin rakenteisiin, joita on kehitetty muun kyberturvalainsäädännön, kuten direktiivin 2016/1148 (verkko- ja tietoturvadirektiivi, NIS), [direktiivin XXX/XXXX (NIS2)] tai asetuksen 2019/881 (kyberturvasäädös) mukaisesti.

1.5.5. Arvio käytettävissä olevista rahoitusvaihtoehdoista, mukaan lukien mahdollisuudet määrärahojen uudelleenkohdentamiseen

ENISAlle osoitettujen toiminta-alojen hallinnointi sopii yhteen sen nykyisen mandaatin ja yleisten tehtävien kanssa. Nämä toiminta-alat voivat edellyttää erityisiä osaamisprofiileja tai uusia toimeksiantoja, mutta ne eivät olisi merkittäviä, ja ne voidaan hoitaa ENISAn nykyisillä resursseilla ja kohdentamalla uudelleen tai yhdistämällä eri tehtäviä. Yksi ENISAlle osoitetuista tärkeimmistä toiminta-aloista on esimerkiksi hyödynnettyjä tuotteiden haavoittuvuuksia koskevien valmistajilta saatujen ilmoitusten kerääminen ja käsittely. [Direktiivillä XXX/XXXX (NIS2)] on jo annettu ENISAlle tehtäväksi perustaa Euroopan haavoittuvuustietokanta, johon voidaan vapaaehtoisesti ilmoittaa ja rekisteröidä julkisesti tunnettuja haavoittuvuuksia, jotta käyttäjät voivat toteuttaa asianmukaisia lieventäviä toimenpiteitä. Tähän tarkoitukseen osoitettuja resursseja voitaisiin käyttää myös edellä mainittuihin uusiin toimeksiantoihin, jotka liittyvät tuotteiden haavoittuvuutta koskeviin ilmoituksiin. Näin voitaisiin varmistaa olemassa olevien resurssien tehokas käyttö ja luoda tällaisten toimeksiantojen välille tarvittavia synergioita, joiden avulla voidaan paremmin hyödyntää kyberturvariskejä ja -uhkia koskevia ENISAn analyyseja.

1.6. Ehdotetun toimen/aloitteen kesto ja rahoitusvaikutukset

☐ **kesto on rajattu**

– ☐ toiminta alkaa [PP/KK]VVVV ja päättyy [PP/KK]VVVV.

– ☐ maksusitoumusmäärärahoihin kohdistuvat rahoitusvaikutukset koskevat vuosia YYYY–YYYY ja maksumäärärahoihin kohdistuvat rahoitusvaikutukset vuosia YYYY–YYYY.

× **kestoa ei ole rajattu**

– Käynnistysvaihe alkaa vuonna 2025,

– minkä jälkeen toteutus täydessä laajuudessa.

1.7. Hallinnointitapa (Hallinnointitavat)[40]

☐ **Suora hallinnointi**, jonka komissio toteuttaa käyttämällä

– × yksiköitään, myös unionin edustustoissa olevaa henkilöstöään

– ☐ toimeenpanovirastoja

☐ **Hallinnointi yhteistyössä** jäsenvaltioiden kanssa

☐ **Välillinen hallinnointi**, jossa täytäntöönpanotehtäviä on siirretty

– ☐ kolmansille maille tai niiden nimeämille elimille

– ☐ kansainvälisille järjestöille ja niiden erityisjärjestöille (tarkennettava)

– ☐ Euroopan investointipankille tai Euroopan investointirahastolle

– ☐ varainhoitoasetuksen 70 ja 71 artiklassa tarkoitetuille elimille

– ☐ julkisoikeudellisille yhteisöille

– ☐ sellaisille julkisen palvelun tehtäviä hoitaville yksityisoikeudellisille elimille, joille annetaan riittävät rahoitustakuut

– ☐ sellaisille jäsenvaltion yksityisoikeuden mukaisille elimille, joille on annettu tehtäväksi julkisen ja yksityisen sektorin kumppanuuden täytäntöönpano ja joille annetaan riittävät rahoitustakuut

– ☐ henkilöille, joille on annettu tehtäväksi toteuttaa SEU-sopimuksen V osaston mukaisia yhteisen ulko- ja turvallisuuspolitiikan erityistoimia ja jotka nimetään asiaa koskevassa perussäädöksessä.

– *Jos käytetään useampaa kuin yhtä hallinnointitapaa, olisi annettava lisätietoja kohdassa ”Huomautukset”.*

Huomautukset

Tässä asetuksessa ENISAlle osoitetaan tiettyjä toimia sen nykyisen toimeksiannon mukaisesti ja noudattaen erityisesti asetuksen (EU) 2019/881 3 artiklan 2 kohtaa, jonka mukaan ENISAn olisi hoidettava sille sellaisissa unionin säädöksissä annetut tehtävät, joissa vahvistetaan toimenpiteitä kyberturvallisuuteen liittyvien jäsenvaltioiden lakien, asetusten ja hallinnollisten määräysten lähentämiseksi. ENISAlle annetaan erityisesti tehtäväksi vastaanottaa valmistajilta ilmoituksia aktiivisesti hyödynnetyistä digitaalisia elementtejä sisältäviin

[40] Kuvaukset eri hallinnointitavoista ja viittaukset varainhoitoasetukseen ovat saatavilla budjettipääosaston verkkosivuilla osoitteessa https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

tuotteisiin sisältyvistä haavoittuvuuksista sekä poikkeamista, jotka vaikuttavat kyseisten tuotteiden tietoturvaan. ENISAn olisi myös toimitettava nämä ilmoitukset edelleen asiaan liittyville tietoturvaloukkauksiin reagoiville ryhmille (CSIRT-toimijat) tai direktiivin [direktiivin XXX/XXXX (NIS2)] [X artiklan] mukaisesti nimetyille jäsenvaltioiden keskitetyille yhteysvirastoille ja ilmoitettava asiasta markkinavalvontaviranomaisille. ENISAn olisi keräämiensä tietojen perusteella laadittava joka toinen vuosi tekninen raportti digitaalisia elementtejä sisältävien tuotteiden kyberturvariskien uusista suuntauksista ja toimitettava se verkko- ja tietoturva-alan yhteistyöryhmälle. Lisäksi kun otetaan huomioon ENISAn asiantuntemus, sen keräämä informaatio ja sen tekemät uhka-analyysit, ENISA voi tukea tämän asetuksen täytäntöönpanoa ehdottamalla kansallisten markkinavalvontaviranomaisten yhteisiä toimia saatuaan tietoa digitaalisia elementtejä sisältävien tuotteiden mahdollisista tämän asetuksen vastaisuuksista, joita ilmenee useissa jäsenvaltioissa, tai määrittää tuoteluokkia, joiden osalta voidaan järjestää samanaikaisia koordinoituja valvontatoimia. Komissio voi pyytää ENISAa suorittamaan poikkeuksellisissa olosuhteissa arviointeja tietyistä digitaalisia elementtejä sisältävistä tuotteista, jotka aiheuttavat merkittävän kyberturvariskin ja joiden suhteen tarvitaan välittömiä toimia sisämarkkinoiden moitteettoman toiminnan ylläpitämiseksi.

Kaikkien näiden toimeksiantojen arvioidaan edellyttävän noin 4,5 kokoaikavastaavaa ENISAn nykyisistä resursseista. Ne perustuvat ENISAn nykyiseen asiantuntemukseen ja valmistelutyöhön, jota ENISA tekee tällä hetkellä muun muassa tukeakseen [direktiivin XXX/XXXX (NIS2)] tulevaa täytäntöönpanoa, jonka osalta ENISAn resursseja on täydennetty.

2. HALLINNOINTI

2.1. Seuranta- ja raportointisäännöt

Ilmoitetaan sovellettavat aikavälit ja edellytykset.

Viimeistään 36 kuukauden kuluttua tämän asetuksen soveltamispäivästä ja sen jälkeen joka neljäs vuosi komissio toimittaa Euroopan parlamentille ja neuvostolle kertomuksen asetuksen arvioinnista ja uudelleentarkastelusta. Kertomukset julkistetaan.

2.2. Hallinnointi- ja valvontajärjestelmä(t)

2.2.1. Perustelut ehdotetu(i)lle hallinnointitavalle(/-tavoille), rahoituksen toteutusmekanismille(/-mekanismeille), maksujärjestelyille sekä valvontastrategialle

Asetuksella luodaan uusi toimintapolitiikka, joka koskee koko elinkaaren aikaisia yhdenmukaistettuja kyberturvavaatimuksia digitaalisia elementtejä sisältäville, sisämarkkinoille saatettaville tuotteille. Säädöksen hyväksymisen jälkeen komissio pyytää eurooppalaisia standardointielimiä laatimaan standardeja.

Näiden uusien tehtävien hoitamiseksi komission yksiköille pitää antaa tarvittavat resurssit. Uuden asetuksen täytäntöönpanon valvonnan arvioidaan edellyttävän 7 kokoaikavastaavaa (joista yksi on kansallinen asiantuntija) hoitamaan seuraavat tehtävät:

– Standardointipyynnön ja/tai jos onnistunutta standardointiprosessia ei ole, täytäntöönpanosäädöksillä vahvistettavien yhteisten eritelmien valmistelu.

– Digitaalisia elementtejä sisältävien kriittisten tuotteiden määritelmät täsmentävän delegoidun säädöksen valmistelu [12 kuukauden kuluessa asetuksen voimaantulosta].

– Sellaisten delegoitujen säädösten mahdollinen valmistelu, joilla päivitetään luokkaan I ja II kuuluvien kriittisten tuotteiden luetteloa; täsmennetään, onko rajoitus tai poissulkeminen tarpeen sellaisten digitaalisia elementtejä sisältävien tuotteiden osalta, jotka kuuluvat muiden sellaisten unionin sääntöjen soveltamisalaan, joissa vahvistetaan vaatimukset, joilla saavutetaan sama suojelun taso kuin tässä asetuksessa; säädetään tässä asetuksessa vahvistettujen kriteerien perusteella pakolliseksi tiettyjen erittäin kriittisten digitaalisia elementtejä sisältävien tuotteiden sertifiointi; ja täsmennetään EU-vaatimustenmukaisuusvakuutuksen vähimmäissisältöä ja täydennetään teknisiin asiakirjoihin sisällytettäviä tekijöitä.

– Sellaisten täytäntöönpanosäädösten mahdollinen valmistelu, jotka liittyvät raportointivelvoitteiden täyttämisen muotoon tai osatekijöihin ja ohjelmistosisältöluetteloon, yhteisiin eritelmiin tai CE-merkinnän kiinnittämiseen.

– Korjaavia tai rajoittava toimia koskevan välittömän intervention mahdollinen valmistelu poikkeuksellisissa olosuhteissa sisämarkkinoiden moitteettoman toiminnan ylläpitämiseksi, mukaan lukien täytäntöönpanosäädöksen valmistelu.

– Jäsenvaltioiden ja ilmoitettujen laitosten tekemien ilmoitusten organisointi ja koordinointi ja ilmoitettujen laitosten toiminnan koordinointi.

– Jäsenvaltioiden markkinavalvontaviranomaisten toiminnan koordinoinnin tukeminen.

2.2.2. Tiedot todetuista riskeistä ja niiden vähentämiseksi käyttöön otetuista sisäisistä valvontajärjestelmistä

Sen varmistamiseksi, että ilmoitetut laitokset ja markkinavalvontaviranomaiset vaihtavat tietoja ja tekevät hyvää yhteistyötä, niiden toiminnan koordinointi annetaan komission tehtäväksi. Teknistä asiantuntemusta ja markkinatuntemusta varten perustettaisiin asiantuntijaryhmä.

2.2.3. Valvonnan kustannustehokkuutta (valvontakustannusten suhde hallinnoitujen varojen arvoon) koskevat arviot ja perustelut sekä arviot maksujen suoritusajankohdan ja toimen päättämisajankohdan odotetuista virheriskitasoista

2.3. Kun otetaan huomioon kokouskulujen alhainen arvo tapahtumaa kohden (esim. kokousedustajan matkakulujen korvaaminen), tavanomaiset valvontamenettelyt vaikuttavat riittäviltä. Toimenpiteet petosten ja sääntöjenvastaisuuksien ehkäisemiseksi

Ilmoitetaan käytössä olevat ja suunnitellut ehkäisy- ja suojatoimenpiteet, esimerkiksi petostentorjuntastrategian pohjalta

Komissioon nykyisin sovellettavat petostentorjunnan toimenpiteet kattavat tämän asetuksen soveltamiseksi tarvittavat lisämäärärahat.

3. EHDOTUKSEN/ALOITTEEN ARVIOIDUT RAHOITUSVAIKUTUKSET

3.1. Kyseeseen tulevat monivuotisen rahoituskehyksen otsakkeet ja menopuolen budjettikohdat

- Talousarviossa jo olevat budjettikohdat

Malli

- Uudet perustettaviksi esitetyt budjettikohdat

Ei sovelleta

3.2. Arvioidut vaikutukset määrärahoihin

3.2.1. Yhteenveto arvioiduista vaikutuksista toimintamäärärahoihin

– ☑ Ehdotus/aloite ei edellytä toimintamäärärahoja.

– ☐ Ehdotus/aloite edellyttää toimintamäärärahoja seuraavasti:

milj. euroa (kolmen desimaalin tarkkuudella)

Monivuotisen rahoituskehyksen otsake	Numero	

PÄÄOSASTO: <…….>			Vuosi **N**[41]	Vuosi **N+1**	Vuosi **N+2**	Vuosi **N+3**	ja näitä seuraavat vuodet (ilmoitetaan kaikki vuodet, joille ehdotuksen/aloitteen vaikutukset ulottuvat, ks. kohta 1.6)			**YHTEENSÄ**
• Toimintamäärärahat										
Budjettikohta[42]	Sitoumukset	(1a)								
	Maksut	(2a)								
Budjettikohta	Sitoumukset	(1b)								
	Maksut	(2b)								
Tiettyjen ohjelmien määrärahoista katettavat hallintomäärärahat[43]										
Budjettikohta		(3)								
PO <…....>:n määrärahat YHTEENSÄ	Sitoumukset	=1a+1b +3								
	Maksut	=2a+2b								

41 Vuosi N on ehdotuksen/aloitteen toteutuksen aloitusvuosi. ”N” korvataan oletetulla ensimmäisellä toteutusvuodella (esimerkiksi: 2021). Seuraavat vuodet täydennetään vastaavasti.

42 Virallisen budjettinimikkeistön mukaisesti.

43 Tekninen ja/tai hallinnollinen apu sekä EU:n ohjelmien ja/tai toimien toteuttamiseen liittyvät tukimenot (entiset BA-budjettikohdat), epäsuora ja suora tutkimustoiminta.

		+3								

• Toimintamäärärahat YHTEENSÄ	Sitoumukset	(4)								
	Maksut	(5)								
• Tiettyjen ohjelmien määrärahoista katettavat hallintomäärärahat YHTEENSÄ		(6)								
Monivuotisen rahoituskehyksen **OTSAKKEESEEN** <….> **kuuluvat määrärahat YHTEENSÄ**	Sitoumukset	=4+6								
	Maksut	=5+6								

Jos ehdotuksella/aloitteella on vaikutuksia useampaan otsakkeeseen, toistetaan edellä oleva osa:

• Toimintamäärärahat (kaikki otsakkeet) YHTEENSÄ	Sitoumukset	(4)								
	Maksut	(5)								
Tiettyjen ohjelmien määrärahoista katettavat hallintomäärärahat (kaikki otsakkeet) YHTEENSÄ		(6)								
Monivuotisen rahoituskehyksen **OTSAKKEISIIN 1–6 kuuluvat määrärahat YHTEENSÄ** (Rahoitusohje)	Sitoumukset	=4+6								
	Maksut	=5+6								

Monivuotisen rahoituskehyksen otsake	**7**	”Hallintomenot”

Tämän osan täyttämisessä on käytettävä rahoitusselvityksen liitteessä (sisäisten sääntöjen liite V) olevaa hallintomäärärahoja koskevaa selvitystä, joka on laadittava ennen rahoitusselvityksen laatimista. Liite ladataan DECIDE-tietokantaan komission sisäistä lausuntokierrosta varten.

milj. euroa (kolmen desimaalin tarkkuudella)

		Vuosi **2024**	Vuosi **2025**	Vuosi **2026**	Vuosi **2027**	**YHTEENSÄ**
PÄÄOSASTO: CNECT						
• Henkilöresurssit		1,030	1,030	1,030	1,030	**4,120**
• Muut hallintomenot		**0,222**	**0,222**	**0,222**	**0,222**	**0,888**
PO CNECT **YHTEENSÄ**	Määrärahat	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

Monivuotisen rahoituskehyksen **OTSAKKEESEEN 7 kuuluvat määrärahat YHTEENSÄ**	(Sitoumukset yhteensä = maksut yhteensä)	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

milj. euroa (kolmen desimaalin tarkkuudella)

		Vuosi **2024**	Vuosi **2025**	Vuosi **2026**	Vuosi **2027**	**YHTEENSÄ**
Monivuotisen rahoituskehyksen **OTSAKKEISIIN 1–7 kuuluvat määrärahat YHTEENSÄ**	Sitoumukset	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**
	Maksut	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

3.2.2. Arvioidut toimintamäärärahoista rahoitetut tuotokset

maksusitoumusmäärärahat, milj. euroa (kolmen desimaalin tarkkuudella)

Tavoitteet ja tuotokset			Vuosi **N**		Vuosi **N+1**		Vuosi **N+2**		Vuosi **N+3**		ja näitä seuraavat vuodet (ilmoitetaan kaikki vuodet, joille ehdotuksen/aloitteen vaikutukset ulottuvat, ks. kohta 1.6)						**YHTEENSÄ**	
	TUOTOKSET																	
⇩	Tyyppi[44]	Keski määr. kustannukset	Lukumäärä	Kustannus	Lukumäärä	Kustannus	Lukumäärä	Kustannus	Lukumäärä	Kustannus	Lukumäärä	Kustannus	Lukumäärä	Kustannus	Lukumäärä	Kustannus	Lukumäärä yhteensä	Kustannukset yhteensä
ERITYISTAVOITE 1[45]…																		
- Tuotos																		
- Tuotos																		
- Tuotos																		
Välisumma, erityistavoite 1																		
ERITYISTAVOITE 2 ...																		
- Tuotos																		
Välisumma, erityistavoite 2																		
KAIKKI YHTEENSÄ																		

[44] Tuotokset ovat tuloksena olevia tuotteita ja palveluita (esim. rahoitettujen opiskelijavaihtojen määrä tai rakennetut tiekilometrit).

[45] Kuten kuvattu kohdassa 1.4.2 ’Erityistavoitteet...’

3.2.3. Yhteenveto arvioiduista vaikutuksista hallintomäärärahoihin

– ☐ Ehdotus/aloite ei edellytä hallintomäärärahoja.

– ☑ Ehdotus/aloite edellyttää hallintomäärärahoja seuraavasti:

milj. euroa (kolmen desimaalin tarkkuudella)

	Vuosi **2024**	Vuosi **2025**	Vuosi **2026**	Vuosi **2027**	
Monivuotisen rahoitus-kehyksen OTSAKE 7					
Henkilöresurssit	1,030	1,030	1,030	1,030	**4,120**
Muut hallintomenot	0,222	0,222	0,222	0,222	**0,888**
Monivuotisen rahoitus-kehyksen OTSAKE 7, välisumma	1,252	1,252	1,252	1,252	**5,008**

Monivuotisen rahoitus-kehyksen OTSAK-KEESEEN 7 sisältymättömät, välisumma[46]					
Henkilöresurssit					
Muut hallintomenot					
Monivuotisen rahoitus-kehyksen OTSAK-KEESEEN 7 sisältymättömät, välisumma					

YHTEENSÄ	1,252	1,252	1,252	1,252	**5,008**

Henkilöresursseja ja muita hallintomenoja koskeva määrärahatarve katetaan toimen hallinnointiin jo osoitetuilla pääosaston määrärahoilla ja/tai pääosastossa toteutettujen uudelleenjärjestelyjen tuloksena saaduilla määrärahoilla sekä tarvittaessa sellaisilla lisäresursseilla, jotka toimea hallinnoiva pääosasto voi saada käyttöönsä vuotuisessa määrärahojen jakomenettelyssä talousarvion puitteissa.

46 Tekninen ja/tai hallinnollinen apu sekä EU:n ohjelmien ja/tai toimien toteuttamiseen liittyvät tukimenot (entiset BA-budjettikohdat), epäsuora ja suora tutkimustoiminta.

3.2.3.1. Henkilöresurssien arvioitu tarve

– ☐ Ehdotus/aloite ei edellytä henkilöresursseja.

– ☑ Ehdotus/aloite edellyttää henkilöresursseja seuraavasti:

Arvio kokoaikaiseksi henkilöstöksi muutettuna

		Vuosi **2024**	Vuosi **2025**	Vuosi **2026**	Vuosi **2027**
20 01 02 01 (päätoimipaikka ja komission edustustot EU:ssa)		6	6	6	6
20 01 02 03 (EU:n ulkopuoliset edustustot)					
01 01 01 01 (epäsuora tutkimustoiminta)					
01 01 01 11 (suora tutkimustoiminta)					
Muu budjettikohta (mikä?)					
• **Ulkopuolinen henkilöstö (kokoaikaiseksi muutettuna)**[47]					
20 02 01 (kokonaismäärärahoista katettavat sopimussuhteiset toimihenkilöt, kansalliset asiantuntijat ja vuokrahenkilöstö)		1	1	1	1
20 02 03 (sopimussuhteiset ja paikalliset toimihenkilöt, kansalliset asiantuntijat, vuokrahenkilöstö ja nuoremmat asiantuntijat EU:n ulkopuolisissa edustustoissa)					
XX 01 xx **yy zz** [48]	- Päätoimipaikassa				
	- EU:n ulkopuolisissa edustustoissa				
01 01 01 02 (sopimussuhteiset toimihenkilöt, kansalliset asiantuntijat ja vuokrahenkilöstö - epäsuora tutkimustoiminta)					
01 01 01 12 (sopimussuhteiset toimihenkilöt, kansalliset asiantuntijat ja vuokrahenkilöstö - suora tutkimustoiminta)					
Muu budjettikohta (mikä?)					
YHTEENSÄ		**7**	**7**	**7**	**7**

XX viittaa kyseessä olevaan toimintalohkoon eli talousarvion osastoon.

Henkilöresurssien tarve katetaan toimen hallinnointiin jo osoitetulla pääosaston henkilöstöllä ja/tai pääosastossa toteutettujen henkilöstön uudelleenjärjestelyjen tuloksena saadulla henkilöstöllä sekä tarvittaessa sellaisilla lisäresursseilla, jotka toimea hallinnoiva pääosasto voi saada käyttöönsä vuotuisessa määrärahojen jakomenettelyssä talousarvion puitteissa.

Kuvaus henkilöstön tehtävistä:

Virkamiehet ja väliaikaiset toimihenkilöt 6 kokoaikaista työntekijää x	Kuten kohdassa 2.2.1 kuvataan: – Standardointipyynnön ja/tai jos onnistunutta standardointiprosessia ei ole, täytäntöönpanosäädöksillä vahvistettavien yhteisten eritelmien valmistelu.

[47] Sopimussuhteiset toimihenkilöt, paikalliset toimihenkilöt, kansalliset asiantuntijat, vuokrahenkilöstö ja nuoremmat asiantuntijat EU:n ulkopuolisissa edustustoissa.

[48] Toimintamäärärahoista katettavan ulkopuolisen henkilöstön enimmäismäärä (entiset BA-budjettikohdat).

157 000 euroa/vuosi = 942 000 euroa	– Digitaalisia elementtejä sisältävien kriittisten tuotteiden määritelmät täsmentävän delegoidun säädöksen valmistelu [12 kuukauden kuluessa asetuksen voimaantulosta]. – Sellaisten delegoitujen säädösten mahdollinen valmistelu, joilla päivitetään luokkaan I ja II kuuluvien kriittisten tuotteiden luetteloa; täsmennetään, onko rajoitus tai poissulkeminen tarpeen sellaisten digitaalisia elementtejä sisältävien tuotteiden osalta, jotka kuuluvat muiden sellaisten unionin sääntöjen soveltamisalaan, joissa vahvistetaan vaatimukset, joilla saavutetaan sama suojelun taso kuin tässä asetuksessa; säädetään tässä asetuksessa vahvistettujen kriteerien perusteella pakolliseksi tiettyjen erittäin kriittisten digitaalisia elementtejä sisältävien tuotteiden sertifiointi; ja täsmennetään EU-vaatimustenmukaisuusvakuutuksen vähimmäissisältöä ja täydennetään teknisiin asiakirjoihin sisällytettäviä tekijöitä. – Sellaisten täytäntöönpanosäädösten mahdollinen valmistelu, jotka liittyvät raportointivelvoitteiden täyttämisen muotoon tai osatekijöihin ja ohjelmistosisältöluetteloon, yhteisiin eritelmiin tai CE-merkinnän kiinnittämiseen. – Korjaavia tai rajoittava toimia koskevan välittömän intervention mahdollinen valmistelu poikkeuksellisissa olosuhteissa sisämarkkinoiden moitteettoman toiminnan ylläpitämiseksi, mukaan lukien täytäntöönpanosäädöksen valmistelu. – Jäsenvaltioiden ja ilmoitettujen laitosten tekemien ilmoitusten organisointi ja koordinointi ja ilmoitettujen laitosten toiminnan koordinointi. – Jäsenvaltioiden markkinavalvontaviranomaisten toiminnan koordinoinnin tukeminen.
Ulkopuolinen henkilöstö 1 kansallinen asiantuntija x 88 000 euroa/vuosi	Kuten kohdassa 2.2.1 kuvataan: – Standardointipyynnön ja/tai jos onnistunutta standardointiprosessia ei ole, täytäntöönpanosäädöksillä vahvistettavien yhteisten eritelmien valmistelu. – Digitaalisia elementtejä sisältävien kriittisten tuotteiden määritelmät täsmentävän delegoidun säädöksen valmistelu [12 kuukauden kuluessa asetuksen voimaantulosta]. – Sellaisten delegoitujen säädösten mahdollinen valmistelu, joilla päivitetään luokkaan I ja II kuuluvien kriittisten tuotteiden luetteloa; täsmennetään, onko rajoitus tai poissulkeminen tarpeen sellaisten digitaalisia elementtejä sisältävien tuotteiden osalta, jotka kuuluvat muiden sellaisten unionin sääntöjen soveltamisalaan, joissa vahvistetaan vaatimukset, joilla saavutetaan sama suojelun taso kuin tässä asetuksessa; säädetään tässä asetuksessa vahvistettujen kriteerien perusteella pakolliseksi tiettyjen erittäin kriittisten digitaalisia elementtejä sisältävien tuotteiden sertifiointi; ja täsmennetään EU-vaatimustenmukaisuusvakuutuksen vähimmäissisältöä ja täydennetään teknisiin asiakirjoihin sisällytettäviä tekijöitä. – Sellaisten täytäntöönpanosäädösten mahdollinen valmistelu, jotka liittyvät raportointivelvoitteiden täyttämisen muotoon tai osatekijöihin ja ohjelmistosisältöluetteloon, yhteisiin eritelmiin tai CE-merkinnän kiinnittämiseen.

	– Korjaavia tai rajoittava toimia koskevan välittömän intervention mahdollinen valmistelu poikkeuksellisissa olosuhteissa sisämarkkinoiden moitteettoman toiminnan ylläpitämiseksi, mukaan lukien täytäntöönpanosäädöksen valmistelu. – Jäsenvaltioiden ja ilmoitettujen laitosten tekemien ilmoitusten organisointi ja koordinointi ja ilmoitettujen laitosten toiminnan koordinointi. – Jäsenvaltioiden markkinavalvontaviranomaisten toiminnan koordinoinnin tukeminen.

3.2.4. Yhteensopivuus nykyisen monivuotisen rahoituskehyksen kanssa

Ehdotus/aloite

– x voidaan rahoittaa kokonaan kohdentamalla menoja uudelleen monivuotisen rahoituskehyksen kyseisen otsakkeen sisällä.

Rahoitussuunnitelmaan ei tarvita muutoksia.

– ☐ edellyttää monivuotisen rahoituskehyksen kyseiseen otsakkeeseen sisältyvän kohdentamattoman liikkumavaran ja/tai monivuotista rahoituskehystä koskevassa asetuksessa määriteltyjen erityisvälineiden käyttöä.

-

– ☐ edellyttää monivuotisen rahoituskehyksen tarkistamista.

-

3.2.5. Ulkopuolisten tahojen rahoitusosuudet

Ehdotuksen/aloitteen

– x rahoittamiseen ei osallistu ulkopuolisia tahoja

– ☐ rahoittamiseen osallistuu ulkopuolisia tahoja seuraavasti (arvio):

Määrärahat, milj. euroa (kolmen desimaalin tarkkuudella)

	Vuosi **N**[49]	Vuosi **N+1**	Vuosi **N+2**	Vuosi **N+3**	ja näitä seuraavat vuodet (ilmoitetaan kaikki vuodet, joille ehdotuksen/aloitteen vaikutukset ulottuvat, ks. kohta 1.6)			Yhteensä
Rahoitukseen osallistuva taho								
Yhteisrahoituksella katettavat määrärahat YHTEENSÄ								

[49] Vuosi N on ehdotuksen/aloitteen toteutuksen aloitusvuosi. ”N” korvataan oletetulla ensimmäisellä toteutusvuodella (esimerkiksi: 2021). Seuraavat vuodet täydennetään vastaavasti.

3.3. Arvioidut vaikutukset tuloihin

– ☐ Ehdotuksella/aloitteella ei ole vaikutuksia tuloihin.

– ☐ Ehdotuksella/aloitteella on vaikutuksia tuloihin seuraavasti:

  – ☐ vaikutukset omiin varoihin

  – ☐ vaikutukset muihin tuloihin

  – tulot on kohdennettu menopuolen budjettikohtiin ☐

milj. euroa (kolmen desimaalin tarkkuudella)

Tulopuolen budjettikohta:	Käytettävissä olevat määrärahat kuluvana varainhoitovuonna	Ehdotuksen/aloitteen vaikutus[50]						
		Vuosi **N**	Vuosi **N+1**	Vuosi **N+2**	Vuosi **N+3**	ja näitä seuraavat vuodet (ilmoitetaan kaikki vuodet, joille ehdotuksen/aloitteen vaikutukset ulottuvat, ks. kohta 1.6)		
Momentti ….								

Vastaava(t) menopuolen budjettikohta (budjettikohdat) käyttötarkoitukseensa sidottujen tulojen tapauksessa:

Muita huomautuksia (esim. tuloihin kohdistuvan vaikutuksen laskentamenetelmä/-kaava tai muita lisätietoja).

[50] Perinteiset omat varat (tulli- ja sokerimaksut) on ilmoitettava nettomääräisinä eli bruttomäärästä on vähennettävä kantokuluja vastaava 20 prosentin osuus.