EUROOPAN UNIONI

EUROOPAN PARLAMENTTI **NEUVOSTO**

Bryssel, 25. syyskuuta 2024
(OR. en)

2022/0272(COD) **PE-CONS 100/23**

CYBER 328
JAI 1731
DATAPROTECT 391
TELECOM 409
MI 1168
CSC 579
CSCI 215
CODEC 2601

SÄÄDÖKSET JA MUUT VÄLINEET

Asia:	EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) N:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta (kyberkestävyyssäädös)

EUROOPAN PARLAMENTIN JA NEUVOSTON
ASETUS (EU) 2024/…,

annettu … päivänä …kuuta …,

digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) N:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta (kyberkestävyyssäädös)

(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],

ovat kuulleet alueiden komiteaa,

noudattavat tavallista lainsäätämisjärjestystä[2],

---

1 EUVL C 100, 16.3.2023, s. 101.

2 Euroopan parlamentin kanta, vahvistettu 12. maaliskuuta 2024 (ei vielä julkaistu virallisessa lehdessä), ja neuvoston päätös, tehty ....

sekä katsovat seuraavaa:

(1) Kyberturvallisuus on yksi unionin keskeisistä haasteista. Tulevina vuosina verkkoon liitettyjen laitteiden määrä ja valikoima lisääntyvät räjähdysmäisesti. Kyberhyökkäykset ovat yleistä etua koskeva asia, sillä niillä on erittäin vakavia vaikutuksia paitsi unionin talouteen myös demokratiaan sekä kuluttajien turvallisuuteen ja terveyteen. Sen vuoksi on tarpeen vahvistaa unionin kyberturvallisuutta koskevaa lähestymistapaa, käsitellä kyberkestävyyttä unionin tasolla ja parantaa sisämarkkinoiden toimintaa vahvistamalla yhtenäinen oikeudellinen kehys olennaisille kyberturvallisuusvaatimuksille, joita sovelletaan digitaalisia elementtejä sisältävien tuotteiden saattamiseen unionin markkinoille. Olisi puututtava kahteen merkittävään ongelmaan, jotka lisäävät kustannuksia käyttäjille ja yhteiskunnalle: digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuuden alhainen taso, josta ovat osoituksena laajalle levinneet haavoittuvuudet ja niihin puuttuvien tietoturvapäivitysten riittämätön ja epäjohdonmukainen tarjonta, ja käyttäjien riittämätön ymmärrys ja tiedonsaanti, mikä estää heitä valitsemasta tuotteita, joilla on asianmukaiset kyberturvallisuusominaisuudet, tai estää heitä käyttämästä tuotteita tietoturvallisesti.

(2) Tämän asetuksen tavoitteena on luoda vähimmäisedellytykset tietoturvallisten digitaalisia elementtejä sisältävien 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, esimerkiksi parantamalla avoimuutta markkinoilla saataville asetettujen digitaalisia elementtejä sisältävien tuotteiden tukiajan osalta.

(3) Voimassa oleva asiaa koskeva unionin oikeus sisältää useita horisontaalisia säännöstöjä, joissa käsitellään tiettyjä kyberturvallisuuteen liittyviä seikkoja eri näkökulmista, mukaan lukien toimenpiteet digitaalisen toimitusketjun tietoturvan parantamiseksi. Kyberturvallisuuteen liittyvä voimassa oleva unionin oikeus, mukaan lukien Euroopan parlamentin ja neuvoston asetus (EU) 2019/881[3] ja Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555[4], ei kuitenkaan suoraan kata digitaalisia elementtejä sisältävien tuotteiden tietoturvaa koskevia pakollisia vaatimuksia.

---

[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] Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi) (EUVL L 333, 27.12.2022, s. 80).

(4) Voimassa olevaa unionin oikeutta sovelletaan tiettyihin digitaalisia elementtejä sisältäviin tuotteisiin, mutta ei ole olemassa horisontaalista unionin sääntelykehystä, jossa vahvistettaisiin kattavat kyberturvallisuusvaatimukset kaikille digitaalisia elementtejä sisältäville tuotteille. Unionin ja jäsenvaltioiden tasolla tähän mennessä käyttöön otetuilla eri säädöksillä ja aloitteilla puututaan havaittuihin kyberturvallisuuteen liittyviin ongelmiin ja riskeihin vain osittain, mikä on luonut lainsäädännön hajanaisuutta sisämarkkinoilla, lisännyt oikeudellista epävarmuutta sekä näiden tuotteiden valmistajien että käyttäjien kannalta ja luonut yrityksille ja organisaatioille tarpeetonta rasitetta, kun ne joutuvat noudattamaan samantyyppisten tuotteiden osalta useita vaatimuksia ja velvoitteita. Kyseisten tuotteiden kyberturvallisuudella on kuitenkin erityisen vahva rajat ylittävä ulottuvuus, sillä yhdessä jäsenvaltiossa tai kolmannessa maassa valmistettuja digitaalisia elementtejä sisältäviä tuotteita käyttävät usein organisaatiot ja kuluttajat kaikkialla sisämarkkinoilla. Tämän vuoksi alaa on tarpeen säännellä unionin tasolla, jotta voidaan varmistaa yhdenmukaistettu sääntelykehys ja oikeusvarmuus käyttäjille, organisaatioille ja yrityksille, mukaan lukien komission suosituksen 2003/361/EY[5] liitteessä määritellyt mikroyritykset sekä pienet ja keskisuuret yritykset. Unionin sääntely-ympäristö olisi yhdenmukaistettava asettamalla digitaalisia elementtejä sisältäville tuotteille horisontaaliset kyberturvallisuusvaatimukset. Lisäksi kaikkialla unionissa olisi taattava oikeusvarmuus talouden toimijoiden ja käyttäjien kannalta sekä yhdenmukaistettava paremmin sisämarkkinoita ja parannettava oikeasuhtaisuutta mikroyritysten sekä pienten ja keskisuurten yritysten osalta ja siten luotava suotuisammat olosuhteet sisämarkkinoille pyrkiville talouden toimijoille.

[5] Komission suositus 2003/361/EY, annettu 6 päivänä toukokuuta 2003, mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä (EUVL L 124, 20.5.2003, s. 36).

(5) Kun määritetään mikroyritysten sekä pienten ja keskisuurten yritysten osalta luokkaa, johon yritys kuuluu, olisi sovellettava kaikkia komission suosituksen 2003/361/EY liitteen säännöksiä. Sen vuoksi yritysluokkien määrittämisessä käytettävien henkilöstömäärien ja rahamääräisten kynnysarvojen laskennassa olisi sovellettava myös komission suosituksen 2003/361/EY liitteen 6 artiklan säännöksiä, jotka koskevat yrityksen tietojen määräytymistä ottaen huomioon tietyntyyppiset yritykset, kuten omistusyhteysyritykset tai sidosyritykset.

(6) Komission olisi annettava ohjeita, joilla autetaan talouden toimijoita, erityisesti mikroyrityksiä sekä pieniä ja keskisuuria yrityksiä, tämän asetuksen soveltamisessa. Tällaisissa ohjeissa olisi käsiteltävä muun muassa tämän asetuksen soveltamisalaa, erityisesti datan etäkäsittelyä ja sen vaikutuksia vapaiden ja avoimen lähdekoodin ohjelmistojen kehittäjiin, digitaalisia elementtejä sisältävien tuotteiden tukiaikojen määrittämiseen käytettävien kriteerien soveltamista, tämän asetuksen ja muun unionin oikeuden välistä vuorovaikutusta sekä merkittävän muutoksen käsitettä.

(7) Unionin tasolla erilaisissa ohjelmakohtaisissa ja poliittisissa asiakirjoissa, kuten komission ja unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan 16 päivänä joulukuuta 2020 antamassa yhteisessä tiedonannossa ”EU:n kyberturvallisuusstrategia digitaaliselle vuosikymmenelle”, internetiin yhdistettyjen laitteiden kyberturvallisuudesta 2 päivänä joulukuuta 2020 ja EU:n kybertoimien kehittämisestä 23 päivänä toukokuuta 2022 annetuissa neuvoston päätelmissä sekä EU:n kyberturvallisuusstrategiasta digitaaliselle vuosikymmenelle[6] 10 päivänä kesäkuuta 2021 annetussa Euroopan parlamentin päätöslauselmassa, on vaadittu erityisiä unionin kyberturvallisuusvaatimuksia digitaalisille tai verkkoon liitetyille tuotteille, ja useat kolmannet maat ovat ottaneet oma-aloitteisesti käyttöön toimenpiteitä asian käsittelemiseksi. Euroopan tulevaisuuskonferenssin loppuraportissa kansalaiset kehottivat vahvistamaan EU:n roolia kyberturvallisuusuhkien torjunnassa. Jotta unioni voi olla kansainvälisesti johtavassa asemassa kyberturvallisuusalalla, on tärkeää luoda kunnianhimoinen sääntelykehys.

(8) Kaikkien sisämarkkinoille saatettujen digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuuden yleisen tason parantamiseksi on tarpeen ottaa käyttöön kyseisille tuotteille horisontaalisesti sovellettavat tavoitelähtöiset ja teknologianeutraalit olennaiset kyberturvallisuusvaatimukset.

---

[6] EUVL C 67, 8.2.2022, s. 81.

(9) Tietyissä olosuhteissa kaikki digitaalisia elementtejä sisältävät tuotteet, jotka on integroitu tai liitetty laajempaan sähköiseen tietojärjestelmään, voivat päätyä pahantahtoisten toimijoiden hyökkäyskanaviksi. Niinpä myös vähemmän kriittisinä pidetyt laitteistot ja ohjelmistot voivat helpottaa laitteen tai verkon ensi vaiheen vaarantumista ja mahdollistaa sen, että pahantahtoiset toimijat saavat korotetut käyttöoikeudet järjestelmään tai siirtyvät lateraalisesti järjestelmien välillä. Tästä syystä valmistajien olisi varmistettava, että kaikki digitaalisia elementtejä sisältävät tuotteet suunnitellaan ja kehitetään tässä asetuksessa säädettyjen olennaisten kyberturvallisuusvaatimusten mukaisesti. Tämä velvoite koskee sekä tuotteita, jotka voidaan liittää fyysisesti laitteistorajapintojen kautta, että tuotteita, jotka liitetään loogisesti, kuten liitäntöjen, liukuhihnoitusten, tiedostojen, sovellusrajapintojen tai muiden ohjelmistorajapintojen kautta. Koska kyberuhat voivat levitä erilaisten digitaalisia elementtejä sisältävien tuotteiden kautta esimerkiksi ketjuttamalla useita haavoittuvuuksia ennen kuin ne saavuttavat tietyn kohteen, valmistajien olisi varmistettava myös sellaisten digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuus, jotka on liitetty muihin laitteisiin tai verkkoihin vain epäsuorasti.

(10) Sillä, että digitaalisia elementtejä sisältävien tuotteiden markkinoille saattamiselle säädetään kyberturvallisuusvaatimuksia, on tarkoitus parantaa kyseisten tuotteiden kyberturvallisuutta sekä kuluttajien että yritysten kannalta. Kyseisillä vaatimuksilla varmistetaan myös, että kyberturvallisuus otetaan huomioon koko toimitusketjussa, mikä tekee digitaalisia elementtejä sisältävistä lopputuotteista ja niiden komponenteista tietoturvallisempia. Tämä pätee myös vaatimuksiin, jotka koskevat haavoittuvassa asemassa oleville kuluttajille tarkoitettujen digitaalisia elementtejä sisältävien kulutustuotteiden, kuten lelujen ja itkuhälyttimien, saattamista markkinoille. Digitaalisia elementtejä sisältävät kulutustuotteet, jotka luokitellaan tässä asetuksessa digitaalisia elementtejä sisältäviksi tärkeiksi tuotteiksi, aiheuttavat suuremman kyberturvallisuusriskin, koska niillä suoritetaan toiminto, jossa on merkittävä haitallisten vaikutusten riski, mitä tulee sen intensiteettiin ja kykyyn vahingoittaa tällaisten tuotteiden käyttäjien terveyttä, tietoturvaa tai turvallisuutta; kyseisille tuotteille olisi tehtävä tiukempi vaatimustenmukaisuuden arviointimenettely. Tämä koskee sellaisia tuotteita kuten älykotituotteet, joissa on turvallisuustoimintoja, mukaan lukien ovien älylukot, itkuhälyttimet ja hälytysjärjestelmät, verkkoon liitettyjä leluja ja henkilökohtaisia puettavia terveysteknologioita. Tiukemmat vaatimustenmukaisuuden arviointimenettelyt, jotka on tehtävä muille digitaalisia elementtejä sisältäville tuotteille, jotka luokitellaan tässä asetuksessa digitaalisia elementtejä sisältäviksi tärkeiksi tai kriittisiksi tuotteiksi, auttavat lisäksi ehkäisemään haavoittuvuuksien hyödyntämisestä kuluttajille mahdollisesti aiheutuvia kielteisiä vaikutuksia.

(11) Tämän asetuksen tarkoituksena on varmistaa digitaalisia elementtejä sisältävien tuotteiden ja niihin integroitujen datan etäkäsittelyratkaisujen kyberturvallisuuden korkea taso. Tällaiset datan etäkäsittelyratkaisut olisi määriteltävä etäältä tapahtuvaksi datan käsittelyksi, jota varten on suunniteltu ja kehitetty ohjelmisto kyseisen digitaalisia elementtejä sisältävän tuotteen valmistajan toimesta tai puolesta ja jota ilman digitaalisia elementtejä sisältävä tuote ei kykenisi suorittamaan jotakin toimintoaan. Tällä lähestymistavalla varmistetaan, että valmistajat suojaavat tällaiset tuotteet asianmukaisesti kokonaisuudessaan riippumatta siitä, suoritetaanko tietojen käsittely ja tallentaminen paikallisesti käyttäjän laitteella vai suorittaako valmistaja sen etäältä. Toisaalta etäältä suoritettu käsittely tai tallennus kuuluu tämän asetuksen soveltamisalaan vain sikäli kuin se on välttämätöntä, jotta digitaalisia elementtejä sisältävä tuote voi suorittaa toimintonsa. Tällainen etäältä suoritettu käsittely tai tallennus käsittää tilanteen, jossa mobiilisovellus edellyttää pääsyä ohjelmistosovellusrajapintaan tai tietokantaan, joka tarjotaan valmistajan kehittämän palvelun avulla. Tällaisessa tapauksessa palvelu kuuluu tämän asetuksen soveltamisalaan datan etäkäsittelyratkaisuna. Tämän asetuksen soveltamisalaan kuuluvia datan etäkäsittelyratkaisuja koskevat vaatimukset eivät sen vuoksi edellytä teknisiä, operatiivisia tai organisatorisia toimenpiteitä, joiden tarkoituksena on hallinnoida valmistajan koko verkko- ja tietojärjestelmien tietoturvaan kohdistuvia riskejä.

(12) Pilvipalveluratkaisut ovat tässä asetuksessa tarkoitettuja datan etäkäsittelyratkaisuja vain, jos ne ovat tässä asetuksessa vahvistetun määritelmän mukaisia. Esimerkiksi älykotilaitteiden valmistajien tarjoamat pilvikäyttöiset toiminnot, joiden avulla käyttäjät voivat käyttää laitetta etäältä, kuuluvat tämän asetuksen soveltamisalaan. Toisaalta verkkosivustot, jotka eivät tue digitaalisia elementtejä sisältävän tuotteen toimintoa, tai pilvipalvelut, joita ei ole suunniteltu ja kehitetty digitaalisia elementtejä sisältävän tuotteen valmistajan vastuulla, eivät kuulu tämän asetuksen soveltamisalaan. Direktiiviä (EU) 2022/2555 sovelletaan pilvipalveluihin ja pilvipalvelumalleihin, kuten ohjelmistopalveluihin (SaaS), alustapalveluihin (PaaS) tai infrastruktuuripalveluihin (IaaS). Pilvipalveluja unionissa tarjoavat toimijat, jotka ovat komission suosituksen 2003/361/EY liitteen 2 artiklan mukaisia keskisuuria yrityksiä tai jotka ylittävät kyseisen artiklan 1 kohdassa säädetyt keskisuurten yritysten kynnysarvot, kuuluvat mainitun direktiivin soveltamisalaan.

(13) Tämän asetuksen tavoitteena on poistaa digitaalisia elementtejä sisältävien tuotteiden vapaan liikkuvuuden esteitä, ja sen mukaisesti jäsenvaltiot eivät saisi tämän asetuksen soveltamisalaan kuuluvien seikkojen osalta estää tämän asetuksen mukaisten digitaalisia elementtejä sisältävien tuotteiden asettamista saataville markkinoilla. Sen vuoksi jäsenvaltiot eivät voi tällä asetuksella yhdenmukaistettujen seikkojen osalta asettaa ylimääräisiä kyberturvallisuusvaatimuksia digitaalisia elementtejä sisältävien tuotteiden markkinoilla saataville asettamista varten. Mikä tahansa julkinen tai yksityinen toimija voi kuitenkin vahvistaa tässä asetuksessa säädettyjen vaatimusten ohella lisävaatimuksia digitaalisia elementtejä sisältävien tuotteiden hankinnalle tai käytölle sen omia erityisiä tarkoituksia varten ja sen vuoksi päättää käyttää digitaalisia elementtejä sisältäviä tuotteita, jotka ovat tämän asetuksen mukaisesti markkinoilla saataville asettamiseen sovellettavia vaatimuksia tiukempien tai tarkempien kyberturvallisuusvaatimusten mukaisia. Kun jäsenvaltiot hankkivat digitaalisia elementtejä sisältäviä tuotteita, joiden on oltava tässä asetuksessa säädettyjen olennaisten kyberturvallisuusvaatimusten mukaisia, mukaan lukien haavoittuvuuksien käsittelyä koskevat vaatimukset, niiden olisi varmistettava, että tällaiset vaatimukset otetaan huomioon hankintaprosessissa ja että otetaan huomioon myös valmistajien kyky soveltaa tehokkaasti kyberturvallisuustoimenpiteitä ja käsitellä kyberuhkia, sanotun kuitenkaan rajoittamatta Euroopan parlamentin ja neuvoston direktiivien 2014/24/EU[7] ja 2014/25/EU[8] soveltamista.

---

[7] Euroopan parlamentin ja neuvoston direktiivi 2014/24/EU, annettu 26 päivänä helmikuuta 2014, julkisista hankinnoista ja direktiivin 2004/18/EY kumoamisesta (EUVL L 94, 28.3.2014, s. 65).

[8] Euroopan parlamentin ja neuvoston direktiivi 2014/25/EU, annettu 26 päivänä helmikuuta 2014, vesi- ja energiahuollon sekä liikenteen ja postipalvelujen alalla toimivien yksiköiden hankinnoista ja direktiivin 2004/17/EY kumoamisesta (EUVL L 94, 28.3.2014, s. 243).

Lisäksi direktiivissä (EU) 2022/2555 vahvistetaan kyseisen direktiivin 3 artiklassa tarkoitettuja keskeisiä ja tärkeitä toimijoita koskevat kyberturvallisuusriskien hallintatoimenpiteet, joihin voisi sisältyä toimitusketjun turvallisuuteen liittyviä toimenpiteitä, jotka edellyttävät tällaisten toimijoiden käyttävän tässä asetuksessa vahvistettuja kyberturvallisuusvaatimuksia tiukemmat kyberturvallisuusvaatimukset täyttäviä digitaalisia elementtejä sisältäviä tuotteita. Direktiivin (EU) 2022/2555 ja sen vähimmäistason yhdenmukaistamisen periaatteen mukaisesti jäsenvaltiot voivat näin ollen asettaa ylimääräisiä kyberturvallisuusvaatimuksia keskeisten tai tärkeiden toimijoiden kyseisen direktiivin nojalla suorittamalle tieto- ja viestintätekniikan tuotteiden käytölle kyberturvallisuuden korkeamman tason varmistamiseksi edellyttäen, että tällaiset vaatimukset ovat yhdenmukaisia unionin oikeudessa vahvistettujen jäsenvaltioiden velvoitteiden kanssa. Tämän asetuksen soveltamisalaan kuulumattomia seikkoja ovat esimerkiksi muut kuin tekniset tekijät, jotka liittyvät digitaalisia elementtejä sisältäviin tuotteisiin ja niiden valmistajiin. Jäsenvaltiot voivat sen vuoksi säätää kansallisia toimenpiteitä, mukaan lukien digitaalisia elementtejä sisältäviä tuotteita tai tällaisten tuotteiden toimittajia koskevia rajoituksia, joissa otetaan huomioon muut kuin tekniset tekijät. Tällaisiin tekijöihin liittyvien kansallisten toimenpiteiden on oltava unionin oikeuden mukaisia.

(14) Tämä asetus ei saisi vaikuttaa jäsenvaltioiden velvollisuuteen turvata kansallinen turvallisuus unionin oikeuden mukaisesti. Jäsenvaltioiden olisi voitava soveltaa ylimääräisiä toimenpiteitä digitaalisia elementtejä sisältäviin tuotteisiin, joita hankitaan tai käytetään kansalliseen turvallisuuteen tai puolustukseen liittyviin tarkoituksiin, edellyttäen, että tällaiset toimenpiteet ovat yhdenmukaisia unionin oikeudessa vahvistettujen jäsenvaltioiden velvoitteiden kanssa.

(15) Tätä asetusta sovelletaan talouden toimijoihin ainoastaan sellaisten digitaalisia elementtejä sisältävien tuotteiden osalta, jotka asetetaan saataville markkinoilla ja toimitetaan näin ollen unionin markkinoille kaupallisen toiminnan yhteydessä jakelua tai käyttöä varten. Toimittamisesta kaupallisen toiminnan yhteydessä voi olla merkkinä paitsi hinnan periminen digitaalisia elementtejä sisältävästä tuotteesta myös hinnan periminen teknisistä tukipalveluista, kun tätä ei käytetä ainoastaan aiheutuneiden kustannusten korvaamiseen, aikomus hankkia tuloja esimerkiksi tarjoamalla ohjelmistoalusta, jonka kautta valmistaja saa tuloja muista palveluista, käytön edellytyksenä oleva vaatimus henkilötietojen käsittelystä muista syistä kuin yksinomaan ohjelmiston tietoturvan, yhteensopivuuden tai yhteentoimivuuden parantamiseksi taikka sellaisten lahjoitusten vastaanottaminen, jotka ylittävät digitaalisia elementtejä sisältävän tuotteen suunnitteluun, kehittämiseen ja tarjoamiseen liittyvät kustannukset. Lahjoitusten vastaanottamista ei saisi katsoa liiketoiminnaksi, jos aikomuksena ei ole tehdä voittoa.

(16) Digitaalisia elementtejä sisältävien tuotteiden tarjoamista osana sellaisen palvelun toimittamista, josta peritään maksu yksinomaan kyseisen palvelun suorittamiseen suoraan liittyvien todellisten kustannusten kattamiseksi, mistä saattaa olla kyse julkishallinnon toimijoiden tarjoamien tiettyjen digitaalisia elementtejä sisältävien tuotteiden tapauksessa, ei saisi pelkästään näistä syistä katsoa kaupalliseksi toiminnaksi tätä asetusta sovellettaessa. Lisäksi digitaalisia elementtejä sisältäviä tuotteita, jotka julkishallinnon toimija on kehittänyt tai joita se on muuttanut yksinomaan omaan käyttöönsä, ei saisi katsoa markkinoilla saataville asetetuiksi tässä asetuksessa tarkoitetulla tavalla.

(17) Avoimesti jaetut ja vapaasti käyttäjien saatavilla olevat ohjelmistot ja data, joita tai joiden muunneltuja versioita käyttäjät voivat vapaasti käyttää, muunnella ja jakaa uudelleen, voivat edistää tutkimusta ja innovointia markkinoilla. Jotta voidaan tukea vapaiden ja avoimen lähdekoodin ohjelmistojen kehittämistä ja käyttöönottoa erityisesti mikroyrityksissä ja pienissä ja keskisuurissa yrityksissä, startup-yritykset mukaan luettuina, sekä yksittäisten henkilöiden toimesta ja voittoa tavoittelemattomissa järjestöissä ja akateemisissa tutkimuslaitoksissa, vapaan ja avoimen lähdekoodin ohjelmiston lisensseillä jaettujen ja kehitettyjen ohjelmistojen erilaisten kehitysmallien luonne olisi otettava huomioon tämän asetuksen soveltamisessa digitaalisia elementtejä sisältäviin tuotteisiin, jotka katsotaan kaupallisen toiminnan yhteydessä jakelua tai käyttöä varten toimitetuiksi vapaiksi ja avoimen lähdekoodin ohjelmistoiksi.

(18) Vapaalla ja avoimen lähdekoodin ohjelmistolla tarkoitetaan ohjelmistoa, jonka lähdekoodi on yleisesti saatavilla ja jonka lisensointi tarjoaa kaikki oikeudet, jotta se on vapaasti saatavilla, käytettävissä, muunneltavissa ja uudelleen jaettavissa. Vapaita ja avoimen lähdekoodin ohjelmistoja kehitetään, ylläpidetään ja jaetaan avoimesti, myös verkkoalustojen kautta. Tämän asetuksen soveltamisalaan kuuluvien talouden toimijoiden osalta ainoastaan sellaisten vapaiden ja avoimen lähdekoodin ohjelmistojen olisi kuuluttava tämän asetuksen soveltamisalaan, jotka on asetettu saataville markkinoilla ja siten toimitettu jakelua tai käyttöä varten kaupallisen toiminnan yhteydessä. Näin ollen kyseisen toiminnan kaupallista tai ei-kaupallista luonnetta määritettäessä ei saisi ottaa huomioon pelkästään digitaalisia elementtejä sisältävän tuotteen kehittämiseen liittyviä olosuhteita tai sitä, miten kehittäminen on rahoitettu. Tarkennuksena ja jotta kehitys- ja toimitusvaiheet erotetaan selkeästi toisistaan, tätä asetusta sovellettaessa ja sen soveltamisalaan kuuluvien talouden toimijoiden osalta sellaisten digitaalisia elementtejä sisältävien tuotteiden tarjoamista, jotka katsotaan vapaiksi ja avoimen lähdekoodin ohjelmistoiksi ja joista niiden valmistajat eivät saa tuloa, ei saisi katsoa kaupalliseksi toiminnaksi. Lisäksi sellaisten digitaalisia elementtejä sisältävien tuotteiden toimittamista, jotka katsotaan vapaiksi ja avoimen lähdekoodin ohjelmistokomponenteiksi ja jotka on tarkoitettu integroitaviksi muiden valmistajien toimesta niiden omiin digitaalisia elementtejä sisältäviin tuotteisiin, olisi pidettävä markkinoilla saataville asettamisena vain, jos komponentin alkuperäinen valmistaja saa siitä tuloa. Toimintaa ei saisi katsoa luonteeltaan kaupalliseksi esimerkiksi ainoastaan sillä perusteella, että digitaalisia elementtejä sisältävä avoimen lähdekoodin ohjelmistotuote saa taloudellista tukea valmistajilta tai valmistajat osallistuvat tällaisen tuotteen kehittämiseen.

Lisäksi pelkkien säännöllisin väliajoin tehtävien julkaisujen ei sellaisenaan pitäisi johtaa päätelmään, että digitaalisia elementtejä sisältävä tuote toimitetaan kaupallisen toiminnan yhteydessä. Tätä asetusta sovellettaessa kaupallisena toimintana ei saisi myöskään pitää sitä, kun voittoa tavoittelemattomat järjestöt kehittävät digitaalisia elementtejä sisältäviä tuotteita, jotka katsotaan vapaiksi ja avoimen lähdekoodin ohjelmistoiksi, edellyttäen, että järjestön perustamistavalla varmistetaan, että kaikki tulot kustannusten jälkeen käytetään voittoa tavoittelemattomaan toimintaan liittyvien tavoitteiden saavuttamiseen. Tätä asetusta ei sovelleta luonnollisiin henkilöihin tai oikeushenkilöihin, jotka kehittävät lähdekoodia vapaiksi ja avoimen lähdekoodin ohjelmistoiksi katsottaviin digitaalisia elementtejä sisältäviin tuotteisiin, jotka eivät ole kyseisten henkilöiden vastuulla.

(19) Koska monilla digitaalisia elementtejä sisältävillä tuotteilla, jotka katsotaan vapaiksi ja avoimen lähdekoodin ohjelmistoiksi ja jotka julkaistaan mutta joita ei aseteta saataville markkinoilla tässä asetuksessa tarkoitetulla tavalla, on suuri merkitys kyberturvallisuuden kannalta, sellaisiin oikeushenkilöihin, jotka tukevat pitkäjänteisesti tällaisten kaupallisiin tarkoituksiin tarkoitettujen tuotteiden kehittämistä ja joilla on keskeinen rooli kyseisten tuotteiden toimintakelpoisuuden varmistamisessa, jäljempänä ’avoimen lähdekoodin ohjelmistovastaavat’, olisi sovellettava kevyttä ja räätälöityä sääntelyjärjestelmää. Avoimen lähdekoodin ohjelmistovastaavia ovat esimerkiksi tietyt säätiöt sekä toimijat, jotka kehittävät ja julkaisevat vapaita ja avoimen lähdekoodin ohjelmistoja liiketoimintaympäristössä, mukaan lukien voittoa tavoittelemattomat toimijat. Sääntelyjärjestelmässä olisi otettava huomioon näiden toimijoiden erityisluonne ja yhteensopivuus asetettujen velvoitteiden tyypin kanssa. Sen olisi katettava ainoastaan sellaiset digitaalisia elementtejä sisältävät tuotteet, jotka katsotaan vapaiksi ja avoimen lähdekoodin ohjelmistoiksi ja jotka on viime kädessä tarkoitettu kaupalliseen toimintaan, kuten integroitavaksi kaupallisiin palveluihin tai digitaalisia elementtejä sisältäviin vastikkeellisiin tuotteisiin. Kyseistä sääntelyjärjestelmää sovellettaessa aikomus integroida tuote digitaalisia elementtejä sisältäviin vastikkeellisiin tuotteisiin käsittää myös tapaukset, joissa valmistajat, jotka integroivat komponentin omiin digitaalisia elementtejä sisältäviin tuotteisiinsa, joko osallistuvat säännöllisesti kyseisen komponentin kehittämiseen tai antavat säännöllistä taloudellista tukea varmistaakseen ohjelmistotuotteen jatkuvuuden. Digitaalisia elementtejä sisältävän tuotteen kehittämisen pitkäjänteinen tukeminen käsittää muun muassa ohjelmistokehityksen yhteistyöalustojen isännöinnin ja hallinnoinnin, lähdekoodin tai ohjelmiston säilyttämisen, sellaisten digitaalisia elementtejä sisältävien tuotteiden hallinnoinnin, jotka katsotaan vapaiksi ja avoimen lähdekoodin ohjelmistoiksi, sekä tällaisten tuotteiden kehittämisen ohjaamisen. Avoimen lähdekoodin ohjelmistovastaavina toimiville ei saisi olla sallittua kiinnittää CE-merkintää digitaalisia elementtejä sisältäviin tuotteisiin, joiden kehittämistä ne tukevat, koska kevyessä ja räätälöidyssä sääntelyjärjestelmässä niihin ei sovelleta samoja velvoitteita kuin tämän asetuksen mukaisesti sovelletaan valmistajina toimiviin.

(20) Digitaalisia elementtejä sisältävien tuotteiden pelkkä säilyttäminen avoimissa arkistoissa, mukaan lukien paketinhallintajärjestelmien avulla tai yhteistyöalustoilla, ei itsessään tarkoita digitaalisia elementtejä sisältävän tuotteen asettamista saataville markkinoilla. Tällaisten palvelujen tarjoajia olisi pidettävä jakelijoina ainoastaan, jos ne asettavat tällaisen ohjelmiston saataville markkinoilla ja näin ollen toimittavat sen unionin markkinoille kaupallisen toiminnan yhteydessä jakelua tai käyttöä varten.

(21) Jotta voidaan tukea ja helpottaa asianmukaista huolellisuutta koskevan velvoitteen noudattamista sellaisten valmistajien osalta, jotka integroivat digitaalisia elementtejä sisältäviin tuotteisiinsa vapaita ja avoimen lähdekoodin ohjelmistokomponentteja, joihin ei sovelleta tässä asetuksessa vahvistettuja olennaisia kyberturvallisuusvaatimuksia, komission olisi voitava perustaa vapaaehtoisia tietoturvatodistusohjelmia joko tätä asetusta täydentävällä delegoidulla säädöksellä tai esittämällä asetuksen (EU) 2019/881 48 artiklan mukaisen pyynnön eurooppalaisesta kyberturvallisuuden sertifiointijärjestelmästä, jossa otetaan huomioon vapaiden ja avoimen lähdekoodin ohjelmistojen kehitysmallien erityispiirteet. Tietoturvatodistusohjelmat olisi suunniteltava siten, että tietoturvatodistuksen voivat panna alulle tai rahoittaa paitsi luonnolliset henkilöt tai oikeushenkilöt, jotka kehittävät vapaaksi ja avoimen lähdekoodin ohjelmistoksi katsottavaa digitaalisia elementtejä sisältävää tuotetta tai osallistuvat sellaisen kehittämiseen, myös kolmannet osapuolet, kuten valmistajat, jotka integroivat tällaisia tuotteita omiin digitaalisia elementtejä sisältäviin tuotteisiinsa, käyttäjät tai unionin ja jäsenvaltioiden julkishallinnot.

(22) Kun otetaan huomioon tämän asetuksen julkista kyberturvallisuutta koskevat tavoitteet ja jotta voidaan parantaa jäsenvaltioiden tilannetietoisuutta unionin riippuvuudesta ohjelmistokomponenteista ja erityisesti mahdollisesti vapaista ja avoimen lähdekoodin ohjelmistokomponenteista, tällä asetuksella perustetun erityisen hallinnollisen yhteistyön ryhmän olisi voitava päättää yhteisen unionin riippuvuusarvioinnin tekemisestä. Markkinavalvontaviranomaisten olisi voitava pyytää hallinnollisen yhteistyön ryhmän vahvistamien digitaalisia elementtejä sisältävien tuotteiden ryhmien valmistajia toimittamaan ohjelmistojen materiaaliluettelot, jotka ne ovat laatineet tämän asetuksen nojalla. Ohjelmistojen materiaaliluetteloiden luottamuksellisuuden suojaamiseksi markkinavalvontaviranomaisten olisi toimitettava hallinnollisen yhteistyön ryhmälle asiaankuuluvat tiedot riippuvuuksista anonymisoidusti ja kootusti.

(23) Tämän asetuksen täytäntöönpanon tehokkuus riippuu myös asianmukaisen kyberturvallisuusosaamisen saatavuudesta. Unionin tasolla erilaisissa ohjelmakohtaisissa ja poliittisissa asiakirjoissa, kuten komission 18 päivänä huhtikuuta 2023 antamassa tiedonannossa ”Kyberturvallisuuteen liittyvän osaamisvajeen pienentäminen EU:n kilpailukyvyn, kasvun ja häiriönsietokyvyn parantamiseksi” ja EU:n kyberpuolustuspolitiikasta 22 päivänä toukokuuta 2023 annetuissa neuvoston päätelmissä, todettiin kyberturvallisuuden osaamisvaje unionissa ja tarve vastata tällaisiin haasteisiin ensi tilassa sekä julkisella että yksityisellä sektorilla. Tämän asetuksen tehokkaan täytäntöönpanon takaamiseksi jäsenvaltioiden olisi varmistettava, että käytettävissä on riittävät resurssit, jotta markkinavalvontaviranomaisilla ja vaatimustenmukaisuuden arviointilaitoksilla on asianmukainen henkilöstö tässä asetuksessa säädettyjen tehtäviensä suorittamista varten. Näillä toimenpiteillä olisi lisättävä työvoiman liikkuvuutta kyberturvallisuusalalla ja parannettava työntekijöiden alaan liittyviä urapolkuja. Niillä olisi myös edistettävä kyberturvallisuusalan työvoiman muutosjoustavuutta ja osallisuutta, myös sukupuolten tasa-arvon osalta. Jäsenvaltioiden olisi sen vuoksi toteutettava toimenpiteitä, joilla varmistetaan, että näitä tehtäviä suorittavat asianmukaisesti koulutetut ammattilaiset, joilla on tarvittavat kyberturvallisuustaidot. Valmistajien olisi vastaavasti varmistettava, että niiden henkilöstöllä on tarvittavat taidot tässä asetuksessa säädettyjen velvoitteidensa täyttämiseksi. Jäsenvaltioiden ja komission olisi oikeuksiensa ja toimivaltansa sekä niille tällä asetuksella annettujen erityisten tehtävien mukaisesti toteutettava toimenpiteitä, joilla tuetaan valmistajia ja erityisesti mikroyrityksiä ja pieniä ja keskisuuria yrityksiä, mukaan lukien startup-yritykset, myös osaamisen kehittämisen kaltaisilla aloilla, jotta ne voivat täyttää tässä asetuksessa säädetyt velvoitteensa. Koska direktiivissä (EU) 2022/2555 lisäksi edellytetään, että jäsenvaltiot hyväksyvät osana kansallisia kyberturvallisuusstrategioitaan toimintapolitiikkoja, joilla edistetään ja kehitetään kyberturvallisuutta koskevaa koulutusta sekä kyberturvallisuustaitoja, jäsenvaltiot voivat tällaisia strategioita hyväksyessään myös harkita, käsittelevätkö ne tästä asetuksesta johtuvia kyberturvallisuusosaamiseen liittyviä tarpeita, kuten uudelleen- ja täydennyskoulutukseen liittyviä tarpeita.

(24) Internetin tietoturvallisuus on välttämätön edellytys kriittisten infrastruktuurien toiminnalle ja koko yhteiskunnalle. Direktiivillä (EU) 2022/2555 pyritään varmistamaan kyseisen direktiivin 3 artiklassa tarkoitettujen keskeisten ja tärkeiden toimijoiden tarjoamien palvelujen korkea kyberturvallisuuden taso, mukaan lukien digitaalisen infrastruktuurin tarjoajat, jotka tukevat avoimen internetin ydintoimintoja, varmistavat pääsyn internetiin ja tarjoavat internetin palveluja. Sen vuoksi on tärkeää, että digitaalisia elementtejä sisältävät tuotteet, joita digitaalisen infrastruktuurin tarjoajat tarvitsevat internetin toiminnan varmistamiseksi, kehitetään tietoturvallisesti 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 (EU) 2022/2555 mukaisia toimitusketjua koskevia vaatimuksia varmistamalla, että digitaalisia elementtejä sisältävät tuotteet, joita ne käyttävät palvelujensa tarjoamiseen, kehitetään tietoturvallisesti ja että infrastruktuurin tarjoajien saatavilla on oikea-aikaisesti tällaisten tuotteiden tietoturvapäivityksiä.

(25) Euroopan parlamentin ja neuvoston asetuksessa (EU) 2017/745[9] vahvistetaan lääkinnällisiä laitteita koskevat säännöt ja Euroopan parlamentin ja neuvoston asetuksessa (EU) 2017/746[10] *in vitro* -diagnostiikkaan tarkoitettuja lääkinnällisiä laitteita koskevat säännöt. Kyseisissä asetuksissa käsitellään kyberturvallisuusriskejä ja noudatetaan tiettyjä lähestymistapoja, joita käsitellään myös tässä asetuksessa. Asetuksissa (EU) 2017/745 ja (EU) 2017/746 vahvistetaan olennaiset vaatimukset lääkinnällisille laitteille, jotka toimivat sähköisen järjestelmän kautta tai jotka ovat itsessään ohjelmistoja. Kyseiset asetukset kattavat myös tietyt sulauttamattomat ohjelmistot ja koko elinkaareen perustuvan lähestymistavan. Kyseisissä vaatimuksissa edellytetään, että valmistajat kehittävät ja toteuttavat tuotteensa soveltaen riskinhallintaperiaatteita ja esittämällä tietoturvatoimenpiteitä koskevat vaatimukset sekä vastaavat vaatimustenmukaisuuden arviointimenettelyt. Lisäksi lääkinnällisten laitteiden kyberturvallisuudesta on annettu joulukuussa 2019 erityisohjeistusta, jossa lääkinnällisten laitteiden, myös *in vitro* -diagnostiikkaan tarkoitettujen laitteiden, valmistajille annetaan ohjeita siitä, miten ne voivat täyttää kaikki kyseisten asetusten liitteissä I vahvistetut kyberturvallisuutta koskevat olennaiset vaatimukset. Sen vuoksi tätä asetusta ei olisi sovellettava digitaalisia elementtejä sisältäviin tuotteisiin, jotka kuuluvat jommankumman edellä mainitun asetuksen soveltamisalaan.

---

9 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).

10 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).

(26) Tämän asetuksen soveltamisalaan eivät kuulu digitaalisia elementtejä sisältävät tuotteet, jotka on kehitetty tai joita on muutettu yksinomaan kansalliseen turvallisuuteen tai puolustukseen liittyviin tarkoituksiin, eivätkä tuotteet, jotka on erityisesti suunniteltu turvallisuusluokiteltujen tietojen käsittelyä varten. Jäsenvaltioita kannustetaan varmistamaan, että kyseisten tuotteiden suojauksen taso on sama tai korkeampi kuin tämän asetuksen soveltamisalaan kuuluvien tuotteiden.

(27) Euroopan parlamentin ja neuvoston asetuksessa (EU) 2019/2144[11] vahvistetaan ajoneuvojen sekä niiden järjestelmien ja komponenttien tyyppihyväksyntää koskevat vaatimukset, joihin kuuluu myös tiettyjä kyberturvallisuusvaatimuksia, mukaan lukien sertifioidun kyberturvallisuuden hallintajärjestelmän toiminta ja ohjelmistopäivitykset, jotka kattavat ajoneuvojen, laitteiden ja palvelujen koko elinkaareen liittyviä kyberturvallisuusriskejä koskevat organisaatioiden toimintaperiaatteet ja prosessit sovellettavien teknisiä eritelmiä ja kyberturvallisuutta koskevien Yhdistyneiden kansakuntien sääntöjen ja erityisesti E-säännön nro 155 (yhdenmukaiset vaatimukset, jotka koskevat ajoneuvojen hyväksyntää kyberturvallisuuden ja sen hallintajärjestelmän osalta) mukaisesti. Kyseisessä asetuksessa säädetään myös erityisistä vaatimustenmukaisuuden arviointimenettelyistä.

---

[11] 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 Euroopan parlamentin ja neuvoston 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).

Ilmailualalla 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, mikä käsittää tietoturvauhkilta suojautumista koskevat velvoitteet. Tässä asetuksessa tavoiteltu varmuustaso varmistetaan asetuksen (EU) 2018/1139 mukaisella sertifiointiprosessilla. Digitaalisia elementtejä sisältäviin tuotteisiin, joihin sovelletaan asetusta (EU) 2019/2144, ja tuotteisiin, jotka on sertifioitu asetuksen (EU) 2018/1139 mukaisesti, ei olisi sen vuoksi sovellettava tässä asetuksessa vahvistettuja olennaisia kyberturvallisuusvaatimuksia ja vaatimustenmukaisuuden arviointimenettelyjä.

[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).

(28) Tässä asetuksessa vahvistetaan horisontaalisia kyberturvallisuussääntöjä, jotka eivät koske pelkästään tiettyjä toimialoja tai tiettyjä digitaalisia elementtejä sisältäviä tuotteita. On kuitenkin mahdollista, että otetaan käyttöön alakohtaisia tai tuotekohtaisia unionin sääntöjä, joissa asetetuilla vaatimuksilla puututaan kaikkiin tai joihinkin tässä asetuksessa vahvistettujen olennaisten kyberturvallisuusvaatimusten kattamiin riskeihin. Tällaisissa tapauksissa tämän asetuksen soveltamista digitaalisia elementtejä sisältäviin tuotteisiin, joihin sovelletaan muita unionin sääntöjä ja niissä asetettuja vaatimuksia, joilla puututaan kaikkiin tässä asetuksessa vahvistettujen olennaisten kyberturvallisuusvaatimusten kattamiin riskeihin tai osaan niistä, voidaan rajoittaa tai tuotteet voidaan jättää kokonaan soveltamisalan ulkopuolelle, jos tällainen rajoittaminen tai soveltamisalan ulkopuolelle jättäminen on johdonmukaista kyseisiin tuotteisiin sovellettavan yleisen sääntelykehyksen kanssa ja jos alakohtaisilla säännöillä saavutetaan vähintään samantasoinen suoja kuin mitä tässä asetuksessa säädetään. Komissiolle olisi siirrettävä valta antaa delegoituja säädöksiä tämän asetuksen täydentämiseksi täsmentämällä tällaiset tuotteet ja säännöt. Sellaisen voimassa olevan unionin oikeuden osalta, jonka suhteen tällaisia rajoituksia tai soveltamisalan ulkopuolelle jättämistä olisi sovellettava, tämä asetus sisältää erityissäännöksiä, joilla selvennetään sen suhdetta kyseiseen unionin oikeuteen.

(29) Jotta voidaan varmistaa, että markkinoilla saataville asetetut digitaalisia elementtejä sisältävät tuotteet voidaan korjata tehokkaasti ja niiden kestoikää voidaan pidentää, olisi säädettävä varaosia koskevasta poikkeuksesta. Kyseisen poikkeuksen olisi koskettava sekä varaosia, joiden tarkoituksena on ennen tämän asetuksen soveltamispäivää saataville asetettujen vanhojen tuotteiden korjaaminen, että varaosia, joille on jo tehty tämän asetuksen mukainen vaatimustenmukaisuuden arviointimenettely.

(30) Komission delegoidussa asetuksessa (EU) 2022/30[13] todetaan, että tiettyihin radiolaitteisiin sovelletaan erinäisiä olennaisia vaatimuksia, joista säädetään Euroopan parlamentin ja neuvoston direktiivin 2014/53/EU[14] 3 artiklan 3 kohdan d, e ja f alakohdassa ja jotka liittyvät verkon vahingoittamiseen ja verkkoresurssien väärinkäyttöön, henkilötietoihin ja yksityisyyteen sekä petoksiin. Euroopan standardointikomitealle ja Euroopan sähkötekniikan standardointikomitealle esitetystä standardointipyynnöstä 5 päivänä elokuuta 2022 annetussa komission täytäntöönpanopäätöksessä C(2022) 5637 vahvistetaan vaatimukset erityisten standardien laatimiseksi sen täsmentämiseksi, miten kyseisiä olennaisia vaatimuksia olisi käsiteltävä. Tässä asetuksessa vahvistetut olennaiset kyberturvallisuusvaatimukset kattavat kaikki direktiivin 2014/53/EU 3 artiklan 3 kohdan d, e ja f alakohdassa tarkoitettujen olennaisten vaatimusten osatekijät. Lisäksi tässä asetuksessa vahvistetut olennaiset kyberturvallisuusvaatimukset ovat yhdenmukaisia kyseiseen standardointipyyntöön sisältyvien erityisiä standardeja koskevien vaatimusten tavoitteiden kanssa. Näin ollen kun komissio kumoaa delegoidun asetuksen (EU) 2022/30 tai muuttaa sitä niin, että sitä ei enää sovelleta tiettyihin tämän asetuksen soveltamisalaan kuuluviin tuotteisiin, komission ja eurooppalaisten standardointiorganisaatioiden olisi tämän asetuksen täytäntöönpanon helpottamiseen tarkoitettuja yhdenmukaistettuja standardeja valmistellessaan ja kehittäessään otettava huomioon standardointityö, joka tehtiin täytäntöönpanopäätöstä C(2022) 5637 varten. Tämän asetuksen soveltamisen siirtymäkauden aikana komission olisi annettava ohjeita niille tämän asetuksen soveltamisalaan kuuluville valmistajille, joihin sovelletaan myös delegoitua asetusta (EU) 2022/30, jotta voidaan helpottaa näiden kahden asetuksen noudattamisen osoittamista.

---

13 Komission delegoitu asetus (EU) 2022/30, annettu 29 päivänä lokakuuta 2021, Euroopan parlamentin ja neuvoston direktiivin 2014/53/EU täydentämisestä sen 3 artiklan 3 kohdan d, e ja f alakohdassa tarkoitettujen olennaisten vaatimusten soveltamisen osalta (EUVL L 7, 12.1.2022, s. 6).

14 Euroopan parlamentin ja neuvoston direktiivi 2014/53/EU, annettu 16 päivänä huhtikuuta 2014, radiolaitteiden asettamista saataville markkinoilla koskevan jäsenvaltioiden lainsäädännön yhdenmukaistamisesta ja direktiivin 1999/5/EY kumoamisesta (EUVL L 153, 22.5.2014, s. 62).

(31) Euroopan parlamentin ja neuvoston direktiivi (EU) 2024/…[15+] täydentää tätä asetusta. Kyseisessä direktiivissä vahvistetaan tuotevastuusäännöt, joiden mukaisesti vahinkoa kärsineet voivat vaatia korvausta, jos vahinko on aiheutunut turvallisuudeltaan puutteellisista tuotteista. Siinä vahvistetaan periaate, jonka mukaan tuotteen valmistaja on tuottamuksellisuudesta riippumatta vastuussa tuotteen puutteellisesta turvallisuudesta johtuvista vahingoista (ankara vastuu). Jos tällainen turvallisuuspuute johtuu siitä, että tuotteen markkinoille saattamisen jälkeen ei ole tehty tietoturvapäivityksiä, ja tämä aiheuttaa vahinkoa, valmistaja voisi joutua vastuuseen. Valmistajien velvollisuudet, jotka koskevat tällaisten tietoturvapäivitysten tarjoamista, olisi vahvistettava tässä asetuksessa.

---

[15] Euroopan parlamentin ja neuvoston direktiivi (EU) .../..., annettu ... päivänä ...kuuta ...., (EUVL ..., ELI: ...).

[+] Lisätään tekstiin asiakirjassa (2022/0302(COD)) olevan direktiivin numero ja lisätään alaviitteeseen kyseisen direktiivin numero, antopäivä, nimi ja EUVL-julkaisuviite.

(32) Tämä asetus ei saisi vaikuttaa Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679[16] 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 kyberturvallisuusvaatimuksilla suojataan kuluttajia ja organisaatioita kyberturvallisuusriskeiltä, ja siten niillä myös pyritään osaltaan parantamaan yksittäisten henkilöiden henkilötietojen ja yksityisyyden suojaa. Kyberturvallisuusnäkökohtien standardoinnin ja sertifioinnin synergioita olisi käsiteltävä komission, eurooppalaisten standardointiorganisaatioiden, Euroopan unionin kyberturvallisuusviraston (ENISA), asetuksella (EU) 2016/679 perustetun Euroopan tietosuojaneuvoston ja kansallisten tietosuojaviranomaisten välisellä yhteistyöllä. 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 soveltamista valvovien viranomaisten kanssa. Viimeksi mainituilla olisi myös oltava pääsy tietoihin, jotka ovat merkityksellisiä niiden tehtävien suorittamisen kannalta.

---

[16] 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).

(33) Siltä osin kuin niiden tuotteet kuuluvat tämän asetuksen soveltamisalaan, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014[17] 5 a artiklan 2 kohdassa tarkoitettujen eurooppalaisten digitaalisen identiteetin lompakoiden tarjoajien olisi noudatettava sekä tässä asetuksessa vahvistettuja horisontaalisia olennaisia kyberturvallisuusvaatimuksia että asetuksen (EU) N:o 910/2014 5 a artiklassa vahvistettuja erityisiä tietoturvavaatimuksia. Vaatimusten noudattamisen helpottamiseksi lompakkojen tarjoajien olisi voitava osoittaa, että eurooppalaiset digitaalisen identiteetin lompakot ovat tässä asetuksessa ja asetuksessa (EU) N:o 910/2014 vahvistettujen vaatimusten mukaisia, sertifioimalla tuotteensa asetuksen (EU) 2019/881 nojalla perustetun sellaisen eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti, jonka osalta komissio on delegoiduilla säädöksillä määrittänyt vaatimustenmukaisuusolettaman tämän asetuksen suhteen, siltä osin kuin sertifikaatti tai sen osat kattavat kyseiset vaatimukset.

[17] Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta (EUVL L 257, 28.8.2014, s. 73).

(34) Kun valmistajat integroivat kolmansilta osapuolilta hankittuja komponentteja digitaalisia elementtejä sisältäviin tuotteisiin suunnittelu- ja kehitysvaiheessa, niiden olisi noudatettava asianmukaista huolellisuutta kyseisten komponenttien osalta, mukaan lukien vapaat ja avoimen lähdekoodin ohjelmistokomponentit, joita ei ole asetettu saataville markkinoilla, sen varmistamiseksi, että tuotteet suunnitellaan, kehitetään ja tuotetaan tässä asetuksessa vahvistettujen olennaisten kyberturvallisuusvaatimusten mukaisesti. Asianmukaisen huolellisuuden asiaankuuluva taso riippuu tiettyyn komponenttiin liittyvän kyberturvallisuusriskin luonteesta ja tasosta, ja tätä varten siinä olisi otettava huomioon yksi tai useampi seuraavista toimista: soveltuvissa tapauksissa sen todentaminen, että komponentin valmistaja on osoittanut tämän asetuksen mukaisuuden, muun muassa tarkastamalla, onko komponentissa jo CE-merkintä; sen todentaminen, että komponenttiin tehdään säännöllisiä tietoturvapäivityksiä, esimerkiksi tarkastamalla sen aiemmat tietoturvapäivitykset; sen todentaminen, ettei komponentissa ole direktiivin (EU) 2022/2555 12 artiklan 2 kohdan nojalla perustettuun Euroopan haavoittuvuustietokantaan tai muihin julkisesti saatavilla oleviin haavoittuvuustietokantoihin kirjattuja haavoittuvuuksia; tai ylimääräisten tietoturvatestien tekeminen. Tässä asetuksessa vahvistettuja haavoittuvuuksien käsittelyä koskevia velvoitteita, joita valmistajien on noudatettava saattaessaan digitaalisia elementtejä sisältävän tuotteen markkinoille ja tukiajan ajan, sovelletaan digitaalisia elementtejä sisältäviin tuotteisiin kokonaisuudessaan, myös kaikkiin niihin integroituihin komponentteihin. Jos digitaalisia elementtejä sisältävän tuotteen valmistaja asianmukaista huolellisuutta noudattaessaan havaitsee komponentissa, mukaan lukien vapaat ja avoimen lähdekoodin komponentit, haavoittuvuuden, sen olisi ilmoitettava siitä komponenttia valmistavalle tai ylläpitävälle henkilölle tai toimijalle, puututtava haavoittuvuuteen ja korjattava se ja tarvittaessa ilmoitettava henkilölle tai toimijalle käytetystä tietoturvakorjauksesta.

(35) On mahdollista, että valmistaja, jonka digitaalisia elementtejä sisältävään tuotteeseen on integroitu yksi tai useampi kolmansilta osapuolilta hankittu komponentti, johon myös sovelletaan tätä asetusta, ei pysty välittömästi tämän asetuksen soveltamiselle asetetun siirtymäkauden jälkeen asianmukaista huolellisuutta koskevaa velvoitetta noudattaessaan todentamaan, että kyseisten komponenttien valmistajat ovat osoittaneet tämän asetuksen mukaisuuden, esimerkiksi tarkistamalla, onko komponenteissa jo CE-merkintä. Tästä voi olla kyse esimerkiksi silloin, kun komponentit on integroitu tuotteeseen ennen kuin tätä asetusta aletaan soveltaa kyseisten komponenttien valmistajiin. Tällaisessa tapauksessa valmistajan, joka integroi tällaisia komponentteja tuotteeseen, olisi noudatettava asianmukaista huolellisuutta muilla keinoin.

(36) Digitaalisia elementtejä sisältävissä tuotteissa olisi oltava CE-merkintä, joka osoittaa näkyvästi, helposti luettavasti ja pysyvästi 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. Jäsenvaltiot eivät myöskään saisi estää esittelemästä tai käyttämästä messuilla, näyttelyissä ja esittelytilaisuuksissa tai vastaavissa tapahtumissa digitaalisia elementtejä sisältäviä tuotteita, jotka eivät ole tämän asetuksen mukaisia, mukaan lukien tuotteiden prototyypit, edellyttäen, että tuotteet esitellään sellaisella näkyvällä merkinnällä varustettuna, josta käy selvästi ilmi, että tuote ei ole tämän asetuksen mukainen eikä sitä saa asettaa saataville markkinoilla ennen kuin se on sitä.

(37) Sen varmistamiseksi, että valmistajat voivat julkaista ohjelmistoja testaustarkoituksiin ennen digitaalisia elementtejä sisältävien tuotteidensa vaatimustenmukaisuuden arviointia, jäsenvaltiot eivät saisi estää keskeneräisten ohjelmistojen, kuten alfaversioiden, beetaversioiden tai julkaisuehdokkaiden, asettamista saataville edellyttäen, että keskeneräinen ohjelmisto 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. Valmistajat eivät saisi pakottaa käyttäjiä päivittämään ohjelmistojaan versioihin, jotka on julkaistu ainoastaan testaustarkoituksiin.

(38) Sen varmistamiseksi, että digitaalisia elementtejä sisältävät tuotteet eivät markkinoille saatettaessa aiheuta kyberturvallisuusriskejä henkilöille ja organisaatioille, tällaisille tuotteille olisi vahvistettava olennaiset kyberturvallisuusvaatimukset. Näitä olennaisia kyberturvallisuusvaatimuksia, mukaan lukien haavoittuvuuksien hallinnan käsittelyä koskevat vaatimukset, sovelletaan jokaiseen yksittäiseen digitaalisia elementtejä sisältävään tuotteeseen, kun se saatetaan markkinoille, riippumatta siitä, valmistetaanko digitaalisia elementtejä sisältävä tuote yksittäiskappaleena vai sarjatuotantona. Esimerkiksi tietyn tuotetyypin osalta kullekin yksittäiselle digitaalisia elementtejä sisältävälle tuotteelle olisi pitänyt suorittaa kaikki saatavilla olevat tietoturvakorjaukset tai -päivitykset, joilla puututaan merkityksellisiin tietoturvaongelmiin, kun tuote saatetaan markkinoille. Jos digitaalisia elementtejä sisältäviä tuotteita myöhemmin muutetaan joko fyysisesti tai digitaalisesti tavalla, jota valmistaja ei ole ennakoinut alkuperäisessä riskinarvioinnissa ja jonka seurauksena ne eivät mahdollisesti enää täytä niitä koskevia olennaisia kyberturvallisuusvaatimuksia, muutos olisi katsottava merkittäväksi. Esimerkiksi korjaukset voitaisiin rinnastaa ylläpitotoimiin edellyttäen, että niillä ei muuteta jo markkinoille saatettua digitaalisia elementtejä sisältävää tuotetta siten, että se voi vaikuttaa sovellettavien vaatimusten mukaisuuteen tai muuttaa käyttötarkoitusta, jota varten tuote on arvioitu.

(39) Kuten fyysisten korjausten tai muutosten tapauksessa, ohjelmiston muutoksen olisi katsottava muuttavan merkittävästi digitaalisia elementtejä sisältävää tuotetta, jos ohjelmistopäivitys muuttaa kyseisen tuotteen käyttötarkoitusta eikä valmistaja ennakoinut kyseisiä muutoksia alkuperäisessä riskinarvioinnissa tai jos ohjelmistopäivityksen seurauksena vaaran luonne on muuttunut tai kyberturvallisuusriskin taso noussut, ja tuotteen päivitetty versio asetetaan saataville markkinoilla. Jos tietoturvapäivitys, jonka tarkoituksena on alentaa digitaalisia elementtejä sisältävän tuotteen kyberturvallisuusriskin tasoa, ei muuta digitaalisia elementtejä sisältävän tuotteen käyttötarkoitusta, sitä ei katsota merkittäväksi muutokseksi. Tämä koskee yleensä tilanteita, joissa tietoturvapäivityksessä tehdään vain pieniä muutoksia lähdekoodiin. Tästä voisi olla kyse esimerkiksi silloin, kun tietoturvapäivityksellä puututaan tunnettuun haavoittuvuuteen muun muassa muuttamalla digitaalisia elementtejä sisältävän tuotteen toimintoja tai suorituskykyä yksinomaan kyberturvallisuusriskin tason alentamiseksi. Vastaavasti vähäistä toimintopäivitystä, kuten visuaalista parannusta tai uusien kuvamerkkien tai kielten lisäämistä käyttöliittymään, ei yleensä pitäisi katsoa merkittäväksi muutokseksi. Sen sijaan ominaisuuspäivitystä olisi pidettävä merkittävänä muutoksena, jos se muuttaa digitaalisia elementtejä sisältävän tuotteen alkuperäisiä aiottuja toimintoja tai tyyppiä tai suorituskykyä ja täyttää edellä mainitut kriteerit, koska uusien ominaisuuksien lisääminen tyypillisesti johtaa laajempaan hyökkäyspinta-alaan, mikä lisää kyberturvallisuusriskiä. Tällainen tilanne voisi syntyä esimerkiksi silloin, kun sovellukseen lisätään uusi syöttöelementti, jolloin valmistajan on varmistettava syötön asianmukainen validointi. Arvioitaessa, pidetäänkö ominaisuuspäivitystä merkittävänä muutoksena, sillä ei ole merkitystä, tarjotaanko se erillisenä päivityksenä vai yhdessä tietoturvapäivityksen kanssa. Komission olisi annettava ohjeet siitä, miten merkittävät muutokset määritetään.

(40) Kun otetaan huomioon ohjelmistokehityksen iteratiivinen luonne, valmistajien, jotka ovat saattaneet ohjelmistotuotteen myöhempiä versioita markkinoille kyseiseen tuotteeseen myöhemmin tehdyn merkittävän muutoksen seurauksena, olisi voitava tarjota tietoturvapäivityksiä tukiajan ajan ainoastaan ohjelmistotuotteen siihen versioon, jonka ne ovat viimeksi saattaneet markkinoille. Niiden olisi voitava tehdä näin vain, jos markkinoille viimeksi saatettu tuoteversio on asiaankuuluvien aiempien tuoteversioiden käyttäjien saatavilla maksutta eikä heille aiheudu lisäkustannuksia sen laitteisto- tai ohjelmistoympäristön mukauttamisesta, jossa he käyttävät tuotetta. Esimerkki tällaisesta tapauksesta voisi olla muun muassa se, kun pöytätietokoneen käyttöjärjestelmän päivitys ei edellytä uutta laitteistoa, kuten nopeampaa keskusyksikköä tai enemmän muistia. Valmistajan olisi kuitenkin edelleen tukiajan ajan noudatettava muita haavoittuvuuksien käsittelyä koskevia vaatimuksia, esimerkiksi sillä on oltava koordinoitua haavoittuvuuksien julkistamista koskevat periaatteet tai käytettävissään toimenpiteitä, joilla helpotetaan mahdollisia haavoittuvuuksia koskevien tietojen jakamista markkinoille saatetun ohjelmistotuotteen kaikkien myöhempien merkittävästi muutettujen versioiden osalta. Valmistajien olisi voitava tarjota pieniä tietoturva- tai toimintopäivityksiä, jotka eivät muodosta merkittävää muutosta, ainoastaan ohjelmistotuotteen viimeisimpään versioon tai alaversioon, jota ei ole merkittävästi muutettu. Samalla jos laitteistotuote, kuten älypuhelin, ei ole yhteensopiva sen käyttöjärjestelmän viimeisimmän version kanssa, jonka kanssa se alun perin toimitettiin, valmistajan olisi tukiajan ajan jatkettava tietoturvapäivitysten tarjoamista ainakin käyttöjärjestelmän viimeisimpään yhteensopivaan versioon.

(41) Unionin yhdenmukaistamislainsäädännön soveltamisalaan kuuluvien tuotteiden osalta yleisesti vahvistetun merkittävän muutoksen käsitteen mukaisesti, kun tapahtuu merkittävä muutos, joka voi vaikuttaa siihen, onko digitaalisia elementtejä sisältävä 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, muutoksesta, joka voi johtaa merkittävään muutokseen, olisi tarvittaessa ilmoitettava kolmannelle osapuolelle.

(42) Digitaalisia elementtejä sisältävän tuotteen kunnostaminen, kunnossapito ja korjaaminen Euroopan parlamentin ja neuvoston asetuksen (EU) 2024/1781[18] 2 artiklan 18, 19 ja 20 alakohdassa määritellyllä tavalla ei välttämättä johda tuotteen merkittävään muutokseen esimerkiksi, jos käyttötarkoitus ja toiminnot eivät muutu ja riskitaso säilyy ennallaan. Valmistajan suorittama digitaalisia elementtejä sisältävän tuotteen parannus voi kuitenkin johtaa muutoksiin kyseisen tuotteen suunnittelussa ja kehittämisessä ja siten vaikuttaa sen käyttötarkoitukseen ja siihen, onko kyseinen tuote tässä asetuksessa vahvistettujen vaatimusten mukainen.

---

[18] Euroopan parlamentin ja neuvoston asetus (EU) 2024/1781, annettu 13 päivänä kesäkuuta 2024, kestävien tuotteiden ekologiselle suunnittelulle asetettavien vaatimusten puitteista, direktiivin (EU) 2020/1828 ja asetuksen (EU) 2023/1542 muuttamisesta sekä direktiivin 2009/125/EY kumoamisesta (EUVL L, 2024/1781, 28.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

(43) Digitaalisia elementtejä sisältävää tuotetta olisi pidettävä tärkeänä, jos tuotteen mahdollisten haavoittuvuuksien hyödyntämisen kielteinen vaikutus voi olla vakava esimerkiksi kyberturvallisuuteen liittyvän toiminnon tai sellaisen toiminnon perusteella, jossa on merkittävä haitallisten vaikutusten riski, mitä tulee sen intensiteettiin ja kykyyn häiritä, hallita tai vahingoittaa suurta määrää digitaalisia elementtejä sisältäviä muita tuotteita tai vahingoittaa sen käyttäjien terveyttä, tietoturvaa tai turvallisuutta suoralla manipuloinnilla, kuten keskeinen järjestelmätoiminto, mukaan lukien verkonhallinta, konfiguraationhallinta, virtualisointi tai henkilötietojen käsittely. Erityisesti sellaisten digitaalisia elementtejä sisältävien tuotteiden haavoittuvuudet, joissa on kyberturvallisuuteen liittyvä toiminto, kuten käynnistysohjelmat, voivat johtaa tietoturvaongelmien leviämiseen koko toimitusketjussa. Poikkeaman vaikutusten vakavuus voi lisääntyä myös, jos tuote ensisijaisesti suorittaa keskeistä järjestelmätoimintoa, mukaan lukien verkonhallinta, konfiguraationhallinta, virtualisointi tai henkilötietojen käsittely.

(44) Tiettyihin digitaalisia elementtejä sisältävien tuotteiden ryhmiin olisi sovellettava tiukempia vaatimustenmukaisuuden arviointimenettelyjä niin, että samalla säilytetään oikeasuhtainen lähestymistapa. Tätä varten digitaalisia elementtejä sisältävät tärkeät tuotteet olisi jaettava kahteen luokkaan, jotka kuvastavat näihin tuoteryhmiin liittyvän kyberturvallisuusriskin tasoa. Luokkaan II kuuluviin digitaalisia elementtejä sisältäviin tärkeisiin tuotteisiin liittyvä poikkeama saattaisi johtaa suurempiin kielteisiin vaikutuksiin kuin luokkaan I kuuluviin digitaalisia elementtejä sisältäviin tärkeisiin tuotteisiin liittyvä poikkeama esimerkiksi niiden kyberturvallisuuteen liittyvän toiminnon luonteen tai jonkin toisen sellaisen toiminnon suorittamisen vuoksi, johon liittyy merkittävä haitallisten vaikutusten riski. Osoituksena tällaisista suuremmista kielteisistä vaikutuksista luokkaan II kuuluvat digitaalisia elementtejä sisältävät tuotteet voisivat joko suorittaa kyberturvallisuuteen liittyvää toimintoa tai jotakin muuta toimintoa, johon liittyy merkittävä haitallisten vaikutusten riski, joka on suurempi kuin luokassa I olevilla tuotteilla, tai ne voisivat täyttää molemmat edellä mainitut kriteerit. Luokkaan II kuuluviin digitaalisia elementtejä sisältäviin tärkeisiin tuotteisiin olisi sen vuoksi sovellettava tiukempaa vaatimustenmukaisuuden arviointimenettelyä.

(45) Tässä asetuksessa tarkoitetut digitaalisia elementtejä sisältävät tärkeät tuotteet olisi ymmärrettävä tuotteiksi, joilla on jonkin tässä asetuksessa vahvistetun digitaalisia elementtejä sisältävien tärkeiden tuotteiden ryhmän ydintoiminto. Tässä asetuksessa vahvistetaan esimerkiksi digitaalisia elementtejä sisältävien tärkeiden tuotteiden ryhmät, jotka määritellään niiden ydintoimintojen perusteella luokkaan II kuuluviksi palomuureiksi tai tunkeutumisen havaitsemis- tai estojärjestelmiksi. Tästä seuraa, että palomuureille ja tunkeutumisen havaitsemis- tai estojärjestelmille on tehtävä pakollinen kolmannen osapuolen suorittama vaatimustenmukaisuuden arviointi. Tämä ei koske digitaalisia elementtejä sisältäviä muita tuotteita, joita ei ole luokiteltu digitaalisia elementtejä sisältäviksi tärkeiksi tuotteiksi ja joihin on voitu integroida palomuureja tai tunkeutumisen havaitsemis- tai estojärjestelmiä. Komission olisi annettava täytäntöönpanosäädös, jossa täsmennetään tässä asetuksessa vahvistettuihin luokkiin I ja II kuuluvien digitaalisia elementtejä sisältävien tärkeiden tuotteiden ryhmien tekninen kuvaus.

(46) Tässä asetuksessa vahvistetuilla digitaalisia elementtejä sisältävien kriittisten tuotteiden ryhmillä on kyberturvallisuuteen liittyvä toiminto ja ne suorittavat toimintoa, jossa on merkittävä haitallisten vaikutusten riski, mitä tulee sen intensiteettiin ja kykyyn häiritä, hallita tai vahingoittaa suurta määrää digitaalisia elementtejä sisältäviä muita tuotteita suoralla manipuloinnilla. Lisäksi kyseisiä digitaalisia elementtejä sisältävien tuotteiden ryhmiä pidetään direktiivin (EU) 2022/2555 3 artiklan 1 kohdassa tarkoitettujen keskeisten toimijoiden kriittisinä riippuvuuksina. Tämän asetuksen liitteessä vahvistetuissa digitaalisia elementtejä sisältävien kriittisten tuotteiden ryhmissä käytetään jo laajalti erityyppisiä sertifiointeja niiden kriittisyyden vuoksi, ja ne kuuluvat myös komission täytäntöönpanoasetuksessa (EU) 2024/482[19] vahvistetun eurooppalaisiin yhteisiin kriteereihin perustuvan kyberturvallisuuden sertifiointijärjestelmän (EUCC) piiriin. Sen vuoksi, jotta voidaan varmistaa digitaalisia elementtejä sisältävien kriittisten tuotteiden yhteinen asianmukainen kyberturvallisuuden suoja unionissa, voisi olla tarkoituksenmukaista ja oikeasuhteista vahvistaa delegoidulla säädöksellä, että tällaisiin tuoteryhmiin sovelletaan pakollista eurooppalaista kyberturvallisuussertifiointia, jos kyseiset tuotteet kattava eurooppalainen kyberturvallisuuden sertifiointijärjestelmä on jo käytössä ja komissio on arvioinut suunnitellun pakollisen sertifioinnin mahdollisia markkinavaikutuksia. Kyseisessä arvioinnissa olisi otettava huomioon sekä tarjonta- että kysyntäpuoli, mukaan lukien se, onko digitaalisia elementtejä sisältäville kyseessä oleville tuotteille riittävästi kysyntää sekä jäsenvaltioista että käyttäjiltä, jotta eurooppalainen kyberturvallisuussertifiointi tarvitaan, sekä tarkoitukset, joihin digitaalisia elementtejä sisältäviä tuotteita aiotaan käyttää, mukaan lukien niiden kriittinen riippuvuus direktiivin (EU) 2022/2555 3 artiklan 1 kohdassa tarkoitetuista keskeisistä toimijoista. Arvioinnissa olisi myös analysoitava pakollisen sertifioinnin mahdollisia vaikutuksia kyseisten tuotteiden saatavuuteen sisämarkkinoilla sekä jäsenvaltioiden kapasiteettia ja valmiutta panna täytäntöön asiaankuuluvat eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät.

---

[19] Komission täytäntöönpanoasetus (EU) 2024/482, annettu 31 päivänä tammikuuta 2024, Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 soveltamissäännöistä siltä osin kuin on kyse yhteisiin kriteereihin perustuvan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän (EUCC) hyväksymisestä (EUVL L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(47) Pakollista eurooppalaista kyberturvallisuussertifiointia edellyttävissä delegoiduissa säädöksissä olisi määritettävä ne digitaalisia elementtejä sisältävät tuotteet, joilla on jonkin tässä asetuksessa vahvistetun digitaalisia elementtejä sisältävien kriittisten tuotteiden ryhmän ydintoiminto ja joihin on tarkoitus soveltaa pakollista sertifiointia, sekä vaadittu varmuustaso, jonka olisi oltava vähintään ”korotettu”. Vaaditun varmuustason olisi oltava oikeassa suhteessa digitaalisia elementtejä sisältävään tuotteeseen liittyvän kyberturvallisuusriskin tasoon. Esimerkiksi jos digitaalisia elementtejä sisältävällä tuotteella on jonkin tässä asetuksessa vahvistetun digitaalisia elementtejä sisältävien kriittisten tuotteiden ryhmän ydintoiminto ja se on tarkoitettu käytettäväksi herkässä tai kriittisessä ympäristössä, kuten tuotteet, jotka on tarkoitettu direktiivin (EU) 2022/2555 3 artiklan 1 kohdassa tarkoitettujen keskeisten toimijoiden käyttöön, se voi vaatia korkeinta varmuustasoa.

(48) Jotta voidaan varmistaa, että unionissa on yhteinen asianmukainen kyberturvallisuuden suoja digitaalisia elementtejä sisältäville tuotteille, joilla on tässä asetuksessa vahvistetun digitaalisia elementtejä sisältävien kriittisten tuotteiden ryhmän ydintoiminto, komissiolle olisi myös siirrettävä valta antaa delegoituja säädöksiä, joilla muutetaan tätä asetusta lisäämällä tai poistamalla digitaalisia elementtejä sisältävien kriittisten tuotteiden ryhmiä, joiden osalta valmistajia voitaisiin edellyttää hankkimaan asetuksen (EU) 2019/881 mukaisen eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukainen eurooppalainen kyberturvallisuussertifikaatti tämän asetuksen mukaisuuden osoittamiseksi. Kyseisiin ryhmiin voidaan lisätä uusi digitaalisia elementtejä sisältävien kriittisten tuotteiden ryhmä, jos direktiivin (EU) 2022/2555 3 artiklan 1 kohdassa tarkoitetut keskeiset toimijat ovat kriittisesti riippuvaisia kyseisistä tuotteista tai jos kyseisiin tuotteisiin vaikuttavat poikkeamat tai niihin sisältyvät hyödynnetyt haavoittuvuudet voisivat johtaa kriittisten toimitusketjujen häiriöihin. Arvioidessaan tarvetta lisätä tai poistaa digitaalisia elementtejä sisältävien kriittisten tuotteiden ryhmiä delegoidulla säädöksellä komission olisi voitava ottaa huomioon, ovatko jäsenvaltiot määrittäneet kansallisella tasolla digitaalisia elementtejä sisältäviä tuotteita, joilla on kriittinen rooli direktiivin (EU) 2022/2555 3 artiklan 1 kohdassa tarkoitettujen keskeisten toimijoiden häiriönsietokyvyn kannalta ja joiden toimitusketjuihin kohdistuu yhä enemmän mahdollisesti vakavia häiriövaikutuksia aiheuttavia kyberhyökkäyksiä. Lisäksi komission olisi voitava ottaa huomioon direktiivin (EU) 2022/2555 22 artiklan mukaisesti tehdyn kriittisiä toimitusketjuja koskevan unionin tason koordinoidun turvallisuusriskinarvioinnin tulokset.

(49) Komission olisi varmistettava, että laajaa joukkoa asiaankuuluvia sidosryhmiä kuullaan jäsennellysti ja säännöllisesti, kun valmistellaan toimenpiteitä tämän asetuksen täytäntöönpanoa varten. Tällaiset kuulemiset olisi varmistettava erityisesti silloin, kun komissio arvioi tarvetta digitaalisia elementtejä sisältävien tärkeiden tai kriittisten tuotteiden ryhmien luetteloiden mahdollisille päivityksille, jolloin asiaankuuluvia valmistajia olisi kuultava ja niiden näkemykset otettava huomioon, jotta voidaan analysoida kyberturvallisuusriskejä sekä tällaisten tuoteryhmien tärkeäksi tai kriittiseksi nimeämisen kustannus-hyötysuhdetta.

(50) Tällä asetuksella puututaan kohdennetusti kyberturvallisuusriskeihin. Digitaalisia elementtejä sisältävät tuotteet saattavat kuitenkin aiheuttaa muita turvallisuusriskejä, jotka eivät aina liity kyberturvallisuuteen mutta voivat olla seurausta tietoturvaloukkauksesta. Näitä riskejä olisi edelleen säänneltävä muulla asiaa koskevalla unionin yhdenmukaistamislainsäädännöllä kuin tällä asetuksella. Jos muuta unionin yhdenmukaistamislainsäädäntöä kuin tätä asetusta ei voida soveltaa, niihin olisi sovellettava Euroopan parlamentin ja neuvoston asetusta (EU) 2023/988[20]. Kun otetaan huomioon tämän asetuksen kohdennettu luonne, poiketen siitä, mitä asetuksen (EU) 2023/988 2 artiklan 1 kohdan kolmannen alakohdan b alakohdassa säädetään, asetuksen (EU) 2023/988 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 asetuksen (EU) 2023/988 3 artiklan 27 alakohdassa tarkoitetussa unionin muussa yhdenmukaistamislainsäädännössä kuin tässä asetuksessa säädettyjä erityisvaatimuksia.

---

[20] Euroopan parlamentin ja neuvoston asetus (EU) 2023/988, annettu 10 päivänä toukokuuta 2023, yleisestä tuoteturvallisuudesta, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1025/2012 ja Euroopan parlamentin ja neuvoston direktiivin (EU) 2020/1828 muuttamisesta sekä Euroopan parlamentin ja neuvoston direktiivin 2001/95/EY ja neuvoston direktiivin 87/357/ETY kumoamisesta (EUVL L 135, 23.5.2023, s. 1).

(51) Euroopan parlamentin ja neuvoston asetuksen (EU) 2024/1689[21] 6 artiklan mukaisesti suuririskisiksi tekoälyjärjestelmiksi luokiteltujen digitaalisia elementtejä sisältävien tuotteiden, jotka kuuluvat tämän asetuksen soveltamisalaan, olisi oltava tässä asetuksessa vahvistettujen olennaisten kyberturvallisuusvaatimusten mukaisia. Jos kyseiset suuririskiset tekoälyjärjestelmät täyttävät tässä asetuksessa vahvistetut olennaiset kyberturvallisuusvaatimukset, niiden olisi katsottava täyttävän asetuksen (EU) 2024/1689 15 artiklassa vahvistetut kyberturvallisuusvaatimukset siltä osin kuin kyseiset vaatimukset kuuluvat tämän asetuksen nojalla annetun EU-vaatimustenmukaisuusvakuutuksen tai sen osien piiriin. Tätä varten sellaisessa arvioinnissa, joka koskee asetuksen (EU) 2024/1689 nojalla suuririskiseksi tekoälyjärjestelmäksi luokiteltuun digitaalisia elementtejä sisältävään tuotteeseen liittyviä kyberturvallisuusriskejä ja joka on otettava huomioon tällaisen tuotteen suunnittelu-, kehitys-, tuotanto-, toimitus- ja ylläpitovaiheissa tässä asetuksessa edellytetyllä tavalla, olisi otettava huomioon tekoälyjärjestelmän kyberkestävyyteen kohdistuvat riskit, jotka liittyvät asiaankuulumattomien ulkopuolisten tahojen yrityksiin muuttaa sen käyttöä, käyttäytymistä tai suorituskykyä, mukaan lukien nimenomaisesti tekoälyyn liittyvät haavoittuvuudet, kuten datan myrkyttäminen tai vihamieliseen koneoppimiseen perustuvat hyökkäykset, sekä tapauksen mukaan perusoikeuksiin kohdistuvat riskit, asetuksen (EU) 2024/1689 mukaisesti. Tämän asetuksen soveltamisalaan kuuluvaan digitaalisia elementtejä sisältävään ja suuririskiseksi tekoälyjärjestelmäksi luokitellun tuotteen olennaisiin kyberturvallisuusvaatimuksiin liittyvien vaatimustenmukaisuuden arviointimenettelyjen osalta olisi sovellettava pääsääntöisesti asetuksen (EU) 2024/1689 43 artiklaa tämän asetuksen asiaa koskevien säännösten sijasta.

---

[21] Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689, annettu 13 päivänä kesäkuuta 2024, tekoälyä koskevista yhdenmukaistetuista säännöistä ja asetusten (EY) N:o 300/2008, (EU) N:o 167/2013, (EU) N:o 168/2013, (EU) 2018/858, (EU) 2018/1139 ja (EU) 2019/2144 sekä direktiivien 2014/90/EU, (EU) 2016/797 ja (EU) 2020/1828 muuttamisesta (tekoälysäädös) (EUVL L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

Tämä pääsääntö ei kuitenkaan saisi johtaa tässä asetuksessa tarkoitettujen digitaalisia elementtejä sisältävien tärkeiden tai kriittisten tuotteiden tarvittavan varmuustason alenemiseen. Sen vuoksi tästä pääsäännöstä poiketen suuririskisiin tekoälyjärjestelmiin, jotka kuuluvat asetuksen (EU) 2024/1689 soveltamisalaan ja jotka ovat myös tässä asetuksessa tarkoitettuja digitaalisia elementtejä sisältäviä tärkeitä tai kriittisiä tuotteita ja joihin sovelletaan asetuksen (EU) 2024/1689 liitteessä VI tarkoitettua sisäiseen valvontaan perustuvaa vaatimustenmukaisuuden arviointimenettelyä, olisi sovellettava tässä asetuksessa säädettyjä vaatimustenmukaisuuden arviointimenettelyjä siltä osin kuin kyse on tämän asetuksen olennaisista kyberturvallisuusvaatimuksista. Tällaisessa tapauksessa kaikkiin muihin asetuksen (EU) 2024/1689 soveltamisalaan kuuluviin näkökohtiin olisi sovellettava kyseisen asetuksen liitteessä VI vahvistettuja asiaankuuluvia säännöksiä, jotka koskevat sisäiseen valvontaan perustuvaa vaatimustenmukaisuuden arviointia.

(52) Sisämarkkinoille saatettavien digitaalisia elementtejä sisältävien tuotteiden tietoturvan parantamiseksi on tarpeen vahvistaa tällaisiin tuotteisiin sovellettavat olennaiset kyberturvallisuusvaatimukset. Nämä olennaiset kyberturvallisuusvaatimukset eivät saisi vaikuttaa kriittisiä toimitusketjuja koskeviin unionin tason koordinoituihin turvallisuusriskinarviointeihin, joista säädetään direktiivin (EU) 2022/2555 22 artiklassa ja joissa otetaan huomioon sekä tekniset että tarvittaessa muut kuin tekniset riskitekijät, kuten kolmannen maan asiaton vaikuttaminen toimittajiin. Lisäksi ne eivät saisi rajoittaa jäsenvaltioiden oikeutta asettaa lisävaatimuksia, joissa otetaan häiriönsietokyvyn korkean tason varmistamiseksi huomioon muita kuin teknisiä tekijöitä, mukaan lukien komission suosituksessa (EU) 2019/534[22], 5G-verkkojen kyberturvallisuutta koskevassa EU:n koordinoidussa riskinarvioinnissa ja direktiivin (EU) 2022/2555 14 artiklan nojalla perustetun yhteistyöryhmän hyväksymässä 5G-kyberturvallisuutta koskevassa EU:n välineistössä määritellyt tekijät.

[22] Komission suositus (EU) 2019/534, annettu 26 päivänä maaliskuuta 2019, 5G-verkkojen kyberturvallisuudesta (EUVL L 88, 29.3.2019, s. 42).

(53) Jos Euroopan parlamentin ja neuvoston asetuksen (EU) 2023/1230[23] soveltamisalaan kuuluvat tuotteet ovat myös tässä asetuksessa tarkoitettuja digitaalisia elementtejä sisältäviä tuotteita, niiden valmistajien olisi noudatettava sekä tässä asetuksessa vahvistettuja olennaisia kyberturvallisuusvaatimuksia että asetuksessa (EU) 2023/1230 vahvistettuja olennaisia terveys- ja turvallisuusvaatimuksia. Tässä asetuksessa vahvistetuilla olennaisilla kyberturvallisuusvaatimuksilla ja tietyillä asetuksen (EU) 2023/1230 olennaisilla vaatimuksilla saatetaan puuttua samankaltaisiin kyberturvallisuusriskeihin. Sen vuoksi tässä asetuksessa vahvistettujen olennaisten kyberturvallisuusvaatimusten noudattaminen voisi helpottaa asetuksessa (EU) 2023/1230 vahvistettujen sellaisten olennaisten vaatimusten noudattamista, jotka kattavat myös tietyt kyberturvallisuusriskit, ja erityisesti kyseisen asetuksen liitteessä III olevissa 1.1.9 ja 1.2.1 kohdassa vahvistettujen suojausta tietojen turmeltumista vastaan ja ohjausjärjestelmien turvallisuutta ja toimintavarmuutta koskevien vaatimusten noudattamista. Valmistajan on osoitettava tällaiset synergiat esimerkiksi soveltamalla kyseiset kyberturvallisuusriskit kattavan riskinarvioinnin jälkeen yhdenmukaistettuja standardeja tai muita teknisiä eritelmiä, jotka kattavat asiaankuuluvat olennaiset kyberturvallisuusvaatimukset, jos sellaisia on saatavilla. Valmistajan olisi myös noudatettava tässä asetuksessa ja asetuksessa (EU) 2023/1230 vahvistettuja sovellettavia vaatimustenmukaisuuden arviointimenettelyjä. Komission ja eurooppalaisten standardointiorganisaatioiden olisi tämän asetuksen ja asetuksen (EU) 2023/1230 täytäntöönpanoa tukevassa valmistelutyössä ja siihen liittyvissä standardointiprosesseissa edistettävä johdonmukaisuutta sen suhteen, miten kyberturvallisuusriskit on arvioitava ja miten kyseiset riskit on katettava yhdenmukaistetuilla standardeilla asiaankuuluvien olennaisten vaatimusten osalta.

---

[23] Euroopan parlamentin ja neuvoston asetus (EU) 2023/1230, annettu 14 päivänä kesäkuuta 2023, koneista ja Euroopan parlamentin ja neuvoston direktiivin 2006/42/EY ja neuvoston direktiivin 73/361/ETY kumoamisesta (EUVL L 165, 29.6.2023, s. 1).

Komission ja eurooppalaisten standardointiorganisaatioiden olisi otettava tämä asetus huomioon varsinkin valmistellessaan ja kehittäessään yhdenmukaistettuja standardeja, joilla helpotetaan asetuksen (EU) 2023/1230 täytäntöönpanoa erityisesti kyseisen asetuksen liitteessä III olevissa 1.1.9 ja 1.2.1 kohdassa vahvistettujen suojaukseen tietojen turmeltumista vastaan ja ohjausjärjestelmien turvallisuuteen ja toimintavarmuuteen liittyvien kyberturvallisuusnäkökohtien osalta. Komission olisi annettava ohjeita, joilla tuetaan tämän asetuksen soveltamisalaan kuuluvia valmistajia, joihin sovelletaan myös asetusta (EU) 2023/1230, erityisesti jotta voidaan helpottaa tässä asetuksessa ja asetuksessa (EU) 2023/1230 vahvistettujen asiaankuuluvien olennaisten vaatimusten mukaisuuden osoittamista.

(54) Sen varmistamiseksi, että digitaalisia elementtejä sisältävät tuotteet ovat tietoturvallisia sekä niiden markkinoille saattamisen ajankohtana että sinä aikana, jona digitaalisia elementtejä sisältävän tuotteen odotetaan olevan käytössä, on tarpeen vahvistaa haavoittuvuuksien käsittelyä koskevat olennaiset kyberturvallisuusvaatimukset ja digitaalisia elementtejä sisältävien tuotteiden ominaisuuksiin liittyvät olennaiset kyberturvallisuusvaatimukset. Valmistajien olisi täytettävä kaikki haavoittuvuuksien käsittelyyn liittyvät olennaiset kyberturvallisuusvaatimukset koko tukiajan ajan, mutta niiden olisi myös määritettävä, mitkä muut tuotteen ominaisuuksiin liittyvät olennaiset kyberturvallisuusvaatimukset ovat merkityksellisiä kyseisen digitaalisia elementtejä sisältävän tuotetyypin kannalta. Tätä varten valmistajien olisi suoritettava digitaalisia elementtejä sisältävään tuotteeseen liittyvien kyberturvallisuusriskien arviointi asiaankuuluvien riskien ja asiaankuuluvien olennaisten kyberturvallisuusvaatimusten määrittämiseksi, jotta ne voivat asettaa digitaalisia elementtejä sisältävät tuotteensa saataville ilman tiedossa olevia hyödynnettävissä olevia haavoittuvuuksia, jotka voisivat vaikuttaa kyseisten tuotteiden tietoturvaan, ja soveltaa asianmukaisesti soveltuvia yhdenmukaistettuja standardeja, yhteisiä eritelmiä tai eurooppalaisia tai kansainvälisiä standardeja.

(55) Jos tietyt olennaiset kyberturvallisuusvaatimukset eivät sovellu digitaalisia elementtejä sisältävään tuotteeseen, valmistajan olisi perusteltava tämä selkeästi teknisiin asiakirjoihin sisältyvässä kyberturvallisuusriskien arvioinnissa. Tällainen tilanne voi syntyä esimerkiksi silloin, kun olennainen kyberturvallisuusvaatimus ei sovi yhteen digitaalisia elementtejä sisältävän tuotteen luonteen kanssa. Digitaalisia elementtejä sisältävän tuotteen käyttötarkoitus voi esimerkiksi edellyttää, että valmistaja noudattaa yleisesti tunnustettuja yhteentoimivuusstandardeja, vaikkei niiden turvaominaisuuksia enää pidetä uusimman teknologian mukaisina. Vastaavasti muussa unionin oikeudessa edellytetään, että valmistajat soveltavat erityisiä yhteentoimivuusvaatimuksia. Jos olennaista kyberturvallisuusvaatimusta ei sovelleta digitaalisia elementtejä sisältävään tuotteeseen, mutta valmistaja on havainnut kyseiseen olennaiseen kyberturvallisuusvaatimukseen liittyviä kyberturvallisuusriskejä, sen olisi toteutettava toimenpiteitä puuttuakseen näihin riskeihin muilla keinoin, esimerkiksi rajoittamalla tuotteen käyttötarkoitus luotettuihin ympäristöihin tai tiedottamalla käyttäjille näistä riskeistä.

(56) Yksi tärkeimmistä toimenpiteistä, joita käyttäjät voivat toteuttaa suojatakseen digitaalisia elementtejä sisältävät tuotteensa kyberhyökkäyksiltä, on uusimpien saatavilla olevien tietoturvapäivitysten asentaminen mahdollisimman pian. Valmistajien olisi sen vuoksi tuotteensa suunnittelulla ja käyttöön ottamillaan prosesseilla varmistettava, että digitaalisia elementtejä sisältäviin tuotteisiin sisältyy toimintoja, jotka mahdollistavat tietoturvapäivityksistä ilmoittamisen sekä niiden jakelun, lataamisen ja asennuksen automaattisesti, erityisesti kun on kyse kulutustuotteista. Niiden olisi myös tarjottava mahdollisuus hyväksyä tietoturvapäivitysten lataaminen ja asentaminen viimeisenä vaiheena. Käyttäjien olisi voitava kytkeä automaattiset päivitykset pois päältä selkeällä ja helppokäyttöisellä mekanismilla, jota tuetaan selkeillä ohjeilla siitä, miten käyttäjät voivat poistaa automaattiset päivitykset käytöstä. Tämän asetuksen liitteessä vahvistettuja automaattisia päivityksiä koskevia vaatimuksia ei sovelleta digitaalisia elementtejä sisältäviin tuotteisiin, jotka on ensisijaisesti tarkoitettu integroitaviksi komponentteina muihin tuotteisiin. Niitä ei myöskään sovelleta digitaalisia elementtejä sisältäviin tuotteisiin, joiden osalta käyttäjät eivät kohtuudella odottaisi automaattisia päivityksiä, mukaan lukien digitaalisia elementtejä sisältävät tuotteet, jotka on tarkoitettu käytettäviksi ammattikäytössä olevissa tieto- ja viestintäverkoissa ja erityisesti kriittisissä ympäristöissä ja teollisuusympäristöissä, joissa automaattinen päivitys voisi aiheuttaa häiriöitä toiminnalle. Riippumatta siitä, onko digitaalisia elementtejä sisältävä tuote suunniteltu vastaanottamaan automaattisia päivityksiä, sen valmistajan olisi tiedotettava käyttäjille haavoittuvuuksista ja asetettava tietoturvapäivitykset saataville viipymättä. Jos digitaalisia elementtejä sisältävällä tuotteella on käyttöliittymä tai vastaava tekninen keino, joka mahdollistaa suoran vuorovaikutuksen sen käyttäjien kanssa, valmistajan olisi käytettävä tällaisia ominaisuuksia ilmoittaakseen käyttäjille, että heidän digitaalisia elementtejä sisältävän tuotteensa tukiaika on päättynyt. Ilmoitukset olisi rajoitettava siihen, mikä on tarpeen näiden tietojen tehokkaan vastaanottamisen varmistamiseksi, eivätkä ne saisi vaikuttaa kielteisesti digitaalisia elementtejä sisältävän tuotteen käyttäjäkokemukseen.

(57) Jotta voidaan parantaa haavoittuvuuksien käsittelyprosessien avoimuutta ja varmistaa, että käyttäjiä ei vaadita asentamaan uusia toimintopäivityksiä ainoastaan viimeisimpien tietoturvapäivitysten saamiseksi, valmistajien olisi varmistettava, että uudet tietoturvapäivitykset tarjotaan erillään toimintopäivityksistä, jos se on teknisesti mahdollista.

(58) Komission ja unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan 20 päivänä kesäkuuta 2023 antamassa yhteisessä tiedonannossa ”Euroopan taloudellisen turvallisuuden strategia” todettiin, että unionin on unionin taloudellista turvallisuutta koskevan yhteisen strategiakehyksen avulla maksimoitava sen talouden avoimuudesta saatavat hyödyt niin, että samalla minimoidaan riskit, joita aiheutuu taloudellisista riippuvuuksista suuririskisistä toimittajista. Riippuvuudet digitaalisia elementtejä sisältävien tuotteiden suuririskisistä toimittajista voivat aiheuttaa strategisen riskin, jota on käsiteltävä unionin tasolla, erityisesti kun digitaalisia elementtejä sisältävät tuotteet on tarkoitettu direktiivin (EU) 2022/2555 3 artiklan 1 kohdassa tarkoitettujen keskeisten toimijoiden käyttöön. Tällaiset riskit voivat liittyä muun muassa valmistajaan sovellettavaan lainkäyttövaltaan, sen yritysomistusrakenteen ominaisuuksiin ja määräysvaltasuhteisiin sen kolmannen maan hallitukseen, johon valmistaja on sijoittautunut, erityisesti jos kolmas maa harjoittaa taloudellista vakoilua tai toimii vastuuttomasti kybertoimintaympäristössä ja sen lainsäädäntö mahdollistaa mielivaltaisen pääsyn kaikkiin yrityksen toimintoihin tai tietoihin, mukaan lukien kaupallisesti arkaluonteiset tiedot, ja se voi asettaa velvoitteita tiedustelutarkoituksissa ilman demokraattista valvontaa, valvontamekanismeja, oikeudenmukaista menettelyä tai oikeutta hakea muutosta riippumattomalta tuomioistuimelta. Kun komissio ja markkinavalvontaviranomaiset määrittävät tässä asetuksessa tarkoitetun kyberturvallisuusriskin merkittävyyttä, niiden olisi tässä asetuksessa vahvistettujen vastuidensa mukaisesti otettava huomioon myös muut kuin tekniset riskitekijät, erityisesti ne, jotka on todettu direktiivin (EU) 2022/2555 22 artiklan mukaisesti suoritettujen kriittisiä toimitusketjuja koskevien unionin tason koordinoitujen turvallisuusriskinarviointien tuloksena.

(59) Digitaalisia elementtejä sisältävien tuotteiden tietoturvan varmistamiseksi niiden markkinoille saattamisen jälkeen valmistajien olisi määritettävä tukiaika, jossa olisi otettava huomioon aika, jonka digitaalisia elementtejä sisältävän tuotteen odotetaan olevan käytössä. Tukiaikaa määrittäessään valmistajan olisi otettava huomioon erityisesti käyttäjien kohtuulliset odotukset, tuotteen luonne sekä asiaa koskeva unionin oikeus, jossa määritetään digitaalisia elementtejä sisältävien tuotteiden käyttöikä. Valmistajien olisi voitava ottaa huomioon myös muita merkityksellisiä tekijöitä. Kriteerejä olisi sovellettava tavalla, jolla varmistetaan oikeasuhtaisuus tukiajan määrittämisessä. Valmistajan olisi pyynnöstä toimitettava markkinavalvontaviranomaisille tiedot, jotka otettiin huomioon digitaalisia elementtejä sisältävän tuotteen tukiaikaa määritettäessä.

(60) Tukiajan, jonka ajan valmistaja varmistaa haavoittuvuuksien tehokkaan käsittelyn, olisi oltava vähintään viisi vuotta, paitsi jos digitaalisia elementtejä sisältävän tuotteen käyttöikä on alle viisi vuotta, jolloin valmistajan olisi varmistettava haavoittuvuuksien käsittely kyseisen käyttöiän ajan. Jos digitaalisia elementtejä sisältävää tuotetta voidaan kohtuudella odottaa käytettävän yli viisi vuotta, mikä pitää usein paikkansa laitteistokomponenttien, kuten emolevyjen tai mikroprosessorien, verkkolaitteiden, kuten reitittimien, modeemien tai kytkinten, sekä ohjelmistojen, kuten käyttöjärjestelmien tai videoneditointityökalujen, kohdalla, valmistajien olisi vastaavasti varmistettava pidemmät tukiajat. Erityisesti teollisuusympäristöissä käytettäväksi tarkoitettuja digitaalisia elementtejä sisältäviä tuotteita, kuten teollisuuden ohjausjärjestelmiä, käytetään usein merkittävästi pidempiä aikoja. Valmistajan olisi voitava määrittää alle viiden vuoden tukiaika ainoastaan, jos se on perusteltua kyseisen digitaalisia elementtejä sisältävän tuotteen luonteen vuoksi ja jos tuotteen odotetaan olevan käytössä alle viisi vuotta, jolloin tukiajan olisi vastattava aikaa, jonka tuotteen odotetaan olevan käytössä. Esimerkiksi pandemian aikana käytettäväksi tarkoitetun kontaktien jäljittämiseen käytettävän sovelluksen käyttöikä voisi olla vain pandemian keston mittainen. Lisäksi joitakin ohjelmistosovelluksia voidaan niiden luonteen vuoksi asettaa saataville vain tilausmallin pohjalta, erityisesti silloin, kun tilauksen päätyttyä sovellus lakkaa olemasta käyttäjän saatavilla eikä näin ollen ole enää käytössä.

(61) Kun digitaalisia elementtejä sisältävien tuotteiden tukiaika päättyy, valmistajien olisi harkittava tällaisten digitaalisia elementtejä sisältävien tuotteiden lähdekoodin luovuttamista joko muille yrityksille, jotka sitoutuvat jatkamaan haavoittuvuuksien käsittelypalvelujen tarjoamista, tai yleisölle, jotta varmistetaan, että haavoittuvuuksia voidaan käsitellä tukiajan päättymisen jälkeen. Jos valmistajat luovuttavat lähdekoodin muille yrityksille, niiden olisi voitava suojata digitaalisia elementtejä sisältävän tuotteen omistusoikeus ja estää lähdekoodin levittäminen yleisölle esimerkiksi sopimusjärjestelyin.

(62) Sen varmistamiseksi, että valmistajat kaikkialla unionissa määrittävät samankaltaisen tukiajan vastaaville digitaalisia elementtejä sisältäville tuotteille, hallinnollisen yhteistyön ryhmän olisi julkaistava tilastoja keskimääräisistä tukiajoista, jotka valmistajat ovat määrittäneet digitaalisia elementtejä sisältävien tuotteiden ryhmille, ja annettava ohjeita, joissa esitetään asianmukaiset tukiajat tällaisille ryhmille. Jotta voidaan varmistaa yhdenmukaistettu lähestymistapa koko sisämarkkinoilla, komission olisi lisäksi voitava antaa delegoituja säädöksiä, joissa täsmennetään tiettyjen tuoteryhmien tukiajan vähimmäiskesto, jos markkinavalvontaviranomaisten toimittamat tiedot viittaavat joko siihen, että valmistajien määrittämät tukiajat järjestelmällisesti eivät ole tässä asetuksessa säädettyjen tukiajan määrittämisperusteiden mukaisia, tai siihen, että valmistajat eri jäsenvaltioissa määrittävät perusteettomasti eripituisia tukiaikoja.

(63) Valmistajien olisi perustettava keskitetty yhteyspiste, jonka kautta käyttäjät voivat helposti viestiä niiden kanssa muun muassa ilmoittaakseen digitaalisia elementtejä sisältävän tuotteen haavoittuvuuksista ja saadakseen niistä tietoa. Niiden olisi asetettava keskitetty yhteyspiste helposti käyttäjien saataville ja ilmoitettava selkeästi, että se on käytettävissä, ja pidettävä nämä tiedot ajan tasalla. Jos valmistajat päättävät tarjota automatisoituja välineitä, kuten chat-palveluja, niiden olisi tarjottava myös puhelinnumero tai muu digitaalinen yhteydenottokeino, kuten sähköpostiosoite tai yhteydenottolomake. Keskitetyn yhteyspisteen ei pitäisi perustua yksinomaan automatisoituihin välineisiin.

(64) Valmistajien olisi asetettava digitaalisia elementtejä sisältävät tuotteensa saataville markkinoilla oletusarvoisesti tietoturvallisin asetuksin ja tarjottava käyttäjille tietoturvapäivityksiä maksutta. Valmistajien olisi voitava poiketa olennaisista kyberturvallisuusvaatimuksista vain sellaisten räätälöityjen tuotteiden osalta, jotka on sovitettu tiettyyn tarkoitukseen tiettyä yrityskäyttäjää varten, ja kun sekä valmistaja että käyttäjä ovat nimenomaisesti sopineet erilaisista sopimusehdoista.

(65) Valmistajien olisi ilmoitettava keskitetyn raportointialustan kautta samanaikaisesti sekä koordinaattoriksi nimetylle tietoturvaloukkauksiin reagoivalle ja niitä tutkivalle yksikölle (CSIRT-yksikkö) että ENISAlle digitaalisia elementtejä sisältäviin tuotteisiin sisältyvistä aktiivisesti hyödynnetyistä haavoittuvuuksista sekä kyseisten tuotteiden tietoturvaan vaikuttavista vakavista poikkeamista. Ilmoitusten tekemiseen olisi käytettävä koordinaattoriksi nimetyn CSIRT-yksikön sähköistä ilmoituspalvelua, ja niiden olisi oltava samanaikaisesti ENISAn saatavilla.

(66) Valmistajien olisi ilmoitettava aktiivisesti hyödynnetyistä haavoittuvuuksista sen varmistamiseksi, että koordinaattoreiksi nimetyillä CSIRT-yksiköillä ja ENISAlla on asianmukainen yleiskuva tällaisista haavoittuvuuksista ja että ne saavat direktiivissä (EU) 2022/2555 vahvistettujen tehtäviensä suorittamiseksi ja kyseisen direktiivin 3 artiklassa tarkoitettujen keskeisten ja tärkeiden toimijoiden kyberturvan yleisen tason nostamiseksi tarvitsemansa tiedot, sekä sen varmistamiseksi, että markkinavalvontaviranomaisten toiminta on tehokasta. Koska useimpia digitaalisia elementtejä sisältäviä tuotteita markkinoidaan koko sisämarkkinoilla, jokainen digitaalisia elementtejä sisältävien tuotteiden hyväksikäytetty haavoittuvuus olisi katsottava uhkaksi sisämarkkinoiden toiminnalle. ENISAn olisi valmistajan suostumuksella julkistettava korjatut haavoittuvuudet direktiivin (EU) 2022/2555 12 artiklan 2 kohdan nojalla perustetussa Euroopan haavoittuvuustietokannassa. Euroopan haavoittuvuustietokanta auttaa valmistajia havaitsemaan tiedossa olevat hyödynnettävissä olevat haavoittuvuudet niiden tuotteissa sen varmistamiseksi, että markkinoilla saataville asetetut tuotteet ovat tietoturvallisia.

(67) Valmistajien olisi myös ilmoitettava koordinaattoriksi nimetylle CSIRT-yksikölle ja ENISAlle kaikista vakavista poikkeamista, jotka vaikuttavat digitaalisia elementtejä sisältävän tuotteen tietoturvaan. Sen varmistamiseksi, että käyttäjät voivat reagoida nopeasti digitaalisia elementtejä sisältävien tuotteidensa tietoturvaan vaikuttaviin vakaviin poikkeamiin, valmistajien olisi ilmoitettava myös käyttäjille kaikista tällaisista poikkeamista ja tarvittaessa mahdollisista korjaavista toimenpiteistä, joita käyttäjät voivat toteuttaa poikkeaman vaikutusten lieventämiseksi, esimerkiksi julkaisemalla asiaankuuluvat tiedot verkkosivustoillaan tai ottamalla käyttäjiin suoraan yhteyttä, jos valmistajalla on tähän mahdollisuus ja se on kyberturvallisuusriskien vuoksi perusteltua.

(68) Aktiivisesti hyödynnetyt haavoittuvuudet koskevat tapauksia, joissa valmistaja toteaa, että sen käyttäjiin tai muihin luonnollisiin henkilöihin tai oikeushenkilöihin vaikuttava tietoturvaloukkaus on seurausta siitä, että pahantahtoinen toimija on hyödyntänyt heikkoutta jossakin digitaalisia elementtejä sisältävässä tuotteessa, jonka valmistaja on asettanut saataville markkinoilla. Esimerkkejä tällaisista haavoittuvuuksista voisivat olla heikkoudet tuotteen tunnistamis- ja todentamistoiminnoissa. Pakollista ilmoittamista ei pitäisi soveltaa sellaisiin haavoittuvuuksiin, jotka havaitaan ilman pahantahtoista aikomusta vilpittömässä mielessä tehtävää testausta, tutkimusta, korjaamista tai paljastamista varten järjestelmän omistajan ja sen käyttäjien tietoturvan tai turvallisuuden edistämiseksi. Digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavilla vakavilla poikkeamilla tarkoitetaan sen sijaan tilanteita, joissa kyberturvallisuuspoikkeama vaikuttaa valmistajan kehitys-, tuotanto- tai ylläpitoprosesseihin siten, että se voisi lisätä käyttäjien tai muiden henkilöiden kyberturvallisuusriskiä. Tällainen vakava poikkeama voisi olla esimerkiksi tilanne, jossa hyökkääjä on onnistunut soluttamaan haittaohjelman julkaisukanavaan, jonka kautta valmistaja julkaisee käyttäjille tietoturvapäivityksiä.

(69) Sen varmistamiseksi, että ilmoitukset voidaan välittää nopeasti kaikille koordinaattoreiksi nimetyille asiaankuuluville CSIRT-yksiköille, ja jotta valmistajat voisivat tehdä vain yhden ilmoituksen ilmoitusprosessin jokaisessa vaiheessa, ENISAn olisi perustettava keskitetty raportointialusta, jossa on kansalliset sähköiset ilmoituspalvelut. ENISAn olisi hallinnoitava ja ylläpidettävä keskitetyn raportointialustan päivittäistä toimintaa. Koordinaattoreiksi nimettyjen CSIRT-yksiköiden olisi ilmoitettava markkinavalvontaviranomaisille ilmoitetuista haavoittuvuuksista tai poikkeamista. Keskitetty raportointialusta olisi suunniteltava siten, että sillä varmistetaan ilmoitusten luottamuksellisuus erityisesti sellaisten haavoittuvuuksien osalta, joihin ei ole vielä saatavilla tietoturvapäivitystä. Lisäksi ENISAn olisi otettava käyttöön menettelyt tietojen tietoturvallista ja luottamuksellista käsittelyä varten. ENISAn olisi keräämiensä tietojen perusteella laadittava joka toinen vuosi tekninen raportti uusista kyberturvallisuusriskeihin liittyvistä suuntauksista digitaalisia elementtejä sisältävien tuotteiden alalla ja toimitettava se direktiivin (EU) 2022/2555 14 artiklan nojalla perustetulle yhteistyöryhmälle.

(70) Poikkeuksellisissa olosuhteissa ja erityisesti valmistajan pyynnöstä koordinaattoriksi nimetyn CSIRT-yksikön, joka alun perin vastaanottaa ilmoituksen, olisi voitava päättää lykätä ilmoituksen välittämistä muille koordinaattoreiksi nimetyille asiaankuuluville CSIRT-yksiköille keskitetyn raportointialustan kautta, jos tämä on aiheellista kyberturvallisuuteen liittyvistä syistä, ja niin, että ilmoituksen välittämistä lykätään vain ehdottoman välttämättömän ajan. Koordinaattoriksi nimetyn CSIRT-yksikön olisi välittömästi ilmoitettava ENISAlle lykkäämistä koskevasta päätöksestä ja päätöksen syistä sekä siitä, milloin se aikoo välittää ilmoituksen eteenpäin. Komission olisi laadittava delegoidulla säädöksellä eritelmät ehdoista, joiden täyttyessä kyberturvallisuuteen liittyviä syitä voitaisiin soveltaa, ja tehtävä yhteistyötä direktiivin (EU) 2022/2555 15 artiklan nojalla perustetun CSIRT-verkoston ja ENISAn kanssa valmistellessaan luonnosta delegoiduksi säädökseksi. Esimerkkejä kyberturvallisuuteen liittyvistä syistä ovat meneillään oleva koordinoitu haavoittuvuuksien julkistamismenettely tai tilanteet, joissa valmistajan odotetaan pian tarjoavan lieventävän toimenpiteen ja ilmoituksen välittämiseen viipymättä keskitetyn raportointialustan kautta liittyvät kyberturvallisuusriskit ovat suuremmat kuin siitä saatavat hyödyt. ENISAn olisi koordinaattoriksi nimetyn CSIRT-yksikön pyynnöstä voitava tukea kyseistä CSIRT-yksikköä, kun se lykkää ilmoituksen välittämistä kyberturvallisuuteen liittyvistä syistä, niiden tietojen perusteella, jotka ENISA on saanut kyseiseltä CSIRT-yksiköltä päätöksestä olla välittämättä ilmoitusta kyseisten kyberturvallisuuteen liittyvien syiden perusteella. Erityisen poikkeuksellisissa olosuhteissa ENISA ei myöskään saisi saada samanaikaisesti aktiivisesti hyödynnettyä haavoittuvuutta koskevan ilmoituksen kaikkia yksityiskohtia.

Tämä koskisi tilanteita, joissa valmistaja toteaa ilmoituksessaan, että pahantahtoinen toimija on aktiivisesti hyödyntänyt ilmoitettua haavoittuvuutta ja käytettävissä olevien tietojen mukaan sitä on hyödynnetty ainoastaan sen koordinaattoriksi nimetyn CSIRT-yksikön jäsenvaltiossa, jolle valmistaja on ilmoittanut haavoittuvuudesta, tai tilanteita, joissa ilmoitettua haavoittuvuutta koskevan tiedon välitön eteenpäin välittäminen johtaisi todennäköisesti sellaisten tietojen toimittamiseen, joiden julkistaminen olisi vastoin kyseisen jäsenvaltion keskeisiä etuja, tai tilanteita, joissa ilmoitettu haavoittuvuus aiheuttaa välittömän korkean kyberturvallisuusriskin, joka johtuu tietojen välittämisestä eteenpäin. Tällaisissa tapauksissa ENISA saa samanaikaisesti vain tiedon siitä, että valmistaja on tehnyt ilmoituksen, yleiset tiedot kyseessä olevasta digitaalisia elementtejä sisältävästä tuotteesta, tiedon hyödyntämisen yleisestä luonteesta ja tiedon siitä, että valmistaja on vedonnut kyseisiin turvallisuussyihin ja että ilmoituksen koko sisältöä ei ole näin ollen annettu. Täydellinen ilmoitus olisi sen jälkeen asetettava ENISAn ja muiden koordinaattoreiksi nimettyjen asiaankuuluvien CSIRT-yksiköiden saataville, kun alun perin ilmoituksen vastaanottanut koordinaattoriksi nimetty CSIRT-yksikkö toteaa, että kyseiset turvallisuussyyt, jotka johtuvat tämän asetuksen mukaisista erityisen poikkeuksellisista olosuhteista, eivät enää ole olemassa. Jos ENISA katsoo saatavilla olevien tietojen perusteella, että on olemassa järjestelmäriski, joka vaikuttaa sisämarkkinoiden turvallisuuteen, ENISAn olisi suositeltava ilmoituksen vastaanottaneelle CSIRT-yksikölle, että se välittää täydellisen ilmoituksen muille koordinaattoreiksi nimetyille CSIRT-yksiköille ja ENISAlle.

(71) Kun valmistajat ilmoittavat aktiivisesti hyödynnetystä haavoittuvuudesta tai vakavasta poikkeamasta, joka vaikuttaa digitaalisia elementtejä sisältävän tuotteen tietoturvaan, niiden olisi ilmoitettava, kuinka arkaluonteisina ne pitävät ilmoitettuja tietoja. Koordinaattoriksi nimetyn CSIRT-yksikön, joka on alun perin vastaanottanut ilmoituksen, olisi otettava nämä tiedot huomioon arvioidessaan, aiheuttaako ilmoitus poikkeuksellisia olosuhteita, joiden vuoksi on aiheellista lykätä ilmoituksen välittämistä muille koordinaattoreiksi nimetyille asiaankuuluville CSIRT-yksiköille aiheellisten kyberturvallisuuteen liittyvien syiden perusteella. Sen olisi myös otettava nämä tiedot huomioon arvioidessaan, aiheuttaako aktiivisesti hyödynnettyä haavoittuvuutta koskeva ilmoitus erityisen poikkeuksellisia olosuhteita, joiden vuoksi täydellistä ilmoitusta ei aseteta samanaikaisesti ENISAn saataville. Koordinaattoreiksi nimettyjen CSIRT-yksiköiden olisi myös voitava ottaa nämä tiedot huomioon määrittäessään asianmukaisia toimenpiteitä tällaisista haavoittuvuuksista ja poikkeamista johtuvien riskien lieventämiseksi.

(72) Jotta voidaan yksinkertaistaa tässä asetuksessa edellytettyjen tietojen raportointia ja ottaa huomioon muut unionin oikeudessa, kuten asetuksessa (EU) 2016/679, Euroopan parlamentin ja neuvoston asetuksessa (EU) 2022/2554[24], Euroopan parlamentin ja neuvoston direktiivissä 2002/58/EY[25] ja direktiivissä (EU) 2022/2555, säädetyt täydentävät raportointivaatimukset sekä keventää toimijoiden hallinnollista rasitetta, jäsenvaltioita kannustetaan harkitsemaan keskitettyjen asiointipisteiden tarjoamista kansallisella tasolla tällaisia raportointivaatimuksia varten. Tällaisten kansallisten keskitettyjen asiointipisteiden käyttö asetuksen (EU) 2016/679 ja direktiivin 2002/58/EY mukaisten tietoturvapoikkeamien ilmoittamiseen ei saisi vaikuttaa asetuksen (EU) 2016/679 ja direktiivin 2002/58/EY säännösten soveltamiseen, etenkään niiden säännösten, jotka koskevat niissä tarkoitettujen viranomaisten riippumattomuutta. Tässä asetuksessa tarkoitettua keskitettyä raportointialustaa perustaessaan ENISAn olisi otettava huomioon, että tässä asetuksessa tarkoitetut kansalliset sähköiset ilmoituspalvelut voidaan sisällyttää kansallisiin keskitettyihin asiointipisteisiin, joiden kautta voi olla mahdollista tehdä myös muita unionin oikeudessa edellytettyjä ilmoituksia.

---

[24] Euroopan parlamentin ja neuvoston asetus (EU) 2022/2554, annettu 14 päivänä joulukuuta 2022, finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU) N:o 600/2014, (EU) N:o 909/2014 ja (EU) 2016/1011 muuttamisesta (EUVL L 333, 27.12.2022, s. 1).

[25] Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (EYVL L 201, 31.7.2002, s. 37).

(73) Kun ENISA perustaa tässä asetuksessa tarkoitettua keskitettyä raportointialustaa, sen olisi aiempien kokemusten hyödyntämiseksi kuultava unionin muita toimielimiä tai virastoja, jotka hallinnoivat alustoja tai tietokantoja, joihin sovelletaan tiukkoja tietoturvavaatimuksia, kuten vapauden, turvallisuuden ja oikeuden alueen laaja-alaisten tietojärjestelmien operatiivisesta hallinnoinnista vastaavaa Euroopan unionin virastoa (eu-LISA). ENISAn olisi myös analysoitava, miten alustalla voitaisiin mahdollisesti täydentää direktiivin (EU) 2022/2555 12 artiklan 2 kohdan nojalla perustettua Euroopan haavoittuvuustietokantaa.

(74) Valmistajien ja muiden luonnollisten henkilöiden ja oikeushenkilöiden olisi voitava vapaaehtoisesti ilmoittaa koordinaattoriksi nimetylle CSIRT-yksikölle tai ENISAlle mahdollisista digitaalisia elementtejä sisältävän tuotteen haavoittuvuuksista, kyberuhkista, jotka voisivat vaikuttaa digitaalisia elementtejä sisältävän tuotteen riskiprofiiliin, mahdollisista digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavista poikkeamista, sekä läheltä piti -tilanteista, jotka olisivat voineet johtaa tällaiseen poikkeamaan.

(75) Jäsenvaltioiden olisi pyrittävä mahdollisuuksien mukaan puuttumaan haavoittuvuuksia tutkivien kohtaamiin haasteisiin, kuten mahdollisuuteen, että he joutuvat rikosoikeudelliseen vastuuseen, kansallisen lainsäädäntönsä mukaisesti. Koska haavoittuvuuksia tutkivat luonnolliset henkilöt ja oikeushenkilöt voisivat joissakin jäsenvaltioissa joutua rikosoikeudelliseen ja siviilioikeudelliseen vastuuseen, jäsenvaltioita kannustetaan antamaan ohjeita tietoturvaa tutkivien syyttämättä jättämisestä ja vapauttamisesta siviilioikeudellisesta vastuusta niiden toiminnan osalta.

(76) Digitaalisia elementtejä sisältävien tuotteiden valmistajien olisi otettava käyttöön koordinoitua haavoittuvuuksien julkistamista koskevat periaatteet, jotka auttaisivat yksityishenkilöitä tai toimijoita ilmoittamaan haavoittuvuuksista joko suoraan valmistajalle tai välillisesti ja pyydettäessä nimettömästi sellaisten CSIRT-yksiköiden kautta, jotka on nimetty koordinaattoreiksi direktiivin (EU) 2022/2555 12 artiklan 1 kohdan mukaista koordinoitua haavoittuvuuksien julkistamista varten. Valmistajien koordinoitua haavoittuvuuksien julkistamista koskevissa periaatteissa olisi määritettävä jäsennelty prosessi, jonka avulla haavoittuvuuksista ilmoitetaan valmistajalle siten, että se voi diagnosoida ja korjata tällaiset haavoittuvuudet ennen kuin haavoittuvuudesta annetaan yksityiskohtaisia tietoja kolmansille osapuolille tai yleisölle. Valmistajien olisi myös harkittava tietoturvaperiaatteidensa julkaisemista koneellisesti luettavassa muodossa. Kun otetaan huomioon, että tietoa yleisesti käytettyjen digitaalisia elementtejä sisältävien tuotteiden hyödynnettävissä olevista haavoittuvuuksista voidaan myydä korkeaan hintaan pimeillä markkinoilla, tällaisten tuotteiden valmistajien olisi voitava käyttää osana koordinoitua haavoittuvuuksien julkistamista koskevia periaatteitaan erityisiä ohjelmia, joilla luodaan kannustimia haavoittuvuuksista ilmoittamiseen varmistamalla, että yksityishenkilöt tai toimijat saavat tunnustusta ja korvauksen toimistaan. Tällä tarkoitetaan niin sanottuja bug bounty -ohjelmia.

(77) Haavoittuvuusanalyysin helpottamiseksi valmistajien olisi yksilöitävä ja dokumentoitava digitaalisia elementtejä sisältävien tuotteidensa komponentit muun muassa laatimalla ohjelmistojen materiaaliluettelo. Ohjelmistojen materiaaliluettelosta ohjelmistojen valmistajat, ostajat ja käyttäjät voivat saada tietoja, jotka parantavat heidän ymmärrystään toimitusketjusta, mistä saadaan monia hyötyjä. Erityisesti se auttaa valmistajia ja käyttäjiä jäljittämään tiedossa olevia uusia haavoittuvuuksia ja kyberturvallisuusriskejä. Valmistajien on erityisen tärkeää varmistaa, että niiden digitaalisia elementtejä sisältävät tuotteet eivät sisällä kolmansien osapuolten kehittämiä haavoittuvia komponentteja. Valmistajia ei pitäisi velvoittaa julkistamaan ohjelmistojen materiaaliluetteloa.

(78) Verkkomyyntiin liittyvien uusien monimutkaisten liiketoimintamallien mukaisesti verkossa toimiva yritys voi tarjota monenlaisia palveluja. Sama toimija voi tietyn digitaalisia elementtejä sisältävän tuotteen osalta tarjoamiensa palvelujen luonteen mukaan kuulua eri liiketoimintamallien tai talouden toimijoiden ryhmiin. Jos toimija tarjoaa ainoastaan verkossa toimivia välityspalveluja tietyn digitaalisia elementtejä sisältävän tuotteen osalta ja on ainoastaan asetuksen (EU) 2023/988 3 artiklan 14 alakohdassa määritelty verkkomarkkinapaikan tarjoaja, sen ei katsota olevan minkään tässä asetuksessa määritellyn tyyppinen talouden toimija. Jos sama toimija on verkkomarkkinapaikan tarjoaja ja myös toimii tässä asetuksessa määriteltynä talouden toimijana tiettyjen digitaalisia elementtejä sisältävien tuotteiden myynnissä, siihen olisi sovellettava tässä asetuksessa tämäntyyppiselle talouden toimijalle vahvistettuja velvoitteita. Jos esimerkiksi verkkomarkkinapaikan tarjoaja myös jakelee jotakin digitaalisia elementtejä sisältävää tuotetta, se katsottaisiin kyseisen tuotteen myynnin osalta jakelijaksi. Vastaavasti jos kyseinen toimija myy omalla tuotemerkillään varustettuja digitaalisia elementtejä sisältäviä tuotteita, se katsottaisiin valmistajaksi ja sen olisi näin ollen noudatettava valmistajiin sovellettavia vaatimuksia. Jotkin toimijat voivat myös olla Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/1020[26] 3 artiklan 11 alakohdassa määriteltyjä jakelupalvelujen tarjoajia, jos ne tarjoavat tällaisia palveluja. Tällaiset tapaukset olisi arvioitava tapauskohtaisesti. Koska verkkomarkkinapaikoilla on merkittävä rooli verkkokaupan mahdollistamisessa, niiden olisi pyrittävä tekemään yhteistyötä jäsenvaltioiden markkinavalvontaviranomaisten kanssa auttaakseen sen varmistamisessa, että verkkomarkkinapaikkojen kautta ostetut digitaalisia elementtejä sisältävät tuotteet ovat tässä asetuksessa säädettyjen kyberturvallisuusvaatimusten mukaisia.

---

[26] 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).

(79) Tässä asetuksessa säädettyjen vaatimusten noudattamisen arvioinnin helpottamiseksi digitaalisia elementtejä sisältävien tuotteiden olisi voitava olettaa olevan vaatimusten mukaisia, jos ne ovat sellaisten Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1025/2012[27] mukaisesti hyväksyttyjen yhdenmukaistettujen standardien mukaisia, jotka muuntavat tässä asetuksessa vahvistetut olennaiset kyberturvallisuusvaatimukset yksityiskohtaisiksi teknisiksi eritelmiksi. Kyseisessä asetuksessa säädetään menettelystä vastalauseiden esittämiseksi yhdenmukaistetuista standardeista tapauksissa, joissa kyseiset standardit eivät kokonaan täytä tässä asetuksessa vahvistettuja vaatimuksia. Standardointiprosessissa olisi varmistettava etujen tasapuolinen edustus ja kansalaisyhteiskunnan sidosryhmien, myös kuluttajajärjestöjen, tehokas osallistuminen. Lisäksi olisi otettava huomioon kansainväliset standardit, jotka ovat tässä asetuksessa vahvistetuilla olennaisilla kyberturvallisuusvaatimuksilla tavoitellun kyberturvallisuuden suojan tason mukaisia, jotta voidaan helpottaa yhdenmukaistettujen standardien kehittämistä ja tämän asetuksen täytäntöönpanoa sekä helpottaa vaatimusten noudattamista yritysten, erityisesti mikroyritysten ja pienten ja keskisuurten yritysten sekä maailmanlaajuisesti toimivien yritysten, kannalta.

---

[27] 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).

(80) Asetuksen tehokkaan täytäntöönpanon kannalta on erityisen tärkeää, että yhdenmukaistetut standardit kehitetään oikea-aikaisesti tämän asetuksen soveltamisen siirtymäkauden aikana ja että ne ovat saatavilla ennen tämän asetuksen soveltamispäivää. Tämä koskee erityisesti digitaalisia elementtejä sisältäviä tärkeitä tuotteita, jotka kuuluvat luokkaan I. Yhdenmukaistettujen standardien saatavuus mahdollistaa sen, että tällaisten tuotteiden valmistajat voivat suorittaa vaatimustenmukaisuuden arviointeja sisäisen valvonnan menettelyllä, ja siten sillä voidaan välttää pullonkaulat ja viivästykset vaatimustenmukaisuuden arviointilaitosten toiminnassa.

(81) Asetuksella (EU) 2019/881 perustetaan vapaaehtoinen eurooppalainen kyberturvallisuuden sertifiointikehys tieto- ja viestintäteknisille tuotteille, tieto- ja viestintäteknisille prosesseille ja tieto- ja viestintäteknisille palveluille. Eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät tarjoavat käyttäjille yhteisen luotettavuuskehyksen tämän asetuksen soveltamisalaan kuuluvien, digitaalisia elementtejä sisältävien tuotteiden käyttöä varten. Niinpä tällä asetuksella olisi luotava synergioita asetuksen (EU) 2019/881 kanssa. Tässä asetuksessa säädettyjen vaatimusten noudattamisen arvioinnin helpottamiseksi digitaalisia elementtejä sisältävien tuotteiden, jotka on sertifioitu tai joista on annettu vaatimustenmukaisuusilmoitus asetuksen (EU) 2019/881 mukaisessa ja komission täytäntöönpanosäädöksellä yksilöimässä eurooppalaisessa kyberturvallisuusjärjestelmässä, katsotaan olevan tässä asetuksessa vahvistettujen olennaisten kyberturvallisuusvaatimusten mukaisia siltä osin kuin eurooppalainen kyberturvallisuussertifikaatti tai vaatimustenmukaisuusilmoitus tai niiden osat kattavat kyseiset vaatimukset. Tarvetta uusille digitaalisia elementtejä sisältäviä tuotteita koskeville eurooppalaisille kyberturvallisuuden sertifiointijärjestelmille olisi arvioitava tämän asetuksen valossa, myös valmisteltaessa unionin jatkuvaa työohjelmaa asetuksen (EU) 2019/881 mukaisesti. Jos muun muassa tämän asetuksen noudattamisen helpottamiseksi tarvitaan uusi järjestelmä, joka kattaa digitaalisia elementtejä sisältävät tuotteet, komissio voi pyytää ENISAa valmistelemaan ehdolla olevia järjestelmiä asetuksen (EU) 2019/881 48 artiklan mukaisesti. Tällaisissa tulevissa eurooppalaisissa kyberturvallisuuden sertifiointijärjestelmissä, jotka kattavat digitaalisia elementtejä sisältävät tuotteet, olisi otettava huomioon tässä asetuksessa vahvistetut olennaiset kyberturvallisuusvaatimukset ja vaatimustenmukaisuuden arviointimenettelyt ja niillä olisi helpotettava tämän asetuksen noudattamista. Ennen tämän asetuksen voimaantuloa voimaan tulevien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien osalta voi olla tarpeen täsmentää yksityiskohtaisia näkökohtia, jotka liittyvät siihen, miten vaatimustenmukaisuusolettamaa voidaan soveltaa.

Komissiolle olisi siirrettävä valta määrittää delegoiduilla säädöksillä ehdot, joiden mukaisesti eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä voidaan käyttää osoittamaan tässä asetuksessa vahvistettujen olennaisten kyberturvallisuusvaatimusten täyttyminen. Lisäksi tarpeettoman hallinnollisen taakan välttämiseksi valmistajia ei saisi velvoittaa teettämään vastaavien vaatimusten osalta tässä asetuksessa säädettyä kolmannen osapuolen suorittamaa vaatimustenmukaisuuden arviointia, jos tällaisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien nojalla on myönnetty vähintään varmuustason ”korotettu” eurooppalainen kyberturvallisuussertifikaatti.

(82) Kun täytäntöönpanoasetus (EU) 2024/482, joka koskee tämän asetuksen soveltamisalaan kuuluvia tuotteita, kuten laitteistoturvamoduuleja ja mikroprosessoreja, tulee voimaan, komission olisi voitava delegoidulla säädöksellä täsmentää, miten eurooppalaisiin yhteisiin kriteereihin perustuva kyberturvallisuuden sertifiointijärjestelmä luo olettaman tässä asetuksessa vahvistettujen olennaisten kyberturvallisuusvaatimusten tai niiden osien täyttymisestä. Lisäksi tällaisessa delegoidussa säädöksessä voidaan täsmentää, miten eurooppalaisiin yhteisiin kriteereihin perustuvan kyberturvallisuuden sertifiointijärjestelmän mukaisesti myönnetty sertifikaatti poistaa valmistajilta velvoitteen teettää vastaavien vaatimusten osalta tämän asetuksen nojalla vaadittu kolmannen osapuolen suorittama arviointi.

(83) Nykyinen eurooppalainen standardointikehys, joka perustuu teknistä yhdenmukaistamista ja standardeja koskevasta uudesta lähestymistavasta 7 päivänä toukokuuta 1985 annetussa neuvoston päätöslauselmassa ja asetuksessa (EU) N:o 1025/2012 vahvistettuihin uuden lähestymistavan periaatteisiin, muodostaa oletusarvoisesti kehyksen sellaisten standardien laatimiselle, jotka luovat tässä asetuksessa vahvistettuja asiaankuuluvia olennaisia kyberturvallisuusvaatimuksia koskevan vaatimustenmukaisuusolettaman. Eurooppalaisten standardien olisi oltava markkinalähtöisiä, niissä olisi otettava huomioon yleinen etu sekä toimintapoliittiset tavoitteet, jotka ilmaistaan selkeästi komission yhdelle tai useammalle eurooppalaiselle standardointiorganisaatiolle esittämässä pyynnössä yhdenmukaistettujen standardien laatimisesta asetetussa määräajassa, ja niiden olisi perustuttava yhteisymmärrykseen. Asiaa koskevien yhdenmukaistettujen standardien viitetietojen puuttuessa komission olisi kuitenkin voitava hyväksyä täytäntöönpanosäädöksiä, joissa vahvistetaan tässä asetuksessa vahvistettuja olennaisia kyberturvallisuusvaatimuksia koskevia yhteisiä eritelmiä edellyttäen, että se näin tehdessään ottaa asianmukaisesti huomioon standardointiorganisaatioiden aseman ja tehtävät. Kyseessä on poikkeuksellinen vararatkaisu, johon turvautumalla valmistaja voi täyttää velvollisuutensa noudattaa kyseisiä olennaisia kyberturvallisuusvaatimuksia tilanteessa, jossa standardointimenettely on keskeytynyt tai asianmukaisten yhdenmukaistettujen standardien laatiminen viivästyy. Jos tällainen viive johtuu kyseessä olevan standardin teknisestä monimutkaisuudesta, komission olisi otettava tämä huomioon ennen kuin se harkitsee yhteisten eritelmien vahvistamista.

(84) Jotta voidaan vahvistaa mahdollisimman tehokkaasti yhteiset eritelmät, jotka kattavat tässä asetuksessa vahvistetut olennaiset kyberturvallisuusvaatimukset, komission olisi otettava asiaankuuluvat sidosryhmät mukaan prosessiin.

(85) Kohtuullisella määräajalla, joka koskee yhdenmukaistettujen standardien viitetietojen julkaisemista *Euroopan unionin virallisessa lehdessä* asetuksen (EU) N:o 1025/2012 mukaisesti, tarkoitetaan ajanjaksoa, jonka aikana standardin viitetietojen, sen oikaisun tai sen muutoksen julkaiseminen *Euroopan unionin virallisessa lehdessä* on odotettavissa ja joka ei saisi olla pidempi kuin vuosi asetuksen (EU) N:o 1025/2012 mukaisesti asetetun eurooppalaisen standardin laatimisen määräajan jälkeen.

(86) Tässä asetuksessa vahvistettujen olennaisten kyberturvallisuusvaatimusten täyttymisen arvioinnin helpottamiseksi olisi voitava olettaa, että digitaalisia elementtejä sisältävät tuotteet ovat vaatimustenmukaisia, jos ne ovat sellaisten yhteisten eritelmien mukaisia, jotka komissio on hyväksynyt tämän asetuksen nojalla antaakseen näitä vaatimuksia koskevat yksityiskohtaiset tekniset eritelmät.

(87) Valmistajien suorittamaa vaatimustenmukaisuuden arviointia voidaan helpottaa soveltamalla asetuksen (EU) 2019/881 nojalla hyväksyttyjä yhdenmukaistettuja standardeja, yhteisiä eritelmiä tai eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä, joilla luodaan vaatimustenmukaisuusolettama digitaalisia elementtejä sisältäviin tuotteisiin sovellettavien olennaisten kyberturvallisuusvaatimusten suhteen. Jos valmistaja päättää olla soveltamatta tällaisia keinoja tiettyjen vaatimusten osalta, sen on ilmoitettava teknisissä asiakirjoissaan, millä muulla tavalla vaatimustenmukaisuus on saavutettu. Lisäksi se, että valmistajat soveltaisivat asetuksen (EU) 2019/881 nojalla hyväksyttyjä yhdenmukaistettuja standardeja, yhteisiä eritelmiä tai eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä, jotka luovat vaatimustenmukaisuusolettaman, helpottaisi markkinavalvontaviranomaisten suorittamaa digitaalisia elementtejä sisältävien tuotteiden vaatimustenmukaisuuden tarkastamista. Sen vuoksi digitaalisia elementtejä sisältävien tuotteiden valmistajia kannustetaan soveltamaan tällaisia yhdenmukaistettuja standardeja, yhteisiä eritelmiä tai eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä.

(88) Valmistajien olisi laadittava EU-vaatimustenmukaisuusvakuutus, jossa annetaan tässä asetuksessa edellytetyt tiedot siitä, että digitaalisia elementtejä sisältävä tuote on tässä asetuksessa vahvistettujen olennaisten kyberturvallisuusvaatimusten sekä soveltuvin osin unionin muun asiaankuuluvan yhdenmukaistamislainsäädännön, jonka piiriin digitaalisia elementtejä sisältävä tuote kuuluu, mukainen. Valmistajilta saatetaan edellyttää EU-vaatimustenmukaisuusvakuutuksen laatimista myös muiden unionin säädösten nojalla. Jotta voidaan varmistaa tehokas tiedonsaanti markkinavalvontaa varten, kaikkien asiaankuuluvien unionin säädösten vaatimusten noudattamisen osalta olisi laadittava yksi ainoa EU-vaatimustenmukaisuusvakuutus. Talouden toimijoiden hallinnollisen rasitteen vähentämiseksi tämän yhden ainoan EU-vaatimustenmukaisuusvakuutuksen olisi voitava olla asiakirja, joka koostuu asiaankuuluvista yksittäisistä vaatimustenmukaisuusvakuutuksista.

(89) 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[28]. CE-merkinnän kiinnittämistä tai liittämistä digitaalisia elementtejä sisältäviin tuotteisiin koskevat säännöt olisi annettava tässä asetuksessa. CE-merkinnän olisi oltava ainoa merkintä, joka takaa, että digitaalisia elementtejä sisältävät tuotteet ovat tässä asetuksessa vahvistettujen vaatimusten mukaisia.

---

[28] 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).

(90) Jotta talouden toimijat voivat osoittaa tässä asetuksessa vahvistettujen olennaisten kyberturvallisuusvaatimusten täyttymisen ja jotta markkinavalvontaviranomaiset voivat varmistaa, että 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[29] vahvistetaan vaatimustenmukaisuuden arviointimenettelyjen moduulit suhteessa kyseiseen riskitasoon ja vaadittuun turvallisuustasoon. Eri toimialojen välisen johdonmukaisuuden varmistamiseksi ja tapauskohtaisten vaihtelun välttämiseksi vaatimustenmukaisuuden arviointimenettelyjen, jotka riittävät sen todentamiseen, että digitaalisia elementtejä sisältävät tuotteet täyttävät tässä asetuksessa vahvistetut olennaiset kyberturvallisuusvaatimukset, olisi perustuttava kyseisiin moduuleihin. Vaatimustenmukaisuuden arviointimenettelyissä olisi tutkittava ja todennettava sekä tuotteisiin että prosesseihin liittyvät vaatimukset digitaalisia elementtejä sisältävien tuotteiden koko elinkaaren ajalta, mukaan lukien digitaalisia elementtejä sisältävän tuotteen suunnittelu, rakenne, kehittäminen tai tuotanto, testaus ja ylläpito.

[29] 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).

(91) Valmistaja voi suorittaa omalla vastuullaan sellaisten digitaalisia elementtejä sisältävien tuotteiden vaatimustenmukaisuuden arvioinnin, jotka eivät ole tässä asetuksessa olevissa digitaalisia elementtejä sisältävien tärkeiden tai kriittisten tuotteiden luetteloissa, noudattaen päätöksen N:o 768/2008/EY moduuliin A perustuvaa sisäiseen valvontaan perustuvaa menettelyä tämän asetuksen mukaisesti. Tämä koskee myös tapauksia, joissa valmistaja päättää olla soveltamatta kokonaan tai osittain sovellettavaa yhdenmukaistettua standardia, yhteistä eritelmää tai eurooppalaista kyberturvallisuuden sertifiointijärjestelmää. Valmistaja voi joustavasti valita tiukemman vaatimustenmukaisuuden arviointimenettelyn, johon osallistuu kolmas osapuoli. Sisäiseen valvontaan perustuvassa vaatimustenmukaisuuden arviointimenettelyssä valmistaja varmistaa ja vakuuttaa yksinomaisella vastuullaan, että digitaalisia elementtejä sisältävä tuote ja valmistajan prosessit täyttävät tässä asetuksessa vahvistetut sovellettavat olennaiset kyberturvallisuusvaatimukset. Jos digitaalisia elementtejä sisältävä tärkeä tuote kuuluu luokkaan I, tarvitaan lisätakeita sen osoittamiseksi, että tuote täyttää tässä asetuksessa vahvistetut olennaiset kyberturvallisuusvaatimukset. Jos valmistaja haluaa suorittaa vaatimustenmukaisuuden arvioinnin omalla vastuullaan (moduuli A), sen olisi sovellettava yhdenmukaistettuja standardeja, yhteisiä eritelmiä tai asetuksen (EU) 2019/881 nojalla hyväksyttyjä ja komission täytäntöönpanosäädöksellä yksilöityjä eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä. Jos valmistaja ei sovella tällaisia yhdenmukaistettuja standardeja, yhteisiä eritelmiä tai eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä, sen olisi tehtävä vaatimustenmukaisuuden arviointi, johon osallistuu kolmas osapuoli (perustuen moduuliin B ja C tai moduuliin H). 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 N:o 768/2008/EY moduuleihin B ja C tai moduuliin H perustuvat vaatimustenmukaisuuden arviointimenettelyt on valittu sopivimmiksi tavoiksi arvioida digitaalisia elementtejä sisältävien tärkeiden tuotteiden vaatimustenmukaisuus oikeasuhteisesti ja tehokkaasti.

Valmistaja, joka käyttää kolmannen osapuolen suorittamaa vaatimustenmukaisuuden arviointia, voi valita suunnittelu- ja tuotantoprosessiinsa parhaiten soveltuvan menettelyn. Koska luokkaan II kuuluvien digitaalisia elementtejä sisältävien tärkeiden tuotteiden käyttöön liittyy vieläkin suurempi kyberturvallisuusriski, vaatimustenmukaisuuden arvioinnissa olisi aina oltava mukana kolmas osapuoli, vaikka tuote olisi kokonaan tai osittain yhdenmukaistettujen standardien, yhteisten eritelmien tai eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukainen. Vapaiksi ja avoimen lähdekoodin ohjelmistoiksi luokiteltavien digitaalisia elementtejä sisältävien tärkeiden tuotteiden valmistajien olisi voitava noudattaa moduuliin A perustuvaa sisäisen valvonnan menettelyä edellyttäen, että ne asettavat tekniset asiakirjat yleisesti saataville.

(92) Digitaalisia elementtejä sisältävien aineellisten tuotteiden luominen edellyttää yleensä valmistajilta huomattavia panostuksia sekä suunnittelu- ja kehitys- että tuotantovaiheessa, kun taas ohjelmistojen muodossa olevien digitaalisia elementtejä sisältävien tuotteiden luominen painottuu lähes yksinomaan suunnitteluun ja kehittämiseen, jolloin tuotantovaiheella on vähäisempi merkitys. Monissa tapauksissa ohjelmistotuotteet on kuitenkin vielä käännettävä, koostettava, pakattava, asetettava saataville ladattavaksi tai kopioitava fyysisille tallennusvälineille ennen markkinoille saattamista. Kyseiset toimet olisi katsottava tuotantoa vastaaviksi toimiksi, kun sovelletaan asiaankuuluvia vaatimustenmukaisuuden arviointimoduuleja sen todentamiseksi, että tuote on tässä asetuksessa suunnittelu-, kehitys- ja tuotantovaiheille vahvistettujen olennaisten kyberturvallisuusvaatimusten mukainen.

(93) Jotta voidaan varmistaa oikeasuhtaisuus mikroyritysten ja pienten yritysten kannalta, on asianmukaista keventää hallinnollisia kustannuksia vaikuttamatta tämän asetuksen soveltamisalaan kuuluvien digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuuden suojan tasoon tai valmistajien tasapuolisiin toimintaedellytyksiin. Niinpä komission on aiheellista vahvistaa yksinkertaistettu teknisten asiakirjojen muoto, joka on kohdennettu mikroyritysten ja pienten yritysten tarpeisiin. Komission hyväksymän yksinkertaistetun teknisten asiakirjojen muodon olisi katettava kaikki teknisiin asiakirjoihin liittyvät tässä asetuksessa vahvistetut sovellettavat tiedot ja siinä olisi täsmennettävä, miten mikroyritys tai pieni yritys voi toimittaa tiiviissä muodossa pyydetyt tiedot, kuten kuvauksen digitaalisia elementtejä sisältävän tuotteen suunnittelusta, kehittämisestä ja tuotannosta. Näin muodolla osaltaan kevennettäisiin vaatimusten noudattamiseen liittyvää hallinnollista rasitetta, koska se antaisi asianomaisille yrityksille oikeusvarmuuden siitä, miten laajat ja yksityiskohtaiset tiedot niiden on toimitettava. Mikroyritysten ja pienten yritysten olisi voitava valita, että ne toimittavat teknisiin asiakirjoihin liittyvät sovellettavat tiedot laajassa muodossa eivätkä hyödynnä käytettävissään olevaa yksinkertaistettua teknisten asiakirjojen muotoa.

(94) Innovoinnin edistämiseksi ja suojelemiseksi on tärkeää, että otetaan erityisesti huomioon sellaisten valmistajien edut, jotka ovat mikroyrityksiä tai pieniä tai keskisuuria yrityksiä, erityisesti mikroyrityksiä ja pieniä yrityksiä, mukaan lukien startup-yritykset. Tätä varten jäsenvaltiot voisivat kehittää valmistajille, jotka ovat mikroyrityksiä tai pieniä yrityksiä, aloitteita, jotka koskevat muun muassa koulutusta, tietoisuuden lisäämistä, tiedotusta, testausta ja kolmansien osapuolten suorittamaa vaatimustenmukaisuuden arviointitoimintaa sekä testiympäristöjen perustamista. Pakollisiin asiakirjoihin, kuten teknisiin asiakirjoihin ja tämän asetuksen nojalla vaadittaviin käyttäjille annettaviin tietoihin ja ohjeisiin, sekä yhteydenpitoon viranomaisten kanssa liittyvät käännöskustannukset voivat aiheuttaa merkittäviä kustannuksia valmistajille, erityisesti pienemmille valmistajille. Niinpä jäsenvaltioiden olisi voitava pitää huolta siitä, että yksi kielistä, jonka ne ovat määrittäneet ja hyväksyneet käytettäväksi valmistajien asiaankuuluvissa asiakirjoissa ja viestinnässä valmistajien kanssa, on kieli, jota mahdollisimman suuri määrä käyttäjiä ymmärtää.

(95) Tämän asetuksen sujuvan soveltamisen varmistamiseksi jäsenvaltioiden olisi pyrittävä ennen tämän asetuksen soveltamispäivää varmistamaan, että käytettävissä on riittävä määrä ilmoitettuja laitoksia kolmannen osapuolen suorittamia vaatimustenmukaisuuden arviointeja varten. Komission olisi pyrittävä auttamaan jäsenvaltioita ja muita asiaankuuluvia tahoja näissä toimissa, jotta vältetään pullonkaulat ja valmistajien markkinoille pääsyn esteet. Jäsenvaltioiden johtamat, tarvittaessa myös komission tuella toteutetut kohdennetut koulutustoimet voivat edistää pätevien ammattihenkilöiden saatavuutta, millä myös tuetaan tämän asetuksen nojalla ilmoitettujen laitosten toimintaa. Kun lisäksi otetaan huomioon kolmannen osapuolen suorittaman vaatimustenmukaisuuden arvioinnin mahdolliset kustannukset, olisi harkittava unionin ja kansallisen tason rahoitusaloitteita, joilla pyritään pienentämään näitä kustannuksia mikroyritysten ja pienten yritysten osalta.

(96) Oikeasuhtaisuuden varmistamiseksi vaatimustenmukaisuuden arviointilaitosten olisi vaatimustenmukaisuuden arviointimenettelyistä perittäviä maksuja määrittäessään otettava huomioon mikroyritysten ja pienten ja keskisuurten yritysten, myös startup-yritysten, erityiset edut ja tarpeet. Vaatimustenmukaisuuden arviointilaitosten olisi erityisesti sovellettava tässä asetuksessa säädettyä asiaankuuluvaa tarkastusmenettelyä ja testejä ainoastaan silloin, kun se on tarkoituksenmukaista ja riskiperusteista lähestymistapaa noudattaen.

(97) Sääntelyn testiympäristöjen tavoitteena olisi oltava yritysten innovoinnin ja kilpailukyvyn edistäminen perustamalla valvottuja testiympäristöjä ennen digitaalisia elementtejä sisältävien tuotteiden markkinoille saattamista. Sääntelyn testiympäristöjen olisi osaltaan parannettava oikeusvarmuutta kaikkien tämän asetuksen soveltamisalaan kuuluvien toimijoiden kannalta ja helpotettava ja nopeutettava digitaalisia elementtejä sisältävien tuotteiden pääsyä unionin markkinoille erityisesti silloin, kun niitä tarjoavat mikroyritykset ja pienet yritykset, mukaan lukien startup-yritykset.

(98) Jotta voidaan toteuttaa kolmannen osapuolen suorittamia digitaalisia elementtejä sisältävien tuotteiden vaatimustenmukaisuuden arviointeja, kansallisten ilmoittamisesta vastaavien viranomaisten olisi ilmoitettava vaatimustenmukaisuuden arviointilaitokset komissiolle ja muille jäsenvaltioille edellyttäen, että laitokset täyttävät tietyt vaatimukset erityisesti riippumattomuuden, pätevyyden ja eturistiriidattomuuden suhteen.

(99) Jotta varmistetaan yhtenäinen laatutaso digitaalisia elementtejä sisältävien tuotteiden vaatimustenmukaisuuden arviointien suorittamisessa, on tarpeen vahvistaa myös ilmoittamisesta vastaavia viranomaisia sekä muita ilmoitettujen laitosten arvioinnissa, ilmoittamisessa ja valvonnassa mukana olevia elimiä koskevat vaatimukset. Tässä asetuksessa esitettyä järjestelmää olisi täydennettävä akkreditointijärjestelmällä, josta säädetään asetuksessa (EY) N:o 765/2008. Koska akkreditointi on olennainen keino todentaa vaatimustenmukaisuuden arviointilaitosten pätevyys, sitä olisi käytettävä myös ilmoittamiseen.

(100) Vaatimustenmukaisuuden arviointilaitokset, jotka on akkreditoitu ja ilmoitettu sellaisen unionin lainsäädännön mukaisesti, jossa säädetään samankaltaisista vaatimuksista kuin tässä asetuksessa, kuten asetuksen (EU) 2019/881 nojalla hyväksyttyä eurooppalaista kyberturvallisuuden sertifiointijärjestelmää varten ilmoitettu vaatimustenmukaisuuden arviointilaitos tai delegoidun asetuksen (EU) 2022/30 mukaisesti ilmoitettu vaatimustenmukaisuuden arviointilaitos, olisi arvioitava ja ilmoitettava uudelleen tämän asetuksen mukaisesti. Asiaankuuluvat viranomaiset voivat kuitenkin määrittää synergioita mahdollisten päällekkäisten vaatimusten osalta, jotta vältetään tarpeeton taloudellinen ja hallinnollinen rasite ja varmistetaan sujuva ja oikea-aikainen ilmoitusprosessi.

(101) Kansallisten viranomaisten olisi kaikkialla unionissa pidettävä ensisijaisena keinona vaatimustenmukaisuuden arviointilaitosten teknisen pätevyyden osoittamiseksi asetuksen (EY) N:o 765/2008 mukaista avointa akkreditointia, jolla varmistetaan tarvittava vaatimustenmukaisuustodistuksia koskeva luottamuksen taso. Kansalliset viranomaiset voivat kuitenkin katsoa, että niillä on käytettävissään asianmukaiset keinot suorittaa tämä arviointi itse. Tällaisessa tapauksessa, jotta voidaan varmistaa muiden kansallisten viranomaisten tekemien arviointien uskottavuuden asianmukainen taso, niiden olisi toimitettava komissiolle ja muille jäsenvaltioille tarvittava asiakirja-aineisto, jolla osoitetaan, että arvioidut vaatimustenmukaisuuden arviointilaitokset täyttävät asian kannalta merkitykselliset sääntelyvaatimukset.

(102) Vaatimustenmukaisuuden arviointilaitokset teettävät usein osan vaatimustenmukaisuuden arviointiin liittyvistä toimistaan alihankintana tai käyttävät tytäryhtiötä. Jotta voidaan turvata suojauksen taso, jota digitaalisia elementtejä sisältävältä tuotteelta edellytetään markkinoille saattamista varten, on olennaisen tärkeää, että vaatimustenmukaisuuden arviointiin osallistuvat alihankkijat ja tytäryhtiöt täyttävät vaatimustenmukaisuuden arviointitehtävien suorittamisen osalta samat vaatimukset kuin ilmoitetut laitokset.

(103) Ilmoittamisesta vastaavan 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.

(104) Koska ilmoitetut laitokset voivat tarjota palvelujaan koko unionin alueella, on aiheellista antaa muille jäsenvaltioille ja komissiolle mahdollisuus esittää vastalauseita ilmoitetusta laitoksesta. Sen vuoksi on tärkeää säätää ajanjaksosta, jonka aikana voidaan selvittää vaatimustenmukaisuuden arviointilaitosten pätevyyteen liittyvät mahdolliset epäilykset tai huolenaiheet, ennen kuin ne alkavat toimia ilmoitettuina laitoksina.

(105) Kilpailukyvyn vuoksi on olennaisen tärkeää, että ilmoitetut laitokset soveltavat vaatimustenmukaisuuden arviointimenettelyjä aiheuttamatta tarpeetonta rasitetta talouden toimijoille. Samasta syystä ja talouden toimijoiden yhdenvertaisen kohtelun takaamiseksi on varmistettava johdonmukaisuus vaatimustenmukaisuuden arviointimenettelyjen teknisessä soveltamisessa. On odotettavissa, että tämä saavutettaisiin parhaiten asianmukaisella koordinoinnilla ja yhteistyöllä ilmoitettujen laitosten välillä.

(106) Markkinavalvonta on keskeinen keino unionin oikeuden asianmukaisen ja yhdenmukaisen soveltamisen varmistamiseksi. Sen vuoksi on aiheellista luoda oikeudellinen kehys, jonka puitteissa markkinavalvontaa voidaan toteuttaa asianmukaisesti. Tämän asetuksen soveltamisalaan kuuluviin digitaalisia elementtejä sisältäviin tuotteisiin sovelletaan asetuksessa (EU) 2019/1020 säädettyjä unionin markkinavalvontaa ja unionin markkinoille tulevien tuotteiden tarkastuksia koskevia sääntöjä.

(107) Asetuksen (EU) 2019/1020 mukaisesti markkinavalvontaviranomainen toteuttaa markkinavalvontaa sen nimenneen jäsenvaltion alueella. Tämä asetus ei saisi estää jäsenvaltioita valitsemasta toimivaltaisia viranomaisia, jotka suorittavat markkinavalvontatehtävät. Jokaisen jäsenvaltion olisi nimettävä alueelleen yksi tai useampi markkinavalvontaviranomainen. Jäsenvaltioiden olisi voitava valita, että ne nimeävät minkä tahansa olemassa olevan tai uuden viranomaisen toimimaan markkinavalvontaviranomaisena, mukaan lukien direktiivin (EU) 2022/2555 8 artiklan mukaisesti nimetyt tai perustetut toimivaltaiset viranomaiset, asetuksen (EU) 2019/881 58 artiklan mukaisesti nimetyt kansalliset kyberturvallisuussertifioinnin myöntävät viranomaiset tai direktiivin 2014/53/EU soveltamista varten nimetyt markkinavalvontaviranomaiset. Talouden toimijoiden olisi tehtävä kaikin tavoin yhteistyötä markkinavalvontaviranomaisten ja muiden toimivaltaisten viranomaisten kanssa. Kunkin jäsenvaltion olisi ilmoitettava komissiolle ja muille jäsenvaltioille markkinavalvontaviranomaisensa ja kunkin viranomaisen toimivaltaan kuuluvat alat sekä varmistettava tarvittavat resurssit ja tarvittava osaaminen tähän asetukseen liittyvien markkinavalvontatehtävien suorittamiseksi. Asetuksen (EU) 2019/1020 10 artiklan 2 ja 3 kohdan nojalla kunkin jäsenvaltion olisi nimettävä yhteyspiste, jonka olisi vastattava muun muassa markkinavalvontaviranomaisten yhteensovitetun kannan esittämisestä ja avustamisesta eri jäsenvaltioiden markkinavalvontaviranomaisten välisessä yhteistyössä.

(108) Tämän asetuksen yhdenmukaista soveltamista varten olisi perustettava erityinen digitaalisia elementtejä sisältävien tuotteiden kyberkestävyyttä käsittelevä hallinnollisen yhteistyön ryhmä asetuksen (EU) 2019/1020 30 artiklan 2 kohdan mukaisesti. Hallinnollisen yhteistyön ryhmän olisi koostuttava nimettyjen markkinavalvontaviranomaisten edustajista ja tarvittaessa yhteyspisteiden 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 edustaja kustakin mainitun asetuksen 10 artiklassa tarkoitetusta yhteyspisteestä ja valinnainen kansallinen asiantuntija, hallinnollisen yhteistyön ryhmien puheenjohtajista ja komission edustajista. Komission olisi osallistuttava tuotteiden vaatimustenmukaisuutta käsittelevän unionin verkoston, sen alaryhmien ja hallinnollisen yhteistyön ryhmän kokouksiin. Sen olisi myös avustettava hallinnollisen yhteistyön ryhmää teknistä ja logistista tukea tarjoavan toimeenpanevan sihteeristön avulla. Hallinnollisen yhteistyön ryhmä voi myös kutsua riippumattomia asiantuntijoita osallistumaan työhönsä ja olla yhteydessä muihin hallinnollisen yhteistyön ryhmiin, kuten direktiivin 2014/53/EU nojalla perustettuun hallinnollisen yhteistyön ryhmään.

(109) Markkinavalvontaviranomaisten olisi tehtävä tiivistä yhteistyötä tämän asetuksen nojalla perustetun hallinnollisen yhteistyön ryhmän kautta, ja niiden olisi voitava laatia ohjeasiakirjoja, joilla helpotetaan markkinavalvontatoimia kansallisella tasolla, esimerkiksi kehittämällä parhaita käytäntöjä ja indikaattoreita, joiden avulla voidaan tehokkaasti tarkastaa, että digitaalisia elementtejä sisältävät tuotteet ovat tämän asetuksen mukaisia.

(110) Jotta voidaan varmistaa oikea-aikaiset, oikeasuhtaiset ja tulokselliset toimenpiteet sellaisten digitaalisia elementtejä sisältävien tuotteiden osalta, joihin liittyy merkittävä kyberturvallisuusriski, olisi säädettävä 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 asiaankuuluvien talouden toimijoiden kanssa. Jos jäsenvaltiot ja komissio ovat yhtä mieltä jäsenvaltion toteuttaman toimenpiteen oikeutuksesta, komissiolta ei pitäisi edellyttää jatkotoimia, paitsi jos vaatimustenvastaisuuden voidaan katsoa johtuvan yhdenmukaistetun standardin puutteista.

(111) Tietyissä tapauksissa tämän asetuksen mukainen digitaalisia elementtejä sisältävä tuote voi kuitenkin aiheuttaa merkittävän kyberturvallisuusriskin tai riskin ihmisten terveydelle tai turvallisuudelle, perusoikeuksien suojeluun tarkoitettujen unionin oikeuden tai kansallisen lainsäädännön mukaisten velvoitteiden noudattamiselle, direktiivin (EU) 2022/2555 3 artiklan 1 kohdassa 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 varmistetaan näiden riskien pienentäminen. Tämän vuoksi markkinavalvontaviranomaisten olisi toteutettava toimenpiteitä, joilla talouden toimijaa vaaditaan varmistamaan, ettei tuote enää aiheuta kyseistä riskiä, tai järjestämään sitä koskeva palautusmenettely tai poistamaan se markkinoilta, riskistä riippuen. Heti kun markkinavalvontaviranomainen rajoittaa digitaalisia elementtejä sisältävän tuotteen vapaata liikkuvuutta tai kieltää sen tällä tavalla, jäsenvaltion olisi ilmoitettava väliaikaisista toimenpiteistä viipymättä komissiolle ja muille jäsenvaltioille ja esitettävä päätöksen syyt ja perustelut. Jos markkinavalvontaviranomainen toteuttaa tällaisia toimenpiteitä riskin aiheuttavien digitaalisia elementtejä sisältävien tuotteiden suhteen, komission olisi viipymättä kuultava jäsenvaltioita ja asiaankuuluvaa talouden toimijaa tai asiaankuuluvia talouden toimijoita ja arvioitava kansallinen toimenpide. Komission olisi tämän arvioinnin tulosten perusteella päätettävä, onko kansallinen toimenpide oikeutettu vai ei. Komission olisi osoitettava päätöksensä kaikille jäsenvaltioille ja annettava se välittömästi tiedoksi niille ja asiaankuuluvalle talouden toimijalle tai asiaankuuluville talouden toimijoille. Jos toimenpide katsotaan oikeutetuksi, komission olisi myös harkittava tehdäänkö ehdotuksia asiaa koskevan unionin oikeuden tarkistamiseksi.

(112) Komission olisi voitava pyytää ENISAa suorittamaan arviointi merkittävän kyberturvallisuusriskin 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, perusoikeuksien suojeluun tarkoitettujen unionin oikeuden tai kansallisen lainsäädännön mukaisten velvoitteiden noudattamiselle, direktiivin (EU) 2022/2555 3 artiklan 1 kohdassa tarkoitettujen keskeisten toimijoiden sähköisen tietojärjestelmän avulla tarjoamien palvelujen saatavuudelle, aitoudelle, eheydelle tai luottamuksellisuudelle. Tämän arvioinnin perusteella komission olisi voitava hyväksyä täytäntöönpanosäädöksillä korjaavia tai rajoittavia toimenpiteitä unionin tasolla, mukaan lukien sen vaatiminen, että asianomaisia digitaalisia elementtejä sisältävät tuotteet vedetään markkinoilta tai järjestetään niitä koskeva palautusmenettely, kohtuullisen ajan kuluessa ja oikeassa suhteessa riskin luonteeseen. Komission olisi voitava turvautua tällaiseen toimeen ainoastaan poikkeuksellisissa olosuhteissa, jotka oikeuttavat välittömät toimet sisämarkkinoiden moitteettoman toiminnan säilyttämiseksi, ja ainoastaan, jos markkinavalvontaviranomaiset eivät ole toteuttaneet tehokkaita toimenpiteitä tilanteen korjaamiseksi. Tällaiset poikkeukselliset olosuhteet voivat olla hätätilanteita, joissa valmistaja esimerkiksi asettaa vaatimustenvastaisen digitaalisia elementtejä sisältävän tuotteen laajalti saataville useissa jäsenvaltioissa, tuotetta käyttävät myös direktiivin (EU) 2022/2555 soveltamisalaan kuuluvat toimijat keskeisillä aloilla ja tuote sisältää tunnettuja haavoittuvuuksia, joita pahantahtoiset toimijat hyödyntävät ja joita varten valmistaja ei tarjoa korjaavia päivityksiä. Komission olisi voitava puuttua tällaisiin hätätilanteisiin vain poikkeuksellisten olosuhteiden keston ajan ja jos tämän asetuksen vastaisuudet tai aiheutuneet merkittävät riskit jatkuvat.

(113) Jos on viitteitä tämän asetuksen vastaisuuksista useissa jäsenvaltioissa, markkinavalvontaviranomaisten olisi voitava toteuttaa yhteisiä toimia muiden viranomaisten kanssa vaatimusten täyttymisen todentamiseksi ja digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuusriskien tunnistamiseksi.

(114) Samanaikaiset koordinoidut valvontatoimet, jäljempänä ’tehotarkastukset’, ovat markkinavalvontaviranomaisten erityisiä täytäntöönpanotoimia, joilla voidaan edelleen parantaa tuoteturvallisuutta. Tehotarkastuksia olisi tehtävä erityisesti silloin, kun markkinasuuntaukset, kuluttajien valitukset tai muut merkit viittaavat siihen, että tiettyjen digitaalisia elementtejä sisältävien tuotteiden ryhmien todetaan usein aiheuttavan kyberturvallisuusriskejä. Lisäksi markkinavalvontaviranomaisten olisi tehotarkastusten kohteeksi asetettavia tuoteryhmiä määrittäessään otettava huomioon myös muihin kuin teknisiin riskitekijöihin liittyvät olosuhteet. Tätä varten markkinavalvontaviranomaisten olisi voitava ottaa huomioon direktiivin (EU) 2022/2555 22 artiklan mukaisesti tehtyjen kriittisiä toimitusketjuja koskevien unionin tason koordinoitujen turvallisuusriskinarviointien tulokset, mukaan lukien muihin kuin teknisiin riskitekijöihin liittyvät olosuhteet. ENISAn olisi muun muassa haavoittuvuuksista ja poikkeamista saamiensa ilmoitusten perusteella esitettävä markkinavalvontaviranomaisille ehdotuksia digitaalisia elementtejä sisältävien tuotteiden ryhmistä, joiden osalta voitaisiin järjestää tehotarkastuksia.

(115) ENISAn asiantuntemus ja toimeksianto huomioon ottaen sen olisi voitava tukea tämän asetuksen täytäntöönpanoprosessia. ENISAn olisi erityisesti voitava ehdottaa yhteisiä toimia markkinavalvontaviranomaisten suoritettavaksi, jos se saa viitteitä tai tietoa digitaalisia elementtejä sisältävien tuotteiden mahdollisista tämän asetuksen vastaisuuksista useissa jäsenvaltioissa, tai määrittää tuoteryhmiä, joiden osalta olisi järjestettävä tehotarkastuksia. Poikkeuksellisissa olosuhteissa ENISAn olisi komission pyynnöstä voitava tehdä arviointeja tietyistä digitaalisia elementtejä sisältävistä tuotteista, jotka aiheuttavat merkittävän kyberturvallisuusriskin, jos sisämarkkinoiden moitteettoman toiminnan säilyttämiseksi tarvitaan välittömiä toimia.

(116) Tällä asetuksella annetaan ENISAlle tiettyjä tehtäviä, jotka edellyttävät sekä asianmukaista asiantuntemusta että asianmukaisia henkilöresursseja, jotta ENISA voi suorittaa kyseiset tehtävät tehokkaasti. Kun komissio laatii luonnosta unionin yleiseksi talousarvioksi, se ehdottaa ENISAn henkilöstötaulukkoa varten tarvittavat talousarvioresurssit asetuksen (EU) 2019/881 29 artiklassa vahvistetun menettelyn mukaisesti. Tämän prosessin aikana komissio ottaa huomioon ENISAn kokonaisresurssit, jotta se voi hoitaa tehtävänsä, mukaan lukien ENISAlle tämän asetuksen nojalla annetut tehtävät.

(117) Jotta sääntelykehystä voitaisiin tarvittaessa mukauttaa, komissiolle olisi siirrettävä valta hyväksyä säädösvallan siirron nojalla annettavia delegoituja säädöksiä Euroopan unionin toiminnasta tehdyn sopimuksen 290 artiklan mukaisesti digitaalisia elementtejä sisältävien tärkeiden tuotteiden luettelon sisältävän liitteen päivittämiseksi. Komissiolle olisi siirrettävä valta antaa kyseisen artiklan mukaisesti delegoituja säädöksiä niiden digitaalisia elementtejä sisältävien tuotteiden määrittämiseksi, jotka kuuluvat sellaisten muiden unionin sääntöjen soveltamisalaan, joilla saavutetaan sama suojelun taso kuin tällä asetuksella, ja sen täsmentämiseksi, olisiko joitain tuotteita tarpeen jättää osittain tai kokonaan tämän asetuksen soveltamisalan ulkopuolelle ja tapauksen mukaan se, miltä osin. Komissiolle olisi myös siirrettävä valta antaa kyseisen artiklan mukaisesti delegoituja säädöksiä, jotka koskevat mahdollista vaatimusta tämän asetuksen liitteessä vahvistettujen digitaalisia elementtejä sisältävien kriittisten tuotteiden sertifioinnista eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti sekä digitaalisia elementtejä sisältävien kriittisten tuotteiden luettelon päivittämistä tässä asetuksessa vahvistettujen kriittisyyskriteerien perusteella ja sellaisten asetuksen (EU) 2019/881 nojalla hyväksyttyjen eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien määrittämistä, joita voidaan käyttää osoittamaan tämän asetuksen liitteessä vahvistettujen olennaisten kyberturvallisuusvaatimusten tai niiden osien täyttyminen. Komissiolle olisi myös siirrettävä valta antaa delegoituja säädöksiä, joissa täsmennetään tukiajan vähimmäiskesto tiettyjen tuoteryhmien osalta, jos markkinavalvontatiedot viittaavat siihen, että tukiajat ovat riittämättömiä, sekä ehdot kyberturvallisuuteen liittyvien syiden soveltamiselle lykättäessä aktiivisesti hyödynnettyjä haavoittuvuuksia koskevien ilmoitusten välittämistä.

Lisäksi komissiolle olisi siirrettävä valta antaa delegoituja säädöksiä, joilla vahvistetaan vapaaehtoisia tietoturvatodistusohjelmia sen arvioimiseksi, ovatko vapaiksi ja avoimen lähdekoodin ohjelmistoiksi luokiteltavat digitaalisia elementtejä sisältävät tuotteet kaikkien tai tiettyjen olennaisten kyberturvallisuusvaatimusten tai muiden tässä asetuksessa säädettyjen velvoitteiden mukaisia, ja joilla täsmennetään EU-vaatimustenmukaisuusvakuutuksen vähimmäissisältö ja täydennetään teknisiin asiakirjoihin sisällytettäviä tietoja. 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[30] 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. Komissiolle olisi … päivästä …kuuta … [tämän asetuksen voimaantulopäivästä] viiden vuoden ajaksi siirrettävä valta antaa tämän asetuksen nojalla delegoituja säädöksiä. Komission olisi laadittava siirrettyä säädösvaltaa koskeva kertomus viimeistään yhdeksän kuukautta ennen tämän viiden vuoden kauden päättymistä. Säädösvallan siirtoa olisi jatkettava ilman eri toimenpiteitä samanpituisiksi kausiksi, jollei Euroopan parlamentti tai neuvosto vastusta tällaista jatkamista viimeistään kolme kuukautta ennen kunkin kauden päättymistä.

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

(118) Jotta voidaan varmistaa tämän asetuksen yhdenmukainen täytäntöönpano, komissiolle olisi siirrettävä täytäntöönpanovaltaa täsmentää tämän asetuksen liitteessä vahvistettujen digitaalisia elementtejä sisältävien tärkeiden tuotteiden ryhmien tekninen kuvaus, täsmentää ohjelmistojen materiaaliluettelon muoto ja siihen sisällytettävät tiedot, täsmentää tarkemmin muoto ja menettely valmistajien toimittamille ilmoituksille aktiivisesti hyödynnetyistä haavoittuvuuksista ja digitaalisia elementtejä sisältävien tuotteiden tietoturvaan vaikuttavista vakavista poikkeamista, vahvistaa tekniset vaatimukset kattavat yhteiset eritelmät, jotka tarjoavat keinon täyttää tämän asetuksen liitteessä vahvistetut olennaiset kyberturvallisuusvaatimukset, säätää teknisiä eritelmiä, jotka koskevat digitaalisia elementtejä sisältävien tuotteiden tietoturvaan liittyviä merkintöjä, kuvamerkkejä tai muita merkkejä, niiden tukiaikoja sekä mekanismeja, joilla edistetään niiden käyttöä ja lisätään yleistä tietoisuutta digitaalisia elementtejä sisältävien tuotteiden tietoturvasta, täsmentää mikroyritysten ja pienten yritysten tarpeisiin kohdennettu yksinkertaistettu asiakirjojen muoto ja päättää unionin tason korjaavista tai rajoittavista toimenpiteistä poikkeuksellisissa olosuhteissa, jotka oikeuttavat välittömät toimet sisämarkkinoiden moitteettoman toiminnan säilyttämiseksi. Tätä valtaa olisi käytettävä Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 182/2011[31] mukaisesti.

(119) Jotta voidaan varmistaa markkinavalvontaviranomaisten luottamukseen perustuva ja rakentava yhteistyö unionin tasolla ja kansallisella tasolla, kaikkien tämän asetuksen soveltamiseen osallistuvien osapuolten olisi kunnioitettava tehtäviään suorittaessaan saamiensa tietojen ja datan luottamuksellisuutta.

---

[31] 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, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(120) Tässä asetuksessa säädettyjen velvoitteiden tehokkaan täytäntöönpanon varmistamiseksi kullakin markkinavalvontaviranomaisella olisi oltava valtuudet määrätä hallinnollisia sakkoja tai pyytää niiden määräämistä. Sen vuoksi olisi vahvistettava enimmäismäärät tässä asetuksessa säädettyjen velvoitteiden noudattamatta jättämisestä määrättäville hallinnollisille sakoille, joista olisi säädettävä kansallisessa lainsäädännössä. Kun päätetään 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, onko valmistaja mikroyritys tai pieni tai keskisuuri yritys, startup-yritykset mukaan luettuina, ja se, onko sama tai jokin muu markkinavalvontaviranomainen jo määrännyt hallinnollisia sakkoja samalle talouden toimijalle samankaltaisesta rikkomisesta. Tällaiset olosuhteet voisivat olla joko raskauttavia, kun saman talouden toimijan rikkominen jatkuu muiden jäsenvaltioiden kuin sille hallinnollisen sakon jo määränneen jäsenvaltion alueella, tai lieventäviä, siten että varmistetaan, että jonkin toisen markkinavalvontaviranomaisen harkitsemassa samalle talouden toimijalle tai samantyyppisestä rikkomisesta määrättävässä mahdollisessa muussa hallinnollisessa sakossa olisi jo otettava huomioon yhdessä muiden merkityksellisten erityisten olosuhteiden kanssa toisessa jäsenvaltioissa määrätty seuraamus ja sen määrä. Kaikissa tällaisissa tapauksissa kumulatiivisella hallinnollisella sakolla, joka koostuu useiden jäsenvaltioiden markkinavalvontaviranomaisten sakoista samalle talouden toimijalle samantyyppisestä rikkomisesta, olisi varmistettava oikeasuhteisuusperiaatteen noudattaminen. Koska mikroyrityksille tai pienille yrityksille ei määrätä hallinnollisia sakkoja, jos ne eivät noudata 24 tunnin määräaikaa ennakkovaroitusilmoituksen antamiseksi aktiivisesti hyödynnetyistä haavoittuvuuksista tai digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavista vakavista poikkeamista, eikä avoimen lähdekoodin ohjelmistovastaaville määrätä hallinnollisia sakkoja minkään tämän asetuksen rikkomisen osalta, ja noudattaen periaatetta, jonka mukaan seuraamusten olisi oltava tehokkaita, oikeasuhteisia ja varoittavia, jäsenvaltiot eivät saisi määrätä kyseisille toimijoille muunlaisia rahallisia seuraamuksia.

(121) Jos hallinnollisia sakkoja määrätään henkilölle, joka ei ole yritys, toimivaltaisen viranomaisen olisi sakon sopivan määrän harkinnassa otettava huomioon jäsenvaltion yleinen tulotaso sekä henkilön taloudellinen tilanne. Jäsenvaltioilla olisi oltava vastuu määrittää, onko viranomaisille määrättävä hallinnollisia sakkoja ja missä määrin.

(122) Jäsenvaltioiden olisi tarkasteltava kansalliset olosuhteet huomioon ottaen mahdollisuutta käyttää tässä asetuksessa säädetyistä seuraamuksista saatavat tulot tai niitä vastaava määrä varoja kyberturvallisuutta koskevien politiikkatoimien tukemiseen ja kyberturvallisuuden tason nostamiseen unionissa muun muassa lisäämällä pätevien kyberturvallisuusalan ammattihenkilöiden määrää, vahvistamalla mikroyritysten sekä pienten ja keskisuurten yritysten valmiuksien kehittämistä ja parantamalla yleistä tietoisuutta kyberuhkista.

(123) Suhteissaan kolmansiin maihin unioni 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. Vastavuoroista tunnustamista koskevia sopimuksia tehdään unionin ja sellaisten kolmansien maiden välillä, joiden tekninen kehitys on vastaavalla tasolla ja joiden lähestymistapa vaatimustenmukaisuuden arviointiin on yhteensopiva. Tällaiset sopimukset perustuvat sopimuspuolten vaatimustenmukaisuuden arviointilaitosten toisen sopimuspuolen lainsäädännön mukaisesti antamien todistusten, vaatimustenmukaisuusmerkintöjen ja testiraporttien vastavuoroiseen hyväksymiseen. Tällä hetkellä vastavuoroista tunnustamista koskevia sopimuksia on voimassa useiden kolmansien maiden kanssa. Kyseiset vastavuoroista tunnustamista koskevat sopimukset on tehty useilla erityisillä aloilla, jotka voivat vaihdella eri kolmansissa maissa. Kaupan helpottamiseksi edelleen ja ottaen huomioon, että digitaalisia elementtejä sisältävien tuotteiden toimitusketjut ovat maailmanlaajuisia, tämän asetuksen nojalla säänneltyjen tuotteiden osalta voidaan Euroopan unionin toiminnasta tehdyn sopimuksen 218 artiklan mukaisesti tehdä vaatimustenmukaisuuden arviointia koskevia sopimuksia vastavuoroisesta tunnustamisesta. Yhteistyö kolmansien kumppanimaiden kanssa on myös tärkeää kyberkestävyyden vahvistamiseksi maailmanlaajuisesti, sillä pitkällä aikavälillä tämä edistää vahvempaa kyberturvallisuuskehystä sekä unionissa että sen ulkopuolella.

(124) Kuluttajilla olisi oltava oikeus valvoa oikeuksiensa toteutumista talouden toimijoille tämän asetuksen nojalla asetettujen velvoitteiden osalta Euroopan parlamentin ja neuvoston direktiivin (EU) 2020/1828[32] mukaisten edustajakanteiden avulla. Tässä asetuksessa olisi tätä varten säädettävä, että direktiiviä (EU) 2020/1828 sovelletaan edustajakanteisiin, jotka on nostettu tämän asetuksen säännösten rikkomisista, jotka vahingoittavat tai voivat vahingoittaa kuluttajien yhteisiä etuja. Kyseisen direktiivin liitettä I olisi sen vuoksi muutettava vastaavasti. Jäsenvaltioiden tehtävänä olisi oltava varmistaa, että kyseiset muutokset otetaan huomioon niiden kyseisen direktiivin nojalla hyväksytyissä toimenpiteissä, jotka koskevat direktiivin saattamista osaksi kansallista lainsäädäntöä, vaikkakaan kyseisten kansallisten toimenpiteiden hyväksyminen tältä osin ei ole edellytys kyseisen direktiivin soveltamiselle kyseisiin edustajakanteisiin. Kyseistä direktiiviä olisi alettava soveltaa edustajakanteisiin, jotka on nostettu talouden toimijoita vastaan tämän asetuksen säännösten rikkomisista, jotka vahingoittavat tai voisivat vahingoittaa kuluttajien yhteisiä etuja, … päivänä …kuuta … [36 kuukauden kuluttua tämän asetuksen voimaantulosta].

(125) Komission olisi säännöllisin väliajoin arvioitava ja tarkasteltava tätä asetusta uudelleen asiaankuuluvia sidosryhmiä kuullen, erityisesti yhteiskunnan ja markkinoiden olosuhteiden sekä politiikkaan ja teknologiaan liittyvien olosuhteiden kehitykseen perustuvien muutostarpeiden selvittämiseksi. Tällä asetuksella helpotetaan toimitusketjun tietoturvaa koskevien velvoitteiden noudattamista sellaisten asetuksen (EU) 2022/2554 ja direktiivin (EU) 2022/2555 soveltamisalaan kuuluvien toimijoiden osalta, jotka käyttävät digitaalisia elementtejä sisältäviä tuotteita. Osana tätä säännöllisin väliajoin tehtävää uudelleentarkastelua komission olisi arvioitava unionin kyberturvallisuuskehyksen yhteisvaikutuksia.

---

[32] Euroopan parlamentin ja neuvoston direktiivi (EU) 2020/1828, annettu 25 päivänä marraskuuta 2020, kuluttajien yhteisten etujen suojaamiseksi nostettavista edustajakanteista ja direktiivin 2009/22/EY kumoamisesta (EUVL L 409, 4.12.2020, s. 1).

(126) Talouden toimijoille olisi annettava riittävästi aikaa mukautua tässä asetuksessa vahvistettuihin vaatimuksiin. Tätä asetusta olisi sovellettava … päivästä …kuuta … [36 kuukauden kuluttua tämän asetuksen voimaantulopäivästä], lukuun ottamatta aktiivisesti hyödynnettyjä haavoittuvuuksia ja digitaalisia elementtejä sisältävien tuotteiden tietoturvaan vaikuttavia vakavia poikkeamia koskevia raportointivelvoitteita, joita olisi sovellettava … päivästä …kuuta … [21 kuukauden kuluttua tämän asetuksen voimaantulopäivästä], ja vaatimustenmukaisuuden arviointilaitosten ilmoittamista koskevia säännöksiä, joita olisi sovellettava … päivästä …kuuta … [18 kuukauden kuluttua tämän asetuksen voimaantulopäivästä].

(127) On tärkeää tarjota tukea mikroyrityksille sekä pienille ja keskisuurille yrityksille, mukaan lukien startup-yritykset, tämän asetuksen täytäntöönpanossa ja minimoida täytäntöönpanoon kohdistuvat riskit, jotka johtuvat tiedon ja asiantuntemuksen puutteesta markkinoilla, ja siten helpottaa valmistajien tässä asetuksessa säädettyjen velvoitteiden noudattamista. Digitaalinen Eurooppa -ohjelmasta ja muista asiaankuuluvista unionin ohjelmista annetaan taloudellista ja teknistä tukea, jonka avulla kyseiset yritykset voivat edistää unionin talouden kasvua ja kyberturvallisuuden yhteisen tason vahvistamista unionissa. Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus ja kansalliset koordinointikeskukset sekä komission ja jäsenvaltioiden unionin tai jäsenvaltioiden tasolla perustamat eurooppalaiset digitaali-innovointikeskittymät voisivat myös tukea yrityksiä ja julkisen sektorin organisaatioita ja edistää tämän asetuksen täytäntöönpanoa. Ne voisivat tehtäviensä ja toimivaltuuksiensa puitteissa antaa mikroyrityksille sekä pienille ja keskisuurille yrityksille teknistä ja tieteellistä tukea esimerkiksi testaustoimia ja kolmansien osapuolten suorittamia vaatimustenmukaisuuden arviointeja varten. Ne voisivat myös tukea tämän asetuksen täytäntöönpanoa helpottavien välineiden käyttöönottoa.

(128) Lisäksi jäsenvaltioiden olisi harkittava täydentäviä toimia, joilla pyritään antamaan ohjeistusta ja tukea mikroyrityksille sekä pienille ja keskisuurille yrityksille, kuten sääntelyn testiympäristöjen ja erityisten viestintäkanavien perustaminen. Jotta voidaan vahvistaa kyberturvallisuuden tasoa unionissa, jäsenvaltiot voivat myös harkita tuen antamista digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuuteen liittyvien valmiuksien ja osaamisen kehittämiseen, talouden toimijoiden, erityisesti mikroyritysten sekä pienten ja keskisuurten yritysten, kyberkestävyyden parantamiseen ja digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuutta koskevan yleisen tietoisuuden lisäämiseen.

(129) Jäsenvaltiot eivät voi riittävällä tavalla saavuttaa tämän asetuksen tavoitetta, vaan se voidaan toiminnan vaikutusten vuoksi saavuttaa paremmin unionin tasolla. Sen vuoksi 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 kyseisen tavoitteen saavuttamiseksi.

(130) Euroopan tietosuojavaltuutettua on kuultu Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1725[33] 42 artiklan 1 kohdan mukaisesti, ja hän on antanut lausuntonsa 9 päivänä marraskuuta 2022[34],

OVAT HYVÄKSYNEET TÄMÄN ASETUKSEN:

---

33 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).

34 EUVL C 452, 29.11.2022, s. 23.

I luku
Yleiset säännökset

1 artikla

Kohde

Tässä asetuksessa vahvistetaan

a) säännöt digitaalisia elementtejä sisältävien tuotteiden asettamiselle saataville markkinoilla tällaisten tuotteiden kyberturvallisuuden varmistamiseksi,

b) olennaiset kyberturvallisuusvaatimukset digitaalisia elementtejä sisältävien tuotteiden suunnittelua, kehittämistä ja tuotantoa koskien ja kyseisiin tuotteisiin liittyvät talouden toimijoiden kyberturvallisuutta koskevat velvoitteet,

c) olennaiset kyberturvallisuusvaatimukset haavoittuvuuksien käsittelyprosesseille, joita valmistajat ottavat käyttöön varmistaakseen digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuuden niiden odotettavissa olevan käyttöiän ajan, sekä kyseisiin prosesseihin liittyvät talouden toimijoiden velvoitteet ja

d) markkinavalvontaa, mukaan lukien markkinaseuranta, ja tässä artiklassa tarkoitettujen sääntöjen ja vaatimusten noudattamisen valvontaa koskevat säännöt.

2 artikla

Soveltamisala

1. Tätä asetusta sovelletaan kaikkiin markkinoilla saataville asetettuihin digitaalisia elementtejä sisältäviin tuotteisiin, joiden käyttötarkoitus tai kohtuudella ennakoitavissa oleva käyttö sisältää suoran tai välillisen loogisen tai fyysisen datayhteyden johonkin laitteeseen tai verkkoon.

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. Tätä asetusta ei sovelleta Euroopan parlamentin ja neuvoston direktiivin 2014/90/EU[35] soveltamisalaan kuuluviin varusteisiin.

[35] Euroopan parlamentin ja neuvoston direktiivi 2014/90/EU, annettu 23 päivänä heinäkuuta 2014, laivavarusteista ja neuvoston direktiivin 96/98/EY kumoamisesta (EUVL L 257, 28.8.2014, s. 146).

5. Tämän asetuksen soveltamista sellaisiin digitaalisia elementtejä sisältäviin tuotteisiin, joihin sovellettavien muiden unionin sääntöjen vaatimuksilla puututaan kaikkiin tai osaan liitteessä I vahvistettujen olennaisten kyberturvallisuusvaatimusten 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 tai korkeampi suojan taso kuin tällä asetuksella.

   Siirretään komissiolle valta antaa 61 artiklan mukaisesti delegoituja säädöksiä, joilla täydennetään tätä asetusta täsmentämällä, onko tällainen rajoitus tai poissulkeminen tarpeen, sekä asianomaiset tuotteet ja säännöt ja tarvittaessa rajoituksen soveltamisala.

6. Tätä asetusta ei sovelleta varaosiin, jotka asetetaan saataville markkinoilla samanlaisten komponenttien korvaamiseksi digitaalisia elementtejä sisältävissä tuotteissa ja jotka valmistetaan samojen eritelmien mukaisesti kuin komponentit, jotka niillä on tarkoitus korvata.

7. Tätä asetusta ei sovelleta digitaalisia elementtejä sisältäviin tuotteisiin, jotka on kehitetty tai joita on muutettu yksinomaan kansalliseen turvallisuuteen tai puolustukseen liittyviin tarkoituksiin, eikä tuotteisiin, jotka on erityisesti suunniteltu turvallisuusluokiteltujen tietojen käsittelyä varten.

8. Tässä direktiivissä säädettyihin velvoitteisiin ei kuulu sellaisten tietojen toimittaminen, joiden ilmaiseminen olisi vastoin jäsenvaltion keskeisiä kansalliseen turvallisuuteen, yleiseen turvallisuuteen tai puolustukseen liittyviä etuja.

3 artikla

Määritelmät

Tässä asetuksessa tarkoitetaan:

1) ’digitaalisia elementtejä sisältävällä tuotteella’ ohjelmisto- tai laitteistotuotetta ja sen ratkaisuja datan etäkäsittelystä, mukaan lukien toisistaan erillään markkinoille saatettavat ohjelmisto- tai laitteistokomponentit;

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

3) ’kyberturvallisuudella’ asetuksen (EU) 2019/881 2 artiklan 1 alakohdassa määriteltyä kyberturvallisuutta;

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

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

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

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

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

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

10) ’välillisellä yhteydellä’ laitteeseen tai verkkoon luotua yhteyttä, joka ei ole suora vaan tapahtuu pikemminkin osana laajempaa järjestelmää, joka voidaan liittää suoraan kyseiseen laitteeseen tai verkkoon;

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

12) ’talouden toimijalla’ valmistajaa, valtuutettua edustajaa, maahantuojaa, jakelijaa tai muuta luonnollista henkilöä tai oikeushenkilöä, jota koskevat digitaalisia elementtejä sisältävien tuotteiden valmistamiseen tai markkinoilla saataville asettamiseen liittyvät tämän asetuksen mukaiset velvoitteet;

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

14) ’avoimen lähdekoodin ohjelmistovastaavalla’ muuta oikeushenkilöä kuin valmistajaa, jonka tarkoituksena tai tavoitteena on järjestelmällisesti ja pitkäjänteisesti tarjota tukea sellaisten tiettyjen digitaalisia elementtejä sisältävien tuotteiden kehittämistä varten, jotka luokitellaan vapaiksi ja avoimen lähdekoodin ohjelmistoiksi ja jotka on tarkoitettu kaupalliseen toimintaan, ja joka varmistaa kyseisten tuotteiden toimintakelpoisuuden;

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

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

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

18) ’kuluttajalla’ luonnollista henkilöä, joka toimii sellaisessa tarkoituksessa, joka ei liity hänen elinkeino- tai ammattitoimintaansa;

19) ’mikroyrityksillä’, ’pienillä yrityksillä’ ja ’keskisuurilla yrityksillä’ komission suosituksen 2003/361/EY liitteessä määriteltyjä mikroyrityksiä, pieniä yrityksiä ja keskisuuria yrityksiä;

20) ’tukiajalla’ ajanjaksoa, jonka aikana valmistajan edellytetään varmistavan, että digitaalisia elementtejä sisältävän tuotteen haavoittuvuudet käsitellään tehokkaasti ja liitteessä I olevassa II osassa vahvistettujen olennaisten kyberturvallisuusvaatimusten mukaisesti;

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

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

23) ’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 teknisissä asiakirjoissa;

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

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

26) ’ilmoittamisesta vastaavalla viranomaisella’ kansallista viranomaista, jonka vastuulla on laatia ja toteuttaa tarvittavat menettelyt, jotka liittyvät vaatimustenmukaisuuden arviointilaitosten arviointiin, nimeämiseen ja ilmoittamiseen, sekä valvoa niitä;

27) ’vaatimustenmukaisuuden arvioinnilla’ prosessia, jossa selvitetään, täyttyvätkö liitteessä I vahvistetut olennaiset kyberturvallisuusvaatimukset;

28) ’vaatimustenmukaisuuden arviointilaitoksella’ asetuksen (EY) N:o 765/2008 2 artiklan 13 alakohdassa määriteltyä vaatimustenmukaisuuden arviointilaitosta;

29) ’ilmoitetulla laitoksella’ vaatimustenmukaisuuden arviointilaitosta, joka on nimetty 43 artiklan ja unionin muun asiaankuuluvan yhdenmukaistamislainsäädännön mukaisesti;

30) ’merkittävällä muutoksella’ digitaalisia elementtejä sisältävään tuotteeseen sen markkinoille saattamisen jälkeen tehtyä muutosta, joka vaikuttaa siihen, täyttääkö digitaalisia elementtejä sisältävä tuote liitteessä I olevassa I osassa vahvistetut olennaiset kyberturvallisuusvaatimukset, tai joka muuttaa käyttötarkoitusta, jota varten digitaalisia elementtejä sisältävä tuote on arvioitu;

31) ’CE-merkinnällä’ merkintää, jolla valmistaja osoittaa, että digitaalisia elementtejä sisältävä tuote ja valmistajan käyttöön ottamat prosessit ovat liitteessä I esitettyjen olennaisten kyberturvallisuusvaatimusten ja muun sovellettavan unionin yhdenmukaistamislainsäädännön, jossa säädetään merkinnän kiinnittämisestä tai liittämisestä tuotteeseen, mukaisia;

32) ’unionin yhdenmukaistamislainsäädännöllä’ asetuksen (EU) 2019/1020 liitteessä I lueteltua unionin lainsäädäntöä ja mitä tahansa muuta unionin lainsäädäntöä, jolla yhdenmukaistetaan niiden tuotteiden kaupan pitämisen ehtoja, joihin mainittua asetusta sovelletaan;

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

34) ’kansainvälisellä standardilla’ asetuksen (EU) N:o 1025/2012 2 artiklan 1 alakohdan a alakohdassa määriteltyä kansainvälistä standardia;

35) ’eurooppalaisella standardilla’ asetuksen (EU) N:o 1025/2012 2 artiklan 1 alakohdan b alakohdassa määriteltyä eurooppalaista standardia;

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

37) ’kyberturvallisuusriskillä’ poikkeaman aiheuttaman menetyksen tai häiriön mahdollisuutta, joka ilmaistaan tällaisen menetyksen tai häiriön suuruuden ja kyseisen poikkeaman toteutumisen todennäköisyyden yhdistelmänä;

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

39) ’ohjelmistojen materiaaliluettelolla’ muodollista selitettä, jossa esitetään digitaalisia elementtejä sisältävän tuotteen ohjelmistoelementteihin sisältyvien komponenttien yksityiskohtaiset tiedot ja toimitusketjusuhteet;

40) ’haavoittuvuudella’ digitaalisia elementtejä sisältävän tuotteen heikkoutta, alttiutta tai vikaa, jota kyberuhka voi hyödyntää;

41) ’hyödynnettävissä olevalla haavoittuvuudella’ haavoittuvuutta, jota vastapuoli voi käyttää tehokkaasti käytännön toimintaolosuhteissa;

42) ’aktiivisesti hyödynnetyllä haavoittuvuudella’ haavoittuvuutta, jonka osalta on luotettavaa näyttöä siitä, että jokin pahantahtoinen toimija on hyödyntänyt sitä järjestelmässä ilman järjestelmän omistajan lupaa;

43) ’poikkeamalla’ direktiivin (EU) 2022/2555 6 artiklan 6 alakohdassa määriteltyä poikkeamaa;

44) ’digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavalla poikkeamalla’ poikkeamaa, joka vaikuttaa tai voi vaikuttaa kielteisesti digitaalisia elementtejä sisältävän tuotteen kykyyn suojella datan tai toimintojen saatavuutta, aitoutta, eheyttä tai luottamuksellisuutta;

45) ’läheltä piti -tilanteella’ direktiivin (EU) 2022/2555 6 artiklan 5 alakohdassa määriteltyä läheltä piti -tilannetta;

46) ’kyberuhkalla’ asetuksen (EU) 2019/881 2 artiklan 8 alakohdassa määriteltyä kyberuhkaa;

47) ’henkilötiedoilla’ asetuksen (EU) 2016/679 4 artiklan 1 alakohdassa määriteltyjä henkilötietoja;

48) ’vapaalla ja avoimen lähdekoodin ohjelmistolla’ ohjelmistoa, jonka lähdekoodi on yleisesti saatavilla ja joka on asetettu saataville vapaalla ja avoimen lähdekoodin lisenssillä, joka tarjoaa kaikki oikeudet, jotta se on vapaasti saatavilla, käytettävissä, muunneltavissa ja uudelleen jaettavissa;

49) ’palautusmenettelyllä’ asetuksen (EU) 2019/1020 3 artiklan 22 alakohdassa määriteltyä palautusmenettelyä;

50) ’markkinoilta poistamisella’ asetuksen (EU) 2019/1020 3 artiklan 23 alakohdassa määriteltyä markkinoilta poistamista;

51) ’koordinaattoriksi nimetyllä CSIRT-yksiköllä’ direktiivin (EU) 2022/2555 12 artiklan 1 alakohdan nojalla koordinaattoriksi nimettyä CSIRT-yksikköä.

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 esittelemästä tai käyttämästä messuilla, näyttelyissä, esittelytilaisuuksissa tai vastaavissa tapahtumissa digitaalisia elementtejä sisältäviä tuotteita, jotka eivät ole tämän asetuksen mukaisia, mukaan lukien tuotteiden prototyypit, edellyttäen, että tuotteet esitellään sellaisella näkyvällä merkinnällä varustettuna, josta käy selvästi ilmi, että tuote ei ole tämän asetuksen mukainen eikä sitä saa asettaa saataville markkinoilla ennen kuin se on sitä.

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

4. Edellä olevaa 3 kohtaa ei sovelleta muussa unionin yhdenmukaistamislainsäädännössä kuin tässä asetuksessa tarkoitettuihin turvakomponentteihin.

5 artikla

Digitaalisia elementtejä sisältävien tuotteiden hankinnat tai käyttö

1. Tämä asetus ei estä jäsenvaltioita asettamasta tiettyihin tarkoituksiin hankittaville tai käytettäville digitaalisia elementtejä sisältäville tuotteille muita kyberturvallisuusvaatimuksia, myös silloin, kun kyseisiä tuotteita hankitaan tai käytetään kansalliseen turvallisuuteen tai puolustukseen liittyviin tarkoituksiin, edellyttäen, että tällaiset vaatimukset ovat yhdenmukaisia unionin oikeudessa vahvistettujen jäsenvaltioiden velvoitteiden kanssa ja että ne ovat tarpeen ja oikeasuhteisia kyseisten tarkoitusten saavuttamiseksi.

2. Kun hankitaan tämän asetuksen soveltamisalaan kuuluvia digitaalisia elementtejä sisältäviä tuotteita, jäsenvaltioiden on varmistettava, että hankintaprosessissa otetaan huomioon tämän asetuksen liitteessä I vahvistettujen olennaisten kyberturvallisuusvaatimusten noudattaminen, mukaan lukien valmistajien kyky käsitellä tehokkaasti haavoittuvuuksia, sanotun kuitenkaan rajoittamatta direktiivien 2014/24/EU ja 2014/25/EU soveltamista.

6 artikla

Digitaalisia elementtejä sisältäviä tuotteita koskevat vaatimukset

Digitaalisia elementtejä sisältäviä tuotteita saa asettaa saataville markkinoilla ainoastaan, jos:

a) ne täyttävät liitteessä I olevassa I osassa vahvistetut olennaiset kyberturvallisuusvaatimukset, edellyttäen että niitä käytetään asianmukaisesti asennettuina ja ylläpidettyinä käyttötarkoituksensa mukaisesti tai kohtuudella ennakoitavissa olosuhteissa ja tarvittaessa tarpeelliset tietoturvapäivitykset on asennettu; ja

b) valmistajan käyttöön ottamat prosessit täyttävät liitteessä I olevassa II osassa vahvistetut olennaiset kyberturvallisuusvaatimukset.

7 artikla

Digitaalisia elementtejä sisältävät tärkeät tuotteet

1. Digitaalisia elementtejä sisältävät tuotteet, joilla on liitteessä III vahvistetun tuoteryhmän ydintoiminto, katsotaan digitaalisia elementtejä sisältäviksi tärkeiksi tuotteiksi, ja niihin on sovellettava 32 artiklan 2 ja 3 kohdassa tarkoitettuja vaatimustenmukaisuuden arviointimenettelyjä. Sellaisen digitaalisia elementtejä sisältävän tuotteen, jolla on liitteessä III vahvistetun tuoteryhmän ydintoiminto, integrointi toiseen tuotteeseen ei itsessään saa johtaa siihen, että tuotteeseen, johon se on integroitu, sovelletaan 32 artiklan 2 ja 3 kohdassa tarkoitettuja vaatimustenmukaisuuden arviointimenettelyjä.

2. Tämän artiklan 1 kohdassa tarkoitetut digitaalisia elementtejä sisältävien tuotteiden ryhmät, jotka on jaettu liitteessä III vahvistettuihin luokkiin I ja II, täyttävät vähintään yhden seuraavista kriteereistä:

a) digitaalisia elementtejä sisältävä tuote suorittaa ensisijaisesti muiden tuotteiden, verkkojen tai palvelujen kyberturvallisuuden kannalta kriittisiä toimintoja, mukaan lukien todentamisen ja pääsyn varmistaminen, tunkeutumisen ehkäiseminen ja havaitseminen, päätepisteen tietoturva tai verkon suojaus;

b) digitaalisia elementtejä sisältävä tuote suorittaa toiminnon, jossa on merkittävä haitallisten vaikutusten riski, mitä tulee sen intensiteettiin ja kykyyn häiritä, hallita tai vahingoittaa suurta määrää muita tuotteita tai vahingoittaa sen käyttäjien terveyttä, tietoturvaa tai turvallisuutta suoralla manipuloinnilla, kuten keskeisen järjestelmätoiminnon, mukaan lukien verkonhallinta, konfiguraationhallinta, virtualisointi tai henkilötietojen käsittely.

3. Siirretään komissiolle valta antaa 61 artiklan mukaisesti delegoituja säädöksiä, joilla muutetaan liitettä III sisällyttämällä luetteloon kuhunkin digitaalisia elementtejä sisältävien tuoteryhmien luokkaan uusi tuoteryhmä ja esittämällä sen määritelmä, siirtämällä tuoteryhmä yhdestä luokasta toiseen tai poistamalla luettelosta olemassa oleva tuoteryhmä. Arvioidessaan tarvetta muuttaa liitteessä III vahvistettua luetteloa komissio ottaa huomioon tämän artiklan 2 kohdassa tarkoitetuissa kriteereissä vahvistetut digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuuteen liittyvät toiminnot tai tehtävän ja niiden aiheuttaman kyberturvallisuusriskin tason.

Tämän kohdan ensimmäisessä alakohdassa tarkoitetuissa delegoiduissa säädöksissä säädetään tarvittaessa vähintään 12 kuukauden siirtymäkaudesta erityisesti, jos liitteessä III vahvistettuun luokkaan I tai II lisätään uusi digitaalisia elementtejä sisältävien tärkeiden tuotteiden ryhmä tai jos tuoteryhmä siirretään luokasta I luokkaan II ennen kuin 32 artiklan 2 ja 3 kohdassa tarkoitettuja asiaankuuluvia vaatimustenmukaisuuden arviointimenettelyjä aletaan soveltaa, paitsi jos lyhyempi siirtymäkausi on perusteltu pakottavasta kiireellisestä syystä.

4. Komissio hyväksyy viimeistään … päivänä …kuuta … [12 kuukauden kuluttua tämän asetuksen voimaantulopäivästä] täytäntöönpanosäädöksen, jossa täsmennetään liitteessä III vahvistettuihin luokkiin I ja II kuuluvien digitaalisia elementtejä sisältävien tuotteiden ryhmien tekninen kuvaus ja liitteessä IV vahvistettuihin digitaalisia elementtejä sisältävien tuotteiden ryhmien tekninen kuvaus. Kyseinen täytäntöönpanosäädös hyväksytään 62 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

8 artikla

Digitaalisia elementtejä sisältävät kriittiset tuotteet

1. Siirretään komissiolle valta antaa 61 artiklan mukaisesti delegoituja säädöksiä, joilla täydennetään tätä asetusta määrittämällä ne digitaalisia elementtejä sisältävät tuotteet, joilla on tämän asetuksen liitteessä IV vahvistetun tuoteryhmän ydintoiminto ja joille on hankittava asetuksen (EU) 2019/881 nojalla hyväksytyn eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukainen, vähintään varmuustason ”korotettu” eurooppalainen kyberturvallisuussertifikaatti sen osoittamiseksi, että ne ovat tämän asetuksen liitteessä I vahvistettujen olennaisten kyberturvallisuusvaatimusten tai niiden osien mukaisia, edellyttäen, että asetuksen (EU) 2019/881 nojalla on hyväksytty eurooppalainen kyberturvallisuuden sertifiointijärjestelmä, joka kattaa kyseiset digitaalisia elementtejä sisältävien tuotteiden ryhmät ja on valmistajien käytettävissä. Näissä delegoiduissa säädöksissä on täsmennettävä vaadittu varmuustaso, jonka on oltava oikeassa suhteessa digitaalisia elementtejä sisältäviin tuotteisiin liittyvän kyberturvallisuusriskin tasoon ja jossa on otettava huomioon niiden käyttötarkoitus, mukaan lukien direktiivin (EU) 2022/2555 3 artiklan 1 kohdassa tarkoitettujen keskeisten toimijoiden kriittinen riippuvuus niistä.

   Ennen tällaisten delegoitujen säädösten antamista komissio arvioi suunniteltujen toimenpiteiden mahdollisia markkinavaikutuksia ja kuulee asiaankuuluvia sidosryhmiä, myös asetuksella (EU) 2019/881 perustettua Euroopan kyberturvallisuuden sertifiointiryhmää. Arvioinnissa on otettava huomioon jäsenvaltioiden valmius ja kapasiteetti panna täytäntöön asiaankuuluva eurooppalainen kyberturvallisuuden sertifiointijärjestelmä. Jos tämän kohdan ensimmäisessä alakohdassa tarkoitettuja delegoituja säädöksiä ei ole annettu, digitaalisia elementtejä sisältäviin tuotteisiin, joilla on liitteessä IV vahvistetun tuoteryhmän ydintoiminto, sovelletaan 32 artiklan 3 kohdassa tarkoitettuja vaatimustenmukaisuuden arviointimenettelyjä.

Ensimmäisessä alakohdassa tarkoitetuissa delegoiduissa säädöksissä säädetään vähintään kuuden kuukauden siirtymäkaudesta, paitsi jos lyhyempi siirtymäkausi on perusteltu pakottavasta kiireellisestä syystä.

2. Siirretään komissiolle valta antaa 61 artiklan mukaisesti delegoituja säädöksiä, joilla muutetaan liitettä IV lisäämällä tai poistamalla digitaalisia elementtejä sisältävien kriittisten tuotteiden ryhmiä. Määrittäessään tällaisia digitaalisia elementtejä sisältävien kriittisten tuotteiden ryhmiä ja vaadittua varmuustasoa tämän artiklan 1 kohdan mukaisesti komissio ottaa huomioon 7 artiklan 2 kohdassa tarkoitetut kriteerit ja varmistaa, että digitaalisia elementtejä sisältävien tuotteiden ryhmät täyttävät vähintään yhden seuraavista kriteereistä:

a) direktiivin (EU) 2022/2555 3 artiklassa tarkoitetut keskeiset toimijat ovat kriittisesti riippuvaisia digitaalisia elementtejä sisältävien tuotteiden ryhmästä;

b) digitaalisia elementtejä sisältävien tuotteiden ryhmää koskevat poikkeamat ja hyödynnetyt haavoittuvuudet saattavat johtaa vakaviin häiriöihin kriittisissä toimitusketjuissa sisämarkkinoilla.

Ennen tällaisten delegoitujen säädösten antamista komissio tekee 1 kohdassa tarkoitetun tyyppisen arvioinnin.

Ensimmäisessä alakohdassa tarkoitetuissa delegoiduissa säädöksissä säädetään vähintään kuuden kuukauden siirtymäkaudesta, paitsi jos lyhyempi siirtymäkausi on perusteltu pakottavasta kiireellisestä syystä.

9 artikla

Sidosryhmien kuuleminen

1. Valmistellessaan toimenpiteitä tämän asetuksen täytäntöönpanemiseksi komissio kuulee asiaankuuluvia sidosryhmiä, kuten asiaankuuluvia jäsenvaltioiden viranomaisia, yksityisen sektorin yrityksiä, mukaan lukien mikroyritykset ja pienet ja keskisuuret yritykset, avoimen lähdekoodin ohjelmistoyhteisöä, kuluttajajärjestöjä, tiedeyhteisöä sekä asiaankuuluvia unionin laitoksia ja elimiä ja unionin tasolla perustettuja asiantuntijaryhmiä, ja ottaa niiden näkemykset huomioon. Komissio kuulee tarvittaessa jäsennellysti kyseisiä sidosryhmiä ja pyytää niiltä näkemyksiä erityisesti silloin, kun se

   a) laatii 26 artiklassa tarkoitettuja ohjeita;

   b) laatii liitteessä III vahvistettujen tuoteryhmien teknisiä kuvauksia 7 artiklan 4 kohdan mukaisesti, arvioi tuoteryhmien luettelon mahdollisten päivitysten tarvetta 7 artiklan 3 kohdan ja 8 artiklan 2 kohdan mukaisesti tai arvioi mahdollisia markkinavaikutuksia 8 artiklan 1 kohdan mukaisesti, sanotun kuitenkaan rajoittamatta 61 artiklan soveltamista;

   c) valmistelee tämän asetuksen arviointia ja uudelleentarkastelua.

2. Komissio järjestää vähintään kerran vuodessa säännöllisiä kuulemis- ja tiedotustilaisuuksia 1 kohdassa tarkoitettujen sidosryhmien näkemysten keräämiseksi tämän asetuksen täytäntöönpanosta.

10 artikla

Osaamisen vahvistaminen kyberkestävässä digitaalisessa ympäristössä

Tätä asetusta sovellettaessa ja jotta voidaan vastata ammattihenkilöiden tarpeisiin ja antaa tukea tämän asetuksen täytäntöönpanossa, jäsenvaltioiden on tarvittaessa komission, Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja ENISAn tuella edistettävä toimenpiteitä ja strategioita, joilla pyritään

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

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

11 artikla

Yleinen tuoteturvallisuus

Poiketen siitä, mitä asetuksen (EU) 2023/988 2 artiklan 1 kohdan kolmannen alakohdan b alakohdassa säädetään, kyseisen asetuksen III luvun 1 jaksoa, V ja VII lukua sekä IX–XI lukua sovelletaan digitaalisia elementtejä sisältäviin tuotteisiin tämän asetuksen soveltamisalaan kuulumattomien näkökohtien ja riskien tai riskiluokkien osalta, jos kyseisiin tuotteisiin ei sovelleta muussa asetuksen (EU) 2023/988 3 artiklan 27 alakohdassa määritellyssä ’unionin yhdenmukaistamislainsäädännössä’ säädettyjä erityisiä turvallisuusvaatimuksia.

12 artikla

Suuririskiset tekoälyjärjestelmät

1. Rajoittamatta asetuksen (EU) 2024/1689 15 artiklassa säädettyjen tarkkuuteen ja luotettavuuteen liittyvien vaatimusten soveltamista digitaalisia elementtejä sisältävien tuotteiden, jotka kuuluvat tämän asetuksen soveltamisalaan ja jotka luokitellaan suuririskisiksi tekoälyjärjestelmiksi kyseisen asetuksen 6 artiklan nojalla, katsotaan täyttävän kyseisen asetuksen 15 artiklassa säädetyt kyberturvallisuusvaatimukset, jos

   a) kyseiset tuotteet täyttävät liitteessä I olevassa I osassa vahvistetut olennaiset kyberturvallisuusvaatimukset;

b) valmistajan käyttöön ottamat prosessit täyttävät liitteessä I olevassa II osassa vahvistetut olennaiset kyberturvallisuusvaatimukset; ja

c) asetuksen (EU) 2024/1689 15 artiklassa vaadittu kyberturvallisuussuojan tason saavuttaminen osoitetaan tämän asetuksen mukaisesti annettavalla EU-vaatimustenmukaisuusvakuutuksella.

2. Tämän artiklan 1 kohdassa tarkoitettuihin digitaalisia elementtejä sisältäviin tuotteisiin ja kyberturvallisuusvaatimuksiin sovelletaan asetuksen (EU) 2024/1689 43 artiklassa säädettyä asiaankuuluvaa vaatimustenmukaisuuden arviointimenettelyä. Kyseistä arviointia varten niiden ilmoitettujen laitosten, jotka ovat toimivaltaisia valvomaan suuririskisten tekoälyjärjestelmien vaatimustenmukaisuutta asetuksen (EU) 2024/1689 nojalla, on oltava myös toimivaltaisia valvomaan, että tämän asetuksen soveltamisalaan kuuluvat suuririskiset tekoälyjärjestelmät täyttävät tämän asetuksen liitteessä I vahvistetut vaatimukset edellyttäen, että se, täyttävätkö kyseiset ilmoitetut laitokset tämän asetuksen 39 artiklassa säädetyt vaatimukset, on arvioitu asetuksen (EU) 2024/1689 mukaisen ilmoitusmenettelyn yhteydessä.

3. Poiketen siitä, mitä tämän artiklan 2 kohdassa säädetään, tämän asetuksen liitteessä III lueteltuihin digitaalisia elementtejä sisältäviin tärkeisiin tuotteisiin, joihin sovelletaan tämän asetuksen 32 artiklan 2 kohdan a ja b alakohdassa ja 32 artiklan 3 kohdassa tarkoitettuja vaatimustenmukaisuuden arviointimenettelyjä, ja tämän asetuksen liitteessä IV lueteltuihin digitaalisia elementtejä sisältäviin kriittisiin tuotteisiin, joille on hankittava eurooppalainen kyberturvallisuussertifikaatti tämän asetuksen 8 artiklan 1 kohdan nojalla tai joihin sertifikaatin puuttuessa sovelletaan tämän asetuksen 32 artiklan 3 kohdassa tarkoitettuja vaatimuksenmukaisuuden arviointimenettelyjä ja jotka luokitellaan asetuksen (EU) 2024/1689 6 artiklan nojalla suuririskisiksi tekoälyjärjestelmiksi ja joihin sovelletaan asetuksen (EU) 2024/1689 liitteessä VI tarkoitettua sisäiseen valvontaan perustuvaa vaatimustenmukaisuuden arviointimenettelyä, sovelletaan tässä asetuksessa säädettyjä vaatimustenmukaisuuden arviointimenettelyjä siltä osin kuin on kyse tässä asetuksessa vahvistettujen olennaisten kyberturvallisuusvaatimusten täyttymisestä.

4. Tämän artiklan 1 kohdassa tarkoitettujen digitaalisia elementtejä sisältävien tuotteiden valmistajat voivat osallistua asetuksen (EU) 2024/1689 57 artiklassa tarkoitettuihin tekoälyn sääntelyn testiympäristöihin.

II luku
Talouden toimijoiden velvollisuudet ja vapaita ja avoimen lähdekoodin ohjelmistoja koskevat säännökset

13 artikla

Valmistajien velvollisuudet

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

2. Edellä olevan 1 kohdan noudattamiseksi valmistajien on arvioitava digitaalisia elementtejä sisältävään tuotteeseen liittyvät kyberturvallisuusriskit ja otettava arvioinnin tulokset huomioon digitaalisia elementtejä sisältävän tuotteen suunnittelu-, kehitys-, tuotanto-, toimitus- ja ylläpitovaiheissa kyberturvallisuusriskien minimoimiseksi, poikkeamien ehkäisemiseksi ja niiden vaikutusten minimoimiseksi, myös käyttäjien terveyden ja turvallisuuden osalta.

3. Kyberturvallisuusriskien arviointi on dokumentoitava ja sitä on päivitettävä tarvittaessa tämän artiklan 8 kohdan mukaisesti määritettävän tukiajan ajan. Kyseiseen kyberturvallisuusriskien arviointiin on sisällyttävä vähintään kyberturvallisuusriskien analyysi, joka perustuu digitaalisia elementtejä sisältävän tuotteen käyttötarkoitukseen ja kohtuudella ennakoitavissa olevaan käyttöön sekä käyttöolosuhteisiin, kuten toimintaympäristöön tai suojattavaan omaisuuteen, ottaen huomioon aika, jonka tuotteen odotetaan olevan käytössä. Kyberturvallisuusriskien arvioinnissa on ilmoitettava, sovelletaanko asiaankuuluvaan digitaalisia elementtejä sisältävään tuotteeseen liitteessä I olevan I osan 2 kohdassa vahvistettuja turvallisuusvaatimuksia, ja jos sovelletaan, millä tavalla, ja miten kyseiset vaatimukset pannaan täytäntöön kyberturvallisuusriskien arvioinnin perusteella. Siinä on myös ilmoitettava, miten valmistajan on sovellettava liitteessä I olevan I osan 1 kohtaa ja liitteessä I olevassa II osassa vahvistettuja haavoittuvuuksien käsittelyä koskevia vaatimuksia.

4. Saattaessaan markkinoille digitaalisia elementtejä sisältävää tuotetta valmistajan on sisällytettävä 31 artiklan ja liitteen VII nojalla vaadittuihin teknisiin asiakirjoihin tämän artiklan 3 kohdassa tarkoitettu kyberturvallisuusriskien arviointi. Kun kyseessä ovat 12 artiklassa tarkoitetut digitaalisia elementtejä sisältävät tuotteet, joihin sovelletaan myös muita unionin säädöksiä, kyberturvallisuusriskien arviointi voi olla osa kyseisissä unionin säädöksissä edellytettyä riskinarviointia. Jos tietyt olennaiset kyberturvallisuusvaatimukset eivät sovellu tiettyyn digitaalisia elementtejä sisältävään tuotteeseen, valmistajan on perusteltava tämä selkeästi kyseisissä teknisissä asiakirjoissa.

5. Edellä olevan 1 kohdan noudattamiseksi valmistajien on noudatettava asianmukaista huolellisuutta, kun ne integroivat tuotteeseensa kolmansilta osapuolilta hankittuja komponentteja, jotta kyseiset komponentit eivät vaaranna digitaalisia elementtejä sisältävän tuotteen kyberturvallisuutta, myös silloin, kun tuotteeseen integroidaan vapaiden ja avoimen lähdekoodin ohjelmistojen komponentteja, joita ei ole asetettu saataville markkinoilla kaupallisen toiminnan yhteydessä.

6. Valmistajien on digitaalisia elementtejä sisältävään tuotteeseen integroidun komponentin, myös avoimen lähdekoodin komponentin, haavoittuvuuden todettuaan ilmoitettava haavoittuvuudesta komponenttia valmistavalle tai ylläpitävälle henkilölle tai yhteisölle ja puututtava haavoittuvuuteen ja korjattava se liitteessä I olevassa II osassa vahvistettujen haavoittuvuuksien käsittelyä koskevien vaatimusten mukaisesti. Jos valmistajat ovat kehittäneet ohjelmiston tai laitteiston muutoksen, jolla puututaan kyseisen komponentin haavoittuvuuteen, niiden on jaettava asiaankuuluvat koodit tai asiakirjat komponenttia valmistavan tai ylläpitävän henkilön tai yhteisön kanssa tarvittaessa koneellisesti luettavassa muodossa.

7. Valmistajien on oikeassa suhteessa kyberturvallisuusriskien luonteeseen nähden järjestelmällisesti dokumentoitava digitaalisia elementtejä sisältävien tuotteiden asiaankuuluvat kyberturvallisuuteen liittyvät seikat, mukaan lukien niiden tietoon tulleet haavoittuvuudet ja kaikki kolmansien osapuolten toimittamat merkitykselliset tiedot, ja tarvittaessa päivitettävä tuotteiden kyberturvallisuusriskien arviointi.

8. Saattaessaan markkinoille digitaalisia elementtejä sisältävää tuotetta ja tuotteen tukiajan ajan valmistajien on varmistettava, että kyseisen tuotteen ja sen komponenttien haavoittuvuudet käsitellään tehokkaasti ja liitteessä I olevassa II osassa vahvistettujen olennaisten kyberturvallisuusvaatimusten mukaisesti.

Valmistajien on määritettävä tukiaika siten, että se vastaa tuotteen odotettavissa olevaa käyttöikää, ottaen erityisesti huomioon käyttäjien kohtuulliset odotukset, tuotteen luonne, mukaan lukien sen käyttötarkoitus, sekä asiaa koskeva unionin oikeus, jossa määritetään aika, jonka digitaalisia elementtejä sisältävien tuotteiden odotetaan olevan käytössä. Tukiaikaa määrittäessään valmistajat voivat myös ottaa huomioon muiden valmistajien markkinoille saattamien samankaltaisen toiminnon tarjoavien digitaalisia elementtejä sisältävien tuotteiden tukiajat, toimintaympäristön saatavuuden, ydintoimintoja tarjoavien ja kolmansilta osapuolilta peräisin olevien integroitujen komponenttien tukiajat sekä 52 artiklan 15 kohdan nojalla perustetun erityisen hallinnollisen yhteistyön ryhmän ja komission antamat asiaa koskevat ohjeet. Tukiaikaa määrittäessä huomioon otettavia seikkoja on tarkasteltava tavalla, jolla varmistetaan oikeasuhtaisuus.

Tukiajan on oltava vähintään viisi vuotta, sanotun kuitenkaan rajoittamatta toisen alakohdan soveltamista. Jos digitaalisia elementtejä sisältävää tuotetta odotetaan käytettävän alle viisi vuotta, tukiajan on vastattava odotettua käyttöaikaa.

Ottaen huomioon 52 artiklan 16 kohdassa tarkoitetut hallinnollisen yhteistyön ryhmän suositukset komissio voi antaa 61 artiklan mukaisesti delegoituja säädöksiä, joilla täydennetään tätä asetusta määrittämällä tukiajan vähimmäiskesto tietyille tuoteryhmille, jos markkinavalvontatiedot viittaavat siihen, että tukiaika on riittämätön.

Valmistajien on sisällytettävä digitaalisia elementtejä sisältävän tuotteen tukiajan määrittämisessä huomioon otetut tiedot liitteessä VII esitettyihin teknisiin asiakirjoihin.

Valmistajilla on oltava asianmukaiset toimintatavat ja menettelyt, mukaan lukien liitteessä I olevan II osan 5 kohdassa tarkoitetut koordinoitua haavoittuvuuksien julkistamista koskevat periaatteet, joilla käsitellään ja korjataan sisäisten tai ulkoisten lähteiden raportoimat digitaalisia elementtejä sisältävän tuotteen mahdolliset haavoittuvuudet.

9. Valmistajien on varmistettava, että jokainen liitteessä I olevan II osan 8 kohdassa tarkoitettu tietoturvapäivitys, joka on asetettu käyttäjien saataville tukiajan aikana, pysyy saatavilla sen julkaisun jälkeen vähintään kymmenen vuoden ajan tai jäljellä olevan tukiajan ajan sen mukaan, kumpi näistä ajanjaksoista on pidempi.

10. Jos valmistaja on saattanut markkinoille ohjelmistotuotteen myöhempiä, olennaisesti muutettuja versioita, kyseinen valmistaja voi varmistaa liitteessä I olevan II osan 2 kohdassa vahvistetun olennaisen kyberturvallisuusvaatimuksen noudattamisen vain viimeksi markkinoille saattamansa version osalta edellyttäen, että aiemmin markkinoille saatettujen versioiden käyttäjät voivat käyttää viimeksi markkinoille saatettua versiota maksutta eikä käyttäjille aiheudu lisäkustannuksia sen laitteisto- ja ohjelmistoympäristön mukauttamisesta, jossa käyttäjät käyttävät kyseisen tuotteen alkuperäistä versiota.

11. Valmistajat voivat ylläpitää julkisia ohjelmistoarkistoja, joilla parannetaan käyttäjien mahdollisuuksia käyttää aiempia versioita. Näissä tapauksissa käyttäjille on tiedotettava selkeästi ja helposti saatavilla olevalla tavalla riskeistä, jotka liittyvät sellaisten ohjelmistojen käyttöön, joita ei tueta.

12. Ennen digitaalisia elementtejä sisältävän tuotteen saattamista markkinoille valmistajien on laadittava 31 artiklassa tarkoitetut tekniset asiakirjat.

    Niiden on suoritettava tai teetettävä valitsemansa 32 artiklassa tarkoitetut vaatimustenmukaisuuden arviointimenettelyt.

    Jos kyseisellä vaatimustenmukaisuuden arviointimenettelyllä on osoitettu, että digitaalisia elementtejä sisältävä tuote täyttää liitteessä I olevassa I osassa vahvistetut olennaiset kyberturvallisuusvaatimukset ja että valmistajan käyttöön ottamat prosessit täyttävät liitteessä I olevassa II osassa vahvistetut olennaiset kyberturvallisuusvaatimukset, valmistajan on laadittava EU-vaatimustenmukaisuusvakuutus 28 artiklan mukaisesti ja kiinnitettävä tai liitettävä tuotteeseen CE-merkintä 30 artiklan mukaisesti.

13. Valmistajien on pidettävä tekniset asiakirjat ja EU-vaatimustenmukaisuusvakuutus markkinavalvontaviranomaisten saatavilla vähintään kymmenen vuoden ajan sen jälkeen, kun digitaalisia elementtejä sisältävä tuote on saatettu markkinoille, tai tukiajan ajan sen mukaan, kumpi näistä ajanjaksoista on pidempi.

14. Valmistajien on huolehdittava siitä, että käytössä on menettelyt, joiden ansiosta sarjatuotantoon kuuluvat digitaalisia elementtejä sisältävät tuotteet ovat edelleen tämän asetuksen mukaisia. Valmistajien on otettava asianmukaisesti huomioon muutokset kehitys- ja tuotantoprosessissa tai digitaalisia elementtejä sisältävän tuotteen rakenteessa tai ominaisuuksissa sekä muutokset yhdenmukaistetuissa standardeissa, eurooppalaisissa kyberturvallisuuden sertifiointijärjestelmissä tai 27 artiklassa tarkoitetuissa yhteisissä eritelmissä, joihin nähden digitaalisia elementtejä sisältävän tuotteen vaatimustenmukaisuus ilmoitetaan tai joiden perusteella tuotteen vaatimustenmukaisuus todennetaan.

15. Valmistajien on varmistettava, että niiden digitaalisia elementtejä sisältävissä tuotteissa on tyyppi-, erä- tai sarjanumero tai muu elementti, josta ne voidaan tunnistaa, tai kun se ei ole mahdollista, niiden on varmistettava, että kyseinen tieto on annettu digitaalisia elementtejä sisältävän tuotteen pakkauksessa tai tuotteen mukana seuraavassa asiakirjassa.

16. Valmistajien on ilmoitettava nimensä, rekisteröity tuotenimensä tai rekisteröity tavaramerkkinsä, postiosoitteensa, sähköpostiosoitteensa tai muut digitaaliset yhteystietonsa sekä tapauksen mukaan verkkosivusto, jonka kautta valmistajaan voi ottaa yhteyttä, joko digitaalisia elementtejä sisältävässä tuotteessa, sen pakkauksessa tai digitaalisia elementtejä sisältävän tuotteen mukana seuraavassa asiakirjassa. Nämä tiedot on sisällytettävä myös liitteessä II esitettyihin käyttäjälle annettaviin tietoihin ja ohjeisiin. Yhteystiedot on annettava käyttäjien ja markkinavalvontaviranomaisten helposti ymmärtämällä kielellä.

17. Tämän asetuksen soveltamiseksi valmistajien on nimettävä keskitetty yhteyspiste, jonka avulla käyttäjät voivat viestiä suoraan ja nopeasti niiden kanssa, muun muassa digitaalisia elementtejä sisältävän tuotteen haavoittuvuuksista ilmoittamisen helpottamiseksi.

Valmistajien on varmistettava, että käyttäjät voivat helposti tunnistaa keskitetyn yhteyspisteen. Niiden on myös sisällytettävä keskitetty yhteyspiste liitteessä II esitettyihin käyttäjälle annettaviin tietoihin ja ohjeisiin.

Keskitetyn yhteyspisteen on annettava käyttäjille mahdollisuus valita haluamansa viestintätapa, eikä sitä saa rajata pelkästään automatisoituihin välineisiin.

18. Valmistajien on varmistettava, että digitaalisia elementtejä sisältävien tuotteiden mukana on paperilla tai sähköisessä muodossa liitteessä II vahvistetut käyttäjälle annettavat tiedot ja ohjeet. Tällaiset tiedot ja ohjeet on annettava kielellä, jota käyttäjät ja markkinavalvontaviranomaiset helposti ymmärtävät. Niiden on oltava selkeitä, ymmärrettäviä, helppotajuisia ja helposti luettavissa. Niiden on mahdollistettava digitaalisia elementtejä sisältävien tuotteiden turvallinen asentaminen, toiminta ja käyttö. Valmistajien on pidettävä liitteessä II esitetyt käyttäjille annettavat tiedot ja ohjeet käyttäjien ja markkinavalvontaviranomaisten saatavilla vähintään kymmenen vuoden ajan sen jälkeen, kun digitaalisia elementtejä sisältävä tuote on saatettu markkinoille, tai tukiajan ajan sen mukaan, kumpi näistä ajanjaksoista on pidempi. Jos tällaiset tiedot ja ohjeet annetaan verkossa, valmistajien on varmistettava, että ne ovat saavutettavia, käyttäjäystävällisiä ja saatavilla verkossa vähintään kymmenen vuoden ajan sen jälkeen, kun digitaalisia elementtejä sisältävä tuote on saatettu markkinoille, tai tukiajan ajan sen mukaan, kumpi näistä ajanjaksoista on pidempi.

19. Valmistajien on varmistettava, että 8 kohdassa tarkoitetun tukiajan päättymispäivä, mukaan lukien ainakin kuukausi ja vuosi, ilmoitetaan selkeästi ja ymmärrettävästi hankinta-ajankohtana helposti saatavilla olevalla tavalla ja tapauksen mukaan digitaalisia elementtejä sisältävässä tuotteessa, sen pakkauksessa tai digitaalisesti.

    Valmistajien on annettava käyttäjille ilmoitus siitä, että heidän digitaalisia elementtejä sisältävän tuotteensa tukiaika on päättynyt, jos se on teknisesti toteutettavissa digitaalisia elementtejä sisältävän tuotteen luonteen vuoksi.

20. Valmistajien on toimitettava joko EU-vaatimustenmukaisuusvakuutuksen jäljennös tai yksinkertaistettu EU-vaatimustenmukaisuusvakuutus digitaalisia elementtejä sisältävän tuotteen mukana. Jos toimitetaan yksinkertaistettu EU-vaatimustenmukaisuusvakuutus, sen on sisällettävä tarkka verkko-osoite, jossa EU-vaatimustenmukaisuusvakuutuksen koko teksti on saatavilla.

21. Digitaalisia elementtejä sisältävän tuotteen markkinoille saattamisesta alkaen ja tuotteen tukiajan ajan valmistajien, jotka tietävät tai joilla on syytä uskoa, että digitaalisia elementtejä sisältävä tuote tai niiden käyttöön ottamat prosessit eivät täytä liitteessä I vahvistettuja olennaisia kyberturvallisuusvaatimuksia, 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.

22. Valmistajien 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 ja valmistajan käyttöön ottamat prosessit täyttävät liitteessä I vahvistetut olennaiset kyberturvallisuusvaatimukset. Valmistajien on tehtävä kyseisen viranomaisen kanssa tämän pyynnöstä yhteistyötä kaikissa toimenpiteissä, joita toteutetaan niiden markkinoille saattaman digitaalisia elementtejä sisältävän tuotteen aiheuttamien kyberturvallisuusriskien poistamiseksi.

23. Valmistajan, joka lopettaa toimintansa eikä sen vuoksi pysty noudattamaan tätä asetusta, on ennen toiminnan lopettamista ilmoitettava asiaankuuluville markkinavalvontaviranomaisille sekä kaikin käytettävissä olevin keinoin ja mahdollisuuksien mukaan markkinoille saatettujen asiaankuuluvien digitaalisia elementtejä sisältävien tuotteiden käyttäjille tulevasta toiminnan lopettamisesta.

24. Komissio voi täytäntöönpanosäädöksillä eurooppalaiset tai kansainväliset standardit ja parhaat käytännöt huomioon ottaen täsmentää liitteessä I olevan II osan 1 kohdassa tarkoitetun ohjelmistojen materiaaliluettelon muodon ja osatekijät. Nämä täytäntöönpanosäädökset hyväksytään 62 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

25. Jotta voidaan arvioida jäsenvaltioiden ja koko unionin riippuvuutta ohjelmistokomponenteista ja erityisesti sellaisista komponenteista, jotka luokitellaan vapaiksi ja avoimen lähdekoodin ohjelmistoiksi, hallinnollisen yhteistyön ryhmä voi päättää tehdä unionin laajuisen riippuvuuden arvioinnin tietyistä digitaalisia elementtejä sisältävien tuotteiden ryhmistä. Markkinavalvontaviranomaiset voivat tätä tarkoitusta varten pyytää tällaisiin ryhmiin kuuluvien digitaalisia elementtejä sisältävien tuotteiden valmistajia toimittamaan asiaankuuluvat liitteessä I olevan II osan 1 kohdassa tarkoitetut ohjelmistojen materiaaliluettelot. Markkinavalvontaviranomaiset voivat toimittaa näiden tietojen perusteella hallinnollisen yhteistyön ryhmälle anonymisoituja ja yhdistettyjä tietoja ohjelmistoriippuvuuksista. Hallinnollisen yhteistyön ryhmä toimittaa riippuvuuden arvioinnin tuloksista kertomuksen direktiivin (EU) 2022/2555 14 artiklan nojalla perustetulle yhteistyöryhmälle.

14 artikla

Valmistajien raportointivelvoitteet

1. Valmistajan on ilmoitettava kaikista digitaalisia elementtejä sisältävään tuotteeseen sisältyvistä aktiivisesti hyödynnetyistä haavoittuvuuksista, joista se on tullut tietoiseksi, samanaikaisesti tämän artiklan 7 kohdan mukaisesti koordinaattoriksi nimetylle CSIRT-yksikölle ja ENISAlle. Valmistajan on ilmoitettava kyseisistä aktiivisesti hyödynnetyistä haavoittuvuuksista 16 artiklan nojalla perustetun keskitetyn raportointialustan kautta.

2. Edellä 1 kohdassa tarkoitettua ilmoitusta varten valmistajan on annettava

   a) ilman aiheetonta viivytystä ja joka tapauksessa 24 tunnin kuluessa siitä, kun valmistaja on tullut tietoiseksi aktiivisesti hyödynnetystä haavoittuvuudesta, sitä koskeva ennakkovaroitusilmoitus, jossa ilmoitetaan tarvittaessa jäsenvaltiot, joiden alueella valmistaja tietää digitaalisia elementtejä sisältävää tuotettaan asetetun saataville;

b) jollei asiaankuuluvia tietoja ole jo toimitettu, ilman aiheetonta viivytystä ja joka tapauksessa 72 tunnin kuluessa siitä, kun valmistaja on tullut tietoiseksi aktiivisesti hyödynnetystä haavoittuvuudesta, haavoittuvuusilmoitus, jossa annetaan saatavilla olevat yleiset tiedot kyseisestä digitaalisia elementtejä sisältävästä tuotteesta, kyseisen hyödyntämisen ja haavoittuvuuden yleisestä luonteesta sekä toteutetuista korjaavista tai lieventävistä toimenpiteistä ja korjaavista tai lieventävistä toimenpiteistä, joita käyttäjät voivat toteuttaa, ja jossa tarvittaessa myös ilmoitetaan, miten arkaluonteisina valmistaja pitää ilmoitettuja tietoja;

c) jollei asiaankuuluvia tietoja ole jo toimitettu, loppuraportti viimeistään 14 päivän kuluttua siitä, kun korjaava tai lieventävä toimenpide on käytettävissä, mukaan lukien vähintään seuraavat tiedot:

   i) kuvaus haavoittuvuudesta, mukaan lukien sen vakavuus ja vaikutukset;

   ii) jos saatavilla, tiedot mahdollisista pahantahtoisista toimijoista, jotka ovat hyödyntäneet tai hyödyntävät haavoittuvuutta;

   iii) yksityiskohtaiset tiedot tietoturvapäivityksestä tai muista korjaavista toimenpiteistä, jotka on asetettu saataville haavoittuvuuden korjaamiseksi.

3. Valmistajan on ilmoitettava kaikista digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavista vakavista poikkeamista, joista se on tullut tietoiseksi, samanaikaisesti tämän artiklan 7 kohdan mukaisesti koordinaattoriksi nimetylle CSIRT-yksikölle ja ENISAlle. Valmistajan on ilmoitettava kyseisistä poikkeamista 16 artiklan nojalla perustetun keskitetyn raportointialustan kautta.

4. Edellä 3 kohdassa tarkoitettua ilmoitusta varten valmistajan on annettava

a) ilman aiheetonta viivytystä ja joka tapauksessa 24 tunnin kuluessa siitä, kun valmistaja on tullut tietoiseksi digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavasta vakavasta poikkeamasta, sitä koskeva ennakkovaroitusilmoitus, johon sisältyy ainakin se, epäilläänkö poikkeamaa laittomien tai pahantahtoisten tekojen aiheuttamaksi ja jossa ilmoitetaan myös tarvittaessa jäsenvaltiot, joiden alueella valmistaja tietää digitaalisia elementtejä sisältävää tuotettaan asetetun saataville;

b) jollei asiaankuuluvia tietoja ole jo toimitettu, ilman aiheetonta viivytystä ja joka tapauksessa 72 tunnin kuluessa siitä, kun valmistaja on tullut tietoiseksi poikkeamasta, poikkeamailmoitus, jossa annetaan saatavilla olevia yleisiä tietoja poikkeaman luonteesta, alustava arvio poikkeamasta sekä tietoa toteutetuista korjaavista tai lieventävistä toimenpiteistä ja korjaavista tai lieventävistä toimenpiteistä, joita käyttäjät voivat toteuttaa, ja jossa tarvittaessa myös ilmoitetaan, miten arkaluonteisina valmistaja pitää ilmoitettuja tietoja;

c) jollei asiaankuuluvia tietoja ole jo toimitettu, viimeistään kuukauden kuluttua b alakohdan mukaisen poikkeamailmoituksen antamisesta loppuraportti, joka sisältää vähintään seuraavat tiedot:

i) yksityiskohtainen kuvaus poikkeamasta, mukaan lukien sen vakavuus ja vaikutukset;

ii) uhkan tyyppi tai poikkeaman todennäköisesti aiheuttanut perimmäinen syy;

iii) toteutetut ja meneillään olevat lieventämistoimenpiteet.

5. Edellä olevan 3 kohdan soveltamiseksi digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttava poikkeama katsotaan vakavaksi, jos

a) se vaikuttaa tai voi vaikuttaa kielteisesti digitaalisia elementtejä sisältävän tuotteen kykyyn suojella arkaluonteisten tai tärkeiden datan tai toimintojen saatavuutta, aitoutta, eheyttä tai luottamuksellisuutta; tai

b) se on johtanut tai voi johtaa haitallisen koodin sisällyttämiseen digitaalisia elementtejä sisältävään tuotteeseen tai digitaalisia elementtejä sisältävän tuotteen käyttäjän verkko- ja tietojärjestelmiin tai ajamiseen niissä.

6. Koordinaattoriksi nimetty CSIRT-yksikkö, joka alun perin on saanut ilmoituksen, voi tarvittaessa pyytää valmistajia toimittamaan väliraportin, joka sisältää merkityksellisiä ajantasaisia tietoja digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavan aktiivisesti hyödynnetyn haavoittuvuuden tai vakavan poikkeaman tilanteesta.

7. Tämän artiklan 1 ja 3 kohdassa tarkoitetut ilmoitukset on annettava 16 artiklassa tarkoitetun keskitetyn raportointialustan kautta käyttäen jotakin 16 artiklan 1 kohdassa tarkoitetuista sähköisistä ilmoituspalveluista. Ilmoitus on annettava käyttäen sen jäsenvaltion koordinaattoriksi nimetyn CSIRT-yksikön sähköistä ilmoituspalvelua, jossa valmistajien päätoimipaikka on unionissa, ja sen on oltava samanaikaisesti ENISAn saatavilla.

Tätä direktiiviä sovellettaessa valmistajan päätoimipaikan katsotaan olevan unionissa siinä jäsenvaltiossa, jossa sen digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuusriskeihin liittyvät päätökset pääsääntöisesti tehdään. Jos tällaista jäsenvaltiota ei voida määrittää, päätoimipaikan katsotaan sijaitsevan jäsenvaltiossa, jossa asianomaisella valmistajalla on eniten työntekijöitä työllistävä toimipaikka unionissa.

Jos valmistajalla ei ole päätoimipaikkaa unionissa, sen on annettava 1 ja 3 kohdassa tarkoitetut ilmoitukset käyttäen siinä jäsenvaltiossa koordinaattoriksi nimetyn CSIRT-yksikön sähköistä ilmoituspalvelua, joka määritetään seuraavaa järjestystä noudattaen ja valmistajan saatavilla olevien tietojen perusteella:

a) jäsenvaltio, johon on sijoittautunut se valmistajan puolesta toimiva valtuutettu edustaja, joka edustaa suurinta määrää kyseisen valmistajan digitaalisia elementtejä sisältäviä tuotteita;

b) jäsenvaltio, johon on sijoittautunut maahantuoja, joka saattaa markkinoille suurimman määrän kyseisen valmistajan digitaalisia elementtejä sisältäviä tuotteita;

c) jäsenvaltio, johon on sijoittautunut jakelija, joka asettaa saataville markkinoilla suurimman määrän kyseisen valmistajan digitaalisia elementtejä sisältäviä tuotteita;

d) jäsenvaltio, jossa sijaitsee suurin määrä kyseisen valmistajan digitaalisia elementtejä sisältävien tuotteiden käyttäjiä.

Kolmannen alakohdan d alakohdan osalta valmistaja voi antaa ilmoituksia mahdollisista myöhemmistä aktiivisesti hyödynnetyistä haavoittuvuuksista tai digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavista vakavista poikkeamista samalle koordinaattoriksi nimetylle CSIRT-yksikölle, jolle se ensimmäisen kerran raportoi.

8. Tultuaan tietoiseksi aktiivisesti hyödynnetystä haavoittuvuudesta tai digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavasta vakavasta poikkeamasta valmistajan on tiedotettava digitaalisia elementtejä sisältävän tuotteen käyttäjille, joihin vaikutukset kohdistuvat, ja tarvittaessa kaikille käyttäjille kyseisestä haavoittuvuudesta tai poikkeamasta ja tarpeen mukaan mahdollisista riskinhallintatoimenpiteistä ja korjaavista toimenpiteistä, joita käyttäjät voivat toteuttaa lieventääkseen haavoittuvuuden tai poikkeaman vaikutuksia, tarvittaessa jäsennellyssä, koneellisesti luettavassa muodossa, jota on helppo käsitellä automaattisesti. Jos valmistaja ei anna digitaalisia elementtejä sisältävän tuotteen käyttäjille tietoja oikea-aikaisesti, koordinaattoreiksi nimetyt CSIRT-yksiköt, joille asiasta on ilmoitettu, voivat antaa näitä tietoja käyttäjille, kun se katsotaan oikeasuhtaiseksi ja tarpeelliseksi haavoittuvuuden tai poikkeaman vaikutusten ehkäisemiseksi tai lieventämiseksi.

9. Komissio antaa viimeistään … päivänä …kuuta … [12 kuukauden kuluttua tämän asetuksen voimaantulosta] tämän asetuksen 61 artiklan mukaisesti delegoituja säädöksiä, joilla täydennetään tätä asetusta määrittelemällä ehdot kyberturvallisuuteen liittyvien syiden soveltamiselle lykättäessä ilmoitusten välittämistä tämän asetuksen 16 artiklan 2 kohdassa tarkoitetulla tavalla. Komissio tekee yhteistyötä direktiivin (EU) 2022/2555 15 artiklan nojalla perustetun CSIRT-verkoston ja ENISAn kanssa valmistellessaan delegoitujen säädösten luonnoksia.

10. Komissio voi täytäntöönpanosäädöksin täsmentää tässä artiklassa sekä 15 ja 16 artiklassa tarkoitettujen ilmoitusten muotoa ja niihin liittyviä menettelyjä. Nämä täytäntöönpanosäädökset hyväksytään 62 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen. Komissio tekee yhteistyötä CSIRT-verkoston ja ENISAn kanssa valmistellessaan kyseisiä täytäntöönpanosäädösten luonnoksia.

15 artikla

Vapaaehtoinen raportointi

1. Valmistajat ja muut luonnolliset henkilöt ja oikeushenkilöt voivat vapaaehtoisesti ilmoittaa koordinaattoriksi nimetylle CSIRT-yksikölle tai ENISAlle mahdollisista digitaalisia elementtejä sisältävään tuotteeseen sisältyvistä haavoittuvuuksista tai kyberuhkista, jotka voisivat vaikuttaa digitaalisia elementtejä sisältävän tuotteen riskiprofiiliin.

2. Valmistajat ja muut luonnolliset henkilöt ja oikeushenkilöt voivat vapaaehtoisesti ilmoittaa koordinaattoriksi nimetylle CSIRT-yksikölle tai ENISAlle mahdollisista digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavista poikkeamista sekä läheltä piti -tilanteista, jotka olisivat voineet johtaa tällaiseen poikkeamaan.

3. Koordinaattoriksi nimetyn CSIRT-yksikön tai ENISAn on käsiteltävä tämän artiklan 1 ja 2 kohdassa tarkoitetut ilmoitukset 16 artiklassa säädetyn menettelyn mukaisesti.

   Koordinaattoriksi nimetty CSIRT-yksikkö voi asettaa etusijalle pakollisten ilmoitusten käsittelyn vapaaehtoisten ilmoitusten käsittelyyn nähden.

4. Jos muu luonnollinen henkilö tai oikeushenkilö kuin valmistaja ilmoittaa 1 tai 2 kohdan mukaisesti aktiivisesti hyödynnetystä haavoittuvuudesta tai digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavasta vakavasta poikkeamasta, koordinaattoriksi nimetyn CSIRT-yksikön on ilman aiheetonta viivytystä ilmoitettava asiasta valmistajalle.

5. Koordinaattoriksi nimettyjen CSIRT-yksikköjen ja ENISAn on varmistettava ilmoituksen tehneen luonnollisen henkilön tai oikeushenkilön toimittamien tietojen luottamuksellisuus ja asianmukainen suoja. Vapaaehtoinen ilmoittaminen ei saa johtaa sellaisten lisävelvoitteiden asettamiseen ilmoituksen tehneelle luonnolliselle henkilölle tai oikeushenkilölle, joita siihen ei olisi sovellettu, jos se ei olisi toimittanut kyseistä ilmoitusta, sanotun kuitenkaan rajoittamatta rikosten ennaltaehkäisemistä, tutkimista, paljastamista ja rikoksiin liittyviä syytetoimia.

16 artikla

Keskitetyn raportointialustan perustaminen

1. Edellä 14 artiklan 1 ja 3 kohdassa ja 15 artiklan 1 ja 2 kohdassa tarkoitettuja ilmoituksia varten ja valmistajien raportointivelvoitteiden yksinkertaistamiseksi ENISA perustaa keskitetyn raportointialustan. ENISA hallinnoi ja ylläpitää keskitetyn raportointialustan päivittäistä toimintaa. Keskitetyn raportointialustan rakenteen on mahdollistettava se, että jäsenvaltiot ja ENISA voivat ottaa käyttöön omat sähköiset ilmoituspalvelunsa.

2. Koordinaattoriksi nimetyn CSIRT-yksikön, joka alun perin on saanut ilmoituksen, on ilmoituksen saamisen jälkeen ilman aiheetonta viivytystä välitettävä ilmoitus keskitetyn raportointialustan kautta koordinaattoreiksi nimetyille CSIRT-yksiköille alueella, jolla valmistaja on ilmoittanut asettaneensa digitaalisia elementtejä sisältävän tuotteen saataville.

Poikkeuksellisissa olosuhteissa ja erityisesti valmistajan pyynnöstä ja valmistajan tämän asetuksen 14 artiklan 2 kohdan a alakohdan mukaisesti toteaman ilmoitettujen tietojen arkaluonteisuuden perusteella ilmoituksen välittämistä voidaan lykätä perustelluista kyberturvallisuuteen liittyvistä syistä ehdottoman välttämättömän ajan, myös silloin, kun haavoittuvuuteen sovelletaan direktiivin (EU) 2022/2555 12 artiklan 1 kohdassa tarkoitettua koordinoitua haavoittuvuuden julkistamismenettelyä. Jos CSIRT-yksikkö päättää olla välittämättä ilmoitusta, sen on välittömästi ilmoitettava ENISAlle tästä päätöksestä ja annettava sekä perustelut ilmoituksen välittämättä jättämiselle että tieto siitä, milloin se aikoo välittää ilmoituksen tässä kohdassa säädetyn välittämismenettelyn mukaisesti. ENISA voi tukea CSIRT-yksikköä kyberturvallisuuteen liittyvien syiden soveltamisessa ilmoituksen välittämisen lykkäämisen yhteydessä.

Erityisen poikkeuksellisissa olosuhteissa, joissa valmistaja ilmoittaa 14 artiklan 2 kohdan b alakohdassa tarkoitetussa ilmoituksessa,

a) että pahantahtoinen toimija on aktiivisesti hyödyntänyt ilmoitettua haavoittuvuutta ja saatavilla olevien tietojen mukaan sitä on hyödynnetty ainoastaan sen koordinaattoriksi nimetyn CSIRT-yksikön jäsenvaltiossa, jolle valmistaja on ilmoittanut haavoittuvuudesta;

b) että ilmoitettua haavoittuvuutta koskevan tiedon välitön välittäminen johtaisi todennäköisesti sellaisten tietojen antamiseen, jotka olisivat kyseisen jäsenvaltion olennaisten etujen vastaisia; tai

c) että ilmoitettu haavoittuvuus aiheuttaa välittömän korkean kyberturvallisuusriskin, joka johtuu tiedon välittämisestä eteenpäin;

vain tieto siitä, että valmistaja on tehnyt ilmoituksen, yleiset tiedot tuotteesta, tiedot hyödyntämisen yleisestä luonteesta ja tieto siitä, että on vedottu turvallisuussyihin, on annettava samanaikaisesti ENISAn saataville, kunnes täydellinen ilmoitus toimitetaan asianomaisille CSIRT-yksiköille ja ENISAlle. Jos ENISA katsoo kyseisten tietojen perusteella, että on olemassa järjestelmäriski, joka vaikuttaa turvallisuuteen sisämarkkinoilla, ENISA suosittelee ilmoituksen vastaanottaneelle CSIRT-yksikölle, että se välittää täydellisen ilmoituksen muille koordinaattoreiksi nimetyille CSIRT-yksiköille ja ENISAlle itselleen.

3. Saatuaan ilmoituksen aktiivisesti hyödynnetystä haavoittuvuudesta digitaalisia elementtejä sisältävässä tuotteessa tai digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavasta vakavasta poikkeamasta, koordinaattoreiksi nimettyjen CSIRT-yksiköiden on annettava jäsenvaltioidensa markkinavalvontaviranomaisille ilmoitetut tiedot, joita markkinavalvontaviranomaiset tarvitsevat täyttääkseen tämän asetuksen mukaiset velvoitteensa.

4. ENISA toteuttaa asianmukaiset ja oikeasuhtaiset tekniset, operatiiviset ja organisatoriset toimenpiteet hallitakseen keskitetyn raportointialustan ja sen kautta annettujen tai välitettyjen tietojen tietoturvaan kohdistuvia riskejä. Se ilmoittaa ilman aiheetonta viivytystä kaikista keskitettyyn raportointialustaan vaikuttavista tietoturvapoikkeamista CSIRT-verkostolle ja komissiolle.

5. ENISA laatii ja panee täytäntöön yhteistyössä CSIRT-verkoston kanssa eritelmät teknisistä, operatiivisista ja organisatorisista toimenpiteistä, jotka koskevat 1 kohdassa tarkoitetun keskitetyn raportointialustan perustamista, ylläpitoa ja turvallista toimintaa, mukaan lukien ainakin keskitetyn raportointialustan perustamiseen, toimintaan ja ylläpitoon liittyvät tietoturvajärjestelyt, sekä kansallisella tasolla koordinaattoreiksi nimettyjen CSIRT-yksiköiden ja unionin tasolla ENISAn perustamia sähköisiä ilmoituspalveluja, mukaan lukien menettelyihin liittyvät näkökohdat sen varmistamiseksi, että jos ilmoitettuun haavoittuvuuteen ei ole saatavilla korjaavia tai lieventäviä toimenpiteitä, tiedot tästä haavoittuvuudesta jaetaan tiukkoja tietoturvakäytäntöjä noudattaen ja tiedonsaantitarpeen perusteella.

6. Jos koordinaattoriksi nimetylle CSIRT-yksikölle on ilmoitettu aktiivisesti hyödynnetystä haavoittuvuudesta osana direktiivin (EU) 2022/2555 12 artiklan 1 kohdassa tarkoitettua koordinoitua haavoittuvuuksien julkistamismenettelyä, koordinaattoriksi nimetty CSIRT-yksikkö, joka alun perin on saanut ilmoituksen, voi perustelluista kyberturvallisuuteen liittyvistä syistä lykätä ilmoituksen välittämistä keskitetyn raportointialustan kautta ehdottoman välttämättömän ajan, kunnes koordinoidun haavoittuvuuden julkistamisen osapuolet ovat antaneet suostumuksensa julkistamiseen. Tämä vaatimus ei estä valmistajia ilmoittamasta tällaisesta haavoittuvuudesta vapaaehtoisesti tässä artiklassa säädettyä menettelyä noudattaen.

17 artikla

Muut raportointiin liittyvät säännökset

1. ENISA voi toimittaa tämän asetuksen 14 artiklan 1 ja 3 kohdan ja 15 artiklan 1 ja 2 kohdan nojalla ilmoitetut tiedot direktiivin (EU) 2022/2555 16 artiklalla perustetulle Euroopan kyberkriisien yhteysorganisaatioiden verkostolle (EU-CyCLONe), jos nämä tiedot ovat operatiivisella tasolla merkityksellisiä laajamittaisten kyberturvapoikkeamien ja -kriisien koordinoidun hallinnan kannalta. Tällaisen merkityksellisyyden määrittämiseksi ENISA voi ottaa huomioon CSIRT-verkoston tekemät tekniset analyysit, jos niitä on saatavilla.

2. Jos yleinen tietoisuus on tarpeen digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttavan vakavan poikkeaman ehkäisemiseksi tai lieventämiseksi tai meneillään olevan poikkeaman käsittelemiseksi tai jos poikkeaman julkistaminen on muutoin yleisen edun mukaista, asiaankuuluvan jäsenvaltion koordinaattoriksi nimetty CSIRT-yksikkö voi asianomaista valmistajaa kuultuaan ja tarvittaessa yhteistyössä ENISAn kanssa tiedottaa poikkeamasta yleisölle tai vaatia valmistajaa tekemään niin.

3. ENISA laatii tämän asetuksen 14 artiklan 1 ja 3 kohdan ja 15 artiklan 1 ja 2 kohdan nojalla saamiensa ilmoitusten perusteella 24 kuukauden välein teknisen raportin digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuusriskien uusista suuntauksista ja toimittaa sen direktiivin (EU) 2022/2555 14 artiklan nojalla perustetulle yhteistyöryhmälle. Ensimmäinen tällainen raportti toimitetaan 24 kuukauden kuluessa tämän asetuksen 14 artiklan 1 ja 3 kohdassa säädettyjen velvoitteiden soveltamispäivästä. ENISA sisällyttää asiaankuuluvia tietoja teknisistä raporteistaan direktiivin (EU) 2022/2555 18 artiklan nojalla antamaansa kertomukseen kyberturvallisuuden tilasta unionissa.

4. Pelkkä 14 artiklan 1 ja 3 kohdan tai 15 artiklan 1 ja 2 kohdan mukainen ilmoittaminen ei lisää ilmoituksen tehneen luonnollisen henkilön tai oikeushenkilön vastuuta.

5. Sen jälkeen kun tietoturvapäivitys tai muu korjaava tai lieventävä toimenpide on saatavilla, ENISA lisää kyseisen digitaalisia elementtejä sisältävän tuotteen valmistajan suostumuksella tämän asetuksen 14 artiklan 1 kohdan tai 15 artiklan 1 kohdan nojalla ilmoitetun yleisesti tiedossa olevan haavoittuvuuden direktiivin (EU) 2022/2555 12 artiklan 2 kohdan nojalla perustettuun Euroopan haavoittuvuustietokantaan.

6. Koordinaattoreiksi nimettyjen CSIRT-yksiköiden on annettava 14 artiklan mukaisiin raportointivelvoitteisiin liittyvää käyttötukea valmistajille ja erityisesti valmistajille, jotka katsotaan mikroyrityksiksi tai pieniksi tai keskisuuriksi yrityksiksi.

18 artikla

Valtuutetut edustajat

1. Valmistaja voi nimittää kirjallisella toimeksiannolla valtuutetun edustajan.

2. Edellä 13 artiklan 1–11 kohdassa, 13 artiklan 12 kohdan ensimmäisessä alakohdassa ja 13 artiklan 14 kohdassa säädetyt velvollisuudet eivät saa kuulua valtuutetun edustajan toimeksiantoon.

3. Valtuutetun edustajan on suoritettava valmistajalta saadussa toimeksiannossa eritellyt tehtävät. Valtuutetun edustajan on pyynnöstä toimitettava markkinavalvontaviranomaisille jäljennös toimeksiannosta. Valtuutetun edustajan on toimeksiannon perusteella voitava suorittaa ainakin seuraavat tehtävät:

a) pidettävä 28 artiklassa tarkoitettu EU-vaatimustenmukaisuusvakuutus ja 31 artiklassa tarkoitetut tekniset asiakirjat markkinavalvontaviranomaisten saatavilla vähintään kymmenen vuoden ajan sen jälkeen, kun digitaalisia elementtejä sisältävä tuote on saatettu markkinoille, tai tukiajan ajan sen mukaan, kumpi näistä ajanjaksoista on pidempi;

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

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

19 artikla

Maahantuojien velvollisuudet

1. Maahantuojat saavat saattaa markkinoille ainoastaan digitaalisia elementtejä sisältäviä tuotteita, jotka täyttävät liitteessä I olevassa I osassa vahvistetut olennaiset kyberturvallisuusvaatimukset ja joiden osalta valmistajan käyttöön ottamat prosessit täyttävät liitteessä I olevassa II osassa vahvistetut olennaiset kyberturvallisuusvaatimukset.

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

   a) valmistaja on suorittanut 32 artiklassa tarkoitetut asianmukaiset vaatimustenmukaisuuden arviointimenettelyt;

   b) valmistaja on laatinut tekniset asiakirjat;

   c) digitaalisia elementtejä sisältävässä tuotteessa on 30 artiklassa tarkoitettu CE-merkintä ja sen mukana on 13 artiklan 20 kohdassa tarkoitettu EU-vaatimustenmukaisuusvakuutus ja liitteessä II esitetyt käyttäjälle annettavat tiedot ja ohjeet kielellä, jota käyttäjät ja markkinavalvontaviranomaiset helposti ymmärtävät;

   d) valmistaja on noudattanut 13 artiklan 15, 16 ja 19 kohdassa säädettyjä vaatimuksia.

   Tätä kohtaa sovellettaessa maahantuojien on voitava toimittaa tarvittavat asiakirjat, joilla todistetaan tässä artiklassa säädettyjen vaatimusten täyttyminen.

3. Jos maahantuoja katsoo tai sillä on syytä uskoa, että digitaalisia elementtejä sisältävä tuote tai valmistajan käyttöönottamat prosessit eivät ole tämän asetuksen mukaisia, maahantuoja ei saa saattaa tuotetta markkinoille ennen kuin kyseinen tuote tai valmistajan käyttöönottamat prosessit on saatettu tämän asetuksen mukaisiksi. Lisäksi jos digitaalisia elementtejä sisältävä tuote aiheuttaa merkittävän kyberturvallisuusriskin, maahantuojan on ilmoitettava asiasta valmistajalle ja markkinavalvontaviranomaisille.

Jos maahantuojalla on syytä uskoa, että digitaalisia elementtejä sisältävä tuote voi muiden kuin teknisten riskitekijöiden vuoksi aiheuttaa merkittävän kyberturvallisuusriskin, sen on ilmoitettava tästä markkinavalvontaviranomaisille. Markkinavalvontaviranomaisten on tällaisen tiedon saatuaan noudatettava 54 artiklan 2 kohdassa tarkoitettuja menettelyjä.

4. Maahantuojien on ilmoitettava nimensä, rekisteröity tuotenimensä tai rekisteröity tavaramerkkinsä, postiosoitteensa, sähköpostiosoitteensa tai muut digitaaliset yhteystietonsa sekä tarvittaessa verkkosivusto, jonka kautta maahantuojaan voi ottaa yhteyttä, joko digitaalisia elementtejä sisältävässä tuotteessa, sen pakkauksessa tai digitaalisia elementtejä sisältävän tuotteen mukana seuraavassa asiakirjassa. Yhteystiedot on annettava käyttäjien ja markkinavalvontaviranomaisten helposti ymmärtämällä kielellä.

5. Maahantuojien, jotka tietävät tai joilla on syytä uskoa, että digitaalisia elementtejä sisältävä tuote, jonka ne ovat saattaneet markkinoille, ei ole tämän asetuksen mukainen, on välittömästi toteutettava tarvittavat korjaavat toimenpiteet sen varmistamiseksi, että digitaalisia elementtejä sisältävä tuote saatetaan tämän asetuksen mukaiseksi, tai tarvittaessa tuotteen poistamiseksi markkinoilta tai sitä koskevan palautusmenettelyn järjestämiseksi.

   Kun maahantuojat ovat tulleet tietoisiksi digitaalisia elementtejä sisältävässä tuotteessa olevasta haavoittuvuudesta, niiden on ilman aiheetonta viivytystä ilmoitettava siitä valmistajalle. Jos digitaalisia elementtejä sisältävä tuote aiheuttaa merkittävän kyberturvallisuusriskin, 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.

6. Maahantuojien on vähintään kymmenen vuoden ajan sen jälkeen, kun digitaalisia elementtejä sisältävä tuote on saatettu markkinoille, tai tukiajan ajan sen mukaan, kumpi näistä ajanjaksoista on pidempi, pidettävä EU-vaatimustenmukaisuusvakuutuksen jäljennös markkinavalvontaviranomaisten saatavilla ja varmistettava, että tekniset asiakirjat voidaan antaa pyynnöstä kyseisten viranomaisten saataville.

7. 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 I osassa vahvistetut olennaiset kyberturvallisuusvaatimukset ja valmistajan käyttöön ottamat prosessit täyttävät liitteessä I olevassa II osassa vahvistetut olennaiset kyberturvallisuusvaatimukset. Niiden on tehtävä kyseisen viranomaisen kanssa tämän pyynnöstä yhteistyötä toimenpiteissä, joilla pyritään poistamaan niiden markkinoille saattaman digitaalisia elementtejä sisältävän tuotteen aiheuttamat kyberturvallisuusriskit.

8. Jos digitaalisia elementtejä sisältävän tuotteen maahantuoja saa tietoonsa, että tuotteen valmistaja on lopettanut toimintansa eikä sen vuoksi pysty noudattamaan tässä asetuksessa säädettyjä velvoitteitaan, maahantuojan on ilmoitettava tilanteesta asiaankuuluville markkinavalvontaviranomaisille sekä kaikin käytettävissä olevin keinoin ja mahdollisuuksien mukaan markkinoille saatettujen digitaalisia elementtejä sisältävien tuotteiden käyttäjille.

20 artikla

Jakelijoiden velvollisuudet

1. Kun jakelijat asettavat digitaalisia elementtejä sisältävän tuotteen saataville markkinoilla, niiden on toimittava noudattaen asiaankuuluvaa huolellisuutta tässä asetuksessa esitettyjen 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 13 artiklan 15, 16, 18, 19 ja 20 kohdassa ja 19 artiklan 4 kohdassa säädetyt velvollisuutensa ja toimittaneet kaikki tarvittavat asiakirjat jakelijalle.

3. Jos jakelija katsoo tai sillä on syytä uskoa hallussaan olevien tietojen perusteella, että digitaalisia elementtejä sisältävä tuote tai valmistajan käyttöön ottamat prosessit eivät täytä liitteessä I vahvistettuja olennaisia kyberturvallisuusvaatimuksia, jakelija ei saa asettaa digitaalisia elementtejä sisältävää tuotetta saataville markkinoilla ennen kuin kyseinen tuote tai valmistajan käyttöön ottamat prosessit on saatettu tämän asetuksen mukaisiksi. Lisäksi jos digitaalisia elementtejä sisältävä tuote aiheuttaa merkittävän kyberturvallisuusriskin, jakelijan on ilmoitettava siitä ilman aiheetonta viivytystä valmistajalle ja markkinavalvontaviranomaisille.

4. Jakelijoiden, jotka tietävät tai joilla on syytä uskoa hallussaan olevien tietojen perusteella, että digitaalisia elementtejä sisältävä tuote, jonka ne ovat asettaneet saataville markkinoilla, tai sen valmistajan käyttöön ottamat prosessit eivät ole tämän asetuksen mukaisia, on varmistettava, että toteutetaan tarvittavat korjaavat toimenpiteet kyseisen digitaalisia elementtejä sisältävän tuotteen tai sen valmistajan käyttöön ottamien prosessien saattamiseksi vaatimusten mukaisiksi tai tarvittaessa tuotteen poistamiseksi markkinoilta tai sitä koskevan palautusmenettelyn järjestämiseksi.

Kun jakelijat ovat tulleet tietoisiksi digitaalisia elementtejä sisältävässä tuotteessa olevasta haavoittuvuudesta, niiden on ilman aiheetonta viivytystä ilmoitettava siitä valmistajalle. Jos digitaalisia elementtejä sisältävä tuote aiheuttaa merkittävän kyberturvallisuusriskin, 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 sisältävä tuote ja valmistajan käyttöön ottamat prosessit ovat tämän asetuksen mukaisia. Niiden on tehtävä kyseisen viranomaisen kanssa tämän pyynnöstä yhteistyötä toimenpiteissä, joilla pyritään poistamaan niiden markkinoille saattaman digitaalisia elementtejä sisältävän tuotteen aiheuttamat kyberturvallisuusriskit.

6. Jos digitaalisia elementtejä sisältävän tuotteen jakelija tulee hallussaan olevien tietojen perusteella tietoiseksi siitä, että tuotteen valmistaja on lopettanut toimintansa eikä sen vuoksi pysty noudattamaan tässä asetuksessa säädettyjä velvoitteitaan, jakelijan on ilman aiheetonta viivytystä ilmoitettava tilanteesta asiaankuuluville markkinavalvontaviranomaisille sekä kaikin käytettävissä olevin keinoin ja mahdollisuuksien mukaan markkinoille saatettujen digitaalisia elementtejä sisältävien tuotteiden käyttäjille.

21 artikla

Tapaukset, joissa valmistajien velvoitteita sovelletaan maahantuojiin ja jakelijoihin

Maahantuojaa tai jakelijaa pidetään tätä asetusta sovellettaessa valmistajana ja siihen sovelletaan 13 ja 14 artiklaa silloin, kun kyseinen maahantuoja tai jakelija saattaa digitaalisia elementtejä sisältävän tuotteen markkinoille omalla nimellään tai tavaramerkillään tai tekee merkittävän muutoksen markkinoille jo saatettuun digitaalisia elementtejä sisältävään tuotteeseen.

22 artikla

Muut tapaukset, joissa sovelletaan valmistajien velvollisuuksia

1. Muuta luonnollista henkilöä tai oikeushenkilöä kuin valmistajaa, maahantuojaa tai jakelijaa, joka tekee digitaalisia elementtejä sisältävään tuotteeseen merkittävän muutoksen ja asettaa kyseisen tuotteen saataville markkinoilla, pidetään tätä asetusta sovellettaessa valmistajana.

2. Tämän artiklan 1 kohdassa tarkoitettuun henkilöön sovelletaan 13 ja 14 artiklassa säädettyjä velvoitteita digitaalisia elementtejä sisältävän tuotteen sen osan osalta, johon merkittävä muutos vaikuttaa, tai jos merkittävä muutos vaikuttaa digitaalisia elementtejä sisältävän tuotteen kyberturvallisuuteen kokonaisuudessaan, koko tuotteen osalta.

23 artikla

Talouden toimijoiden yksilöiminen

1. Talouden toimijoiden on pyynnöstä annettava markkinavalvontaviranomaisille seuraavat tiedot:

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

   b) jokaisen sellaisen talouden toimijan nimi ja osoite, jolle ne ovat toimittaneet digitaalisia elementtejä sisältävän tuotteen, jos nämä tiedot ovat saatavilla.

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.

24 artikla

Avoimen lähdekoodin ohjelmistovastaavien velvollisuudet

1. Avoimen lähdekoodin ohjelmistovastaavien on otettava käyttöön ja dokumentoitava todennettavissa olevalla tavalla kyberturvallisuusperiaatteet, joilla edistetään turvallisen digitaalisia elementtejä sisältävän tuotteen kehittämistä ja sitä, että kyseisen tuotteen kehittäjät voivat käsitellä haavoittuvuuksia tehokkaasti. Kyseisillä periaatteilla on myös edistettävä tuotteen kehittäjien 15 artiklassa säädettyä vapaaehtoista raportointia haavoittuvuuksista, ja niissä on otettava huomioon avoimen lähdekoodin ohjelmistovastaavan erityisluonne sekä siihen sovellettavat oikeudelliset ja organisatoriset järjestelyt. Kyseisiin periaatteisiin on sisällyttävä erityisesti näkökohtia, jotka liittyvät haavoittuvuuksien dokumentointiin, niihin puuttumiseen ja niiden korjaamiseen, ja niillä on edistettävä havaittuja haavoittuvuuksia koskevien tietojen jakamista avoimen lähdekoodin yhteisössä.

2. Avoimen lähdekoodin ohjelmistovastaavan on tehtävä yhteistyötä markkinavalvontaviranomaisten kanssa näiden pyynnöstä tarkoituksena lieventää sellaisen digitaalisia elementtejä sisältävän tuotteen aiheuttamia kyberturvallisuusriskejä, joka luokitellaan vapaaksi ja avoimen lähdekoodin ohjelmistoksi.

   Avoimen lähdekoodin ohjelmistovastaavan on markkinavalvontaviranomaisen perustellusta pyynnöstä annettava tälle tämän helposti ymmärtämällä kielellä 1 kohdassa tarkoitetut asiakirjat paperiversiona tai sähköisessä muodossa.

3. Edellä 14 artiklan 1 kohdassa säädettyjä velvoitteita sovelletaan avoimen lähdekoodin ohjelmistovastaaviin siltä osin kuin ne osallistuvat digitaalisia elementtejä sisältävien tuotteiden kehittämiseen. Edellä 14 artiklan 3 ja 8 kohdassa säädettyjä velvoitteita sovelletaan avoimen lähdekoodin ohjelmistovastaaviin siltä osin kuin digitaalisia elementtejä sisältävien tuotteiden tietoturvaan vaikuttavat vakavat poikkeamat vaikuttavat verkko- ja tietojärjestelmiin, jotka avoimen lähdekoodin ohjelmistovastaavat antavat käyttöön tällaisten tuotteiden kehittämistä varten.

25 artikla

Vapaan ja avoimen lähdekoodin ohjelmiston tietoturvatodistus

Jotta voidaan helpottaa 13 artiklan 5 kohdassa säädetyn asianmukaista huolellisuutta koskevan velvoitteen noudattamista, erityisesti kun on kyse valmistajista, jotka integroivat digitaalisia elementtejä sisältäviin tuotteisiinsa vapaita ja avoimen lähdekoodin ohjelmistokomponentteja, komissiolle siirretään valta hyväksyä 61 artiklan mukaisesti delegoituja säädöksiä, joilla täydennetään tätä asetusta perustamalla vapaaehtoisia tietoturvatodistusohjelmia, joiden avulla vapaiksi ja avoimen lähdekoodin ohjelmistoiksi luokiteltavien digitaalisia elementtejä sisältävien tuotteiden kehittäjät tai käyttäjät sekä muut kolmannet osapuolet voivat arvioida, ovatko tällaiset tuotteet kaikkien tai tiettyjen olennaisten kyberturvallisuusvaatimusten tai muiden tässä asetuksessa säädettyjen velvoitteiden mukaisia.

26 artikla

Ohjeet

1. Jotta voidaan helpottaa täytäntöönpanoa ja varmistaa sen johdonmukaisuus, komissio julkaisee ohjeita, joilla autetaan talouden toimijoita soveltamaan tätä asetusta ja joilla pyritään erityisesti tekemään sen noudattamisesta helpompaa mikroyrityksille sekä pienille ja keskisuurille yrityksille.

2. Jos komissio aikoo antaa 1 kohdassa tarkoitettuja ohjeita, se käsittelee niissä ainakin seuraavia näkökohtia:

   a) tämän asetuksen soveltamisala ja erityisesti datan etäkäsittelyratkaisut sekä vapaat ja avoimen lähdekoodin ohjelmistot;

   b) tukiaikojen soveltaminen tiettyihin digitaalisia elementtejä sisältävien tuotteiden ryhmiin;

   c) ohjeet valmistajille, joihin sovelletaan tätä asetusta ja joihin sovelletaan myös muuta unionin yhdenmukaistamislainsäädäntöä kuin tätä asetusta tai muita asiaan liittyviä unionin säädöksiä;

   d) merkittävän muutoksen käsite.

   Komissio pitää myös yllä helposti saatavilla olevaa luetteloa tämän asetuksen nojalla annetuista delegoiduista säädöksistä ja täytäntöönpanosäädöksistä.

3. Komissio kuulee asiaankuuluvia sidosryhmiä, kun se laatii ohjeita tämän artiklan nojalla.

III luku

Digitaalisia elementtejä sisältävän tuotteen vaatimustenmukaisuus

27 artikla

Vaatimustenmukaisuusolettama

1. Digitaalisia elementtejä sisältäviä tuotteita ja valmistajan käyttöön ottamia prosesseja, jotka ovat sellaisten yhdenmukaistettujen standardien tai niiden osien mukaisia, joiden viitetiedot on julkaistu *Euroopan unionin virallisessa lehdessä*, on pidettävä niiden liitteessä I vahvistettujen olennaisten kyberturvallisuusvaatimusten mukaisina, jotka kyseiset standardit tai niiden osat kattavat.

   Komissio pyytää asetuksen (EU) N:o 1025/2012 10 artiklan 1 kohdan mukaisesti yhtä tai useampaa eurooppalaista standardointiorganisaatiota laatimaan tämän asetuksen liitteessä I vahvistettuja olennaisia kyberturvallisuusvaatimuksia koskevia yhdenmukaistettuja standardeja. Kun komissio valmistelee tähän asetukseen liittyviä standardointipyyntöjä, se pyrkii ottamaan huomioon sillä hetkellä jo olemassa tai kehitteillä olevat kyberturvallisuutta koskevat eurooppalaiset ja kansainväliset standardit, jotta voidaan yksinkertaistaa yhdenmukaistettujen standardien kehittämistä asetuksen (EU) N:o 1025/2012 mukaisesti.

2. Komissio voi hyväksyä täytäntöönpanosäädöksiä, joissa vahvistetaan teknisiä vaatimuksia koskevia yhteisiä eritelmiä, joiden avulla voidaan täyttää tämän asetuksen soveltamisalaan kuuluville digitaalisia elementtejä sisältäville tuotteille liitteessä I vahvistetut olennaiset kyberturvallisuusvaatimukset.

Nämä täytäntöönpanosäädökset hyväksytään ainoastaan, jos seuraavat edellytykset täyttyvät:

a) komissio on pyytänyt asetuksen (EU) N:o 1025/2012 10 artiklan 1 kohdan nojalla yhtä tai useampaa eurooppalaista standardointiorganisaatiota laatimaan liitteessä I vahvistettuja olennaisia kyberturvallisuusvaatimuksia koskevan yhdenmukaistetun standardin ja

i) pyyntöä ei ole hyväksytty;

ii) kyseistä pyyntöä koskevia yhdenmukaistettuja standardeja ei ole toimitettu asetuksen (EU) N:o 1025/2012 10 artiklan 1 kohdan mukaisesti asetetussa määräajassa; tai

iii) yhdenmukaistetut standardit eivät ole pyynnön mukaisia; ja

b) liitteessä I vahvistetut olennaiset kyberturvallisuusvaatimukset kattavien yhdenmukaistettujen standardien viitetietoja ei ole julkaistu *Euroopan unionin virallisessa lehdessä* asetuksen (EU) N:o 1025/2012 mukaisesti, eikä ole odotettavissa, että tällaiset viitetiedot julkaistaan kohtuullisen ajan kuluessa.

Nämä täytäntöönpanosäädökset hyväksytään 62 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

3. Ennen kuin komissio laatii luonnoksen tämän artiklan 2 kohdassa tarkoitetuksi täytäntöönpanosäädökseksi, se ilmoittaa asetuksen (EU) N:o 1025/2012 22 artiklassa tarkoitetulle komitealle katsovansa, että tämän artiklan 2 kohdassa esitetyt edellytykset täyttyvät.

4. Laatiessaan luonnosta tämän artiklan 2 kohdassa tarkoitetuksi täytäntöönpanosäädökseksi komissio ottaa huomioon asiaankuuluvien elinten näkemykset ja kuulee asianmukaisesti kaikkia asiaankuuluvia sidosryhmiä.

5. Digitaalisia elementtejä sisältäviä tuotteita ja valmistajan käyttöön ottamia prosesseja, jotka ovat tämän artiklan 2 kohdassa tarkoitetuilla täytäntöönpanosäädöksillä vahvistettujen yhteisten eritelmien tai niiden osien mukaisia, on pidettävä niiden liitteessä I vahvistettujen olennaisten kyberturvallisuusvaatimusten mukaisina, jotka kyseiset standardit tai niiden osat kattavat.

6. Jos eurooppalainen standardointiorganisaatio hyväksyy yhdenmukaistetun standardin ja sitä ehdotetaan komissiolle sen viitetietojen julkaisemiseksi *Euroopan unionin virallisessa lehdessä*, komissio arvioi yhdenmukaistetun standardin asetuksen (EU) N:o 1025/2012 mukaisesti. Kun yhdenmukaistetun standardin viitetiedot julkaistaan *Euroopan unionin virallisessa lehdessä*, komissio kumoaa 2 kohdassa tarkoitetut täytäntöönpanosäädökset tai niiden osat, jotka kattavat samat olennaiset kyberturvallisuusvaatimukset kuin kyseinen yhdenmukaistettu standardi.

7. Jos jäsenvaltio katsoo, että yhteinen eritelmä ei täysin täytä liitteessä I vahvistettuja olennaisia kyberturvallisuusvaatimuksia, sen on ilmoitettava asiasta komissiolle toimittamalla yksityiskohtainen selvitys. Komissio arvioi kyseisen yksityiskohtaisen selvityksen ja voi tarvittaessa muuttaa täytäntöönpanosäädöstä, jossa kyseinen yhteinen eritelmä vahvistetaan.

8. Digitaalisia elementtejä sisältävien tuotteiden ja valmistajan käyttöön ottamien prosessien, joille on annettu asetuksen (EU) 2019/881 nojalla hyväksytyn eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukainen EU-vaatimustenmukaisuusilmoitus tai sertifikaatti, katsotaan olevan liitteessä I vahvistettujen olennaisten kyberturvallisuusvaatimusten mukaisia, jos EU-vaatimustenmukaisuusilmoitus tai eurooppalainen kyberturvallisuussertifikaatti tai niiden osat kattavat kyseiset vaatimukset.

9. Siirretään komissiolle valta antaa tämän asetuksen 61 artiklan mukaisesti delegoituja säädöksiä, joilla täydennetään tätä asetusta yksilöimällä ne asetuksen (EU) 2019/881 nojalla hyväksytyt eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät, joita voidaan käyttää osoittamaan, että digitaalisia elementtejä sisältävät tuotteet ovat tämän asetuksen liitteessä I vahvistettujen olennaisten kyberturvallisuusvaatimusten tai niiden osien mukaisia. Lisäksi eurooppalaisen kyberturvallisuussertifikaatin myöntäminen vähintään varmuustasolla ”korotettu” tällaisten järjestelmien mukaisesti poistaa valmistajan velvoitteen teettää tämän asetuksen 32 artiklan 2 kohdan a ja b alakohdassa ja 32 artiklan 3 kohdan a ja b alakohdassa säädettyjen vaatimusten osalta vaatimustenmukaisuuden arviointi kolmannella osapuolella.

28 artikla

EU-vaatimustenmukaisuusvakuutus

1. Valmistajien on laadittava EU-vaatimustenmukaisuusvakuutus 13 artiklan 12 kohdan mukaisesti, ja siinä on mainittava, että liitteessä I vahvistettujen sovellettavien olennaisten kyberturvallisuusvaatimusten täyttyminen on osoitettu.

2. EU-vaatimustenmukaisuusvakuutuksen on oltava rakenteeltaan liitteessä V vahvistetun mallin mukainen, ja sen on sisällettävä liitteessä VIII vahvistetuissa asiaankuuluvissa vaatimustenmukaisuuden arviointimenettelyissä eritellyt tekijät. Tällaista vakuutusta on tarvittaessa päivitettävä. Se on asetettava saataville sen jäsenvaltion vaatimilla kielillä, jossa digitaalisia elementtejä sisältävä tuote saatetaan markkinoille tai asetetaan saataville markkinoilla.

Edellä 13 artiklan 20 kohdassa tarkoitetun yksinkertaistetun EU-vaatimustenmukaisuusvakuutuksen on oltava rakenteeltaan liitteessä VI vahvistetun mallin mukainen. Se on asetettava saataville sen jäsenvaltion vaatimilla kielillä, jossa digitaalisia elementtejä sisältävä tuote saatetaan markkinoille tai asetetaan saataville markkinoilla.

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

4. Laatimalla EU-vaatimustenmukaisuusvakuutuksen valmistaja ottaa vastuun digitaalisia elementtejä sisältävän tuotteen vaatimustenmukaisuudesta.

5. Siirretään komissiolle valta antaa 61 artiklan mukaisesti delegoituja säädöksiä, joilla täydennetään tätä asetusta lisäämällä teknologian kehittymisen huomioon ottamiseksi elementtejä liitteessä V vahvistetun EU-vaatimustenmukaisuusvakuutuksen vähimmäissisältöön.

29 artikla

CE-merkintää koskevat yleiset periaatteet

CE-merkintää koskevat asetuksen (EY) N:o 765/2008 30 artiklassa säädetyt yleiset periaatteet.

30 artikla

CE-merkinnän tuotteeseen kiinnittämistä tai liittämistä koskevat säännöt ja ehdot

1. CE-merkintä on kiinnitettävä 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 28 artiklassa tarkoitettuun tuotteen mukana toimitettavaan EU-vaatimustenmukaisuusvakuutukseen. Ohjelmistojen muodossa olevien digitaalisia elementtejä sisältävien tuotteiden osalta CE-merkintä on liitettävä joko 28 artiklassa tarkoitettuun EU-vaatimustenmukaisuusvakuutukseen tai esitettävä ohjelmistotuotteen verkkosivustolla. Jälkimmäisessä tapauksessa verkkosivuston asianomaisen osion on oltava helposti ja suoraan kuluttajien saatavilla.

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

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

4. CE-merkinnän yhteydessä on esitettävä ilmoitetun laitoksen tunnusnumero, jos kyseinen laitos on osallistunut 32 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 toteutettava tarkoituksenmukaiset toimet, jos tätä merkintää käytetään sääntöjenvastaisesti. Jos digitaalisia elementtejä sisältävät tuotteet kuuluvat sellaisen muun unionin yhdenmukaistamislainsäädännön kuin tämän asetuksen soveltamisalaan, jossa myös säädetään CE-merkinnän kiinnittämisestä, CE-merkinnän on osoitettava, että tuotteet täyttävät myös tällaisessa muussa unionin yhdenmukaistamislainsäädännössä vahvistetut vaatimukset.

6. Komissio voi täytäntöönpanosäädöksin vahvistaa teknisiä eritelmiä, jotka koskevat digitaalisia elementtejä sisältävien tuotteiden tietoturvaan liittyviä merkintöjä, kuvamerkkejä tai muita merkkejä, niiden tukiaikoja sekä mekanismeja, joilla edistetään niiden käyttöä ja lisätään yleistä tietoisuutta digitaalisia elementtejä sisältävien tuotteiden tietoturvasta. Laatiessaan luonnoksia täytäntöönpanosäädöksiksi komissio kuulee asiaankuuluvia sidosryhmiä ja hallinnollisen yhteistyön ryhmää, jos se on jo perustettu 52 artiklan 15 kohdan nojalla. Nämä täytäntöönpanosäädökset hyväksytään 62 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

31 artikla

Tekniset asiakirjat

1. Teknisten asiakirjojen on sisällettävä kaikki asiaankuuluvat tiedot tai yksityiskohtaiset kuvaukset keinoista, joilla valmistaja on varmistanut, että digitaalisia elementtejä sisältävä tuote ja valmistajan käyttöön ottamat prosessit täyttävät liitteessä I vahvistetut olennaiset kyberturvallisuusvaatimukset. Asiakirjojen on sisällettävä vähintään liitteessä VII vahvistetut osat.

2. Tekniset asiakirjat on laadittava ennen digitaalisia elementtejä sisältävän tuotteen saattamista markkinoille, ja niitä on tarvittaessa päivitettävä jatkuvasti vähintään tukiajan ajan.

3. Sellaisten 12 artiklassa tarkoitettujen digitaalisia elementtejä sisältävien tuotteiden osalta, joihin sovelletaan myös muita unionin säädöksiä, joissa säädetään teknisistä asiakirjoista, on laadittava kootusti tekniset asiakirjat, jotka sisältävät tämän asetuksen liitteessä VII 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 kyseisen laitoksen hyväksymällä kielellä.

5. Siirretään komissiolle valta antaa 61 artiklan mukaisesti delegoituja säädöksiä, joilla täydennetään tätä asetusta lisäämällä liitteessä VII vahvistettuihin teknisiin asiakirjoihin sisällytettäviä osia, jotta voidaan ottaa huomioon teknologian kehitys sekä tämän asetuksen täytäntöönpanoprosessissa havaittu kehitys. Tätä varten komissio pyrkii varmistamaan, että mikroyrityksille sekä pienille ja keskisuurille yrityksille aiheutuva hallinnollinen rasite on oikeasuhtainen.

32 artikla

Digitaalisia elementtejä sisältävien tuotteiden vaatimustenmukaisuuden arviointimenettelyt

1. Valmistajan on suoritettava digitaalisia elementtejä sisältävän tuotteen ja käyttöön ottamiensa prosessien vaatimustenmukaisuuden arviointi selvittääkseen, täyttävätkö ne liitteessä I vahvistetut olennaiset kyberturvallisuusvaatimukset. Valmistajan on osoitettava olennaisten kyberturvallisuusvaatimusten täyttyminen jollakin seuraavista menettelyistä:

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

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

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

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

2. Jos valmistaja arvioidessaan, täyttävätkö liitteessä III esitetyn mukainen luokkaan I kuuluva digitaalisia elementtejä sisältävä tärkeä tuote ja sen valmistajan käyttöön ottamat prosessit liitteessä I vahvistetut olennaiset kyberturvallisuusvaatimukset, ei ole käyttänyt tai on käyttänyt vain osittain 27 artiklassa tarkoitettuja yhdenmukaistettuja standardeja, yhteisiä eritelmiä tai eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä varmuustasolla ”korotettu” tai jos tällaisia yhdenmukaistettuja standardeja, yhteisiä eritelmiä tai eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä ei ole olemassa, kyseistä digitaalisia elementtejä sisältävää tuotetta ja valmistajan käyttöön ottamia prosesseja on arvioitava jommassakummassa seuraavista menettelyistä suhteessa kyseisiin olennaisiin kyberturvallisuusvaatimuksiin:

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

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

3. Jos tuote on liitteessä III esitetyn mukainen luokkaan II kuuluva digitaalisia elementtejä sisältävä tärkeä tuote, valmistajan on osoitettava, että tuote on täyttää liitteessä I vahvistetut olennaiset kyberturvallisuusvaatimukset käyttäen jotakin seuraavista menettelyistä:

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

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

c) jos saatavilla ja sovellettavissa, tämän asetuksen 27 artiklan 9 kohdan mukainen eurooppalainen kyberturvallisuuden sertifiointijärjestelmä vähintään varmuustasolla ”korotettu” asetuksen (EU) 2019/881 nojalla.

4. Liitteessä IV luetelluista digitaalisia elementtejä sisältävistä kriittisistä tuotteista on osoitettava, että ne täyttävät liitteessä I vahvistetut olennaiset kyberturvallisuusvaatimukset, käyttäen jompaakumpaa seuraavista menettelyistä:

a) 8 artiklan 1 kohdan mukainen eurooppalainen kyberturvallisuuden sertifiointijärjestelmä; tai

b) jos 8 artiklan 1 kohdassa säädetyt edellytykset eivät täyty, jokin tämän artiklan 3 kohdassa tarkoitetuista menettelyistä.

5. Sellaisten vapaiksi ja avoimen lähdekoodin ohjelmistoiksi luokiteltavien digitaalisia elementtejä sisältävien tuotteiden valmistajien, jotka kuuluvat liitteessä III vahvistettuihin ryhmiin, on voitava osoittaa, että tuotteet täyttävät liitteessä I vahvistetut olennaiset kyberturvallisuusvaatimukset, käyttäen jotakin tämän artiklan 1 kohdassa tarkoitetuista menettelyistä edellyttäen, että 31 artiklassa tarkoitetut tekniset asiakirjat ovat yleisesti saatavilla näiden tuotteiden markkinoille saattamisen ajankohtana.

6. Mikroyritysten ja pienten ja keskisuurten yritysten, mukaan lukien startup-yritykset, erityiset edut ja tarpeet on otettava huomioon vaatimustenmukaisuuden arviointimenettelyistä perittäviä maksuja vahvistettaessa ja näitä maksuja on alennettava suhteessa näiden yritysten etuihin ja tarpeisiin.

33 artikla

Tukitoimet mikroyrityksille ja
pienille ja keskisuurille yritykselle, mukaan lukien startup-yritykset

1. Jäsenvaltioiden on tarvittaessa toteutettava seuraavat mikroyritysten ja pienten yritysten tarpeisiin räätälöidyt toimet:

   a) järjestettävä erityisiä tiedotus- ja koulutustoimia tämän asetuksen soveltamisesta;

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

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

2. Jäsenvaltiot voivat tarvittaessa perustaa kyberkestävyyden sääntelyn testiympäristöjä. Tällaisissa sääntelyn testiympäristöissä on oltava innovatiivisille digitaalisia elementtejä sisältäville tuotteille valvottuja testausympäristöjä, joilla helpotetaan niiden kehittämistä, suunnittelua, validointia ja testausta tämän asetuksen noudattamiseksi, rajoitetun ajan ennen markkinoille saattamista. Komissio ja tarvittaessa ENISA voivat tarjota teknistä tukea, neuvontaa ja välineitä sääntelyn testiympäristöjen perustamista ja toimintaa varten. Sääntelyn testiympäristöt on perustettava markkinavalvontaviranomaisten suorassa valvonnassa, ohjauksessa ja niiden tuella. Jäsenvaltioiden on ilmoitettava komissiolle ja muille markkinavalvontaviranomaisille sääntelyn testiympäristön perustamisesta hallinnollisen yhteistyön ryhmän kautta. Sääntelyn testiympäristöt eivät vaikuta toimivaltaisten viranomaisten valvonta- ja korjausvaltuuksiin. Jäsenvaltioiden on varmistettava avoin, oikeudenmukainen ja läpinäkyvä pääsy sääntelyn testiympäristöihin ja erityisesti helpotettava mikroyritysten ja pienten yritysten, myös startup-yritysten, pääsyä niihin.

3. Komissio antaa 26 artiklan mukaisesti mikroyrityksille ja pienille ja keskisuurille yrityksille ohjeita, jotka koskevat tämän asetuksen täytäntöönpanoa.

4. Komissio tekee tunnetuksi unionin nykyisten ohjelmien sääntelykehyksessä saatavilla olevaa taloudellista tukea, jotta se voi erityisesti helpottaa mikroyrityksille ja pienille yrityksille aiheutuvaa taloudellista rasitetta.

5. Mikroyritykset ja pienet yritykset voivat toimittaa liitteessä VII täsmennetyt tekniset asiakirjat yksinkertaistetussa muodossa. Komissio täsmentää tätä varten täytäntöönpanosäädöksin mikroyritysten ja pienten yritysten tarpeisiin suunnattujen yksinkertaistettujen teknisten asiakirjojen muodot, mukaan lukien se, miten liitteessä VII esitetyt osat on toimitettava. Jos mikroyritys tai pieni yritys päättää toimittaa liitteessä VII vahvistetut tiedot yksinkertaistetussa muodossa, sen on käytettävä tässä kohdassa tarkoitettua muotoa. Ilmoitettujen laitosten on hyväksyttävä kyseinen muoto vaatimustenmukaisuuden arviointia varten.

   Nämä täytäntöönpanosäädökset hyväksytään 62 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

34 artikla

Vastavuoroista tunnustamista koskevat sopimukset

Ottaen huomioon kolmannen maan teknisen kehityksen tason ja vaatimustenmukaisuuden arviointia koskevan toimintamallin unioni voi tehdä vastavuoroista tunnustamista koskevia sopimuksia kolmansien maiden kanssa Euroopan unionin toiminnasta tehdyn sopimuksen 218 artiklan mukaisesti kansainvälisen kaupan edistämiseksi ja helpottamiseksi.

IV luku

Vaatimustenmukaisuuden arviointilaitosten ilmoittaminen

35 artikla

Ilmoittaminen

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

2. Jäsenvaltioiden on pyrittävä varmistamaan … päivään …kuuta … [24 kuukauden kuluttua tämän asetuksen voimaantulopäivästä] mennessä, että unionissa on riittävä määrä ilmoitettuja laitoksia vaatimustenmukaisuuden arviointien suorittamiseksi, jotta voidaan välttää pullonkaulat ja markkinoille pääsyn esteet.

36 artikla

Ilmoittamisesta vastaavat viranomaiset

1. Kunkin jäsenvaltion on nimettävä ilmoittamisesta vastaava viranomainen, jonka vastuulla on laatia ja toteuttaa tarvittavat menettelyt, jotka liittyvät vaatimustenmukaisuuden arviointilaitosten arviointiin, nimeämiseen ja ilmoittamiseen, sekä valvoa niitä, mukaan lukien sitä, että ne noudattavat 41 artiklaa.

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

3. Jos ilmoittamisesta vastaava viranomainen delegoi tai muulla tavoin antaa tehtäväksi tämän artiklan 1 kohdassa tarkoitetun arvioinnin, ilmoittamisen tai valvonnan laitokselle, joka ei ole valtiollinen yksikkö, kyseisen laitoksen on oltava oikeushenkilö ja sen on noudatettava soveltuvin osin 37 artiklaa. Lisäksi kyseisellä laitoksella on oltava käytössä järjestelyt toiminnastaan syntyvien vastuiden kattamiseksi.

4. Ilmoittamisesta vastaavan viranomaisen on otettava täysi vastuu tehtävistä, joita 3 kohdassa tarkoitettu laitos hoitaa.

37 artikla

Ilmoittamisesta vastaavia viranomaisia koskevat vaatimukset

1. Ilmoittamisesta vastaava viranomainen on perustettava siten, ettei vaatimustenmukaisuuden arviointilaitosten kanssa synny eturistiriitaa.

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

3. Ilmoittamisesta vastaavan viranomaisen on oltava organisaatioltaan sellainen, että kunkin päätöksen, joka koskee vaatimustenmukaisuuden arviointilaitoksen ilmoittamista, tekevät eri toimivaltaiset henkilöt kuin ne, jotka suorittivat arvioinnin.

4. Ilmoittamisesta vastaava viranomainen ei saa tarjota eikä suorittaa mitään toimintoja, joita vaatimustenmukaisuuden arviointilaitokset suorittavat, eikä konsultointipalveluja kaupallisin tai kilpailullisin perustein.

5. Ilmoittamisesta vastaavan viranomaisen on turvattava saamiensa tietojen luottamuksellisuus.

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

38 artikla

Ilmoittamisesta vastaavien viranomaisten tiedotusvelvollisuus

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

2. Komissio asettaa 1 kohdassa tarkoitetut tiedot julkisesti saataville.

39 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 digitaalisia elementtejä sisältävästä 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, kokoonpanemisessa, käytössä tai ylläpidossa, voidaan pitää tällaisena kolmantena osapuolena 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 suunnittelijoita, kehittäjiä, valmistajia, toimittajia, maahantuojia, jakelijoita, asentajia, ostajia, omistajia, käyttäjiä tai ylläpitäjiä eivätkä minkään tällaisen osapuolen valtuutettuja edustajia. Tämä ei sulje pois sellaisten arvioitujen tuotteiden käyttöä, jotka ovat vaatimustenmukaisuuden arviointilaitoksen toimien kannalta tarpeellisia, tai tällaisten tuotteiden käyttöä henkilökohtaisiin tarkoituksiin.

Vaatimustenmukaisuuden arviointilaitos, sen ylin johto ja vaatimustenmukaisuuden arviointitehtävien suorittamisesta vastaava henkilöstö eivät myöskään saa olla suoranaisesti mukana arvioimiensa digitaalisia elementtejä sisältävien tuotteiden suunnittelussa, kehittämisessä tai tuotannossa, tuonnissa, jakelussa, markkinoinnissa, asentamisessa, käytössä tai ylläpidossa eivätkä edustaa näissä toiminnoissa mukana olevia osapuolia. Ne eivät saa osallistua mihinkään toimintaan, joka voi olla ristiriidassa niiden suorittaman arvioinnin riippumattomuuden kanssa tai vaarantaa niiden luotettavuuden vaatimuksenmukaisuuden arviointitoimissa, joita varten ne on ilmoitettu. Tämä koskee erityisesti konsultointipalveluja.

Vaatimustenmukaisuuden arviointilaitosten on varmistettava, että niiden tytäryhtiöiden tai alihankkijoiden toimet eivät vaikuta niiden suorittamien vaatimustenmukaisuuden arviointitoimien luottamuksellisuuteen, objektiivisuuteen ja 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 arviointiin tai vaatimustenmukaisuuden arviointitoimien tuloksiin, erityisesti niiden henkilöiden tai henkilöryhmien taholta, joille näiden toimien tuloksilla on merkitystä.

6. Vaatimustenmukaisuuden arviointilaitoksen on kyettävä suorittamaan kaikki liitteessä VIII tarkoitetut vaatimustenmukaisuuden arviointitehtävät, 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 digitaalisia elementtejä sisältävien tuotteiden tyypin 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 on suoritettava, siten, että varmistetaan näiden menettelyiden avoimuus 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 yrityksen koko, toimiala ja rakenne, kyseisissä tuotteissa käytettävän teknologian monimutkaisuus sekä tuotantoprosessin massa- tai sarjatuotantoluonne otetaan asianmukaisesti huomioon.

Vaatimustenmukaisuuden arviointilaitoksella on oltava käytössään tarvittavat keinot vaatimustenmukaisuuden arviointitoimiin liittyvien teknisten ja hallinnollisten tehtävien asianmukaiseen hoitamiseen sekä pääsy kaikkiin tarvittaviin laitteisiin tai tiloihin.

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 liitteessä I vahvistetuista olennaisista kyberturvallisuusvaatimuksista, sovellettavista yhdenmukaistetuista standardeista ja yhteisistä eritelmistä sekä asiaa koskevista unionin yhdenmukaistamislainsäädännön ja täytäntöönpanosäädösten säännöksistä;

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 kyseisten arviointien tuloksista.

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

10. Vaatimustenmukaisuuden arviointilaitosten henkilöstöllä on vaitiolovelvollisuus kaikkien niiden tietojen suhteen, jotka se saa suorittaessaan tehtäviään liitteen VIII 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 noudattaminen.

11. Vaatimustenmukaisuuden arviointilaitosten on osallistuttava asiaankuuluviin standardointitoimiin ja 51 artiklan nojalla perustetun ilmoitettujen laitosten koordinointiryhmän toimiin tai varmistettava, että niiden arviointihenkilöstö saa niistä tiedon, ja sovellettava yleisinä ohjeina kyseisen ryhmän työn tuloksena laadittuja hallinnollisia päätöksiä ja asiakirjoja.

12. Vaatimustenmukaisuuden arviointilaitosten on toimittava johdonmukaisilla, oikeudenmukaisilla, oikeasuhtaisilla ja kohtuullisilla ehdoilla ja vältettävä aiheuttamasta talouden toimijoille tarpeetonta rasitetta sekä otettava erityisesti huomioon maksuihin liittyvät mikroyritysten sekä pienten ja keskisuurten yritysten edut.

40 artikla

Ilmoitettujen laitosten vaatimustenmukaisuusolettama

Jos vaatimustenmukaisuuden arviointilaitos voi osoittaa olevansa sellaisissa olennaisissa yhdenmukaistetuissa standardeissa tai niiden osissa vahvistettujen edellytysten mukainen, joiden viitetiedot on julkaistu *Euroopan unionin virallisessa lehdessä*, sen oletetaan täyttävän 39 artiklassa säädetyt vaatimukset siltä osin kuin sovellettavat yhdenmukaistetut standardit kattavat nämä vaatimukset.

41 artikla

Ilmoitettujen laitosten tytäryhtiöt ja alihankinta

1. Jos ilmoitettu laitos teettää yksittäisiä vaatimustenmukaisuuden arviointiin liittyviä tehtäviä alihankintana tai käyttää tytäryhtiötä, sen on varmistettava, että alihankkija tai tytäryhtiö täyttää 39 artiklassa säädetyt vaatimukset, ja ilmoitettava asiasta ilmoittamisesta vastaavalle 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 ilmoittamisesta vastaavan viranomaisen saatavilla asiakirjat, jotka koskevat alihankkijan tai tytäryhtiön pätevyyden arviointia sekä työtä, jota nämä suorittavat tämän asetuksen nojalla.

42 artikla

Ilmoittamista koskeva hakemus

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

2. Hakemukseen on liitettävä kuvaus vaatimustenmukaisuuden arviointitoimista, vaatimustenmukaisuuden arviointimenettelystä tai -menettelyistä ja yhdestä tai useammasta digitaalisia elementtejä sisältävästä tuotteesta, jonka osalta laitos katsoo olevansa pätevä, sekä tapauksen mukaan akkreditointitodistus, jonka kansallinen akkreditointielin on antanut ja jossa todistetaan, että vaatimustenmukaisuuden arviointilaitos täyttää 39 artiklassa säädetyt vaatimukset.

3. Jos asianomainen vaatimustenmukaisuuden arviointilaitos ei voi toimittaa akkreditointitodistusta, sen on toimitettava ilmoittamisesta vastaavalle viranomaiselle kaikki tarpeelliset asiakirjatodisteet, joiden avulla voidaan varmentaa, todeta ja säännöllisesti valvoa, että se täyttää 39 artiklassa säädetyt vaatimukset.

43 artikla

Ilmoitusmenettely

1. Ilmoittamisesta vastaavien viranomaisten on ilmoitettava ainoastaan sellaiset vaatimustenmukaisuuden arviointilaitokset, jotka ovat täyttäneet 39 artiklassa säädetyt vaatimukset.

2. Ilmoittamisesta vastaavan viranomaisen on ilmoitettava asiasta komissiolle ja muille jäsenvaltioille käyttäen komission kehittämää ja hallinnoimaa uuden lähestymistavan mukaista ilmoitettujen ja nimettyjen organisaatioiden tietojärjestelmää.

3. Ilmoituksessa on oltava tarkat tiedot vaatimustenmukaisuuden arviointitoimista, vaatimustenmukaisuuden arviointimoduulista tai -moduuleista sekä kyseessä olevasta yhdestä tai useammasta digitaalisia elementtejä sisältävästä tuotteesta sekä asiaankuuluva todistus pätevyydestä.

4. Jos ilmoitus ei perustu 42 artiklan 2 kohdassa tarkoitettuun akkreditointitodistukseen, ilmoittamisesta vastaavan viranomaisen on toimitettava komissiolle ja muille jäsenvaltioille asiakirjatodisteet, joiden avulla voidaan todistaa vaatimustenmukaisuuden arviointilaitoksen pätevyys ja käytössä olevat järjestelyt, joilla varmistetaan, että laitosta valvotaan säännöllisesti ja että se täyttää edelleen 39 artiklassa säädetyt vaatimukset.

5. Asianomainen laitos voi suorittaa ilmoitetun laitoksen tehtäviä ainoastaan, jos komissio ja muut jäsenvaltiot eivät esitä vastalauseita kahden viikon kuluessa ilmoittamisesta siinä tapauksessa, että käytetään akkreditointitodistusta, tai kahden kuukauden kuluessa ilmoittamisesta siinä tapauksessa, että akkreditointia ei käytetä.

   Ainoastaan tällaista laitosta on pidettävä tässä asetuksessa tarkoitettuna ilmoitettuna laitoksena.

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

44 artikla

Ilmoitettujen laitosten tunnusnumerot ja luettelot

1. Komissio antaa ilmoitetulle laitokselle tunnusnumeron.

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

2. Komissio asettaa yleisesti saataville tämän asetuksen nojalla ilmoitettujen laitosten luettelon, joka sisältää laitoksille annetut tunnusnumerot ja toimet, joita varten ne on ilmoitettu.

   Komissio huolehtii luettelon pitämisestä ajan tasalla.

45 artikla

Muutokset ilmoituksiin

1. Jos ilmoittamisesta vastaava viranomainen on todennut tai saanut tietää, ettei ilmoitettu laitos enää täytä 39 artiklassa säädettyjä vaatimuksia tai ettei se noudata velvollisuuksiaan, ilmoittamisesta vastaavan viranomaisen on tarpeen mukaan rajoitettava ilmoitusta taikka peruutettava se toistaiseksi tai kokonaan sen mukaan, miten vakavaa vaatimusten täyttämättä jättäminen tai velvollisuuksien noudattamatta jättäminen on ollut. 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, ilmoituksen tehneen jäsenvaltion on toteutettava asianmukaiset toimenpiteet varmistaakseen, että kyseisen laitoksen asiakirja-aineistot joko käsittelee toinen ilmoitettu laitos tai ne ovat asianomaisten ilmoittamisesta vastaavien viranomaisten ja markkinavalvontaviranomaisten saatavilla näiden pyynnöstä.

46 artikla

Ilmoitettujen laitosten pätevyyden riitauttaminen

1. Komissio tutkii kaikki tapaukset, joissa sillä on tai sen tietoon saatetaan epäilyksiä, jotka koskevat ilmoitetun laitoksen pätevyyttä tai sitä, onko se täyttänyt tai täyttääkö se edelleen sille asetetut 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 ole täyttänyt tai ei enää täytä sen ilmoittamiselle asetettuja vaatimuksia, se ilmoittaa asiasta ilmoituksen tehneelle jäsenvaltiolle ja pyytää sitä toteuttamaan tarvittavat korjaavat toimenpiteet, mukaan lukien ilmoituksen peruuttaminen tarvittaessa.

47 artikla

Ilmoitettujen laitosten toimintaan liittyvät velvollisuudet

1. Ilmoitettujen laitosten on suoritettava vaatimustenmukaisuuden arvioinnit 32 artiklassa ja liitteessä VIII säädettyjen vaatimustenmukaisuuden arviointimenettelyjen mukaisesti.

2. Vaatimustenmukaisuuden arvioinnit on suoritettava oikeasuhtaisesti siten, ettei talouden toimijoille aiheuteta tarpeetonta rasitetta. Vaatimustenmukaisuuden arviointilaitosten on tehtäviään hoitaessaan otettava asianmukaisesti huomioon yrityksen koko, erityisesti mikroyritysten sekä pienten ja keskisuurten yritysten osalta, toimiala ja rakenne, kyseisten digitaalisia elementtejä sisältävien tuotteiden ja käytettävän teknologian monimutkaisuus ja kyberturvallisuusriskien taso sekä tuotantoprosessin massa- tai sarjatuotantoluonne.

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

4. Jos ilmoitettu laitos katsoo, että valmistaja ei ole täyttänyt vaatimuksia, jotka vahvistetaan liitteessä I tai vastaavissa yhdenmukaistetuissa standardeissa tai 27 artiklassa tarkoitetuissa yhteisissä eritelmissä, sen on vaadittava valmistajaa toteuttamaan asianmukaiset korjaavat toimenpiteet eikä se saa antaa vaatimustenmukaisuustodistusta.

5. Jos ilmoitettu laitos katsoo todistuksen antamisen jälkeen suoritettavan vaatimustenmukaisuuden valvonnan yhteydessä, ettei digitaalisia elementtejä sisältävä tuote enää täytä tässä asetuksessa säädettyjä vaatimuksia, sen on vaadittava valmistajaa toteuttamaan asianmukaiset korjaavat toimenpiteet 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.

48 artikla

Muutoksenhaku ilmoitettujen laitosten päätöksiin

Jäsenvaltioiden on varmistettava, että käytettävissä on menettely muutoksen hakemiseksi ilmoitettujen laitosten päätöksiin.

49 artikla

Ilmoitettujen laitosten tiedotusvelvollisuus

1. Ilmoitettujen laitosten on tiedotettava ilmoittamisesta vastaavalle viranomaiselle seuraavista:

   a) todistusten epäämiset, rajoittamiset taikka peruuttamiset toistaiseksi 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 soveltamisalalla, ja mahdollisesti suoritetut muut toimet, mukaan lukien rajat ylittävä toiminta ja alihankinta.

2. Ilmoitettujen laitosten on toimitettava muille tämän asetuksen nojalla ilmoitetuille laitoksille, jotka suorittavat samat digitaalisia elementtejä sisältävät tuotteet kattavia samanlaisia vaatimustenmukaisuuden arviointitoimia, asiaankuuluvat tiedot kysymyksistä, jotka liittyvät vaatimustenmukaisuuden arvioinnin kielteisiin tuloksiin ja pyynnöstä myös myönteisiin tuloksiin.

50 artikla

Kokemusten vaihto

Komissio huolehtii kokemusten vaihdon järjestämisestä ilmoittamista koskevista toimintalinjoista vastaavien jäsenvaltioiden kansallisten viranomaisten välillä.

51 artikla

Ilmoitettujen laitosten koordinointi

1. Komissio varmistaa, että ilmoitettujen laitosten välillä otetaan käyttöön asianmukainen koordinointi ja yhteistyö ja että näitä harjoitetaan asianmukaisella tavalla 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

52 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 tehokkaan täytäntöönpanon varmistamiseksi. Jäsenvaltiot voivat nimetä tätä asetusta varten markkinavalvontaviranomaiseksi jo olemassa olevan tai uuden viranomaisen.

3. Tämän artiklan 2 kohdan mukaisesti nimetyt markkinavalvontaviranomaiset vastaavat myös markkinavalvontatoimista, jotka liittyvät 24 artiklassa säädettyihin avoimen lähdekoodin ohjelmistovastaavien velvollisuuksiin. Jos markkinavalvontaviranomainen toteaa, että avoimen lähdekoodin ohjelmistovastaava ei noudata mainitussa artiklassa säädettyjä velvollisuuksia, sen on vaadittava avoimen lähdekoodin ohjelmistovastaavaa varmistamaan, että kaikki asianmukaiset korjaavat toimenpiteet toteutetaan. Avoimen lähdekoodin ohjelmistovastaavien on varmistettava, että kaikki asianmukaiset korjaavat toimenpiteet toteutetaan niiden tämän asetuksen mukaisten velvollisuuksien noudattamiseksi.

4. Markkinavalvontaviranomaisten on tarvittaessa tehtävä yhteistyötä asetuksen (EU) 2019/881 58 artiklan nojalla nimettyjen kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten kanssa ja vaihdettava säännöllisesti niiden kanssa tietoja. Tämän asetuksen 14 artiklan mukaisten raportointivelvoitteiden noudattamisen valvonnan osalta nimettyjen markkinavalvontaviranomaisten on tehtävä yhteistyötä ja vaihdettava säännöllisesti tietoja koordinaattoreiksi nimettyjen CSIRT-yksiköiden ja ENISAn kanssa.

5. Markkinavalvontaviranomaiset voivat pyytää koordinaattoriksi nimettyä CSIRT-yksikköä tai ENISAa antamaan teknistä neuvontaa asioissa, jotka liittyvät tämän asetuksen täytäntöönpanoon ja sen noudattamisen valvontaan. Markkinavalvontaviranomaiset voivat 54 artiklan mukaista tutkimusta suorittaessaan pyytää koordinaattoriksi nimettyä CSIRT-yksikköä tai ENISAa esittämään analyysin digitaalisia elementtejä sisältävien tuotteiden vaatimustenmukaisuuden arviointien tueksi.

6. Markkinavalvontaviranomaisten on tarvittaessa tehtävä yhteistyötä muiden markkinavalvontaviranomaisten kanssa, jotka on nimetty muun unionin yhdenmukaistamislainsäädännön kuin tämän asetuksen perusteella, ja vaihdettava säännöllisesti niiden kanssa tietoja.

7. Markkinavalvontaviranomaisten on tarvittaessa tehtävä yhteistyötä unionin tietosuojalainsäädäntöä valvovien viranomaisten kanssa. Tällaiseen yhteistyöhön sisältyy tiedottaminen kyseisille viranomaisille niiden toimivaltuuksien käytön kannalta merkityksellisistä havainnoista, myös silloin, kun annetaan ohjeita ja neuvoja 10 kohdan mukaisesti, jos ohjeet 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 hoitamiseksi. Niiden on ilmoitettava tällaisesta pyynnöstä asianomaisen jäsenvaltion nimetyille markkinavalvontaviranomaisille.

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

9. Komissio kannustaa kokemusten vaihtoon nimettyjen markkinavalvontaviranomaisten välillä ja helpottaa tätä vaihtoa.

10. Markkinavalvontaviranomaiset voivat komission sekä tarvittaessa CSIRT-yksiköiden ja ENISAn tuella antaa talouden toimijoille ohjeita ja neuvoja tämän asetuksen täytäntöönpanosta.

11. Markkinavalvontaviranomaisten on ilmoitettava kuluttajille, mitä kautta he voivat tehdä valituksia, jotka saattavat viitata tämän asetuksen vaatimusten vastaisuuteen, asetuksen (EU) 2019/1020 11 artiklan mukaisesti, ja annettava kuluttajille tietoa siitä, mistä löytää ja miten käyttää mekanismeja, joilla helpotetaan sellaisista haavoittuvuuksista, poikkeamista ja kyberuhkista ilmoittamista, jotka voivat vaikuttaa digitaalisia elementtejä sisältäviin tuotteisiin.

12. Markkinavalvontaviranomaisten on tarvittaessa helpotettava yhteistyötä asiaankuuluvien sidosryhmien, myös tiede-, tutkimus- ja kuluttajajärjestöjen, kanssa.

13. 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 kilpailulainsäädännön soveltamisen kannalta.

14. Kun on kyse tämän asetuksen soveltamisalaan kuuluvista digitaalisia elementtejä sisältävistä tuotteista, jotka luokitellaan suuririskisiksi tekoälyjärjestelmiksi asetuksen (EU) 2024/1689 6 artiklan nojalla, asetusta (EU) 2024/1689 varten nimetyt markkinavalvontaviranomaiset vastaavat myös tämän asetuksen nojalla vaadituista markkinavalvontatoimista. Asetuksen (EU) 2024/1689 nojalla nimettyjen markkinavalvontaviranomaisten on tarvittaessa tehtävä yhteistyötä tämän asetuksen nojalla nimettyjen markkinavalvontaviranomaisten kanssa ja tämän asetuksen 14 artiklan mukaisten raportointivelvoitteiden noudattamisen valvonnan osalta koordinaattoreiksi nimettyjen CSIRT-yksiköiden ja ENISAn kanssa. Asetuksen (EU) 2024/1689 nojalla nimettyjen markkinavalvontaviranomaisten on erityisesti ilmoitettava tämän asetuksen nojalla nimetyille markkinavalvontaviranomaisille kaikista havainnoista, joilla on merkitystä niiden tämän asetuksen täytäntöönpanoon liittyvien tehtävien hoitamisen kannalta.

15. Tämän asetuksen yhdenmukaista soveltamista varten perustetaan hallinnollisen yhteistyön ryhmä asetuksen (EU) 2019/1020 30 artiklan 2 kohdan nojalla. Hallinnollisen yhteistyön ryhmä koostuu nimettyjen markkinavalvontaviranomaisten edustajista ja tarvittaessa yhteyspisteiden edustajista. Hallinnollisen yhteistyön ryhmä käsittelee myös markkinavalvontatoimiin liittyviä erityiskysymyksiä, jotka koskevat avoimen lähdekoodin ohjelmistovastaaville asetettuja velvollisuuksia.

16. Markkinavalvontaviranomaisten on seurattava, miten valmistajat ovat soveltaneet 13 artiklan 8 kohdassa tarkoitettuja kriteerejä määrittäessään digitaalisia elementtejä sisältävien tuotteidensa tukiaikaa.

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

Jos tiedot viittaavat siihen, että tukiaika on tietyissä digitaalisia elementtejä sisältävien tuotteiden ryhmissä riittämätön, hallinnollisen yhteistyön ryhmä voi antaa markkinavalvontaviranomaisille suosituksia, että ne keskittyisivät toiminnassaan tällaisiin digitaalisia elementtejä sisältävien tuotteiden ryhmiin.

53 artikla

Tietojen ja dokumentaation saatavuus

Jos se on tarpeen sen arvioimiseksi, täyttävätkö digitaalisia elementtejä sisältävät tuotteet ja niiden valmistajien käyttöön ottamat prosessit liitteessä I vahvistetut olennaiset kyberturvallisuusvaatimukset, markkinavalvontaviranomaisille on myönnettävä perustellusta pyynnöstä pääsy niiden helposti ymmärtämällä kielellä tietoihin, joita tarvitaan tällaisten tuotteiden suunnittelun, kehittämisen, tuotannon ja haavoittuvuuksien käsittelyn arvioimiseksi, mukaan lukien asiaankuuluvan talouden toimijan asiaan liittyvä sisäinen dokumentaatio.

54 artikla

Kansallisen tason menettely digitaalisia elementtejä sisältäviä merkittävän kyberturvallisuusriskin aiheuttavia tuotteita varten

1. Jos jäsenvaltion markkinavalvontaviranomaisella on riittävä peruste katsoa, että digitaalisia elementtejä sisältävä tuote, mukaan lukien sen haavoittuvuuksien käsittely, aiheuttaa merkittävän kyberturvallisuusriskin, sen on arvioitava ilman aiheetonta viivytystä ja tarvittaessa yhteistyössä asiaankuuluvan CSIRT-yksikön kanssa, täyttääkö kyseinen digitaalisia elementtejä sisältävä tuote kaikki tässä asetuksessa säädetyt vaatimukset. Asiaankuuluvien talouden toimijoiden on tehtävä tarpeen mukaan yhteistyötä markkinavalvontaviranomaisen kanssa.

Jos markkinavalvontaviranomainen havaitsee arvioinnin yhteydessä, että digitaalisia elementtejä sisältävä tuote ei täytä tässä asetuksessa säädettyjä vaatimuksia, sen on vaadittava viipymättä asiaankuuluvaa talouden toimijaa toteuttamaan kaikki tarvittavat korjaavat toimenpiteet digitaalisia elementtejä sisältävän tuotteen saattamiseksi vastaamaan kyseisiä vaatimuksia tai sen poistamiseksi markkinoilta tai sitä koskevan palautusmenettelyn järjestämiseksi markkinavalvontaviranomaisen määrittämän sellaisen kohtuullisen ajanjakson kuluessa, joka on oikeassa suhteessa kyberturvallisuusriskin luonteeseen.

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

2. Kun markkinavalvontaviranomaiset määrittävät tämän artiklan 1 kohdassa tarkoitetun kyberturvallisuusriskin merkittävyyttä, niiden on otettava huomioon myös muut kuin tekniset riskitekijät, erityisesti ne, jotka on vahvistettu direktiivin (EU) 2022/2555 22 artiklan mukaisesti tehtyjen kriittisiä toimitusketjuja koskevien unionin tason koordinoitujen turvallisuusriskinarviointien tuloksena. Jos markkinavalvontaviranomaisella on riittävä peruste katsoa, että digitaalisia elementtejä sisältävä tuote aiheuttaa merkittävän kyberturvallisuusriskin muiden kuin teknisten riskitekijöiden vuoksi, sen on ilmoitettava tästä direktiivin (EU) 2022/2555 8 artiklan nojalla nimetyille tai perustetuille toimivaltaisille viranomaisille sekä tehtävä tarpeen mukaan yhteistyötä kyseisten viranomaisten kanssa.

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

4. Talouden toimijan on varmistettava, että kaikki asianmukaiset korjaavat toimenpiteet toteutetaan kaikkien niiden digitaalisia elementtejä sisältävien tuotteiden osalta, jotka se on asettanut saataville markkinoilla unionin alueella.

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

   Markkinavalvontaviranomaisen on viipymättä ilmoitettava komissiolle ja muille jäsenvaltioille näistä toimenpiteistä.

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

   a) digitaalisia elementtejä sisältävät tuotteet tai valmistajan käyttöön ottamat prosessit eivät täytä liitteessä I vahvistettuja olennaisia kyberturvallisuusvaatimuksia;

   b) yhdenmukaistetuissa standardeissa, eurooppalaisissa kyberturvallisuuden sertifiointijärjestelmissä tai 27 artiklassa tarkoitetuissa yhteisissä eritelmissä on puutteita.

7. 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 kyseisen digitaalisia elementtejä sisältävän tuotteen vaatimustenvastaisuuteen, sekä vastalauseensa siinä tapauksessa, että ilmoitetusta kansallisesta toimenpiteestä on erimielisyyttä.

8. Jos mikään jäsenvaltio tai komissio ei ole kolmen kuukauden kuluessa tämän artiklan 5 kohdassa tarkoitetun ilmoituksen vastaanottamisesta esittänyt vastalausetta jonkin jäsenvaltion toteuttaman väliaikaisen toimenpiteen johdosta, toimenpiteen katsotaan olevan oikeutettu. Tämä ei rajoita asianomaisen talouden toimijan asetuksen (EU) 2019/1020 18 artiklan mukaisia menettelyllisiä oikeuksia.

9. Kaikkien jäsenvaltioiden markkinavalvontaviranomaisten on varmistettava, että kyseistä digitaalisia elementtejä sisältävää tuotetta koskevat asianmukaiset rajoittavat toimenpiteet, kuten kyseisen tuotteen poistaminen markkinoilta, toteutetaan viipymättä.

55 artikla

Unionin suojamenettely

1. Jos kolmen kuukauden kuluessa 54 artiklan 5 kohdassa tarkoitetun ilmoituksen vastaanottamisesta jokin jäsenvaltio esittää vastalauseen toisen jäsenvaltion toteuttaman toimenpiteen johdosta tai jos komissio pitää toimenpidettä unionin oikeuden vastaisena, komissio ryhtyy viipymättä kuulemaan asianomaista jäsenvaltiota ja asianomaista talouden toimijaa tai asianomaisia talouden toimijoita ja arvioi kansallisen toimenpiteen. Tämän arvioinnin tulosten perusteella komissio päättää, onko kansallinen toimenpide oikeutettu vai ei, yhdeksän kuukauden kuluessa 54 artiklan 5 kohdassa tarkoitetusta ilmoituksesta ja antaa kyseisen päätöksen tiedoksi asianomaiselle jäsenvaltiolle.

2. Jos kansallisen toimenpiteen katsotaan olevan oikeutettu, kaikkien jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että vaatimustenvastainen digitaalisia elementtejä sisältävä tuote poistetaan niiden markkinoilta, ja niiden on ilmoitettava asiasta komissiolle. Jos kansallisen toimenpiteen ei katsota olevan oikeutettu, asianomaisen jäsenvaltion on peruutettava toimenpide.

3. Jos kansallisen toimenpiteen katsotaan olevan oikeutettu ja digitaalisia elementtejä sisältävän tuotteen vaatimustenvastaisuuden katsotaan johtuvan puutteista yhdenmukaistetuissa standardeissa, komissio soveltaa asetuksen (EU) N:o 1025/2012 11 artiklassa säädettyä menettelyä.

4. Jos kansallisen toimenpiteen katsotaan olevan oikeutettu ja digitaalisia elementtejä sisältävän tuotteen vaatimustenvastaisuuden katsotaan johtuvan puutteista 27 artiklassa tarkoitetussa eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä, komissio harkitsee, muutetaanko tai kumotaanko 27 artiklan 9 kohdan nojalla annettu delegoitu säädös, jossa vahvistetaan kyseistä sertifiointijärjestelmää koskeva vaatimustenmukaisuusolettama.

5. Jos kansallisen toimenpiteen katsotaan olevan oikeutettu ja digitaalisia elementtejä sisältävän tuotteen vaatimustenvastaisuuden katsotaan johtuvan puutteista 27 artiklassa tarkoitetuissa yhteisissä eritelmissä, komissio harkitsee, muutetaanko tai kumotaanko 27 artiklan 2 kohdan nojalla annettu täytäntöönpanosäädös, jossa vahvistetaan kyseiset yhteiset eritelmät.

56 artikla

Unionin tason menettely digitaalisia elementtejä sisältäviä merkittävän kyberturvallisuusriskin aiheuttavia tuotteita varten

1. Jos komissiolla on riittävä peruste katsoa, myös ENISAn toimittamien tietojen perusteella, että merkittävän kyberturvallisuusriskin aiheuttava digitaalisia elementtejä sisältävä tuote ei täytä tässä asetuksessa säädettyjä vaatimuksia, se ilmoittaa tästä asiaankuuluville markkinavalvontaviranomaisille. Jos markkinavalvontaviranomaiset suorittavat arvioinnin siitä, täyttääkö kyseinen digitaalisia elementtejä sisältävä tuote, joka voi aiheuttaa merkittävän kyberturvallisuusriskin, tässä asetuksessa säädetyt vaatimukset, sovelletaan 54 ja 55 artiklassa tarkoitettuja menettelyjä.

2. Jos komissiolla on riittävä peruste katsoa, että digitaalisia elementtejä sisältävä tuote aiheuttaa merkittävän kyberturvallisuusriskin muiden kuin teknisten riskitekijöiden vuoksi, se ilmoittaa tästä asiaankuuluville markkinavalvontaviranomaisille ja tarvittaessa direktiivin (EU) 2022/2555 8 artiklan nojalla nimetyille tai perustetuille toimivaltaisille viranomaisille ja tekee tarpeen mukaan yhteistyötä kyseisten viranomaisten kanssa. Komissio tarkastelee myös kyseiseen digitaalisia elementtejä sisältävään tuotteeseen liittyvien tunnistettujen riskien merkityksellisyyttä osana tehtäviään, jotka liittyvät direktiivin (EU) 2022/2555 22 artiklassa säädettyihin kriittisten toimitusketjujen unionin tason koordinoituihin turvallisuusriskinarviointeihin, ja kuulee tarvittaessa direktiivin (EU) 2022/2555 14 artiklan nojalla perustettua yhteistyöryhmää ja ENISAa.

3. Olosuhteissa, joissa on perusteltua toteuttaa välittömiä toimia sisämarkkinoiden moitteettoman toiminnan säilyttämiseksi, ja jos komissiolla on riittävä peruste katsoa, että 1 kohdassa tarkoitettu digitaalisia elementtejä sisältävä tuote ei edelleenkään täytä tässä asetuksessa säädettyjä vaatimuksia, eivätkä asiaankuuluvat markkinavalvontaviranomaiset ole toteuttaneet tuloksellisia toimenpiteitä, komissio suorittaa vaatimustenmukaisuuden arvioinnin ja voi pyytää ENISAa esittämään analyysin sen tueksi. Komissio ilmoittaa asiasta asiaankuuluville markkinavalvontaviranomaisille. Asiaankuuluvien talouden toimijoiden on tehtävä tarpeen mukaan yhteistyötä ENISAn kanssa.

4. Edellä 3 kohdassa tarkoitetun arvioinnin perusteella komissio voi päättää, että unionin tasolla tarvitaan korjaava tai rajoittava toimenpide. Tätä varten se kuulee viipymättä asianomaisia jäsenvaltioita ja asiaankuuluvaa talouden toimijaa tai asiaankuuluvia talouden toimijoita.

5. Tämän artiklan 4 kohdassa tarkoitetun kuulemisen perusteella komissio voi antaa täytäntöönpanosäädöksiä, joissa säädetään unionin tason korjaavista tai rajoittavista toimenpiteistä, joihin voi sisältyä vaatimus asianomaisia digitaalisia elementtejä sisältävien tuotteiden poistamisesta markkinoilta tai niitä koskevan palautusmenettelyn järjestämisestä sellaisen kohtuullisen ajan kuluessa, joka on oikeassa suhteessa riskin luonteeseen. Nämä täytäntöönpanosäädökset hyväksytään 62 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

6. Komissio antaa 5 kohdassa tarkoitetut täytäntöönpanosäädökset viipymättä tiedoksi asiaankuuluvalle talouden toimijalle tai asiaankuuluville talouden toimijoille. Jäsenvaltioiden on pantava nämä täytäntöönpanosäädökset täytäntöön viipymättä ja ilmoitettava tästä komissiolle.

7. Edellä olevia 3–6 kohtaa sovelletaan komission toimenpiteen perusteena olleen poikkeuksellisen tilanteen keston ajan, mikäli kyseistä digitaalisia elementtejä sisältävää tuotetta ei ole saatettu tämän asetuksen mukaiseksi.

57 artikla

Vaatimustenmukaiset digitaalisia elementtejä sisältävät tuotteet, jotka aiheuttavat merkittävän kyberturvallisuusriskin

1. Jäsenvaltion markkinavalvontaviranomaisen on vaadittava talouden toimijaa toteuttamaan kaikki asianmukaiset toimenpiteet, jos se 54 artiklan mukaisen arvioinnin suoritettuaan toteaa, että vaikka digitaalisia elementtejä sisältävä tuote ja valmistajan käyttöön ottamat prosessit täyttävät tämän asetuksen vaatimukset, tuote aiheuttaa merkittävän kyberturvallisuusriskin sekä riskin

   a) ihmisten terveydelle tai turvallisuudelle;

   b) perusoikeuksien suojaamiseen tarkoitettujen unionin oikeuden tai kansallisen lainsäädännön mukaisten velvoitteiden noudattamiselle;

c) direktiivin (EU) 2022/2555 3 artiklan 1 kohdassa tarkoitettujen keskeisten toimijoiden sähköisen tietojärjestelmän avulla tarjoamien palvelujen saatavuudelle, aitoudelle, eheydelle tai luottamuksellisuudelle; tai

d) muille yleisen edun suojaamiseen liittyville näkökohdille.

Ensimmäisessä alakohdassa tarkoitettuihin toimenpiteisiin voi sisältyä toimenpiteitä, joilla varmistetaan, että kyseinen digitaalisia elementtejä sisältävä tuote ja valmistajan käyttöön ottamat prosessit eivät enää aiheuta kyseisiä riskejä, kun ne asetetaan saataville markkinoilla, tai varmistetaan kyseisen digitaalisia elementtejä sisältävän tuotteen poistaminen markkinoilta tai sitä koskevan palautusmenettelyn järjestäminen, ja näiden toimenpiteiden on oltava oikeassa suhteessa kyseisten riskien luonteeseen.

2. Valmistajan tai muiden asiaankuuluvien talouden toimijoiden on varmistettava, että korjaavat toimenpiteet toteutetaan niiden 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 ja erityisesti tiedot, jotka ovat tarpeen kyseisten 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 asiaankuuluvaa talouden toimijaa ja arvioi toteutetut kansalliset toimenpiteet. Tämän arvioinnin tulosten perusteella komissio päättää, onko toimenpide oikeutettu vai ei, ja ehdottaa tarvittaessa soveltuvia toimenpiteitä.

5. Komissio osoittaa 4 kohdassa tarkoitetun päätöksen jäsenvaltioille.

6. Jos komissiolla on riittävä peruste katsoa, myös ENISAn toimittamien tietojen perusteella, että vaikka digitaalisia elementtejä sisältävä tuote täyttää tämän asetuksen vaatimukset, se aiheuttaa tämän artiklan 1 kohdassa tarkoitettuja riskejä, komissio ilmoittaa tästä asiaankuuluvalle markkinavalvontaviranomaiselle tai asiaankuuluville markkinavalvontaviranomaisille ja voi pyytää sitä tai niitä suorittamaan arvioinnin ja noudattamaan 54 artiklassa ja tämän artiklan 1, 2 ja 3 kohdassa tarkoitettuja menettelyjä.

7. Olosuhteissa, joissa on perusteltua toteuttaa välittömiä toimia sisämarkkinoiden moitteettoman toiminnan säilyttämiseksi, ja jos komissiolla on riittävä peruste katsoa, että 6 kohdassa tarkoitettu digitaalisia elementtejä sisältävä tuote aiheuttaa edelleen 1 kohdassa tarkoitettuja riskejä, eivätkä asiaankuuluvat kansalliset markkinavalvontaviranomaiset ole toteuttaneet tuloksellisia toimenpiteitä, komissio arvioi kyseisen digitaalisia elementtejä sisältävän tuotteen aiheuttamat riskit ja voi pyytää ENISAa esittämään analyysin kyseisen arvioinnin tueksi sekä ilmoittaa tästä asiaankuuluville markkinavalvontaviranomaisille. Asiaankuuluvin talouden toimijoiden on tehtävä tarpeen mukaan yhteistyötä ENISAn kanssa.

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

9. Tämän artiklan 8 kohdassa tarkoitetun kuulemisen perusteella komissio voi antaa täytäntöönpanosäädöksiä päättääkseen unionin tason korjaavista tai rajoittavista toimenpiteistä, joihin voi sisältyä vaatimus asianomaisia digitaalisia elementtejä sisältävien tuotteiden poistamisesta markkinoilta tai niitä koskevan palautusmenettelyn järjestämisestä sellaisen kohtuullisen ajan kuluessa, joka on oikeassa suhteessa riskin luonteeseen. Nämä täytäntöönpanosäädökset hyväksytään 62 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

10. Komissio antaa 9 kohdassa tarkoitetut täytäntöönpanosäädökset viipymättä tiedoksi asiaankuuluvalle talouden toimijalle tai asiaankuuluville talouden toimijoille. Jäsenvaltioiden on pantava nämä täytäntöönpanosäädökset täytäntöön viipymättä ja ilmoitettava tästä komissiolle.

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

58 artikla

Muodollinen vaatimustenvastaisuus

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

a) CE-merkintä on kiinnitetty 29 ja 30 artiklan vastaisesti;

b) CE-merkintää ei ole kiinnitetty;

c) EU-vaatimustenmukaisuusvakuutusta ei ole laadittu;

d) EU-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 puutteellisia.

2. Jos 1 kohdassa tarkoitettu vaatimustenvastaisuus jatkuu, asianomaisen jäsenvaltion on toteutettava kaikki tarvittavat toimenpiteet, joilla rajoitetaan kyseisen digitaalisia elementtejä sisältävän tuotteen asettamista saataville markkinoilla tai kielletään se tai joilla varmistetaan tuotetta koskevan palautusmenettelyn järjestäminen tai sen poistaminen markkinoilta.

59 artikla

Markkinavalvontaviranomaisten yhteistoimet

1. Markkinavalvontaviranomaiset voivat sopia muiden asiaankuuluvien viranomaisten kanssa sellaisten yhteistoimien suorittamisesta, joiden tarkoituksena on varmistaa kyberturvallisuus ja kuluttajien suojelu tiettyjen markkinoille saatettujen tai markkinoilla saataville asetettujen digitaalisia elementtejä sisältävien tuotteiden osalta, erityisesti sellaisten digitaalisia elementtejä sisältävien tuotteiden osalta, joiden havaitaan usein aiheuttavan kyberturvallisuusriskejä.

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

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

4. Markkinavalvontaviranomainen voi käyttää yhteistoimien tuloksena saatuja tietoja missä tahansa tutkimuksissaan.

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

60 artikla

Tehotarkastukset

1. Markkinavalvontaviranomaisten on suoritettava tiettyjen digitaalisia elementtejä sisältävien tuotteiden tai tuoteryhmien samanaikaisia koordinoituja valvontatoimia, jäljempänä ’tehotarkastukset’, joiden tarkoituksena on tarkistaa tämän asetuksen noudattaminen ja havaita sen rikkomiset. Tehotarkastuksiin voi kuulua valehenkilöllisyyden turvin hankittujen digitaalisia elementtejä sisältävien tuotteiden tarkastuksia.

2. Tehotarkastuksia koordinoi komissio, paitsi jos asianomaisten markkinavalvontaviranomaisten kesken on sovittu toisin. Tehotarkastuksen koordinoijan on tarvittaessa asetettava aggregoidut tulokset yleisesti saataville.

3. Jos ENISA yksilöi tehtäviään suorittaessaan, myös 14 artiklan 1 ja 3 kohdan nojalla vastaanotettujen ilmoitusten perusteella, digitaalisia elementtejä sisältävien tuotteiden ryhmiä, joille voidaan järjestää tehotarkastuksia, se toimittaa tämän artiklan 2 kohdassa tarkoitetulle koordinoijalle tehotarkastusta koskevan ehdotuksen markkinavalvontaviranomaisten tarkasteltavaksi.

4. Markkinavalvontaviranomaiset voivat tehotarkastuksia suorittaessaan käyttää 52–58 artiklassa vahvistettuja tutkintavaltuuksia ja kaikkia muita niille kansallisen oikeuden nojalla kuuluvia valtuuksia.

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

VI luku

Säädösvallan siirtäminen ja komiteamenettely

61 artikla

Siirretyn säädösvallan käyttäminen

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

2. Siirretään komissiolle … päivästä …kuuta … [tämän asetuksen voimaantulopäivä] viiden vuoden ajaksi 2 artiklan 5 kohdan toisessa alakohdassa, 7 artiklan 3 kohdassa, 8 artiklan 1 ja 2 kohdassa, 13 artiklan 8 kohdan neljännessä alakohdassa, 14 artiklan 9 kohdassa, 25 artiklassa, 27 artiklan 9 kohdassa, 28 artiklan 5 kohdassa ja 31 artiklan 5 kohdassa tarkoitettu valta antaa delegoituja säädöksiä. Komissio laatii siirrettyä säädösvaltaa koskevan kertomuksen viimeistään yhdeksän kuukautta ennen tämän viiden vuoden kauden päättymistä. Säädösvallan siirtoa jatketaan ilman eri toimenpiteitä samanpituisiksi kausiksi, jollei Euroopan parlamentti tai neuvosto vastusta tällaista jatkamista viimeistään kolme kuukautta ennen kunkin kauden päättymistä.

3. Euroopan parlamentti tai neuvosto voi milloin tahansa peruuttaa 2 artiklan 5 kohdan toisessa alakohdassa, 7 artiklan 3 kohdassa, 8 artiklan 1 ja 2 kohdassa, 13 artiklan 8 kohdan neljännessä alakohdassa, 14 artiklan 9 kohdassa, 25 artiklassa, 27 artiklan 9 kohdassa, 28 artiklan 5 kohdassa ja 31 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 5 kohdan toisen alakohdan, 7 artiklan 3 kohdan, 8 artiklan 1 tai 2 kohdan, 13 artiklan 8 kohdan neljännen alakohdan, 14 artiklan 9 kohdan, 25 artiklan, 27 artiklan 9 kohdan, 28 artiklan 5 kohdan tai 31 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.

62 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 määrä 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

63 artikla

Luottamuksellisuus

1. Kaikkien tämän asetuksen soveltamiseen osallistuvien osapuolten on kunnioitettava 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 (EU) 2016/943[36] 5 artiklassa tarkoitettuja tapauksia;

   b) tämän asetuksen tehokasta täytäntöönpanoa, etenkin tarkastusten, tutkimusten ja auditointien tarkoituksia varten;

   c) yleisiä ja kansallisia turvallisuusetuja;

   d) rikosoikeudellisten tai hallinnollisten menettelyjen luotettavuutta.

[36] 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).

2. Markkinavalvontaviranomaisten kesken tai markkinavalvontaviranomaisten ja komission välillä luottamuksellisesti vaihdettuja tietoja ei saa ilmaista ilman tiedot luovuttaneen markkinavalvontaviranomaisen etukäteen antamaa suostumusta, sanotun kuitenkaan rajoittamatta 1 kohdan soveltamista.

3. Edellä olevat 1 ja 2 kohta eivät vaikuta komission, jäsenvaltioiden ja ilmoitettujen laitosten tietojenvaihtoa ja varoitusten antamista koskeviin oikeuksiin ja velvollisuuksiin eivätkä asianomaisten henkilöiden jäsenvaltioiden rikosoikeuden mukaiseen tiedonantovelvollisuuteen.

4. Komissio ja jäsenvaltiot voivat tarvittaessa vaihtaa arkaluonteisia tietoja sellaisten kolmansien maiden asiaankuuluvien viranomaisten kanssa, joiden kanssa ne ovat tehneet kahdenvälisiä tai monenvälisiä luottamuksellisuutta koskevia järjestelyjä, joilla taataan riittävä suojan taso.

64 artikla

Seuraamukset

1. Jäsenvaltioiden on säädettävä tämän asetuksen säännösten rikkomiseen sovellettavista seuraamuksista ja toteutettava kaikki tarvittavat toimenpiteet niiden täytäntöönpanon varmistamiseksi. Seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia. Jäsenvaltioiden on ilmoitettava nämä säännökset ja toimenpiteet komissiolle viipymättä, ja jäsenvaltioiden on ilmoitettava komissiolle kaikki niitä koskevat myöhemmät muutokset viipymättä.

2. Liitteessä I vahvistettujen olennaisten kyberturvallisuusvaatimusten ja 13 ja 14 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 edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

3. Edellä 18–23 artiklassa, 28 artiklassa, 30 artiklan 1–4 kohdassa, 31 artiklan 1–4 kohdassa, 32 artiklan 1, 2 ja 3 kohdassa, 33 artiklan 5 kohdassa sekä 39, 41, 47, 49 ja 53 artiklassa säädettyjen velvoitteiden täyttämättä jättämisestä on määrättävä hallinnollinen sakko, joka on enimmillään 10 000 000 euroa tai, jos rikkomiseen syyllistynyt on yritys, enimmillään 2 prosenttia sen edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

4. 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 edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

5. Kun päätetään hallinnollisen sakon määrästä, kussakin yksittäisessä tapauksessa on otettava asianmukaisesti huomioon kaikki kyseisen tilanteen kannalta merkittävät olosuhteet sekä seuraavat seikat:

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

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

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

6. Hallinnollisia sakkoja määräävien markkinavalvontaviranomaisten on välitettävä tiedot sakkojen määräämisestä muiden jäsenvaltioiden markkinavalvontaviranomaisille asetuksen (EU) 2019/1020 34 artiklassa tarkoitetun tieto- ja viestintäjärjestelmän kautta.

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

8. 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.

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

10. Poiketen siitä, mitä 3–9 kohdassa säädetään, kyseisissä kohdissa tarkoitettuja hallinnollisia sakkoja ei sovelleta seuraaviin:

    a) valmistajat, jotka katsotaan mikroyrityksiksi tai pieniksi yrityksiksi, 14 artiklan 2 kohdan a alakohdassa tai 14 artiklan 4 kohdan a alakohdassa tarkoitetun määräajan noudattamatta jättämisen osalta;

    b) avoimen lähdekoodin ohjelmistovastaavat tämän asetuksen rikkomisen osalta.

65 artikla

Edustajakanteet

Direktiiviä (EU) 2020/1828 sovelletaan edustajakanteisiin, jotka on nostettu talouden toimijoita vastaan johtuen tämän asetuksen säännösten rikkomisista, jotka vahingoittavat tai voivat vahingoittaa kuluttajien yhteisiä etuja.

VIII luku

Siirtymäsäännökset ja loppusäännökset

66 artikla

Asetuksen (EU) 2019/1020 muuttaminen

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

”XX.[+] Euroopan parlamentin ja neuvoston asetus (EU) 2024/…[*++].

---

[*] Euroopan parlamentin ja neuvoston asetus (EU) 2024/… digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) N:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta (kyberkestävyyssäädös) (EUVL …, ELI: …).”.

[+] Virallinen lehti: lisätään tekstiin asetuksen (EU) 2019/1020 liitteessä I olevan luettelon järjestyksessä seuraava numero.

[++] Virallinen lehti: lisätään tekstiin asiakirjassa PE-CONS 100/23 (2022/0272(COD)) olevan asetuksen numero ja lisätään alaviitteeseen kyseisen asetuksen numero, päivämäärä ja EUVL-viite.

67 artikla

Direktiivin (EU) 2020/1828 muuttaminen

Lisätään direktiivin (EU) 2020/1828 liitteeseen I kohta seuraavasti:

”XX)[+] Euroopan parlamentin ja neuvoston asetus (EU) 2024/…[*++].

---

[*] Euroopan parlamentin ja neuvoston asetus (EU) 2024/… digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) N:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta (kyberkestävyyssäädös) (EUVL …, ELI: …).”.

[+] Virallinen lehti: lisätään tekstiin direktiivin (EU) 2020/1828 liitteessä I olevan luettelon järjestyksessä seuraava numero.

[++] Virallinen lehti: lisätään tekstiin asiakirjassa PE-CONS 100/23 (2022/0272(COD)) olevan asetuksen numero ja lisätään alaviitteeseen kyseisen asetuksen numero, päivämäärä ja EUVL-viite.

68 artikla

Asetuksen (EU) N:o 168/2013 muuttaminen

Muutetaan Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 168/2013[37] liite II seuraavasti:

Lisätään taulukon C1 osaan kohta seuraavasti:

”

XX+	18	ajoneuvon suojaus kyberhyökkäyksiltä		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

”.

[37] Euroopan parlamentin ja neuvoston asetus (EU) N:o 168/2013, annettu 15 päivänä tammikuuta 2013, kaksi- ja kolmipyöräisten ajoneuvojen ja nelipyörien hyväksynnästä ja markkinavalvonnasta (EUVL L 60, 2.3.2013, s. 52).

+ Virallinen lehti: lisätään tekstiin asetuksen (EU) N:o 168/2013 liitteessä II olevan C1 osan järjestyksessä seuraava numero.

69 artikla

Siirtymäsäännökset

1. EU-tyyppitarkastustodistukset ja hyväksymispäätökset, jotka on annettu digitaalisia elementtejä sisältävien tuotteiden, joihin sovelletaan muuta unionin yhdenmukaistamislainsäädäntöä kuin tätä asetusta, kyberturvallisuusvaatimuksista, pysyvät voimassa … päivään …kuuta … [42 kuukauden kuluttua tämän asetuksen voimaantulopäivästä] saakka, paitsi jos niiden voimassaolo päättyy ennen kyseistä ajankohtaa tai jos tällaisessa muussa unionin yhdenmukaistamislainsäädännössä toisin säädetään, jolloin ne pysyvät voimassa kyseisessä lainsäädännössä tarkoitetulla tavalla.

2. Ennen … päivää …kuuta … [36 kuukauden kuluttua tämän asetuksen voimaantulopäivästä] markkinoille saatettuihin digitaalisia elementtejä sisältäviin tuotteisiin sovelletaan tässä asetuksessa säädettyjä vaatimuksia ainoastaan, jos kyseisiin tuotteisiin tehdään kyseisen ajankohdan jälkeen merkittävä muutos.

3. Poiketen siitä, mitä tämän artiklan 2 kohdassa säädetään, 14 artiklassa säädettyjä velvoitteita sovelletaan kaikkiin tämän asetuksen soveltamisalaan kuuluviin digitaalisia elementtejä sisältäviin tuotteisiin, jotka on saatettu markkinoille ennen … päivää …kuuta … [36 kuukauden kuluttua tämän asetuksen voimaantulopäivästä].

70 artikla

Arviointi ja uudelleentarkastelu

1. Komissio toimittaa viimeistään … päivänä …kuuta … [72 kuukauden kuluttua tämän asetuksen voimaantulopäivästä] ja sen jälkeen joka neljäs vuosi Euroopan parlamentille ja neuvostolle kertomuksen tämän asetuksen arvioinnista ja uudelleentarkastelusta. Nämä kertomukset julkistetaan.

2. Komissio toimittaa viimeistään … päivänä …kuuta … [45 kuukauden kuluttua tämän asetuksen voimaantulopäivästä] ENISAa ja CSIRT-verkostoa kuultuaan Euroopan parlamentille ja neuvostolle kertomuksen, jossa arvioidaan 16 artiklassa perustetun keskitetyn raportointialustan tehokkuutta ja sitä, miten se, että koordinaattoreiksi nimetyt CSIRT-yksiköt soveltavat 16 artiklan 2 kohdassa tarkoitettuja kyberturvallisuuteen liittyviä syitä, vaikuttaa keskitetyn raportointialustan tehokkuuteen, tarkemmin sanoen vastaanotettujen ilmoitusten oikea-aikaiseen välittämiseen muille asiaankuuluville CSIRT-yksiköille.

71 artikla

Voimaantulo ja soveltaminen

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

2. Tätä asetusta sovelletaan … päivästä …kuuta … [36 kuukauden kuluttua tämän asetuksen voimaantulopäivästä].

   Sen 14 artiklaa sovelletaan kuitenkin … päivästä …kuuta … [21 kuukauden kuluttua tämän asetuksen voimaantulopäivästä] ja IV lukua (35–51 artiklaa) sovelletaan … päivästä …kuuta … [18 kuukauden kuluttua tämän asetuksen voimaantulopäivästä].

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

Tehty …ssa/ssä …päivänä …kuuta …

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puhemies	*Puheenjohtaja*

LIITE I

OLENNAISET KYBERTURVALLISUUSVAATIMUKSET

I osa Digitaalisia elementtejä sisältävien tuotteiden ominaisuuksiin liittyvät kyberturvallisuusvaatimukset

1) Digitaalisia elementtejä sisältävät tuotteet on suunniteltava, kehitettävä ja tuotettava siten, että niiden kyberturvallisuuden taso on oikeassa suhteessa riskeihin.

2) Digitaalisia elementtejä sisältävien tuotteiden on tämän asetuksen 13 artiklan 2 kohdassa tarkoitetun kyberturvallisuusriskien arvioinnin perusteella ja soveltuvin osin täytettävä seuraavat vaatimukset:

   a) ne on asetettava saataville markkinoilla ilman tiedossa olevia hyödynnettävissä olevia haavoittuvuuksia;

   b) ne on asetettava saataville markkinoilla oletusarvoisesti tietoturvallisin asetuksin, jolleivät valmistaja ja yrityskäyttäjä ole digitaalisia elementtejä sisältävän räätälöidyn tuotteen osalta sopineet toisin, ja ne on voitava palauttaa alkuperäiseen tilaansa;

   c) niissä on varmistettava, että haavoittuvuuksiin voidaan puuttua tietoturvapäivityksillä, kuten tapauksen mukaan automaattisilla tietoturvapäivityksillä, joiden asentaminen asianmukaisessa ajassa on oletusasetuksena sallittu, että käytettävissä on selkeä ja helppokäyttöinen estomekanismi ja että käyttäjille ilmoitetaan saatavilla olevista päivityksistä ja mahdollisuudesta lykätä niitä tilapäisesti;

d) niissä on varmistettava suojaaminen luvattomalta käytöltä asianmukaisin valvontamekanismein, joita sovelletaan muun muassa todennus-, identiteetinhallinta- tai pääsynhallintajärjestelmiin, ja ilmoitettava mahdollisesta luvattomasta käytöstä;

e) niissä on suojattava tallennettujen, siirrettyjen tai muulla tavoin käsiteltyjen henkilötietojen tai muiden tietojen luottamuksellisuus esimerkiksi salaamalla asiaankuuluvat tiedot uusimman tekniikan mukaisilla mekanismeilla tietoja siirrettäessä tai säilytettäessä ja käyttämällä muita teknisiä keinoja;

f) niissä on suojattava tallennettujen, siirrettyjen tai muulla tavoin käsiteltyjen henkilötietojen tai muiden tietojen eheys, komennot, ohjelmat ja asetukset kaikelta manipuloinnilta tai muuttamiselta, johon käyttäjä ei ole antanut lupaa, ja ilmoitettava turmeltumisesta;

g) niissä on käsiteltävä ainoastaan sellaisia henkilötietoja tai muita tietoja, jotka ovat asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa digitaalisia elementtejä sisältävän tuotteen käyttötarkoitukseen (tietojen minimointi);

h) niissä on suojattava olennaisten toimintojen ja perustoimintojen saatavuus, myös poikkeaman jälkeen, mihin kuuluvat myös palvelunestohyökkäysten varalta toteutettavat häiriönsietokykyä parantavat ja hyökkäysten vaikutuksia lieventävät toimenpiteet;

i) niissä on minimoitava kielteinen vaikutus, joka tuotteilla itsellään tai verkkoon liitetyillä laitteilla on muiden laitteiden tai verkkojen tarjoamien palvelujen saatavuuteen;

j) ne on suunniteltava, kehitettävä ja tuotettava siten, että hyökkäyspintoja, kuten ulkoisia rajapintoja, on mahdollisimman vähän;

k) ne on suunniteltava, kehitettävä ja tuotettava siten, että poikkeaman vaikutukset pidetään mahdollisimman vähäisinä käyttäen asianmukaisia haavoittuvuuden hyödyntämisen vaikutusten lieventämismekanismeja ja -tekniikoita;

l) niiden on tuotettava tietoturvaan liittyvää informaatiota tallentamalla ja seuraamalla asiaan liittyvää sisäistä toimintaa, kuten tietojen, palvelujen tai toimintojen käyttöä tai muutoksia, sekä tarjottava käyttäjän käyttöön estomekanismi;

m) tarjottava käyttäjille mahdollisuus poistaa kaikki tiedot ja asetukset pysyvästi turvallisella ja helpolla tavalla ja, jos tällaisia tietoja voidaan siirtää muihin tuotteisiin tai järjestelmiin, varmistettava, että tämä tapahtuu turvatusti.

II osa Haavoittuvuuksien käsittelyä koskevat vaatimukset

Digitaalisia elementtejä sisältävien tuotteiden valmistajien on

1) tunnistettava ja dokumentoitava digitaalisia elementtejä sisältävään tuotteeseen sisältyvät haavoittuvuudet ja komponentit muun muassa laatimalla vähintään tuotteiden ylimmän tason riippuvuudet kattava ohjelmistojen materiaaliluettelo yleisesti käytetyssä ja koneluettavassa muodossa;

2) digitaalisia elementtejä sisältäviin tuotteisiin kohdistuvien riskien yhteydessä puututtava haavoittuvuuksiin ja korjattava ne viipymättä, esimerkiksi tarjoamalla tietoturvapäivityksiä; jos se on teknisesti mahdollista, uudet tietoturvapäivitykset on tarjottava erillään toimintopäivityksistä;

3) tehtävä säännöllisesti digitaalisia elementtejä sisältävän tuotteen tietoturvaan liittyviä tehokkaita testejä ja arviointeja;

4) kun tietoturvapäivitys on asetettu saataville, jaettava ja julkistettava tiedot korjatuista haavoittuvuuksista, mukaan lukien kuvaus haavoittuvuuksista, tiedot, joiden avulla käyttäjät voivat tunnistaa kyseisen digitaalisia elementtejä sisältävän tuotteen, haavoittuvuuksien vaikutukset ja vakavuus sekä selkeät ja saavutettavat tiedot, jotka auttavat käyttäjiä korjaamaan haavoittuvuudet; asianmukaisesti perustelluissa tapauksissa, joissa valmistajat pitävät julkistamisen turvallisuusriskejä sen turvallisuushyötyjä merkittävämpinä, ne voivat lykätä korjattua haavoittuvuutta koskevien tietojen julkistamista, kunnes käyttäjille on annettu mahdollisuus asentaa asiaankuuluva korjaava päivitys;

5) otettava käyttöön koordinoitua haavoittuvuuksien julkistamista koskevat periaatteet ja valvottava niiden noudattamista;

6) toteutettava toimenpiteitä, joilla helpotetaan tietojen jakamista oman digitaalisia elementtejä sisältävän tuotteensa ja kyseisen tuotteen sisältämien kolmannen osapuolen komponenttien mahdollisista haavoittuvuuksista, muun muassa ilmoittamalla yhteysosoite digitaalisia elementtejä sisältävässä tuotteessa havaittujen haavoittuvuuksien raportointia varten;

7) huolehdittava mekanismeista digitaalisia elementtejä sisältävien tuotteiden päivitysten tietoturvallisen jakelun varmistamiseksi, jotta haavoittuvuudet korjataan tai niiden vaikutuksia lievennetään pikaisesti ja tietoturvapäivitysten tapauksessa soveltuvin osin automaattisesti;

8) varmistettava, että jos havaittujen tietoturvaongelmien ratkaisemiseksi on saatavilla tietoturvapäivityksiä, niitä levitetään viipymättä ja, jolleivat valmistaja ja yrityskäyttäjä ole digitaalisia elementtejä sisältävän räätälöidyn tuotteen osalta sopineet toisin, maksutta ja että niihin liitetään tarvittavat ohjeet, myös mahdollisista käyttäjältä edellytettävistä toimista.

LIITE II

KÄYTTÄJÄLLE ANNETTAVAT TIEDOT JA OHJEET

Digitaalisia elementtejä sisältävän tuotteen mukana on toimitettava vähintään seuraavat tiedot:

1. valmistajan nimi, rekisteröity toiminimi tai rekisteröity tavaramerkki sekä postiosoite, sähköpostiosoite tai muu digitaalinen yhteystieto ja, jos sellainen on saatavilla, verkkosivusto, jonka kautta valmistajaan saa yhteyden;

2. keskitetty yhteyspiste, johon voi ilmoittaa ja josta saa tietoja digitaalisia elementtejä sisältävän tuotteen haavoittuvuuksista ja josta löytyvät valmistajan soveltamat koordinoitua haavoittuvuuksien julkistamista koskevat periaatteet;

3. digitaalisia elementtejä sisältävän tuotteen nimi ja tyyppi sekä kaikki lisätiedot, joiden avulla tuote voidaan yksilöidä;

4. digitaalisia elementtejä sisältävän tuotteen käyttötarkoitus, mukaan lukien valmistajan tarjoama tietoturvaympäristö, sekä tuotteen olennaiset toiminnot ja tiedot tietoturvaominaisuuksista;

5. kaikki tunnetut tai ennakoitavissa olevat olosuhteet, jotka liittyvät digitaalisia elementtejä sisältävän tuotteen käyttöön sen käyttötarkoituksen mukaisesti tai kohtuudella ennakoitavissa olevissa väärinkäyttöolosuhteissa ja jotka voivat johtaa merkittäviin kyberturvallisuusriskeihin;

6. tarvittaessa internetosoite, josta EU-vaatimustenmukaisuusvakuutus on saatavilla;

7. valmistajan tarjoaman teknisen tietoturvatuen tyyppi ja päättymispäivä tukiajalle, jonka aikana käyttäjät voivat odottaa, että haavoittuvuudet käsitellään, ja voivat odottaa saavansa tietoturvapäivityksiä;

8. yksityiskohtaiset ohjeet seuraavista tai internetosoite, josta yksityiskohtaiset ohjeet ovat saatavilla:

   a) tarvittavat toimenpiteet digitaalisia elementtejä sisältävän tuotteen käyttöönoton yhteydessä ja koko sen elinkaaren ajan tietoturvallisen käytön varmistamiseksi;

   b) miten digitaalisia elementtejä sisältävän tuotteen muutokset voivat vaikuttaa tietoturvaan;

   c) miten tietoturvan kannalta merkitykselliset päivitykset voidaan asentaa;

   d) digitaalisia elementtejä sisältävän tuotteen turvallinen käytöstä poistaminen, mukaan lukien ohjeet siitä, miten käyttäjätiedot voidaan tietoturvallisesti poistaa;

   e) miten liitteessä I olevan I osan 2 kohdan c alakohdassa edellytetty oletusasetus, joka mahdollistaa tietoturvapäivitysten automaattisen asennuksen, voidaan kytkeä pois päältä;

   f) jos digitaalisia elementtejä sisältävä tuote on tarkoitettu integroitavaksi toisiin digitaalisia elementtejä sisältäviin tuotteisiin, tiedot, jotka integroinnin suorittaja tarvitsee täyttääkseen liitteessä I vahvistetut olennaiset kyberturvallisuusvaatimukset ja liitteessä VII vahvistetut asiakirjoja koskevat vaatimukset;

9. jos valmistaja päättää asettaa ohjelmistojen materiaaliluettelon käyttäjän saataville, tiedot siitä, missä ohjelmistojen materiaaliluettelo on saatavilla.

LIITE III

DIGITAALISIA ELEMENTTEJÄ SISÄLTÄVÄT TÄRKEÄT TUOTTEET

Luokka I

1. Identiteetinhallintajärjestelmät ja korotettujen käyttöoikeuksien hallintaohjelmistot ja -laitteistot, mukaan lukien todennuksessa ja pääsynvalvonnassa käytettävät lukijat, myös biometriset lukijat.

2. Erilliset ja sulautetut selaimet.

3. Salasanojen hallinnointityökalut.

4. Ohjelmistot, jotka etsivät, poistavat tai asettavat karanteeniin haittaohjelmistoja.

5. Digitaalisia elementtejä sisältävät tuotteet, jotka liittyvät virtuaalisen yksityisverkon (VPN) luomiseen.

6. Verkonhallintajärjestelmät.

7. Tietoturvatietojen ja tapahtumien hallintajärjestelmät (SIEM).

8. Käynnistysohjelmat.

9. Julkisen avaimen infrastruktuuri ja digitaalisen varmenteen luomiseen käytettävät ohjelmistot.

10. Fyysiset ja virtuaaliset verkkorajapinnat.

11. Käyttöjärjestelmät.

12. Reitittimet, internetyhteyden muodostamiseen tarkoitetut modeemit sekä kytkimet.

13. Mikroprosessorit, joissa on turvallisuustoimintoja.

14. Mikro-ohjaimet, joissa on turvallisuustoimintoja.

15. Sovelluskohtaiset integroidut piirit (ASIC) ja kenttäohjelmoitavat porttimatriisit (FPGA), joissa on turvallisuustoimintoja.

16. Älykodin yleiskäyttöiset virtuaaliavustajat.

17. Älykodin tuotteet, joissa on turvallisuustoimintoja, mukaan lukien ovien älylukot, turvakamerat, itkuhälyttimet ja hälytysjärjestelmät.

18. Euroopan parlamentin ja neuvoston direktiivin 2009/48/EY[1] soveltamisalaan kuuluvat verkkoon liitetyt lelut, joissa on vuorovaikutustoimintoja (esimerkiksi puhe tai kuvaaminen) tai paikannustoimintoja.

19. Henkilökohtaiset puettavat tuotteet, joita pidetään yllä tai jotka sijoitetaan ihmiskeholle ja joita käytetään terveyden monitorointiin (kuten seurantaan) ja joihin ei sovelleta asetusta (EU) 2017/745 tai asetusta (EU) 2017/746, tai henkilökohtaiset puettavat tuotteet, jotka on tarkoitettu lasten käyttöön ja käytettäväksi lapsilla.

Luokka II

1. Virtualisointialustat ja konttien ajonaikaiset järjestelmät, jotka tukevat käyttöjärjestelmien ja vastaavien ympäristöjen virtualisoitua ajoa.

2. Palomuurit ja tunkeutumisen havaitsemis- ja estojärjestelmät.

3. Väärinkäytöltä suojatut mikroprosessorit.

4. Väärinkäytöltä suojatut mikro-ohjaimet.

---

[1] Euroopan parlamentin ja neuvoston direktiivi 2009/48/EY, annettu 18 päivänä kesäkuuta 2009, lelujen turvallisuudesta (EUVL L 170, 30.6.2009, s. 1).

LIITE IV

DIGITAALISIA ELEMENTTEJÄ SISÄLTÄVÄT KRIITTISET TUOTTEET

1. Fyysiset laitteet, joissa on peukaloinnilta suojaavia turvamekanismeja.

2. Älymittareiden yhdyskäytävät Euroopan parlamentin ja neuvoston direktiivin (EU) 2019/944[1] 2 artiklan 23 alakohdassa määritellyissä älykkäissä mittausjärjestelmissä ja muut kehittyneisiin turvallisuustarkoituksiin, myös kryptolaskentaan, käytettävät laitteet.

3. Älykortit tai vastaavat laitteet, mukaan lukien turvaelementit.

---

[1] Euroopan parlamentin ja neuvoston direktiivi (EU) 2019/944, annettu 5 päivänä kesäkuuta 2019, sähkön sisämarkkinoita koskevista yhteisistä säännöistä ja direktiivin 2012/27/EU muuttamisesta (EUVL L 158, 14.6.2019, s. 125).

LIITE V

EU-VAATIMUSTENMUKAISUUSVAKUUTUS

Tämän asetuksen 28 artiklassa tarkoitetun EU-vaatimustenmukaisuusvakuutuksen on sisällettävä kaikki seuraavat tiedot:

1. Digitaalisia elementtejä sisältävän tuotteen nimi ja tyyppi sekä kaikki lisätiedot, joiden avulla tuote voidaan yksilöidä.

2. Valmistajan tai valmistajan valtuutetun edustajan nimi ja osoite.

3. Ilmoitus siitä, että EU-vaatimustenmukaisuusvakuutus on annettu antajan yksinomaisella vastuulla.

4. Vakuutuksen kohde (jäljitettävyyden mahdollistava digitaalisia elementtejä sisältävän tuotteen tunniste, joka voi tarvittaessa sisältää valokuvan).

5. Lausuma siitä, että edellä kuvattu vakuutuksen kohde on asiaa koskevan unionin yhdenmukaistamislainsäädännön vaatimusten mukainen.

6. Viittaukset käytettyihin asiaankuuluviin yhdenmukaistettuihin standardeihin tai muihin yhteisiin eritelmiin tai kyberturvallisuussertifiointeihin, joiden suhteen vaatimustenmukaisuusvakuutus on annettu.

7. Tarvittaessa ilmoitetun laitoksen nimi ja tunnusnumero, kuvaus suoritetusta vaatimustenmukaisuuden arviointimenettelystä sekä annetun todistuksen tunniste.

8. Lisätiedot:

Allekirjoitettu seuraavan puolesta: ……

(antamispaikka ja -päivämäärä):

(nimi, tehtävä) (allekirjoitus):

LIITE VI

YKSINKERTAISTETTU EU-VAATIMUSTENMUKAISUUSVAKUUTUS

Tämän asetuksen 13 artiklan 20 kohdassa tarkoitettu yksinkertaistettu EU-vaatimustenmukaisuusvakuutus on annettava seuraavasti:

[Valmistajan nimi] vakuuttaa, että digitaalisia elementtejä sisältävä tuote [digitaalisia elementtejä sisältävän tuotteen tyypin kuvaus] täyttää Euroopan parlamentin ja neuvoston asetuksen (EU) …/…[1] vaatimukset.

EU-vaatimustenmukaisuusvakuutuksen koko teksti on saatavilla seuraavassa internetosoitteessa:

---

[1] Virallinen lehti: lisätään tekstiin asiakirjassa PE-CONS .../... (2022/0272(COD)) olevan asetuksen numero.

LIITE VII

TEKNISTEN ASIAKIRJOJEN SISÄLTÖ

Tämän asetuksen 31 artiklassa tarkoitettuihin teknisiin asiakirjoihin on sisällyttävä soveltuvin osin vähintään seuraavat tiedot kyseisestä digitaalisia elementtejä sisältävästä tuotteesta:

1. Digitaalisia elementtejä sisältävän tuotteen yleinen kuvaus, mukaan lukien

   a) käyttötarkoitus;

   b) niiden ohjelmistojen versiot, joilla on vaikutusta olennaisten kyberturvallisuusvaatimusten täyttymiseen;

   c) jos digitaalisia elementtejä sisältävä tuote on laite, valokuvat tai kaaviot ulkoisista piirteistä, merkinnöistä ja sisäisestä rakenteesta;

   d) liitteessä II esitetyt käyttäjälle annettavat tiedot ja ohjeet.

2. Kuvaus digitaalisia elementtejä sisältävän tuotteen suunnittelusta, kehittämisestä ja tuotannosta sekä haavoittuvuuksien käsittelyprosesseista, mukaan lukien

   a) tarvittavat tiedot digitaalisia elementtejä sisältävän tuotteen suunnittelusta ja kehittämisestä, mukaan lukien tarvittaessa piirustukset ja kaaviot ja kuvaus järjestelmäarkkitehtuurista, jossa selitetään, miten ohjelmistokomponentit rakentuvat toisilleen tai vaikuttavat toisiinsa ja miten ne on integroitu kokonaisprosessointiin;

b) tarvittavat tiedot ja eritelmät valmistajan käyttöön ottamista haavoittuvuuksien käsittelyprosesseista, mukaan lukien ohjelmistojen materiaaliluettelo, koordinoitua haavoittuvuuksien julkistamista koskevat periaatteet, todisteet yhteysosoitteen antamisesta haavoittuvuuksista ilmoittamista varten ja kuvaus teknisistä ratkaisuista, jotka on valittu päivitysten suojattua jakelua varten;

c) tarvittavat tiedot ja eritelmät, jotka koskevat digitaalisia elementtejä sisältävän tuotteen tuotanto- ja seurantaprosesseja ja kyseisten prosessien validointia.

3. Arvio kyberturvallisuusriskeistä, joiden torjumiseksi digitaalisia elementtejä sisältävä tuote on suunniteltu, kehitetty, tuotettu, toimitettu ja otettu ylläpidettäväksi 13 artiklan mukaisesti, myös siitä, miten liitteessä I olevassa I osassa vahvistetut olennaiset kyberturvallisuusvaatimukset ovat sovellettavissa.

4. Asiaankuuluvat tiedot, jotka on otettu huomioon digitaalisia elementtejä sisältävän tuotteen 13 artiklan 8 kohdan mukaisen tukiajan määrittämisessä.

5. Luettelo kokonaan tai osittain sovellettavista yhdenmukaistetuista standardeista, joiden viitetiedot on julkaistu *Euroopan unionin virallisessa lehdessä*, tämän asetuksen 27 artiklassa tarkoitetuista yhteisistä eritelmistä tai tämän asetuksen 27 artiklan 8 kohdassa tarkoitetuista asetuksen (EU) 2019/881 nojalla hyväksytyistä eurooppalaisista kyberturvallisuuden sertifiointijärjestelmistä, ja jos kyseisiä yhdenmukaistettuja standardeja, yhteisiä eritelmiä tai eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä ei ole sovellettu, kuvaukset ratkaisuista, jotka on valittu liitteessä I olevissa I ja II osassa vahvistettujen olennaisten kyberturvallisuusvaatimusten täyttämiseksi, mukaan lukien luettelo sovellettavista muista asiaankuuluvista teknisistä eritelmistä. Osittain sovellettavien yhdenmukaistettujen standardien, yhteisten eritelmien tai eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien tapauksessa teknisissä asiakirjoissa on täsmennettävä osat, joita on sovellettu.

6. Raportit testeistä, jotka on tehty sen varmistamiseksi, että digitaalisia elementtejä sisältävät tuotteet ja haavoittuvuuksien käsittelyprosessit täyttävät sovellettavat liitteessä I olevissa I ja II osassa vahvistetut olennaiset kyberturvallisuusvaatimukset.

7. Jäljennös EU-vaatimustenmukaisuusvakuutuksesta.

8. Tarvittaessa ohjelmistojen materiaaliluettelo markkinavalvontaviranomaisen perustellusta pyynnöstä edellyttäen, että se on tarpeen, jotta kyseinen viranomainen voi tarkastaa, että liitteessä I vahvistetut olennaiset kyberturvallisuusvaatimukset täyttyvät.

LIITE VIII

VAATIMUSTENMUKAISUUDEN ARVIOINTIMENETTELYT

I osa Sisäiseen valvontaan perustuva vaatimustenmukaisuuden arviointimenettely (perustuen moduuliin A)

1. Sisäinen valvonta on vaatimustenmukaisuuden arviointimenettely, jossa valmistaja täyttää tämän osan 2, 3 ja 4 kohdassa vahvistetut velvoitteet sekä varmistaa ja vakuuttaa yksinomaisella vastuullaan, että digitaalisia elementtejä sisältävät tuotteet täyttävät kaikki liitteessä I olevassa I osassa vahvistetut olennaiset kyberturvallisuusvaatimukset ja että valmistaja täyttää liitteessä I olevassa II osassa vahvistetut olennaiset kyberturvallisuusvaatimukset.

2. Valmistajan on laadittava liitteessä VII kuvatut tekniset asiakirjat.

3. Digitaalisia elementtejä sisältävien tuotteiden suunnittelu, kehittäminen, tuotanto ja haavoittuvuuksien käsittely

Valmistajan on toteutettava kaikki tarvittavat toimenpiteet sen varmistamiseksi, että suunnittelu-, kehitys- ja tuotantoprosesseilla ja haavoittuvuuksien käsittelyprosesseilla sekä niiden valvonnalla varmistetaan, että valmistetut tai kehitetyt digitaalisia elementtejä sisältävät tuotteet ja valmistajan käyttöön ottamat prosessit täyttävät liitteessä I olevissa I ja II osassa vahvistetut olennaiset kyberturvallisuusvaatimukset.

4. CE-merkintä ja vaatimustenmukaisuusvakuutus

4.1. Valmistajan on kiinnitettävä CE-merkintä kuhunkin yksittäiseen digitaalisia elementtejä sisältävään tuotteeseen, joka täyttää tässä asetuksessa vahvistetut sovellettavat vaatimukset.

4.2. Valmistajan on laadittava kirjallinen EU-vaatimustenmukaisuusvakuutus kullekin digitaalisia elementtejä sisältävälle tuotteelle 28 artiklan mukaisesti ja pidettävä se yhdessä teknisten asiakirjojen kanssa kansallisten viranomaisten saatavilla kymmenen vuoden ajan sen jälkeen, kun digitaalisia elementtejä sisältävä tuote on saatettu markkinoille, tai tukiajan ajan sen mukaan, kumpi näistä ajanjaksoista on pidempi. EU-vaatimustenmukaisuusvakuutuksessa on yksilöitävä digitaalisia elementtejä sisältävä tuote, jota varten se on laadittu. Jäljennös EU-vaatimustenmukaisuusvakuutuksesta on pyynnöstä toimitettava asiaankuuluville viranomaisille.

5. Valtuutetut edustajat

Valmistajan valtuutettu edustaja voi täyttää valmistajan puolesta ja tämän vastuulla 4 kohdassa esitetyt valmistajan velvollisuudet edellyttäen, että asiaankuuluvat velvollisuudet on eritelty toimeksiannossa.

II osa EU-tyyppitarkastus (perustuen moduuliin B)

1. EU-tyyppitarkastus on se vaatimustenmukaisuuden arviointimenettelyn osa, jossa ilmoitettu laitos tutkii digitaalisia elementtejä sisältävän tuotteen teknisen suunnittelun ja kehittämistavan sekä valmistajan käyttöön ottamat haavoittuvuuksien käsittelyprosessit ja todistaa, että digitaalisia elementtejä sisältävä tuote täyttää liitteessä I olevassa I osassa vahvistetut olennaiset kyberturvallisuusvaatimukset ja että valmistaja täyttää liitteessä I olevassa II osassa vahvistetut olennaiset kyberturvallisuusvaatimukset.

2. EU-tyyppitarkastuksessa tehdään digitaalisia elementtejä sisältävän tuotteen teknisen suunnittelun ja kehittämistavan asianmukaisuuden arviointi 3 kohdassa tarkoitettujen teknisten asiakirjojen ja niitä tukevan aineiston tarkastelun perusteella sekä tuotteen yhden tai useamman kriittisen osan näytteiden tarkastus (tuotantotyypin ja suunnittelutyypin yhdistelmä).

3. Valmistaja tekee EU-tyyppitarkastusta koskevan hakemuksen yhdelle valitsemalleen ilmoitetulle laitokselle.

   Hakemuksen on sisällettävä:

   3.1 valmistajan nimi ja osoite sekä valtuutetun edustajan nimi ja osoite, jos tämä tekee hakemuksen;

3.2 kirjallinen vakuutus siitä, että samaa hakemusta ei ole tehty toiselle ilmoitetulle laitokselle;

3.3 tekniset asiakirjat, joiden perusteella on voitava arvioida, täyttääkö digitaalisia elementtejä sisältävä tuote liitteessä I olevassa I osassa vahvistetut sovellettavat olennaiset kyberturvallisuusvaatimukset ja täyttävätkö valmistajan käyttämät haavoittuvuuksien käsittelyprosessit liitteessä I olevassa II osassa vahvistetut olennaiset kyberturvallisuusvaatimukset, ja niihin on sisällyttävä asianmukainen analyysi ja arviointi riskeistä. Teknisissä asiakirjoissa on täsmennettävä sovellettavat vaatimukset, ja niiden on katettava digitaalisia elementtejä sisältävän tuotteen suunnittelu, valmistus ja toiminta siinä määrin kuin se on olennaista arvioinnin kannalta. Teknisten asiakirjojen on kaikissa soveltuvissa tapauksissa sisällettävä ainakin liitteessä VII esitetyt tekijät;

3.4 teknisten suunnittelu- ja kehitysratkaisujen ja haavoittuvuuksien käsittelyprosessien riittävyyttä tukeva näyttö. Tässä aineistossa on mainittava kaikki asiaankuuluvat asiakirjat, joita on käytetty, erityisesti siinä tapauksessa, että asiaankuuluvia yhdenmukaistettuja standardeja tai teknisiä eritelmiä ei ole sovellettu kokonaisuudessaan. Aineistoon on sisällytettävä tarvittaessa niiden testien tulokset, jotka valmistaja on tehnyt asianmukaisessa laboratoriossaan tai jotka on teetetty valmistajan puolesta ja tämän vastuulla jossain toisessa testilaboratoriossa.

4. Ilmoitetun laitoksen on:

4.1. tutkittava tekniset asiakirjat ja niitä tukeva aineisto sen arvioimiseksi, täyttääkö digitaalisia elementtejä sisältävän tuotteen tekninen suunnittelu ja kehittäminen liitteessä I olevassa I osassa vahvistetut olennaiset kyberturvallisuusvaatimukset ja täyttävätkö valmistajan käyttöön ottamat haavoittuvuuksien käsittelyprosessit liitteessä I olevassa II osassa vahvistetut olennaiset kyberturvallisuusvaatimukset;

4.2. varmennettava, että näytteet on kehitetty tai valmistettu teknisten asiakirjojen mukaisesti, sekä yksilöitävä ne osat, jotka on suunniteltu ja kehitetty asiaa koskevien yhdenmukaistettujen standardien tai teknisten eritelmien sovellettavien määräysten mukaisesti, samoin kuin osat, joiden suunnittelussa ja kehittämisessä ei ole noudatettu näiden standardien asiaa koskevia vaatimuksia;

4.3. tehtävä tai teetettävä asianmukaiset tarkastukset ja testit sen todentamiseksi, että ratkaisuja on sovellettu oikein silloin, kun valmistaja on valinnut asiaa koskevissa yhdenmukaistetuissa standardeissa tai teknisissä eritelmissä esitettyjen ratkaisujen soveltamisen liitteessä I vahvistettujen vaatimusten täyttämiseksi;

4.4. tehtävä tai teetettävä asianmukaiset tarkastukset ja testit sen todentamiseksi, täyttävätkö valmistajan soveltamat ratkaisut vastaavat olennaiset vaatimukset silloin, kun asiaa koskevissa yhdenmukaistetuissa standardeissa tai teknisissä eritelmissä esitettyjä ratkaisuja ei ole sovellettu liitteessä I vahvistettujen olennaisten kyberturvallisuusvaatimusten täyttämiseksi;

4.5. sovittava valmistajan kanssa paikka, jossa tarkastukset ja tarvittavat testit tehdään.

5. Ilmoitetun laitoksen on laadittava arviointiraportti, johon kirjataan 4 kohdan mukaisesti toteutetut toimet ja niiden tulokset. Ilmoitettu laitos voi julkistaa raportin sisällön joko kokonaan tai osittain ainoastaan valmistajan suostumuksella, sanotun kuitenkaan rajoittamatta sen velvoitteita ilmoittamisesta vastaavia viranomaisia kohtaan.

6. Jos tyyppi ja haavoittuvuuksien käsittelyprosessit täyttävät liitteessä I vahvistetut olennaiset kyberturvallisuusvaatimukset, ilmoitetun laitoksen on annettava valmistajalle EU-tyyppitarkastustodistus. Todistuksessa on oltava valmistajan nimi ja osoite, tarkastuksessa tehdyt päätelmät, (mahdolliset) todistuksen voimassaolon edellytykset ja hyväksyttyjen tyypin ja haavoittuvuuksien käsittelyprosessien tunnistamiseen tarvittavat tiedot. Todistuksessa voi olla yksi tai useampi liite.

Todistuksessa ja sen liitteissä on oltava kaikki asiaankuuluvat tiedot, jotta voidaan arvioida, ovatko valmistetut tai kehitetyt digitaalisia elementtejä sisältävät tuotteet tarkastettujen tyypin ja haavoittuvuuksien käsittelyprosessien mukaisia, ja jotta käytön aikainen valvonta on mahdollista.

Jos tyyppi ja haavoittuvuuksien käsittelyprosessi eivät täytä liitteessä I vahvistettuja sovellettavia olennaisia kyberturvallisuusvaatimuksia, ilmoitetun laitoksen on kieltäydyttävä antamasta EU-tyyppitarkastustodistusta ja ilmoitettava siitä hakijalle sekä esitettävä yksityiskohtaiset perustelut todistuksen epäämiselle.

7. Ilmoitetun laitoksen on pysyttävä ajan tasalla yleisesti tunnustetussa uusimmassa tekniikassa mahdollisesti tapahtuvista muutoksista, jotka viittaavat siihen, että hyväksytty tyyppi ja haavoittuvuuksien käsittelyprosessit eivät ehkä enää täytä tämän asetuksen liitteessä I vahvistettuja sovellettavia olennaisia kyberturvallisuusvaatimuksia, ja määritettävä, edellyttävätkö tällaiset muutokset lisätutkimuksia. Jos näin on, ilmoitetun laitoksen on ilmoitettava asiasta valmistajalle.

Valmistajan on ilmoitettava ilmoitetulle laitokselle, joka pitää hallussaan EU-tyyppitarkastustodistusta koskevia teknisiä asiakirjoja, kaikista hyväksyttyyn tyyppiin tai haavoittuvuuksien käsittelyprosesseihin tehdyistä muutoksista, jotka voivat vaikuttaa siihen, täyttyvätkö liitteessä I vahvistetut olennaiset kyberturvallisuusvaatimukset, tai voivat vaikuttaa todistuksen voimassaolon edellytyksiin. Tällaiset muutokset vaativat lisähyväksynnän, joka annetaan alkuperäiseen EU-tyyppitarkastustodistukseen tehtävän lisäyksen muodossa.

8. Ilmoitetun laitoksen on tehtävä määräajoin auditointeja varmistaakseen, että liitteessä I olevassa II osassa esitetyt haavoittuvuuksien käsittelyprosessit toteutetaan asianmukaisesti.

9. Kunkin ilmoitetun laitoksen on annettava ilmoittamisesta vastaavalle viranomaiselleen tiedoksi EU-tyyppitarkastustodistukset ja niiden lisäykset, jotka se on antanut tai peruuttanut kokonaan, ja sen on asetettava säännöllisesti tai pyynnöstä ilmoittamisesta vastaavan viranomaisensa saataville luettelo todistuksista ja niiden lisäyksistä, jotka on evätty tai peruutettu toistaiseksi tai joita on muutoin rajoitettu.

Kunkin ilmoitetun laitoksen on annettava muille ilmoitetuille laitoksille tiedoksi EU-tyyppitarkastustodistukset ja niiden lisäykset, jotka se on evännyt tai peruuttanut kokonaan tai toistaiseksi tai joita se on muutoin rajoittanut, sekä pyynnöstä ne todistukset ja niiden lisäykset, jotka se on antanut.

Komissio, jäsenvaltiot ja muut ilmoitetut laitokset voivat pyynnöstä saada jäljennöksen EU-tyyppitarkastustodistuksista ja niihin mahdollisesti tehdyistä lisäyksistä. Komissio ja jäsenvaltiot voivat pyynnöstä saada jäljennöksen teknisistä asiakirjoista ja ilmoitetun laitoksen suorittamien tarkastusten tuloksista. Ilmoitetun laitoksen on säilytettävä jäljennös EU-tyyppitarkastustodistuksesta, sen liitteistä ja lisäyksistä sekä teknisistä asiakirjoista, valmistajan toimittamat asiakirjat mukaan luettuina, todistuksen voimassaolon päättymiseen saakka.

10. Valmistajan on pidettävä kansallisten viranomaisten saatavilla jäljennös EU-tyyppitarkastustodistuksesta, sen liitteistä ja lisäyksistä sekä tekniset asiakirjat kymmenen vuoden ajan sen jälkeen, kun digitaalisia elementtejä sisältävä tuote on saatettu markkinoille, tai tukiajan ajan sen mukaan, kumpi näistä ajanjaksoista on pidempi.

11. Valmistajan valtuutettu edustaja voi tehdä 3 kohdassa tarkoitetun hakemuksen ja täyttää 7 ja 10 kohdassa vahvistetut velvollisuudet edellyttäen, että asiaankuuluvat velvollisuudet on eritelty toimeksiannossa.

III osa Sisäiseen tuotannonvalvontaan perustuva tyypinmukaisuus (perustuen moduuliin C)

1. Sisäiseen tuotannonvalvontaan perustuva tyypinmukaisuus on vaatimustenmukaisuuden arviointimenettelyn osa, jossa valmistaja täyttää tämän osan 2 ja 3 kohdassa vahvistetut velvollisuudet sekä varmistaa ja vakuuttaa, että kyseiset digitaalisia elementtejä sisältävät tuotteet ovat EU-tyyppitarkastustodistuksessa kuvatun tyypin mukaisia ja täyttävät liitteessä I olevassa I osassa vahvistetut olennaiset kyberturvallisuusvaatimukset ja että valmistaja täyttää liitteessä I olevassa II osassa vahvistetut olennaiset kyberturvallisuusvaatimukset.

2. Tuotanto

Valmistajan on toteutettava kaikki tarvittavat toimenpiteet sen varmistamiseksi, että tuotannolla ja sen valvonnalla taataan, että valmistettu digitaalisia elementtejä sisältävä tuote on EU-tyyppitarkastustodistuksessa kuvaillun hyväksytyn tyypin ja liitteessä I olevassa I osassa vahvistettujen olennaisten kyberturvallisuusvaatimusten mukainen, ja että valmistaja täyttää liitteessä I olevassa II osassa vahvistetut olennaiset kyberturvallisuusvaatimukset.

3. CE-merkintä ja vaatimustenmukaisuusvakuutus

3.1. Valmistajan on kiinnitettävä CE-merkintä kuhunkin yksittäiseen digitaalisia elementtejä sisältävään tuotteeseen, joka on EU-tyyppitarkastustodistuksessa kuvatun tyypin mukainen ja täyttää sovellettavat säädöksessä vahvistetut vaatimukset.

3.2. Valmistajan on laadittava kirjallinen vaatimustenmukaisuusvakuutus tuotemallille ja pidettävä se kansallisten viranomaisten saatavilla kymmenen vuoden ajan sen jälkeen, kun digitaalisia elementtejä sisältävä tuote on saatettu markkinoille, tai tukiajan ajan sen mukaan, kumpi näistä ajanjaksoista on pidempi. Vaatimustenmukaisuusvakuutuksessa on yksilöitävä tuotemalli, jota varten se on laadittu. Vaatimustenmukaisuusvakuutuksen jäljennös on toimitettava pyynnöstä asiaankuuluville viranomaisille.

4. Valtuutettu edustaja

Valmistajan valtuutettu edustaja voi täyttää valmistajan puolesta ja tämän vastuulla 3 kohdassa esitetyt valmistajan velvollisuudet edellyttäen, että asiaankuuluvat velvollisuudet on eritelty toimeksiannossa.

IV osa Täydelliseen laadunvarmistukseen perustuva vaatimustenmukaisuus (perustuen moduuliin H)

1. Täydelliseen laadunvarmistukseen perustuva vaatimustenmukaisuus on vaatimustenmukaisuuden arviointimenettely, jossa valmistaja täyttää tämän osan 2 ja 5 kohdassa vahvistetut velvollisuudet sekä varmistaa ja vakuuttaa yksinomaisella vastuullaan, että kyseiset digitaalisia elementtejä sisältävät tuotteet tai tuoteryhmät täyttävät liitteessä I olevassa I osassa vahvistetut olennaiset kyberturvallisuusvaatimukset ja että valmistajan käyttöön ottamat haavoittuvuuksien käsittelyprosessit täyttävät liitteessä I olevassa II osassa vahvistetut vaatimukset.

2. Digitaalisia elementtejä sisältävien tuotteiden suunnittelu, kehittäminen, tuotanto ja haavoittuvuuksien käsittely

Valmistajan on sovellettava 3 kohdan mukaista hyväksyttyä laatujärjestelmää digitaalisia elementtejä sisältävien tuotteiden suunnittelussa, kehittämisessä ja tuotteen lopputarkastuksessa ja testauksessa sekä haavoittuvuuksien käsittelyssä sekä ylläpidettävä järjestelmän tehokkuutta koko tukiajan ajan, ja sen on oltava 4 kohdan mukaisen valvonnan alainen.

3. Laatujärjestelmä

3.1. Valmistajan on tehtävä kyseisten digitaalisia elementtejä sisältävien tuotteiden osalta käyttämänsä laatujärjestelmän arviointia koskeva hakemus valitsemalleen ilmoitetulle laitokselle.

Hakemuksen on sisällettävä:

– valmistajan nimi ja osoite sekä valtuutetun edustajan nimi ja osoite, jos tämä tekee hakemuksen;

– tekniset asiakirjat yhdestä mallista kutakin valmistettavaksi tai kehitettäväksi kaavailtujen digitaalisia elementtejä sisältävien tuotteiden ryhmää kohti. Teknisten asiakirjojen on kaikissa soveltuvissa tapauksissa sisällettävä ainakin liitteessä VII esitetyt tekijät;

– laatujärjestelmää koskevat asiakirjat; ja

– kirjallinen vakuutus siitä, että samaa hakemusta ei ole tehty toiselle ilmoitetulle laitokselle.

3.2. Laatujärjestelmän on varmistettava, että digitaalisia elementtejä sisältävät tuotteet täyttävät liitteessä I olevassa I osassa vahvistetut olennaiset kyberturvallisuusvaatimukset ja että valmistajan käyttöön ottamat haavoittuvuuksien käsittelyprosessit täyttävät liitteessä I olevassa II osassa vahvistetut vaatimukset.

Kaikki valmistajan käyttöön ottamat tekijät, vaatimukset ja määräykset on kirjattava järjestelmällisesti ja täsmällisesti kirjallisiksi ohjelmiksi, menettelyiksi ja ohjeiksi. Kyseisten laatujärjestelmää koskevien asiakirjojen avulla on voitava tulkita yhdenmukaisesti laatuohjelmia, suunnitelmia, käsikirjoja ja tallenteita.

Niissä on erityisesti oltava riittävä kuvaus seuraavista:

– laatutavoitteet ja organisaation rakenne, johdon vastuualueet ja toimivalta suunnittelun, kehittämisen, tuotteiden laadun ja haavoittuvuuksien käsittelyn osalta;

– sovellettavat tekniset suunnittelu- ja kehityseritelmät, standardit mukaan lukien, ja jos asiaa koskevia yhdenmukaistettuja standardeja tai teknisiä eritelmiä ei noudateta kaikilta osin, käytettävät keinot, joilla varmistetaan, että kyseisiin digitaalisia elementtejä sisältäviin tuotteisiin sovellettavat liitteessä I olevassa I osassa vahvistetut olennaiset kyberturvallisuusvaatimukset täyttyvät;

– sovellettavat menettelylliset eritelmät, standardit mukaan lukien, ja jos asiaa koskevia yhdenmukaistettuja standardeja tai teknisiä eritelmiä ei noudateta kaikilta osin, käytettävät keinot, joilla varmistetaan, että valmistajaan sovellettavat liitteessä I olevassa II osassa vahvistetut olennaiset kyberturvallisuusvaatimukset täyttyvät;

– suunnittelun ja kehittämisen valvonta, mukaan lukien suunnittelun ja kehittämistapojen todentamistekniikat, menetelmät ja järjestelmälliset toimenpiteet, joita käytetään kyseiseen tuoteryhmään kuuluvien digitaalisia elementtejä sisältävien tuotteiden suunnittelussa ja kehittämisessä;

– vastaavat tuotannossa sekä laadunvalvonnassa ja -varmistuksessa käytettävät tekniikat, menetelmät ja järjestelmälliset toimenpiteet;

– ennen tuotantoa, tuotannon aikana ja sen jälkeen tehtävät tarkastukset ja testit sekä niiden suoritustiheys;

– laatupöytäkirjat, kuten tarkastusraportit ja testaus- ja kalibrointitiedot sekä asianomaisen henkilöstön pätevyyteen liittyvät selvitykset;

– keinot, joilla valvotaan tuotteilta ja suunnittelulta vaaditun laadun toteutumista ja laatujärjestelmän toiminnan tehokkuutta.

3.3. Ilmoitetun laitoksen on arvioitava laatujärjestelmä määrittääkseen, täyttääkö se 3.2 kohdassa tarkoitetut vaatimukset.

Ilmoitetun laitoksen on oletettava, että laatujärjestelmän osat, joissa noudatetaan asiaa koskevan yhdenmukaistetun standardin tai teknisen eritelmän käyttöönottamiseksi annetun kansallisen standardin vastaavia eritelmiä, ovat näiden vaatimusten mukaisia.

Sen lisäksi, että auditointiryhmällä on oltava kokemusta laadunhallintajärjestelmistä, ryhmässä on oltava vähintään yksi jäsen, jolla on kokemusta kyseisen tuotealan ja tuoteteknologian arvioimisesta, ja sen on tunnettava tässä asetuksessa vahvistetut sovellettavat vaatimukset. Auditointiin on sisällyttävä tarkastuskäynti valmistajan toimitiloihin, jos sellaisia on. Auditointiryhmän on tarkastettava 3.1 kohdan toisessa luetelmakohdassa tarkoitetut tekniset asiakirjat sen varmistamiseksi, että valmistaja kykenee yksilöimään tässä asetuksessa vahvistetut sovellettavat vaatimukset ja suorittamaan tarvittavat tutkimukset, joiden tarkoituksena on varmistaa, että digitaalisia elementtejä sisältävä tuote on näiden vaatimusten mukainen.

Päätöksestä on ilmoitettava valmistajalle tai tämän valtuutetulle edustajalle.

Ilmoitukseen on sisällyttävä auditoinnin päätelmät ja perusteltu arviointipäätös.

3.4. Valmistaja sitoutuu täyttämään laatujärjestelmästä, sellaisena kuin se on hyväksytty, johtuvat velvollisuudet ja ylläpitämään laatujärjestelmää niin, että se pysyy riittävänä ja tehokkaana.

3.5. Valmistajan on ilmoitettava laatujärjestelmän hyväksyneelle ilmoitetulle laitokselle kaikista laatujärjestelmään suunnitelluista muutoksista.

Ilmoitetun laitoksen on arvioitava ehdotetut muutokset ja päätettävä, täyttääkö muutettu laatujärjestelmä edelleen 3.2 kohdassa tarkoitetut vaatimukset vai onko tarpeen suorittaa uusi arviointi.

Sen on ilmoitettava päätöksestään valmistajalle. Ilmoitukseen on sisällyttävä selvityksen päätelmät ja arviointipäätöksen perustelut.

4. Ilmoitetun laitoksen vastuulla oleva valvonta

4.1. Valvonnan tarkoituksena on varmistaa, että valmistaja täyttää hyväksytystä laatujärjestelmästä aiheutuvat velvollisuutensa asianmukaisesti.

4.2. Valmistajan on sallittava ilmoitetulle laitokselle arviointitarkoituksia varten pääsy suunnittelu-, kehitys-, tuotanto-, tarkastus-, testaus- ja varastotiloihin sekä annettava sille kaikki tarvittavat tiedot, erityisesti

– laatujärjestelmää koskevat asiakirjat;

– laatujärjestelmän suunnittelua koskevaan osaan liittyvät laatupöytäkirjat, kuten tutkimusten, laskelmien ja testien tulokset,

– laatujärjestelmän valmistusta koskevaan osaan liittyvät laatupöytäkirjat, kuten tarkastusraportit ja testaus- ja kalibrointitiedot sekä asianomaisen henkilöstön pätevyyteen liittyvät selvitykset.

4.3. Ilmoitetun laitoksen on tehtävä määräajoin auditointeja varmistaakseen, että valmistaja ylläpitää ja noudattaa laatujärjestelmää, ja toimitettava auditointiraportti valmistajalle.

5. CE-merkintä ja vaatimustenmukaisuusvakuutus

5.1. Valmistajan on kiinnitettävä CE-merkintä sekä 3.1 kohdassa tarkoitetun ilmoitetun laitoksen vastuulla kyseisen laitoksen tunnusnumero kuhunkin yksittäiseen digitaalisia elementtejä sisältävään tuotteeseen, joka täyttää tämän asetuksen liitteessä I olevassa I osassa vahvistetut vaatimukset.

5.2. Valmistajan on laadittava kirjallinen vaatimustenmukaisuusvakuutus kullekin tuotemallille ja pidettävä se kansallisten viranomaisten saatavilla kymmenen vuoden ajan sen jälkeen, kun digitaalisia elementtejä sisältävä tuote on saatettu markkinoille, tai tukiajan ajan sen mukaan, kumpi näistä ajanjaksoista on pidempi. Vaatimustenmukaisuusvakuutuksessa on yksilöitävä tuotemalli, jota varten se on laadittu.

Vaatimustenmukaisuusvakuutuksen jäljennös on toimitettava pyynnöstä asiaankuuluville viranomaisille.

6. Valmistajan on vähintään kymmenen vuoden ajan sen jälkeen, kun digitaalisia elementtejä sisältävä tuote on saatettu markkinoille, tai tukiajan ajan sen mukaan, kumpi näistä ajanjaksoista on pidempi, pidettävä kansallisten viranomaisten saatavilla:

6.1 edellä 3.1 kohdassa tarkoitetut tekniset asiakirjat;

6.2 edellä 3.1 kohdassa tarkoitetut laatujärjestelmää koskevat asiakirjat;

6.3 edellä 3.5 kohdassa tarkoitetut muutokset, sellaisina kuin ne on hyväksytty;

6.4 edellä 3.5 ja 4.3 kohdassa tarkoitetut ilmoitetun laitoksen päätökset ja raportit.

7. Kunkin ilmoitetun laitoksen on annettava ilmoittamisesta vastaavalle viranomaiselleen tiedoksi myönnetyt ja kokonaan peruutetut laatujärjestelmien hyväksynnät, ja sen on asetettava säännöllisesti tai pyynnöstä ilmoittamisesta vastaavan viranomaisensa saataville luettelo laatujärjestelmien hyväksynnöistä, jotka on evätty tai peruutettu toistaiseksi tai joita on muutoin rajoitettu.

Kunkin ilmoitetun laitoksen on annettava muille ilmoitetuille laitoksille tiedoksi laatujärjestelmien hyväksynnät, jotka se on evännyt tai peruuttanut toistaiseksi tai kokonaan, sekä pyynnöstä laatujärjestelmien hyväksynnät, jotka se on antanut.

8. Valtuutettu edustaja

Valmistajan valtuutettu edustaja voi täyttää valmistajan puolesta ja valmistajan vastuulla 3.1, 3.5, 5 ja 6 kohdassa säädetyt valmistajan velvollisuudet sillä edellytyksellä, että asiaankuuluvat velvollisuudet on eritelty toimeksiannossa.

Tämän säädöksen osalta on annettu lausuma, joka on saatavilla virallisessa lehdessä [julkaisutoimisto lisää EUVL C XXX, XX.XX.2024, s. XX] ja seuraavasta linkistä: [julkaisutoimisto lisää linkin lausumaan].