EUROOPAN
KOMISSIO

Strasbourg 18.4.2023
COM(2023) 208 final

2023/0108 (COD)

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS

asetuksen (EU) 2019/881 muuttamisesta tietoturvapalvelujen osalta

(ETA:n kannalta merkityksellinen teksti)

PERUSTELUT

1. EHDOTUKSEN TAUSTA

• Ehdotuksen perustelut ja tavoitteet

Nämä perustelut liittyvät ehdotukseen Euroopan parlamentin ja neuvoston asetukseksi asetuksen (EU) 2019/881[1] muuttamisesta tietoturvapalvelujen osalta.

Ehdotettujen kohdennettujen muutosten tarkoituksena on mahdollistaa komission täytäntöönpanosäädöksillä eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien hyväksyminen ”tietoturvapalveluille” niiden tieto- ja teknologiatuotteiden, -palvelujen ja -prosessien lisäksi, jotka kuuluvat jo kyberturvallisuusasetuksen soveltamisalaan. Tietoturvapalveluilla on yhä tärkeämpi rooli kyberturvallisuuspoikkeamien ehkäisemisessä ja lieventämisessä.

Euroopan unionin kybertoimien kehittämisestä 23. toukokuuta 2022 antamissaan päätelmissä[2] neuvosto kehotti unionia ja jäsenvaltioita tehostamaan yleistä kyberturvatasoa parantavia toimia esimerkiksi helpottamalla luotettavien kyberturvallisuuspalvelujen tarjoajien tuloa alalle. Neuvosto korosti, että tällaisten palveluntarjoajien kehittämisen kannustamisen olisi oltava unionin teollisuuspolitiikan prioriteetti kyberturvallisuuden alalla. Se myös pyysi komissiota ehdottamaan vaihtoehtoja, joilla edistetään luotettavan kyberturvallisuuspalvelualan kehittymistä. Tietoturvapalveluntarjoajien sertifiointi on tehokas keino lisätä luottamusta näiden palvelujen laatuun ja siten edistää luotettavan eurooppalaisen kyberturvallisuuspalvelualan syntymistä.

Komission ja korkean edustajan 10. marraskuuta 2022 antamassa yhteisessä tiedonannossa ”EU:n kyberpuolustuspolitiikka”[3] ilmoitettiin, että komissio aikoo tarkastella EU:n tason kyberturvallisuuden sertifiointijärjestelmien kehittämistä kyberturvallisuustoimialalle ja yksityisille yrityksille. Tietoturvapalveluntarjoajilla on myös tärkeä rooli EU:n kyberturvallisuusreservissä, jonka asteittaista perustamista tuetaan tämän asetuksen kanssa rinnakkain ehdotettavalla kybersolidaarisuussäädöksellä. EU:n kyberturvallisuusreserviä on tarkoitus käyttää tukemaan merkittävien ja laajamittaisten kyberturvallisuuspoikkeamien hallintaa ja niiden jälkeisiä välittömiä palautumistoimia. Tässä ehdotuksessa ”tietoturvapalveluilla” tarkoitetaan kybersolidaarisuussäädöksessä tarkoitettuja ”luotettavien palveluntarjoajien” asiaankuuluvia kyberturvallisuuspalveluja.

Jotkin jäsenvaltiot ovat jo alkaneet ottaa käyttöön tietoturvapalvelujen sertifiointijärjestelmiä. Näin ollen riski tietoturvapalveluiden sisämarkkinoiden pirstoutumisesta kasvaa eri puolilla unionia käytössä olevien kyberturvallisuuden sertifiointijärjestelmien epäjohdonmukaisuuksien vuoksi. Tämä ehdotus mahdollistaa eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien luomisen kyseisille palveluille markkinoiden pirstoutumisen estämiseksi.

• Yhdenmukaisuus muiden alaa koskevien politiikkojen säännösten kanssa

Tämä ehdotus on yhdenmukainen sen kyberturvallisuusasetuksen kanssa, jota sillä muutetaan. Se perustuu kyseisen asetuksen säännöksiin ja mukauttaa niitä niin, että niihin sisällytetään

---

[1] 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).

[2] 9364/22.

[3] JOIN(2022) 49 final.

myös tietoturvapalvelut. Ehdotetut muutokset rajoittuvat siihen, mikä on ehdottoman välttämätöntä, eivätkä ne muuta kyberturvallisuusasetuksen ominaisuuksia tai toimintaa.

Tämä ehdotus on myös yhdenmukainen 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 14 päivänä joulukuuta 2022 annetun Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 (NIS 2 -direktiivi)[4] kanssa. Tietoturvapalveluntarjoajia pidetään direktiivin (EU) 2022/2555 mukaiseen erittäin kriittiseen toimialaan kuuluvina keskeisinä tai tärkeinä toimijoina. Kyseisen direktiivin johdanto-osan 86 kappaleen mukaan palveluntarjoajista erityisen tärkeällä sijalla ovat muun muassa poikkeamanhallintaa, tunkeutumisenestotestausta, turvallisuusauditointeja ja konsultointia tarjoavat tietoturvapalveluntarjoajat, jotka avustavat toimijoita niiden pyrkiessä ehkäisemään, havaitsemaan ja hallitsemaan poikkeamia tai palautumaan niistä. Tietoturvapalveluntarjoajat ovat kuitenkin myös itse olleet kyberhyökkäysten kohteena, ja ne muodostavat erityisen riskin, koska ne ovat tiiviisti integroituneet asiakkaidensa toimintaan. Direktiivissä (EU) 2022/2555 tarkoitettujen keskeisten ja tärkeiden toimijoiden olisi sen vuoksi noudatettava erityisen suurta huolellisuutta tietoturvapalveluntarjoajaa valitessaan.

Tällä ehdotuksella pyritään parantamaan tietoturvapalvelujen laatua ja vertailukelpoisuutta. Näin keskeiset ja tärkeät toimijat voivat tietoturvapalveluntarjoajaa valitessaan noudattaa direktiivissä (EU) 2022/2555 edellytettyä erityisen suurta huolellisuutta. Lisäksi tässä ehdotuksessa oleva ”tietoturvapalvelujen” määritelmä on johdettu direktiivissä (EU) 2022/2555 olevasta ”tietoturvapalveluntarjoajan” määritelmästä ja hyvin samankaltainen. Näistä syistä ehdotus täydentää merkittävästi NIS 2 -direktiiviä.

Tämä ehdotus täydentää myös ehdotettua kybersolidaarisuussäädöstä. Ehdotetussa kybersolidaarisuussäädöksessä säädetään prosessista, jolla valitaan palveluntarjoajat EU:n kyberturvallisuusreserviin. Prosessissa olisi muun muassa otettava huomioon, ovatko kyseiset palveluntarjoajat saaneet eurooppalaisen tai kansallisen kyberturvallisuussertifioinnin. Tietoturvapalvelujen tulevilla sertifiointijärjestelmillä on näin ollen merkittävä rooli kybersolidaarisuussäädöksen täytäntöönpanossa.

- **Yhdenmukaisuus unionin muiden politiikkojen kanssa**

Tämä ehdotus ei vaikuta kyberturvallisuusasetuksen johdonmukaisuuteen asetuksen (EU) 2016/679[5], jäljempänä ’yleinen tietosuoja-asetus’, tai siinä olevien säännösten kanssa, jotka koskevat sellaisten sertifiointimekanismien ja tietosuojasinettien ja -merkkien käyttöön ottamista, joilla osoitetaan, että rekisterinpitäjät ja henkilötietojen käsittelijät noudattavat tätä asetusta käsittelytoimia suorittaessaan. Kyberturvallisuusasetus ei jatkossakaan rajoita tietojenkäsittelytoimintojen sertifiointia yleisen tietosuoja-asetuksen mukaisesti, ei myöskään silloin, kun nämä toimet on sisällytetty tuotteisiin ja palveluihin.

Tämä ehdotus ei myöskään vaikuta kyberturvallisuusasetuksen yhteensopivuuteen akkreditointi- ja markkinavalvontavaatimuksia koskevan asetuksen (EY) N:o 765/2008[6] kanssa, etenkään kansallisia akkreditointielimiä ja vaatimustenmukaisuuden arviointilaitoksia tai kansallisia sertifioinnin valvontaviranomaisia koskevan kehyksen osalta.

---

4 EUVL L 333, 27.12.2022, s. 810.
5 EUVL L 119, 4.5.2016, s. 1.
6 EUVL L 218, 13.8.2008, s. 30.

2. OIKEUSPERUSTA, TOISSIJAISUUSPERIAATE JA SUHTEELLISUUSPERIAATE

- **Oikeusperusta**

Tällä ehdotuksella muutetaan kyberturvallisuusasetusta, joka perustuu Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT-sopimus) 114 artiklaan. Kuten kyberturvallisuusasetuksen tapauksessa, tällä ehdotuksella pyritään välttämään sisämarkkinoiden pirstoutumista erityisesti mahdollistamalla eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien käyttöön ottaminen tietoturvapalveluille. Jäsenvaltiot ovat jo alkaneet ottaa käyttöön kansallisia tietoturvapalvelujen sertifiointijärjestelmiä. Näin ollen on olemassa konkreettinen riski tällaisten palvelujen sisämarkkinoiden pirstoutumisesta, mitä tällä ehdotuksella pyritään estämään. Sen vuoksi tämän aloitteen asianmukainen oikeusperusta on SEUT-sopimuksen 114 artikla.

- **Toissijaisuusperiaate (jaetun toimivallan osalta)**

Tavoitetta mahdollistaa eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien käyttöön ottaminen tietoturvapalveluille ja välttää sisämarkkinoiden pirstoutuminen ei voida saavuttaa kansallisella tasolla vaan ainoastaan unionin tason toimilla. Lisäksi ehdotetun muutoksen kohteena olevien tietoturvapalvelujen tarjoajat sekä niiden suurimmat potentiaaliset asiakkaat toimivat koko unionin laajuisesti. Unionin tason toimet ovat sen vuoksi tarpeellisia ja tehokkaampia kuin kansallisen tason toimet.

- **Suhteellisuusperiaate**

Ehdotus on kohdennettu muutos kyberturvallisuusasetukseen. Se rajoittuu siihen, mikä on ehdottoman välttämätöntä sen tavoitteen saavuttamiseksi eli eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien käyttöönoton mahdollistamiseksi tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien lisäksi myös tietoturvapalveluille. Ehdotetuilla muutoksilla mukautetaan erityisesti eurooppalaisen kyberturvallisuuden sertifiointikehyksen soveltamisalaa siten, että siihen sisällytetään ”tietoturvapalvelut”, määritellään kyseiset palvelut NIS 2 -direktiivin mukaisesti ja muutetaan eurooppalaisen kyberturvallisuuden sertifioinnin turvallisuustavoitteita ”tietoturvapalvelujen” huomioon ottamiseksi. Muut muutokset ovat luonteeltaan teknisiä, ja niiden tarkoituksena on varmistaa, että asiaan liittyviä artikloja sovelletaan myös ”tietoturvapalveluihin”. Ehdotettu aloite on näin ollen oikeassa suhteessa tavoitteeseen nähden.

- **Toimintatavan valinta**

Koska ehdotuksella muutetaan asetusta (EU) 2019/881, asianmukainen oikeudellinen väline on asetus.

3. JÄLKIARVIOINTIEN, SIDOSRYHMIEN KUULEMISTEN JA VAIKUTUSTENARVIOINTIEN TULOKSET

- **Jälkiarvioinnit/toimivuustarkastukset**

Ei sovelleta.

- **Sidosryhmien kuuleminen**

Jäsenvaltioita ja ENISAa on kuultu kohdennetusti. Näissä kuulemisissa jäsenvaltiot kuvailivat tietoturvapalvelujen sertifiointiin liittyviä nykyisiä toimiaan ja näkemyksiään. ENISA selvitti näkemyksiään ja havaintojaan jäsenvaltioiden ja sidosryhmien kanssa käymistään keskusteluista. Jäsenvaltioilta ja ENISAlta saadut huomautukset ja tiedot on otettu huomioon tässä ehdotuksessa.

- **Asiantuntijatiedon keruu ja käyttö**

Ei sovelleta.

- **Vaikutustenarviointi**

Koska ehdotus on hyvin rajallinen ja kohdistettu muutos kyberturvallisuusasetukseen, on pyydetty lupaa jättää vaikutustenarviointi tekemättä. Ehdotuksella annettaisiin komissiolle valta antaa täytäntöönpanosäädöksiä, joilla otetaan käyttöön eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät kyberturvallisuusasetuksen soveltamisalaan jo kuuluvien tieto- ja teknologiatuotteiden, -palvelujen ja -prosessien lisäksi myös ”tietoturvapalveluille”. Muutokset tulisivat kuitenkin voimaan vasta, kun tällaiset sertifiointijärjestelmät hyväksytään myöhemmässä vaiheessa. Muutoksilla ei olisi vaikutusta sertifiointijärjestelmien vapaaehtoisuuteen.

- **Säätelyn toimivuus ja yksinkertaistaminen**

Ei sovelleta.

- **Perusoikeudet**

Ehdotuksella ei ole ennakoituja vaikutuksia perusoikeuksien suojeluun.

4. TALOUSARVIOVAIKUTUKSET

Ei ole.

5. LISÄTIEDOT

- **Toteuttamissuunnitelmat, seuranta, arviointi ja raportointijärjestelyt**

Ehdotuksella muutettavat säännökset arvioidaan osana kyberturvallisuusasetuksen säännöllistä arviointia, jonka komissio suorittaa sen 67 artiklan mukaisesti. Arvioinnissa tarkastellaan myös muun muassa kyberturvallisuuden sertifiointikehystä koskevien säännösten vaikutusta, tehokkuutta ja tuloksellisuutta suhteessa tavoitteisiin varmistaa tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien kyberturvallisuuden riittävä taso unionissa ja parantaa sisämarkkinoiden toimintaa. Ehdotus sisältää muutoksen, jolla varmistetaan, että arviointi kattaa myös tietoturvapalvelut. Komissio toimittaa arviointikertomuksen ja sen päätelmät Euroopan parlamentille, neuvostolle ja ENISAn johtokunnalle ja julkistaa kertomuksen tulokset.

- **Ehdotukseen sisältyvien säännösten yksityiskohtaiset selitykset**

Ehdotuksessa on kaksi artiklaa. Ehdotuksen 1 artikla sisältää muutokset asetukseen (EU) 2019/881. Ehdotuksen 2 artikla koskee voimaantuloa. Ehdotuksen 1 artiklassa esitetään kohdennetut muutokset, joilla muutetaan kyberturvallisuusasetuksessa esitetyn eurooppalaisen kyberturvallisuuden sertifiointikehyksen soveltamisalaa siten, että siihen sisällytetään ”tietoturvapalvelut” (kyberturvallisuusasetuksen 1 ja 46 artikla). Siinä vahvistetaan tällaisten palvelujen määritelmä, joka on hyvin lähellä NIS 2 -direktiivissä olevaa ”tietoturvapalveluntarjoajan” määritelmää (kyberturvallisuusasetuksen 2 artikla). Siinä myös lisätään uusi tietoturvapalveluihin mukautettuja eurooppalaisen kyberturvallisuussertifioinnin turvallisuustavoitteita koskeva 51 a artikla. Lopuksi ehdotukseen sisältyy useita teknisiä

muutoksia, joilla varmistetaan, että asian kannalta merkityksellisiä artikloja sovelletaan myös ”tietoturvapalveluihin”.

2023/0108 (COD)

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS

asetuksen (EU) 2019/881 muuttamisesta tietoturvapalvelujen osalta

(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,

ottavat huomioon alueiden komitean lausunnon,

noudattavat tavallista lainsäätämisjärjestystä,

sekä katsovat seuraavaa:

(1) Euroopan parlamentin ja neuvoston asetuksessa (EU) 2019/881[7] vahvistetaan kehys eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien perustamiselle, jotta voidaan varmistaa riittävän tasoinen kyberturvallisuus tieto- ja viestintätekniikan tuotteille, palveluille ja prosesseille unionissa sekä välttää sisämarkkinoiden pirstoutuminen unionissa kyberturvallisuuden sertifiointijärjestelmien osalta.

(2) Tietoturvapalvelut ovat palveluja, jotka koostuvat asiakkaiden kyberturvallisuusriskien hallintaan liittyvien toimien toteuttamisesta tai niissä avustamisesta, ja ne ovat tulleet yhä tärkeämmiksi kyberturvallisuuspoikkeamien ehkäisemisessä ja lieventämisessä. Näin ollen kyseisten palvelujen tarjoajia pidetään Euroopan parlamentin ja neuvoston direktiivissä (EU) 2022/2555[8] tarkoitettuina erittäin kriittisen toimialan keskeisinä tai tärkeinä toimijoina. Kyseisen direktiivin johdanto-osan 86 kappaleen mukaan palveluntarjoajista erityisen tärkeällä sijalla ovat muun muassa poikkeamanhallintaa, tunkeutumisenestotestausta, turvallisuusauditointeja ja konsultointia tarjoavat tietoturvapalveluntarjoajat, jotka avustavat toimijoita niiden pyrkiessä ehkäisemään, havaitsemaan ja hallitsemaan poikkeamia tai palautumaan niistä.

[7] 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).

[8] 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).

Tietoturvapalveluntarjoajat ovat kuitenkin myös itse olleet kyberhyökkäysten kohteena, ja ne muodostavat erityisen riskin, koska ne ovat tiiviisti integroituneet asiakkaidensa toimintaan. Direktiivissä (EU) 2022/2555 tarkoitettujen keskeisten ja tärkeiden toimijoiden olisi sen vuoksi noudatettava erityisen suurta huolellisuutta tietoturvapalveluntarjoajaa valitessaan.

(3) Tietoturvapalveluntarjoajilla on myös tärkeä rooli EU:n kyberturvallisuusreservissä, jonka asteittaista perustamista tuetaan [toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten] annetulla asetuksella (EU) .../.... EU:n kyberturvallisuusreserviä on määrä käyttää tukemaan merkittävien ja laajamittaisten kyberturvallisuuspoikkeamien hallintaa ja niiden jälkeisiä välittömiä palautumistoimia. [Toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten] annetulla asetuksella (EU) .../... säädetään prosessista, jolla palveluntarjoajat valitaan EU:n kyberturvallisuusreserviin ja jossa olisi muun muassa otettava huomioon, ovatko kyseiset palveluntarjoajat saaneet eurooppalaisen tai kansallisen kyberturvallisuussertifioinnin. [Toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten] annetun asetuksen (EU) .../... mukaiset ”luotettavien palveluntarjoajien” tarjoamat asiaankuuluvat palvelut vastaavat tämän asetuksen mukaisia tietoturvapalveluja.

(4) Tietoturvapalvelujen sertifiointi ei ole merkityksellistä ainoastaan EU:n kyberturvallisuusreservin valintaprosessissa, vaan se on myös olennainen laatuindikaattori yksityisille ja julkisille tahoille, jotka aikovat hankkia tällaisia palveluja. Kun otetaan huomioon miten kriittisiä tietoturvapalvelut ovat ja miten arkaluonteisia tietoja niissä käsitellään, sertifioinnilla voitaisiin antaa mahdollisille asiakkaille tärkeää tietoa ja lisätä varmuutta näiden palvelujen luotettavuudesta. Tietoturvapalvelujen eurooppalaiset sertifiointijärjestelmät auttavat välttämään sisämarkkinoiden pirstoutumista. Sen vuoksi tällä asetuksella pyritään parantamaan sisämarkkinoiden toimintaa.

(5) Tietoturvapalvelut tarjoavat tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien käyttöönoton lisäksi usein lisäpalveluja, jotka perustuvat niiden henkilöstön osaamiseen, asiantuntemukseen ja kokemukseen. Osaamisen, asiantuntemuksen ja kokemuksen erittäin korkean tason sekä asianmukaisten sisäisten menettelyjen olisi oltava osa turvallisuustavoitteita, jotta voidaan varmistaa tarjottujen tietoturvapalvelujen erittäin korkea laatu. Asetusta (EU) 2019/881 on tarpeen muuttaa sen varmistamiseksi, että sertifiointijärjestelmä kattaa kaikki tietoturvapalveluihin liittyvät näkökohdat.

Euroopan tietosuojavaltuutettua on kuultu Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1725 42 artiklan 1 kohdan mukaisesti, ja hän on antanut lausuntonsa PP päivänä KKkuuta VVVV,

OVAT HYVÄKSYNEET TÄMÄN ASETUKSEN:

1 artikla

Asetuksen (EU) 2019/881 muuttaminen

Muutetaan asetus (EU) 2019/881 seuraavasti:

1) Korvataan 1 artiklan 1 kohdan ensimmäisen alakohdan b alakohta seuraavasti:

”b) vahvistetaan kehys eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien perustamiselle, jotta voidaan varmistaa riittävän tasoinen kyberturvallisuus tieto- ja viestintätekniikan tuotteille, palveluille ja prosesseille sekä tietoturvapalveluille unionissa sekä välttää sisämarkkinoiden hajautuminen unionissa kyberturvallisuuden sertifiointijärjestelmien osalta.”

2) Muutetaan 2 artikla seuraavasti:

a) korvataan 9, 10 ja 11 alakohta seuraavasti:

”9) ’eurooppalaisella kyberturvallisuuden sertifiointijärjestelmällä’ unionin tasolla vahvistettua kattavaa sellaisten sääntöjen, teknisten vaatimusten, standardien ja menettelyjen muodostamaa kokonaisuutta, joita sovelletaan tiettyjen tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sekä tietoturvapalvelujen sertifiointiin tai vaatimustenmukaisuuden arviointiin;

10) ’kansallisella kyberturvallisuuden sertifiointijärjestelmällä’ kansallisen viranomaisen kehittämää ja käyttöön ottamaa kattavaa sellaisten sääntöjen, teknisten vaatimusten, standardien ja menettelyjen kokonaisuutta, joita sovelletaan kyseisen erityisen järjestelmän kattamien tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sekä tietoturvapalvelujen sertifiointiin tai vaatimustenmukaisuuden arviointiin;

11) ’eurooppalaisella kyberturvallisuussertifikaatilla’ asiaa koskevan elimen myöntämää asiakirjaa, jolla todistetaan, että tietty tieto- ja viestintätekniikan tuote, palvelu tai prosessi tai tietoturvapalvelu on arvioitu eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä vahvistettujen erityisten turvallisuusvaatimusten mukaiseksi;”

b) lisätään alakohta seuraavasti:

”14 a) ’tietoturvapalvelulla’ palvelua, joka koostuu kyberturvallisuusriskien hallintaan liittyvien toimien toteuttamisesta tai niissä avustamisesta, mukaan lukien poikkeamiin reagointi, tunkeutumisenestotestaus, turvallisuustarkastukset ja konsultointi;”

c) korvataan 20, 21 ja 22 alakohta seuraavasti:

”20) ’*teknisellä eritelmällä*’ asiakirjaa, jossa määrätään tekniset vaatimukset, jotka tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin tai tietoturvapalvelun on täytettävä, tai vaatimustenmukaisuuden arviointimenettelyt liittyen tällaiseen tuotteeseen, palveluun, prosessiin tai tietoturvapalveluun;

21) ’varmuustasolla’ perustaa luottamukselle sen osalta, että tietty tieto- ja viestintätekniikan tuote, palvelu tai prosessi tai tietoturvapalvelu täyttää tietyn eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaiset turvallisuusvaatimukset; varmuustaso osoittaa myös, millä tasolla tieto- ja viestintätekniikan tuotetta, palvelua tai prosessia tai tietoturvapalvelua on arvioitu; varmuustaso ei sellaisenaan ilmaise itse tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin tai tietoturvapalvelun turvallisuutta;

22) 'vaatimustenmukaisuuden itsearvioinnilla' tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien tai tietoturvapalvelujen valmistajan tai tarjoajan toimintaa, jossa arvioidaan sitä, täyttävätkö kyseiset tieto- ja viestintätekniikan tuotteet, palvelut tai prosessit tai tietoturvapalvelut tietyn eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimukset."

3) Korvataan 4 artiklan 6 kohta seuraavasti:

"6. ENISA edistää eurooppalaisen sertifioinnin käyttöä, jotta voidaan välttää sisämarkkinoiden hajanaisuus. ENISA edistää eurooppalaisen kyberturvallisuuden sertifiointikehyksen perustamista ja ylläpitoa tämän asetuksen III osaston mukaisesti, jotta voidaan lisätä avoimuutta tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sekä tietoturvapalvelujen kyberturvallisuuden varmistuksessa ja tällä tavoin vahvistaa luottamusta digitaalisiin sisämarkkinoihin ja parantaa niiden kilpailukykyä."

4) Muutetaan 8 artikla seuraavasti:

a) korvataan 1 kohta seuraavasti:

"1. ENISA tukee ja edistää tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sekä tietoturvapalvelujen kyberturvallisuussertifiointiin liittyvän, tämän asetuksen III osastossa vahvistetun unionin politiikan kehittämistä ja täytäntöönpanoa tehtävänään

a) seurata jatkuvasti asiaan liittyvien standardointialojen kehitystä ja suositella asianmukaisia teknisiä eritelmiä käytettäväksi eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien kehittämisessä 54 artiklan 1 kohdan c alakohdassa tarkoitetulla tavalla tapauksissa, joissa standardeja ei ole saatavilla;

b) valmistella ehdolla olevat eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät, jäljempänä 'ehdolla olevat järjestelmät', tieto- ja viestintätekniikan tuotteille, palveluille ja prosesseille sekä tietoturvapalveluille 49 artiklan mukaisesti;

c) arvioida hyväksyttyjä eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä 49 artiklan 8 kohdan mukaisesti;

d) osallistua vertaisarviointeihin 59 artiklan 4 kohdan mukaisesti;

e) avustaa komissiota toimimalla Euroopan kyberturvallisuuden sertifiointiryhmän sihteeristönä 62 artiklan 5 kohdan mukaisesti;"

b) korvataan 3 kohta seuraavasti:

"3. ENISA kokoaa ja julkaisee ohjeita ja laatii hyviä käytäntöjä, jotka koskevat tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sekä tietoturvapalvelujen kyberturvallisuusvaatimuksia, yhteistyössä kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten ja toimialan kanssa virallisella, jäsennellyllä ja avoimella tavalla;"

c) korvataan 5 kohta seuraavasti:

"5. ENISA helpottaa tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sekä tietoturvapalvelujen riskinhallintaan ja turvallisuuteen

liittyvien eurooppalaisten ja kansainvälisten standardien laatimista ja käyttöönottoa;”

5) Korvataan 46 artiklan 1 ja 2 kohta seuraavasti:

”1. Eurooppalainen kyberturvallisuuden sertifiointikehys perustetaan, jotta voidaan nostaa kyberturvallisuustasoa unionissa ja yhdenmukaistaa eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät unionin tasolla ja siten parantaa sisämarkkinoiden toimintaedellytyksiä digitaalisten sisämarkkinoiden luomiseksi tieto- ja viestintätekniikan tuotteille, palveluille ja prosesseille sekä tietoturvapalveluille.

2. Eurooppalaisessa kyberturvallisuuden sertifiointikehyksessä vahvistetaan mekanismi, jonka avulla laaditaan eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä. Siinä annetaan vahvistus siitä, että tällaisten järjestelmien mukaisesti arvioidut tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit ovat niille määritettyjen turvallisuusvaatimusten mukaisia, jotta voidaan suojella tallennettavien, siirrettävien tai käsiteltävien tietojen tai kyseisissä tuotteissa, palveluissa ja prosesseissa tarjottavien tai välitettävien toimintojen tai palvelujen käytettävyyttä, aitoutta, eheyttä ja luottamuksellisuutta niiden koko elinkaaren ajan. Lisäksi siinä annetaan vahvistus siitä, että tällaisten järjestelmien mukaisesti arvioidut tietoturvapalvelut ovat niille määritettyjen turvallisuusvaatimusten mukaisia, jotta voidaan suojella kyseisten palvelujen tarjoamisen yhteydessä saatavien, käsiteltävien, tallennettavien tai siirrettävien tietojen käytettävyyttä, aitoutta, eheyttä ja luotettavuutta, että kyseisiä palveluja tarjotaan jatkuvasti ja että niistä vastaavalla henkilöstöllä on vaadittava osaaminen, asiantuntemus ja kokemus sekä erittäin korkeatasoinen tekninen tietämys ja ammatillinen luotettavuus.”

6) Korvataan 47 artiklan 2 ja 3 kohta seuraavasti:

”2. Unionin jatkuvaan työohjelmaan on sisällyttävä erityisesti luettelo sellaisista tieto- ja viestintätekniikan tuotteista, palveluista ja prosesseista tai niiden luokista sekä tietoturvapalveluista, joille voi olla hyötyä eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan kuulumisesta.

3. Tietyn tieto- ja viestintätekniikan tuotteen, palvelun ja prosessin tai niiden luokan tai tietoturvapalvelun sisällyttäminen unionin jatkuvaan työohjelmaan on perusteltava jollakin seuraavista:

a) tiettyä tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien luokkaa tai tietoturvapalveluja koskevien kansallisten kyberturvallisuuden sertifiointijärjestelmien saatavuus tai kehittäminen, erityisesti siltä osin, onko uhkana syntyä hajanaisuutta;

b) asiaa koskevat unionin tai jäsenvaltion politiikat tai lainsäädäntö;

c) markkinoiden kysyntä;

d) kyberuhkaympäristön kehitys;

e) Euroopan kyberturvallisuuden sertifiointiryhmän esittämä pyyntö valmistella ehdolla oleva järjestelmä.”

7) Korvataan 49 artiklan 7 kohta seuraavasti:

”7. Komissio voi ENISAn valmisteleman ehdolla olevan järjestelmän pohjalta hyväksyä täytäntöönpanosäädöksiä tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sekä tietoturvapalvelujen eurooppalaisesta kyberturvallisuuden sertifiointijärjestelmästä, joka täyttää 51, 52 ja 54 artiklassa esitetyt vaatimukset. Nämä täytäntöönpanosäädökset hyväksytään 66 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.”

8) Muutetaan 51 artikla seuraavasti:

a) korvataan otsikko seuraavasti:

Tieto- ja viestintätekniikan tuotteisiin, palveluihin ja prosesseihin sovellettavien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien turvallisuustavoitteet

b) korvataan johdantokappale seuraavasti:

”Tieto- ja viestintätekniikan tuotteisiin, palveluihin tai prosesseihin sovellettava eurooppalainen kyberturvallisuuden sertifiointijärjestelmä olisi suunniteltava täyttämään soveltuvin osin vähintään seuraavat turvallisuustavoitteet:”

9) Lisätään artikla seuraavasti:

”51 a artikla

Tietoturvapalveluihin sovellettavien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien turvallisuustavoitteet

Tietoturvapalveluihin sovellettava eurooppalainen kyberturvallisuuden sertifiointijärjestelmä olisi suunniteltava täyttämään soveltuvin osin vähintään seuraavat turvallisuustavoitteet:

a) varmistetaan, että tietoturvapalveluiden tarjoajalla on vaadittava osaaminen, asiantuntemus ja kokemus, mukaan lukien sen varmistaminen, että näiden palvelujen tarjoamisesta vastaavalla henkilöstöllä on erittäin korkeatasoinen erikoisalan tekninen tietämys ja pätevyys, riittävä ja asianmukainen kokemus sekä mahdollisimman korkeatasoinen ammatillinen luotettavuus;

b) varmistetaan, että palveluntarjoajalla on käytössään asianmukaiset sisäiset menettelyt sen varmistamiseksi, että tarjotut tietoturvapalvelut ovat kaikkina aikoina erittäin korkealaatuisia;

c) suojataan tietoturvapalvelujen tarjoamisen yhteydessä saatavat, tallennettavat, siirrettävät tai muutoin käsiteltävät tiedot vahingossa tapahtuvalta tai luvattomalta käytöltä, tallentamiselta, luovuttamiselta,

tuhoamiselta, muulta käsittelyltä, hävittämiseltä tai muuttamiselta taikka saatavuuden rajoittamiselta;

d) varmistetaan, että tietojen, palvelujen ja toimintojen saatavuus ja käytettävyys palautetaan mahdollisimman pian fyysisen tai teknisen poikkeaman sattuessa;

e) varmistetaan, että valtuutettujen henkilöiden, ohjelmien tai koneiden saatavilla on ainoastaan ne tiedot, palvelut tai toiminnot, joihin näillä on käyttöoikeudet;

f) kirjataan, mitä tietoja, palveluja tai toimintoja on käytetty, hyödynnetty tai muutoin käsitelty, mihin aikaan ja kenen toimesta ja mahdollistetaan näiden tietojen tarkastaminen;

g) varmistetaan, että tietoturvapalveluiden tarjoamiseen käytettävät tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit [sekä laitteistot] ovat oletusarvoisesti ja sisäänrakennetusti turvallisia, että niissä ei ole tunnettuja haavoittuvuuksia ja että niihin on tehty uusimmat turvallisuuspäivitykset.”

10) Muutetaan 52 artikla seuraavasti:

a) korvataan 1 kohta seuraavasti:

”1. Eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan määritellä tieto- ja viestintätekniikan tuotteille, palveluille ja prosesseille sekä tietoturvapalveluille yksi tai useampi seuraavista varmuustasoista: ”perustaso”, ”korotettu” tai ”korkea”. Varmuustason on vastattava tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin tai tietoturvapalvelun käyttötarkoitukseen liittyvän riskin tasoa, joka perustuu mahdollisen poikkeaman todennäköisyyteen ja vaikutuksiin.”

b) korvataan 3 kohta seuraavasti:

”3. Kunkin varmuustason osalta on asianomaisessa eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä täsmennettävä turvallisuusvaatimukset, jotka vastaavat kyseistä varmuustasoa, mukaan lukien vastaavat turvallisuustoiminnot, ja niitä vastaava suoritettavan tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin tai tietoturvapalvelun arvioinnin tiukkuuden ja kattavuuden taso.”

c) korvataan 5, 6 ja 7 kohta seuraavasti:

”5. Varmuustasoon ”perustaso” viittaavan eurooppalaisen kyberturvallisuussertifikaatin tai EU-vaatimustenmukaisuusilmoituksen on annettava varmuus siitä, että tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit sekä tietoturvapalvelut, joille kyseinen sertifikaatti on annettu tai joista EU-vaatimustenmukaisuusilmoitus on tehty, täyttävät vastaavat turvallisuusvaatimukset, myös turvallisuustoimintojen osalta, ja että ne on arvioitu tasolla, joka on tarkoitettu tunnettujen perustason poikkeamien ja kyberhyökkäysten tunnettujen perusriskien minimoimiseksi. Toteutettavassa arvioinnissa on vähintään arvioitava tekniset asiakirjat. Jos tällainen arviointi ei ole asianmukainen, on käytettävä vaikutukseltaan vastaavia korvaavia arviointitoimia.

6. Varmuustasoon ”korotettu” viittaava eurooppalainen kyberturvallisuussertifikaatti antaa varmuuden siitä, että tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit sekä tietoturvapalvelut, joille kyseinen sertifikaatti on annettu, täyttävät vastaavat turvallisuusvaatimukset, myös turvallisuustoimintojen osalta, ja että ne on arvioitu tasolla, joka on tarkoitettu tunnettujen kyberriskien ja poikkeamien sekä sellaisten tahojen, joilla on niukat kyvyt ja resurssit, tekemien kyberhyökkäysten vaikutusten muodostaman riskin minimoimiseen. Toteutettaviin arviointitoimiin on sisällyttävä vähintään seuraavat toimet: tarkastelu, jolla osoitetaan, että julkisesti tiedossa olevia haavoittuvuuksia ei ole, ja testaus, jolla osoitetaan, että kyseiset tieto- ja viestintätekniikan tuotteet, palvelut tai prosessit tai tietoturvapalvelut toteuttavat välttämättömän turvallisuustoiminnon oikein. Jos tällaiset arviointitoimet eivät ole asianmukaisia, on toteutettava vaikutukseltaan vastaavia korvaavia arviointitoimia.

7. Varmuustasoon ”korkea” viittaava eurooppalainen kyberturvallisuussertifikaatti antaa varmuuden siitä, että tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit sekä tietoturvapalvelut, joille kyseinen sertifikaatti on annettu, täyttävät vastaavat turvallisuusvaatimukset, myös turvallisuustoimintojen osalta, ja että ne on arvioitu tasolla, joka on tarkoitettu sellaisten tahojen, joilla on merkittävät kyvyt ja resurssit, tekemien uusinta tekniikkaa hyödyntävien kyberhyökkäysten riskin minimoimiseen. Toteutettaviin arviointitoimiin on sisällyttävä vähintään seuraavat toimet: tarkastelu, jolla osoitetaan, että julkisesti tiedossa olevia haavoittuvuuksia ei ole; testaus, jolla osoitetaan, että kyseiset tieto- ja viestintätekniikan tuotteet, palvelut tai prosessit tai tietoturvapalvelut toteuttavat uusimman tekniikan mukaiset välttämättömät turvallisuustoiminnot oikein; ja arviointi tunkeutumisenestotestauksen avulla kyseisten prosessien, tuotteiden tai palvelujen tai tietoturvapalvelujen kyvystä vastustaa kyvykkäitä hyökkääjiä. Jos tällaiset arviointitoimet eivät ole riittäviä, on toteutettava vaikutukseltaan vastaavia korvaavia toimia.”

11) Korvataan 53 artiklan 1, 2 ja 3 kohta seuraavasti:

”1. Eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan sallia, että vaatimustenmukaisuuden itsearviointi on yksinomaan tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sekä tietoturvapalvelujen valmistajan tai tarjoajan vastuulla. Vaatimustenmukaisuuden itsearviointia voidaan soveltaa vain sellaisiin tieto- ja viestintätekniikan tuotteisiin, palveluihin ja prosesseihin sekä tietoturvapalveluihin, joihin liittyvät riskit ovat vähäisiä ja vastaavat eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien varmuustasoa ”perustaso”.

2. Tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien tai tietoturvapalvelujen valmistaja tai tarjoaja voi antaa EU-vaatimustenmukaisuusilmoituksen, jossa todetaan, että järjestelmässä määriteltyjen vaatimusten täyttyminen on osoitettu. Antamalla tällaisen ilmoituksen tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien tai tietoturvapalvelujen valmistaja tai tarjoaja ottaa vastuun siitä, että tieto- ja viestintätekniikan tuotteet, palvelut tai prosessit tai tietoturvapalvelut ovat kyseisen järjestelmän vaatimusten mukaisia.

3. Tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien tai tietoturvapalvelujen valmistaja tai tarjoaja asettavat EU-vaatimustenmukaisuusilmoituksen, tekniset asiakirjat ja kaikki muut järjestelmässä määriteltyä tieto- ja viestintätekniikan tuotteiden ja palvelujen tai tietoturvapalvelujen vaatimustenmukaisuutta koskevat asiaankuuluvat tiedot 58 artiklassa tarkoitetun kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen saataville asiaankuuluvassa eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä määrätyn ajanjakson ajaksi. Jäljennös EU-vaatimustenmukaisuusilmoituksesta toimitetaan kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle ja ENISAlle.”

12) Muutetaan 54 artiklan 1 kohta seuraavasti:

a) korvataan a alakohta seuraavasti:

”a) sertifiointijärjestelmän kohde ja soveltamisala, mukaan lukien sen kattamien tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sekä tietoturvapalvelujen tyyppi tai luokat;”

b) korvataan j alakohta seuraavasti:

”j) säännöt tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sekä tietoturvapalvelujen eurooppalaisten kyberturvallisuussertifikaattien tai EU-vaatimustenmukaisuusilmoitusten vaatimustenmukaisuuden seurantaa varten ja mekanismit, joilla voidaan osoittaa, että määriteltyjä kyberturvallisuusvaatimuksia noudatetaan jatkuvasti;”

c) korvataan l alakohta seuraavasti:

”l) säännöt seurauksista tapauksissa, joissa tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit sekä tietoturvapalvelut on sertifioitu tai niistä on tehty EU-vaatimustenmukaisuusilmoitus, mutta ne eivät vastaa järjestelmässä määriteltyjä vaatimuksia;”

d) korvataan o alakohta seuraavasti:

”o) sellaisten kansallisten tai kansainvälisten kyberturvallisuuden sertifiointijärjestelmien yksilöinti, jotka kattavat saman tyypin tai samojen luokkien tieto- ja viestintätekniikan tuotteita, palveluja ja prosesseja sekä tietoturvapalveluja, turvallisuusvaatimuksia, arviointiperusteita ja -menetelmiä sekä varmuustasoja;”

e) korvataan q kohta seuraavasti:

”q) EU-vaatimustenmukaisuusilmoituksen, teknisten asiakirjojen ja kaikkien tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien tai tietoturvapalvelujen valmistajan tai tarjoajan toimittamien muiden saataville asetettavien asiaan liittyvien tietojen saatavillaoloaika;”

13) Muutetaan 56 artikla seuraavasti:

a) korvataan 1 kohta seuraavasti:

”1. Tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit sekä tietoturvapalvelut, jotka on sertifioitu jossain 49 artiklan mukaisesti hyväksytyssä eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä, oletetaan kyseisen järjestelmän vaatimusten mukaisiksi.”

b) muutetaan 3 kohta seuraavasti:

i) korvataan ensimmäinen alakohta seuraavasti:

”Komissio arvioi säännöllisesti hyväksyttyjen eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien tehokkuutta ja käyttöastetta sekä sitä, pitäisikö tietystä eurooppalaisesta kyberturvallisuuden sertifiointijärjestelmästä tehdä pakollinen asiaankuuluvan unionin lainsäädännön avulla, jotta varmistetaan, että tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sekä tietoturvapalvelujen kyberturvallisuus on unionissa riittävällä tasolla, ja parannetaan sisämarkkinoiden toimintaa. Ensimmäinen tällainen arviointi on suoritettava viimeistään 31 päivänä joulukuuta 2023 ja sen jälkeen arvioinnit on suoritettava vähintään kahden vuoden välein. Komissio määrittää kyseisten arviointien tulosten perusteella sellaiset voimassa olevan sertifiointijärjestelmän soveltamisalaan kuuluvat tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit sekä tietoturvapalvelut, joiden olisi kuuluttava pakollisen sertifiointijärjestelmän soveltamisalaan.”

ii) muutetaan kolmas alakohta seuraavasti:

aa) korvataan a alakohta seuraavasti:

”a) ottaa huomioon toimenpiteiden vaikutukset tällaisten tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien tai tietoturvapalvelujen valmistajiin tai tarjoajiin sekä käyttäjiin kyseisten toimenpiteiden kustannusten ja kohteena olevien tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien tai tietoturvapalvelujen ennakoidusta parantuneesta turvallisuustasosta johtuvien yhteiskunnallisten tai taloudellisten hyötyjen osalta;”

bb) korvataan d alakohta seuraavasti:

”d) ottaa huomioon täytäntöönpanon määräajat, siirtymätoimenpiteet ja -kaudet, erityisesti siltä osin kuin ne mahdollisesti vaikuttavat tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien tai tietoturvapalvelujen valmistajiin tai tarjoajiin, pk-yritykset mukaan lukien;”

c) korvataan 7 ja 8 kohta seuraavasti:

”7. Luonnollisen henkilön tai oikeushenkilön, joka jättää tieto- ja viestintätekniikan tuotteita, palveluja tai prosesseja tai tietoturvapalveluja sertifioitavaksi, on asetettava 58 artiklassa tarkoitetun kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen, jos eurooppalaisen kyberturvallisuussertifikaatin myöntää kyseinen viranomainen, tai 60 artiklassa tarkoitetun vaatimustenmukaisuuden arviointilaitoksen saataville kaikki sertifiointimenettelyn suorittamiseen tarvittavat tiedot.

8. Eurooppalaisen kyberturvallisuuden sertifikaatin haltijan on ilmoitettava 7 kohdassa tarkoitetulle sertifikaatin myöntävälle viranomaiselle tai elimelle, jos myöhemmin ilmenee sertifioidun tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin tai tietoturvapalvelun turvallisuutta koskevia haavoittuvuuksia tai epäsäännönmukaisuuksia, jotka saattavat vaikuttaa sertifiointiin liittyvien vaatimusten mukaisuuteen. Kyseinen viranomainen tai elin välittää nämä tiedot ilman aiheetonta viivytystä asianomaiselle kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle."

14) Korvataan 57 artiklan 1 ja 2 kohta seuraavasti:

"1. Sellaisia tieto- ja viestintätekniikan tuotteita, palveluja ja prosesseja sekä tietoturvapalveluja varten voimassa olevat kansalliset kyberturvallisuuden sertifiointijärjestelmät ja niihin liittyvät menettelyt, jotka kuuluvat jonkin eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan, lakkaavat tuottamasta oikeusvaikutuksia alkaen päivästä, joka vahvistetaan 49 artiklan 7 kohdan nojalla hyväksytyssä täytäntöönpanosäädöksessä, sanotun kuitenkaan rajoittamatta tämän artiklan 3 kohdan soveltamista. Sellaisia tieto- ja viestintätekniikan tuotteita, palveluja ja prosesseja sekä tietoturvapalveluja varten voimassa olevat kansalliset kyberturvallisuuden sertifiointijärjestelmät ja niihin liittyvät menettelyt, jotka eivät kuulu jonkin eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan, pysyvät edelleen voimassa.

2. Jäsenvaltiot eivät saa ottaa käyttöön uusia kansallisia kyberturvallisuuden sertifiointijärjestelmiä tieto- ja viestintätekniikan tuotteille, palveluille ja prosesseille tai tietoturvapalveluille, jotka kuuluvat jo jonkin voimassa olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan."

15) Muutetaan 58 artikla seuraavasti:

a) muutetaan 7 kohta seuraavasti:

i) korvataan a ja b alakohta seuraavasti:

"a) valvottava ja pantava täytäntöön yhteistyössä muiden asiaankuuluvien markkinavalvontaviranomaisten kanssa niiden sääntöjen noudattamista, jotka sisältyvät 54 artiklan 1 kohdan j alakohdan mukaisiin eurooppalaisiin kyberturvallisuuden sertifiointijärjestelmiin sen valvomiseksi, noudattavatko tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit sekä tietoturvapalvelut niiden alueilla myönnettyjen eurooppalaisten kyberturvallisuussertifikaattien vaatimuksia;

b) seurattava alueelleen sijoittautuneiden ja vaatimustenmukaisuuden itsearviointia soveltavien tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien tai tietoturvapalvelujen valmistajien tai tarjoajien velvollisuuksien noudattamista ja pantava täytäntöön näitä velvollisuuksia, erityisesti valvottava ja seurattava 53 artiklan 2 ja 3 kohdassa sekä vastaavassa eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä vahvistettujen tällaisten valmistajien tai palveluntarjoajien velvollisuuksien osalta;"

ii) korvataan h alakohta seuraavasti:

”h) tehtävä yhteistyötä muiden kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten tai muiden viranomaisten kanssa esimerkiksi jakamalla tietoa mahdollisista tapauksista, joissa tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit tai tietoturvapalvelut eivät vastaa tämän asetuksen tai yksittäisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien vaatimuksia;”

b) korvataan 9 kohta seuraavasti:

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

16) Korvataan 59 artiklan 3 kohdan b ja c alakohta seuraavasti:

”b) menettelyt, joilla valvotaan ja pannaan täytäntöön säännöt, jotka koskevat sen seuraamista, noudattavatko tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit sekä tietoturvapalvelut eurooppalaisia kyberturvallisuussertifikaatteja 58 artiklan 7 kohdan a alakohdan mukaisesti;

c) menettelyt, joilla seurataan tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien tai tietoturvapalvelujen valmistajien ja tarjoajien velvollisuuksien noudattamista ja pannaan täytäntöön näitä velvollisuuksia 58 artiklan 7 kohdan b alakohdan mukaisesti;”

17) Korvataan 67 artiklan 2 ja 3 kohta seuraavasti:

”2. Arvioinnissa arvioidaan myös tämän asetuksen III osaston säännösten vaikutusta, tehokkuutta ja tuloksellisuutta suhteessa tavoitteisiin varmistaa tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sekä tietoturvapalvelujen kyberturvallisuuden riittävä taso unionissa ja parantaa sisämarkkinoiden toimintaa.

3. Arvioinnissa arvioidaan, ovatko sisämarkkinoille pääsyä koskevat keskeiset kyberturvallisuusvaatimukset tarpeen, jotta voidaan estää sellaisten tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sekä tietoturvapalveluiden pääsy unionin markkinoille, jotka eivät täytä kybertuvallisuuden perusvaatimuksia.”

2 artikla

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

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

Tehty Strasbourgissa

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puhemies	*Puheenjohtaja*