2025/37

15.1.2025

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2025/37,

annettu 19 päivänä joulukuuta 2024,

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 ([1]),

ovat kuulleet alueiden komiteaa,

noudattavat tavallista lainsäätämisjärjestystä ([2]),

sekä katsovat seuraavaa:

(1) Euroopan parlamentin ja neuvoston asetuksessa (EU) 2019/881 ([3]) 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) Jotta voidaan varmistaa unionin kestävyys kyberhyökkäyksiä vastaan ja ehkäistä haavoittuvuuksia sisämarkkinoilla, tällä asetuksella on tarkoitus täydentää horisontaalista sääntelykehystä, jossa vahvistetaan kattavat kyberturvavaatimukset digitaalisia elementtejä sisältäville tuotteille Euroopan parlamentin ja neuvoston asetuksen (EU) 2024/2847 ([4]) nojalla, säätämällä turvallisuustavoitteista tietoturvapalveluille sekä kyseisten palvelujen soveltamiselle ja luotettavuudelle.

(3) Tietoturvapalveluja tarjoavat Euroopan parlamentin ja neuvoston direktiivin (EU) 2022/2555 ([5]) 6 artiklan 40 alakohdassa määritellyt tietoturvapalveluntarjoajat. Tämän vuoksi tässä asetuksessa olevan tietoturvapalvelujen määritelmän olisi oltava johdonmukainen direktiivissä (EU) 2022/2555 olevan tietoturvapalveluntarjoajan määritelmän kanssa. Kyseiset palvelut koostuvat asiakkaiden kyberturvallisuusriskien hallintaan liittyvien toimien toteuttamisesta tai niissä avustamisesta, ja ne ovat tulleet yhä tärkeämmiksi poikkeamien ehkäisemisessä ja lieventämisessä. Näin ollen kyseisten palvelujen tarjoajia pidetään direktiivissä (EU) 2022/2555 tarkoitettuina erittäin kriittisen toimialan keskeisinä tai tärkeinä toimijoina. Kyseisen direktiivin johdanto-osan 86 kappaleen mukaan erityisen tärkeällä sijalla ovat muun muassa poikkeamanhallintaa, tunkeutumistestausta, 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. Sen vuoksi on tärkeää, että direktiivissä (EU) 2022/2555 tarkoitetut keskeiset ja tärkeät toimijat noudattavat erityisen suurta huolellisuutta tietoturvapalveluntarjoajia valitessaan.

([1]) EUVL C 349, 29.9.2023, s. 167.

([2]) Euroopan parlamentin kanta, vahvistettu 24. huhtikuuta 2024 (ei vielä julkaistu virallisessa lehdessä), ja neuvoston päätös, tehty 2. joulukuuta 2024.

([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 asetus (EU) 2024/2847, annettu 23 päivänä lokakuuta 2024, digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) N:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta (kyberkestävyyssäädös) (EUVL L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([5]) 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) Tässä asetuksessa oleva tietoturvapalvelujen määritelmä sisältää ei-tyhjentävän luettelon tietoturvapalveluista, joihin voitaisiin soveltaa eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä, kuten poikkeamien käsittely, tunkeutumistestaus, turvallisuusauditoinnit ja tekniseen tukeen liittyvä konsultointi. Tietoturvapalveluihin voisi sisältyä kyberturvallisuuspalveluja, jotka tukevat poikkeamiin varautumista, niiden ehkäisemistä, havaitsemista, analysointia, lieventämistä, niihin reagoimista ja niistä palautumista. Kyberuhkatiedustelutiedon tarjoaminen ja tekniseen tukeen liittyvä riskinarviointi voitaisiin myös katsoa tietoturvapalveluiksi. Eri tietoturvapalveluihin voitaisiin soveltaa erillisiä eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä. Tällaisten järjestelmien mukaisesti myönnetyissä eurooppalaisissa kyberturvallisuussertifikaateissa olisi viitattava kyseisiä palveluja tarjoavan tietyn palveluntarjoajan tiettyihin tietoturvapalveluihin.

(5) Tietoturvapalveluntarjoajilla voi myös olla tärkeä rooli unionin toimissa, joilla tuetaan reagointia merkittäviin poikkeamiin ja laajamittaisiin kyberturvallisuuspoikkeamiin sekä niistä palautumisen käynnistämistä, joissa hyödynnetään luotettavien yksityisten palveluntarjoajien palveluja ja joissa testataan kriittisiä toimijoita mahdollisten haavoittuvuuksien varalta unionin tason koordinoitujen turvallisuusriskinarviointien perusteella. Tietoturvapalvelujen sertifioinnilla voisi olla merkitystä Euroopan parlamentin ja neuvoston asetuksessa (EU) 2025/38 ([6]) määriteltyjen luotettavien tietoturvapalveluntarjoajien valinnassa.

(6) Tietoturvapalvelujen sertifiointi ei ole merkityksellistä ainoastaan asetuksella (EU) 2025/38 perustetun 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 käsitellään, sertifioinnilla voitaisiin antaa mahdollisille asiakkaille tärkeää ohjeistusta ja lisätä varmuutta kyseisten palvelujen luotettavuudesta. Tietoturvapalveluihin sovellettavilla eurooppalaisilla kyberturvallisuuden sertifiointijärjestelmillä on tarkoitus välttää sisämarkkinoiden pirstoutuminen. Sen vuoksi tällä asetuksella pyritään parantamaan sisämarkkinoiden toimintaa.

(7) Tietoturvapalveluihin sovellettavien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien olisi johdettava kyseisten palvelujen käyttöönottoon ja lisätä tietoturvapalveluntarjoajien välistä kilpailua. Tällaisilla sertifiointijärjestelmillä olisi sen vuoksi helpotettava tietoturvapalvelujen markkinoille pääsyä ja tarjoamista vähentämällä siinä määrin kuin mahdollista palveluntarjoajille ja erityisesti pienille ja keskisuurille yrityksille, jäljempänä 'pk-yritykset', mukaan lukien mikroyritykset, tietoturvapalvelujen tarjoamisen yhteydessä aiheutuvaa mahdollista sääntelytaakkaa sekä hallinnollista ja taloudellista taakkaa, sanotun kuitenkaan rajoittamatta tavoitetta varmistaa tällaisten palveluntarjoajien riittävä ja asianmukaisen tasoinen asiaankuuluva tekninen tietämys ja ammatillinen luotettavuus. Lisäksi, jotta voidaan edistää tietoturvapalvelujen käyttöönottoa ja kysyntää, eurooppalaisilla kyberturvallisuuden sertifiointijärjestelmillä olisi edistettävä tietoturvapalvelujen saatavuutta erityisesti pienempien toimijoiden, kuten pk-yritysten, mukaan lukien mikroyritykset, sekä paikallis- ja alueviranomaisten kannalta, joilla on rajalliset valmiudet ja resurssit mutta jotka ovat alttiimpia kyberturvallisuusloukkauksille, joilla on taloudellisia, oikeudellisia, maineelle haitallisia tai toimintaan kohdistuvia vaikutuksia.

(8) On tärkeää tukea pk-yrityksiä, myös mikroyrityksiä, tämän asetuksen täytäntöönpanossa ja sellaisen henkilöstön rekrytoinnissa, jolla on kyberturvallisuuteen liittyvää erikoisosaamista ja tarvittavaa asiantuntemusta tietoturvapalvelujen tarjoamiseksi tässä asetuksessa säädettyjen vaatimusten mukaisesti. Euroopan parlamentin ja neuvoston asetuksella (EU) 2021/694 ([7]) perustetussa Digitaalinen Eurooppa -ohjelmassa ja muissa asiaankuuluvissa unionin ohjelmissa edellytetään, että komissio ottaa käyttöön taloudellista ja teknistä tukea, jonka avulla kyseiset yritykset voivat edistää unionin talouden kasvua ja vahvistaa kyberturvallisuuden yhteistä tasoa unionissa, muun muassa yksinkertaistamalla Digitaalinen Eurooppa -ohjelmasta ja muista asiaankuuluvista unionin ohjelmista myönnettävää rahoitustukea sekä tukemalla pk-yrityksiä, myös mikroyrityksiä.

(9) Tietoturvapalveluihin sovellettavilla eurooppalaisilla kyberturvallisuuden sertifiointijärjestelmillä olisi edistettävä sellaisten turvallisten ja laadukkaiden palvelujen saatavuutta, jotka takaavat turvallisen digitaalisen siirtymän ja edistävät Euroopan parlamentin ja neuvoston päätöksellä (EU) 2022/2481 ([8]) perustetussa digitaalinen vuosikymmen 2030 -ohjelmassa asetettujen tavoitteiden saavuttamista, erityisesti sen tavoitteen osalta, että 75 prosenttia unionin yrityksistä alkaa käyttää pilvipalveluja, massadataa tai tekoälyä, että digitaaliteknologian

([6]) Euroopan parlamentin ja neuvoston asetus (EU) 2025/38, annettu 19 päivänä joulukuuta 2024, toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberuhkien ja poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten sekä asetuksen (EU) 2021/694 muuttamisesta (kybersolidaarisuussäädös) (EUVL L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

([7]) Euroopan parlamentin ja neuvoston asetus (EU) 2021/694, annettu 29 päivänä huhtikuuta 2021, Digitaalinen Eurooppa -ohjelman perustamisesta ja päätöksen (EU) 2015/2240 kumoamisesta (EUVL L 166, 11.5.2021, s. 1).

([8]) Euroopan parlamentin ja neuvoston päätös (EU) 2022/2481, annettu 14 päivänä joulukuuta 2022, digitaalinen vuosikymmen 2030 -ohjelman perustamisesta (EUVL L 323, 19.12.2022, s. 4).

käyttöaste on vähintään perustasoa yli 90 prosentissa pk-yrityksistä, mukaan lukien mikroyritykset, ja että tärkeimmät julkiset palvelut ovat saatavilla verkossa.

(10) Tietoturvapalvelut mahdollistavat tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien käyttöönoton ohella usein lisäpalveluja, jotka perustuvat niiden henkilöstön osaamiseen, asiantuntemukseen ja kokemukseen. Kyseisen osaamisen, asiantuntemuksen ja kokemuksen erittäin korkean tason sekä asianmukaisten sisäisten menettelyjen olisi kuuluttava turvallisuustavoitteisiin, jotta voidaan varmistaa tarjottujen tietoturvapalvelujen erittäin korkea laatu. Asetusta (EU) 2019/881 on sen vuoksi tarpeen muuttaa sen varmistamiseksi, että erityiset eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät voivat kattaa kaikki tietoturvapalveluihin liittyvät näkökohdat. Asetuksessa (EU) 2019/881 säädettyjen arvioinnin ja uudelleentarkastelun tulokset ja suositukset olisi otettava huomioon.

(11) Jotta voidaan helpottaa luotettavien sisämarkkinoiden kasvua ja samalla solmia kumppanuuksia samanmielisten kolmansien maiden kanssa, asetuksessa (EU) 2019/881 säädetyn eurooppalaisen kyberturvallisuuden sertifiointikehyksen mukaisesti vahvistettu sertifiointiprosessi olisi pantava täytäntöön siten, että edistetään kansainvälistä tunnustamista ja yhdenmukaisuutta kansainvälisten standardien kanssa.

(12) Unionissa on osaamisvaje, jolle on luonteenomaista pätevien ammattilaisten puute, ja unionin uhkaympäristö kehittyy nopeasti, kuten todetaan 18 päivänä huhtikuuta 2023 annetussa komission tiedonannossa ”Kyberturvallisuuteen liittyvän osaamisvajeen pienentäminen EU:n kilpailukyvyn, kasvun ja häiriönsietokyvyn parantamiseksi (’Kyberturvallisuusakatemia’)”. Koulutusresurssit ja virallisen koulutuksen muodot vaihtelevat, ja tietämystä voidaan hankkia monin eri tavoin: virallisen koulutuksen, kuten yliopistossa tai kursseja käymällä saatavan koulutuksen, tai arkioppimisen, kuten työpaikkakoulutuksen tai alalla saadun pitkäaikaisen työkokemuksen, kautta. Jotta voidaan helpottaa laadukkaiden tietoturvapalvelujen syntymistä ja saada parempi yleiskuva unionin kyberturvallisuusalan työvoiman rakenteesta, olisikin tärkeää, että jäsenvaltioiden, komission, asetuksella (EU) 2019/881 perustetun Euroopan unionin kyberturvallisuusviraston (ENISA) ja sidosryhmien, myös yksityisen sektorin ja tiedeyhteisön, välistä yhteistyötä vahvistetaan kehittämällä julkisen ja yksityisen sektorin kumppanuuksia, tukemalla tutkimus- ja innovointialoitteita, kehittämällä yhteisiä normeja ja tunnustamalla ne vastavuoroisesti sekä sertifioimalla kyberturvallisuustaitoja muun muassa eurooppalaisen kyberturvallisuustaitoja koskevan kehyksen avulla. Tällainen yhteistyö helpottaisi myös kyberturvallisuusalan ammattilaisten liikkuvuutta unionissa sekä kyberturvallisuustietämyksen ja -koulutuksen sisällyttämistä opetusohjelmiin ja auttaisi samalla varmistamaan nuorten ja erityisesti epäsuotuisilla alueilla, kuten saarilla, harvaan asutuilla alueilla, maaseudulla ja syrjäisillä alueilla, asuvien nuorten mahdollisuudet päästä oppisopimuskoulutukseen ja harjoitteluun. On tärkeää, että tällaisella yhteistyöllä pyritään houkuttelemaan enemmän naisia ja tyttöjä alalle ja edistämään sukupuolten välisen kuilun kaventamista luonnontieteiden, teknologian, insinööritieteiden ja matematiikan aloilla ja että yksityinen sektori pyrkii tarjoamaan työpaikkakoulutusta kysytyimmissä taidoissa, ottaen mukaan julkishallinnon ja startup-yritykset sekä pk-yritykset, myös mikroyritykset. Lisäksi on tärkeää, että palvelujen tarjoajat ja jäsenvaltiot tekevät yhteistyötä ja edistävät tietojen keruuta kyberturvallisuusalan työmarkkinoiden tilanteesta ja kehityksestä.

(13) ENISAlla on tärkeä rooli ehdolla olevien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien valmistelussa. Kun komissio laatii esitystä unionin yleiseksi talousarvioksi, sen olisi arvioitava ENISAn henkilöstötaulukkoa varten tarvittavat talousarviovarat asetuksen (EU) 2019/881 29 artiklassa vahvistetun menettelyn mukaisesti.

(14) Tässä asetuksessa säädetään kohdennetuista muutoksista asetukseen (EU) 2019/881 tietoturvapalveluihin sovellettavien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien perustamisen mahdollistamiseksi. Samalla siinä myös täsmennetään ja selvennetään tiettyjä kyseisen asetuksen säännöksiä, jotka koskevat kaikkien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien valmistelua ja toimintaa, jotta voidaan varmistaa niiden läpinäkyvyys ja avoimuus. Viimeksi mainitut muutokset, jotka rajoittuvat asetuksen (EU) 2019/881 täsmentämiseen tai selventämiseen, erityisesti muutokset, jotka koskevat tietoja, jotka ENISAn on määrä antaa ehdolla olevaa järjestelmää toimittaessaan, jokaista ehdolla olevaa järjestelmää varten perustettavia tilapäisiä työryhmiä sekä eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä koskevia tietoja ja kuulemista, eivät saisi millään tavoin vaikuttaa kyseisen asetuksen 67 artiklan nojalla edellytettyyn kyseisen asetuksen laajempaan arviointiin ja uudelleentarkasteluun, erityisesti kyseisen asetuksen kyberturvallisuuden sertifiointikehystä koskevan osaston vaikutuksen, tehokkuuden ja tuloksellisuuden arviointiin. Kyseisen osaston arvioinnin ja uudelleentarkastelun olisi perustuttava sidosryhmien laajaan kuulemiseen ja asiaan liittyvien menettelyjen kattavaan ja perusteelliseen analyysiin.

(15) Jäsenvaltiot eivät voi riittävällä tavalla saavuttaa tämän asetuksen tavoitetta eli mahdollistaa tietoturvapalveluihin sovellettavien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien perustamista, vaan se voidaan laajuutensa ja vaikutustensa 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.

(16) Euroopan tietosuojavaltuutettua on kuultu Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1725 ([9]) 42 artiklan 1 kohdan mukaisesti, ja hän on antanut lausuntonsa 10 päivänä tammikuuta 2024,

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 tai 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 järjestelmän kattamien tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien taikka tietoturvapalvelujen sertifiointiin tai vaatimustenmukaisuuden arviointiin;

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

b) lisätään alakohta seuraavasti:

”14 a) ’tietoturvapalvelulla’ kolmannelle osapuolelle tarjottavaa palvelua, joka koostuu kyberturvallisuusriskien hallintaan liittyvien toimien, kuten poikkeamien käsittelyn, tunkeutumistestauksen, turvallisuusauditointien ja tekniseen tukeen liittyvän konsultoinnin, myös asiantuntijaneuvonnan, toteuttamisesta tai niissä avustamisesta;”;

c) korvataan 20, 21 ja 22 alakohta seuraavasti:

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

([9]) 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).

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

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

3) korvataan 4 artiklan 6 kohta seuraavasti:

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

4) muutetaan 8 artikla seuraavasti:

a) muutetaan 1 kohta seuraavasti:

i) korvataan johdantokappale 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”;

ii) korvataan b alakohta seuraavasti:

”b) valmistella tieto- ja viestintätekniikan tuotteisiin, palveluihin ja prosesseihin sekä tietoturvapalveluihin sovellettavat ehdolla olevat eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät, jäljempänä ’ehdolla olevat järjestelmät’, 49 artiklan 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 artikla seuraavasti:

”*46 artikla*

Eurooppalainen kyberturvallisuuden sertifiointikehys

1. Eurooppalainen kyberturvallisuuden sertifiointikehys perustetaan, jotta voidaan parantaa sisämarkkinoiden toimintaedellytyksiä nostamalla kyberturvallisuuden tasoa unionissa ja mahdollistamalla unionin tasolla yhdenmukainen lähestymistapa eurooppalaisiin kyberturvallisuuden sertifiointijärjestelmiin digitaalisten sisämarkkinoiden luomiseksi tieto- ja viestintätekniikan tuotteille, palveluille ja prosesseille sekä tietoturvapalveluille.

2. Eurooppalaisessa kyberturvallisuuden sertifiointikehyksessä vahvistetaan mekanismi eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien perustamista varten ja sen todistamiseksi, 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 todistetaan, että tällaisten järjestelmien mukaisesti arvioidut tietoturvapalvelut ovat niille määritettyjen turvallisuusvaatimusten mukaisia, jotta voidaan suojella kyseisten palvelujen tarjoamisen yhteydessä käytettävien, käsiteltävien, tallennettavien tai siirrettävien tietojen käytettävyyttä, aitoutta, eheyttä ja luottamuksellisuutta, että kyseisiä palveluja tarjotaan jatkuvasti ja että niistä vastaavalla henkilöstöllä on vaadittava osaaminen, asiantuntemus ja kokemus sekä riittävä ja asianmukaisen tasoinen asiaankuuluva tekninen tietämys ja ammatillinen luotettavuus.";

6) muutetaan 47 artikla seuraavasti:

a) korvataan 2 kohta seuraavasti:

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

b) muutetaan 3 kohta seuraavasti:

i) korvataan johdantokappale seuraavasti:

"3. Tiettyjen tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien tai tietoturvapalvelujen tai niiden luokkien sisällyttäminen unionin jatkuvaan työohjelmaan on perusteltava yhdellä tai useammalla seuraavista:";

ii) korvataan a alakohta seuraavasti:

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

iii) lisätään alakohta seuraavasti:

"c a) teknologian kehitys sekä kansainvälisten kyberturvallisuuden sertifiointijärjestelmien sekä kansainvälisten standardien ja toimialan käyttämien standardien saatavuus ja kehitys;";

7) muutetaan 49 artikla seuraavasti:

a) korvataan 1–4 kohta seuraavasti:

"1. Kun komissio on esittänyt 48 artiklan mukaisen pyynnön, ENISA valmistelee ehdolla olevan järjestelmän, joka täyttää 51, 51 a, 52 ja 54 artiklassa vahvistetut sovellettavat vaatimukset.

2. Kun Euroopan kyberturvallisuuden sertifiointiryhmä on esittänyt 48 artiklan 2 kohdan mukaisen pyynnön, ENISA voi valmistella ehdolla olevan järjestelmän, joka täyttää 51, 51 a, 52 ja 54 artiklassa vahvistetut sovellettavat vaatimukset. Jos ENISA hylkää tällaisen pyynnön, se perustelee päätöksensä. Tällaisen pyynnön hylkäämisestä päättää johtokunta.

3. Valmistellessaan ehdolla olevaa järjestelmää ENISA kuulee kohtuullisessa ajassa kaikkia asiaankuuluvia sidosryhmiä virallisesti, avoimesti, läpinäkyvästi ja osallistavasti. Kun ENISA toimittaa ehdolla olevan järjestelmän komissiolle 6 kohdan nojalla, se antaa tietoja siitä, miten se on noudattanut tätä kohtaa.

4. ENISA perustaa jokaista ehdolla olevaa järjestelmää varten 20 artiklan 4 kohdan mukaisesti tilapäisen työryhmän, jonka tarkoituksena on antaa ENISAlle erityistä neuvontaa ja asiantuntemusta. Kyseisiin tilapäisiin työryhmiin on tarvittaessa kuuluttava asiantuntijoita jäsenvaltioiden julkishallinnoista, unionin toimielimistä, elimistä, ja laitoksista sekä yksityiseltä sektorilta, sanotun kuitenkaan rajoittamatta 20 artiklan 4 kohdassa säädettyjen menettelyjen ja harkintavallan soveltamista.";

b) korvataan 7 kohta seuraavasti:

"7. Komissio voi ENISAn valmisteleman ehdolla olevan järjestelmän perusteella hyväksyä täytäntöönpanosäädöksiä tieto- ja viestintätekniikan tuotteisiin, palveluihin ja prosesseihin sekä tietoturvapalveluihin sovellettavasta eurooppalaisesta kyberturvallisuuden sertifiointijärjestelmästä, joka täyttää 51, 51 a, 52 ja 54 artiklassa vahvistetut asiaankuuluvat vaatimukset. Nämä täytäntöönpanosäädökset hyväksytään 66 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.";

8) lisätään artikla seuraavasti:

”*49 a artikla*

Eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä koskevat tiedot ja kuuleminen

1. Komissio asettaa julkisesti saataville tiedot 48 artiklassa tarkoitetusta ENISAlle esittämästään pyynnöstä, joka koskee ehdolla olevan järjestelmän valmistelemista tai voimassa olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän tarkistamista.

2. Kun ENISA valmistelee ehdolla olevaa järjestelmää 49 artiklan nojalla, Euroopan parlamentti, neuvosto tai molemmat voivat pyytää Euroopan kyberturvallisuuden sertifiointiryhmän puheenjohtajana toimivaa komissiota sekä ENISAa esittämään neljännesvuosittain asiaankuuluvat tiedot ehdolla olevan järjestelmän luonnoksesta. ENISA voi Euroopan parlamentin tai neuvoston pyynnöstä yhteisymmärryksessä komission kanssa asettaa Euroopan parlamentin ja neuvoston saataville ehdolla olevan järjestelmän luonnoksen asiaankuuluvia osia tavalla, joka on asianmukainen vaaditun luottamuksellisuuden tason kannalta, ja tarvittaessa rajoitetusti, sanotun kuitenkaan rajoittamatta 27 artiklan soveltamista.

3. Jotta voidaan tehostaa unionin toimielinten välistä vuoropuhelua ja edistää virallista, avointa, läpinäkyvää ja osallistavaa kuulemisprosessia, Euroopan parlamentti, neuvosto tai molemmat voivat pyytää komissiota ja ENISAa keskustelemaan kysymyksistä, jotka koskevat tieto- ja viestintätekniikan tuotteisiin, palveluihin tai prosesseihin taikka tietoturvapalveluihin sovellettavien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien toimintaa.

4. Kun komissio arvioi tätä asetusta 67 artiklan nojalla, se ottaa tarvittaessa huomioon tämän artiklan 3 kohdassa tarkoitetuista kysymyksistä annettuihin Euroopan parlamentin ja neuvoston ilmaisemiin näkemyksiin perustuvat seikat.”;

9) 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 on suunniteltava täyttämään soveltuvin osin vähintään seuraavat turvallisuustavoitteet:”;

10) lisätään artikla seuraavasti:

”*51 a artikla*

Tietoturvapalveluihin sovellettavien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien turvallisuustavoitteet

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

a) tietoturvapalveluiden tarjoajalla on vaadittava osaaminen, asiantuntemus ja kokemus, mukaan lukien se, että kyseisten palvelujen tarjoamiseen osallistuvalla henkilöstöllä on riittävä ja asianmukaisen tasoinen erikoisalan tekninen tietämys ja pätevyys, riittävä ja asianmukainen kokemus sekä mahdollisimman korkeatasoinen ammatillinen luotettavuus;

b) palveluntarjoajalla on käytössään asianmukaiset sisäiset menettelyt sen varmistamiseksi, että tarjottujen tietoturvapalvelujen laatu on kaikkina aikoina riittävällä ja asianmukaisella tasolla;

c) tietoturvapalvelujen tarjoamisen yhteydessä käytettävät, tallennettavat, siirrettävät tai muutoin käsiteltävät tiedot suojataan vahingossa tapahtuvalta tai luvattomalta käytöltä, tallentamiselta, luovuttamiselta, tuhoamiselta, muulta käsittelyltä, hävittämiseltä tai muuttamiselta taikka saatavuuden rajoittamiselta;

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

e) valtuutettujen henkilöiden, ohjelmien tai koneiden käytettävissä 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 arvioiminen;

g) tietoturvapalveluiden tarjoamiseen käytettävät tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit ovat sisäänrakennetusti ja oletusarvoisesti turvallisia ja niihin on tarvittaessa tehty uusimmat tietoturvapäivitykset eikä niissä ole julkisesti tiedossa olevia haavoittuvuuksia.”;

11) 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 taikka tietoturvapalvelun käyttötarkoitukseen liittyvän riskin tasoa, joka perustuu mahdollisen poikkeaman todennäköisyyteen ja vaikutuksiin.”;

b) korvataan 3 kohta seuraavasti:

”3. Asiaankuuluvassa eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä on täsmennettävä kutakin varmuustasoa vastaavat turvallisuusvaatimukset, mukaan lukien vastaavat turvallisuustoiminnot ja niitä vastaava suoritettavan tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin taikka 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 tai prosessit taikka 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 minimoimaan poikkeamien ja kyberhyökkäysten tunnetut perustason riskit. Toteutettavissa arviointitoimissa 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 tai prosessit taikka tietoturvapalvelut, joille kyseinen sertifikaatti on annettu, täyttävät vastaavat turvallisuusvaatimukset, myös turvallisuustoimintojen osalta, ja että ne on arvioitu tasolla, joka on tarkoitettu minimoimaan tunnetut kyberturvallisuusriskit ja sellaisten poikkeamien ja kyberhyökkäysten riski, joiden tekijöillä on rajalliset kyvyt ja resurssit. 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 taikka tietoturvapalvelut toteuttavat välttämättömät turvallisuustoiminnot 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 tai prosessit taikka tietoturvapalvelut, joille kyseinen sertifikaatti on annettu, täyttävät vastaavat turvallisuusvaatimukset, myös turvallisuustoimintojen osalta, ja että ne on arvioitu tasolla, joka on tarkoitettu minimoimaan sellaisten uusinta tekniikkaa hyödyntävien kyberhyökkäysten riski, joiden tekijöillä on merkittävät kyvyt ja resurssit. 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 taikka tietoturvapalvelut toteuttavat uusimman tekniikan mukaiset välttämättömät turvallisuustoiminnot oikein; ja arviointi tunkeutumistestauksen avulla kyseisten prosessien, tuotteiden tai palvelujen taikka tietoturvapalvelujen kyvystä vastustaa kyvykkäitä hyökkääjiä. Jos tällaiset arviointitoimet eivät ole asianmukaisia, on toteutettava vaikutukseltaan vastaavia korvaavia toimia.”;

12) korvataan 53 artiklan 1, 2 ja 3 kohta seuraavasti:

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

2. Tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien taikka 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 tai prosessien taikka tietoturvapalvelujen valmistaja tai tarjoaja ottaa vastuun siitä, että tieto- ja viestintätekniikan tuotteet, palvelut tai prosessit taikka tietoturvapalvelut ovat kyseisen järjestelmän vaatimusten mukaisia.

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

13) 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 tai prosessien taikka tietoturvapalvelujen tyyppi tai luokat;”;

b) korvataan g alakohta seuraavasti:

”g) yksittäiset arvioinnissa käytettävät perusteet ja menetelmät, mukaan lukien arvioinnin tyypit, jotta voidaan osoittaa, että 51 ja 51 a artiklassa tarkoitetut sovellettavat turvallisuustavoitteet saavutetaan;”;

c) korvataan j alakohta seuraavasti:

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

d) korvataan l alakohta seuraavasti:

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

e) korvataan o alakohta seuraavasti:

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

f) korvataan q kohta seuraavasti:

”q) EU-vaatimustenmukaisuusilmoituksen, teknisten asiakirjojen ja kaikkien muiden asiaankuuluvien tietojen, jotka tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien taikka tietoturvapalvelujen valmistaja tai tarjoaja asettaa saataville, saatavillaoloaika;”;

14) muutetaan 56 artikla seuraavasti:

a) korvataan 1 kohta seuraavasti:

”1. Tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sekä tietoturvapalvelujen, jotka on sertifioitu jossain 49 artiklan mukaisesti hyväksytyssä eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä, oletetaan täyttävän tällaisen järjestelmän vaatimukset.”;

b) muutetaan 3 kohta seuraavasti:

i) korvataan ensimmäinen alakohta seuraavasti:

”Komissio arvioi säännöllisesti hyväksyttyjen eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien tehokkuutta ja käyttöä sekä sitä, pitäisikö tietystä eurooppalaisesta kyberturvallisuuden sertifiointijärjestelmästä tehdä pakollinen asiaankuuluvan unionin oikeuden avulla, jotta varmistetaan, että tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sekä 4 päivästä helmikuuta 2025 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 joka toinen vuosi. Komissio määrittää kyseisten arviointien tulosten perusteella sellaiset voimassa olevan sertifiointijärjestelmän soveltamisalaan kuuluvat tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit sekä tietoturvapalvelut, joiden on kuuluttava pakollisen sertifiointijärjestelmän soveltamisalaan.”;

ii) muutetaan kolmas alakohta seuraavasti:

— korvataan a alakohta seuraavasti:

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

— 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 taikka tietoturvapalvelujen valmistajiin tai tarjoajiin, myös pk-yritysten, mukaan lukien mikroyritykset, erityisetuihin ja -tarpeisiin;”;

c) korvataan 7 ja 8 kohta seuraavasti:

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

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

15) korvataan 57 artiklan 1 ja 2 kohta seuraavasti:

”1. Kansalliset kyberturvallisuuden sertifiointijärjestelmät ja niihin liittyvät menettelyt, joita sovelletaan sellaisiin tieto- ja viestintätekniikan tuotteisiin, palveluihin ja prosesseihin sekä tietoturvapalveluihin, 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. Kansalliset kyberturvallisuuden sertifiointijärjestelmät ja niihin liittyvät menettelyt, joita sovelletaan tieto- ja viestintätekniikan tuotteisiin, palveluihin ja prosesseihin sekä tietoturvapalveluihin, 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 sekä tietoturvapalveluille, jotka kuuluvat jo jonkin voimassa olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan.”;

16) 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 eurooppalaisiin kyberturvallisuuden sertifiointijärjestelmiin 54 artiklan 1 kohdan j alakohdan nojalla sisältyviä sääntöjä sen seuraamiseksi, noudattavatko tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit sekä tietoturvapalvelut niiden alueella myönnettyjen eurooppalaisten kyberturvallisuussertifikaattien vaatimuksia;

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

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 tai prosessit taikka tietoturvapalvelut eivät vastaa tämän asetuksen tai yksittäisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien vaatimuksia; ja”;

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.”;

17) 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 eurooppalaisten kyberturvallisuussertifikaattien vaatimuksia 58 artiklan 7 kohdan a alakohdan mukaisesti;

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

18) korvataan 67 artiklan 2 ja 3 kohta seuraavasti:

”2. Arvioinnissa arvioidaan myös tämän asetuksen III osaston säännösten, myös eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien ja niiden perustana olevan näytön hyväksymiseen johtavien menettelyjen, 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 sisämarkkinoille, jotka eivät täytä kybertuvallisuuden perusvaatimuksia.”;

19) muutetaan liite tämän asetuksen liitteen mukaisesti.

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 Brysselissä 19 päivänä joulukuuta 2024.

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puheenjohtaja	*Puheenjohtaja*
R. METSOLA	BÓKA J.

LIITE

Muutetaan asetuksen (EU) 2019/881 liite seuraavasti:

1) korvataan kohdat 2–5 seuraavasti:

”2. Vaatimustenmukaisuuden arviointilaitoksen on oltava arvioimastaan organisaatiosta tai tieto- ja viestintätekniikan tuotteesta, palvelusta tai prosessista taikka tietoturvapalvelusta riippumaton kolmas osapuoli.

3. Elintä, joka kuuluu yrittäjäjärjestöön tai ammattialajärjestöön, joka edustaa yrityksiä, jotka ovat osallisina elimen arvioimien tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien taikka tietoturvapalvelujen suunnittelussa, valmistuksessa, toimittamisessa, kokoamisessa, käytössä tai ylläpidossa, voidaan pitää vaatimustenmukaisuuden arviointilaitoksena edellyttäen, että osoitetaan sen riippumattomuus ja eturistiriitojen pois sulkeminen.

4. Vaatimustenmukaisuuden arviointilaitokset, niiden ylin johto ja vaatimustenmukaisuuden arviointitehtävien suorittamisesta vastaavat henkilöt eivät saa olla arvioitavan tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin taikka tietoturvapalvelun suunnittelijoita, valmistajia, toimittajia, asentajia, ostajia, omistajia, käyttäjiä tai ylläpitäjiä taikka minkään tällaisen osapuolen valtuutettuja edustajia. Kyseinen kielto ei sulje pois sellaisten arvioitujen tieto- ja viestintätekniikan tuotteiden käyttöä, jotka ovat vaatimustenmukaisuuden arviointilaitoksen toimien kannalta tarpeellisia, tai tällaisten tuotteiden käyttöä henkilökohtaisiin tarkoituksiin.

5. Vaatimustenmukaisuuden arviointilaitokset, niiden ylin johto ja vaatimustenmukaisuusarviointitehtävien suorittamisesta vastaavat henkilöt eivät myöskään saa olla suoranaisesti mukana arvioinnin kohteena olevien tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien taikka tietoturvapalvelujen suunnittelussa, valmistuksessa tai rakentamisessa, toimittamisessa, kaupan pitämisessä, asentamisessa, käytössä tai ylläpidossa eivätkä edustaa kyseisissä toiminnoissa mukana olevia osapuolia. Vaatimustenmukaisuuden arviointilaitokset, niiden ylin johto ja vaatimustenmukaisuusarviointitehtävien suorittamisesta vastaavat henkilöt eivät saa osallistua mihinkään toimintaan, joka voi olla ristiriidassa sen kanssa, että ne ovat arvioissaan riippumattomia, tai joka voi vaarantaa niiden luotettavuuden vaatimuksenmukaisuuden arviointitoimissa. Kyseinen kielto koskee erityisesti konsultointipalveluja.”;

2) muutetaan kohta 10 seuraavasti:

a) korvataan johdantokappale seuraavasti:

”10. Vaatimustenmukaisuuden arviointilaitoksella on kaikkina aikoina sekä kunkin vaatimustenmukaisuuden arviointimenettelyn ja kunkin tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien taikka tietoturvapalvelujen tyypin, luokan tai alaluokan osalta oltava käytössään”;

b) korvataan c alakohta seuraavasti:

”c) menettelyt, joiden mukaisesti se hoitaa tehtäviään siten, että yritysten koko, toimiala ja rakenne, asianomaisissa tieto- ja viestintätekniikan tuotteissa, palveluissa tai prosesseissa taikka tietoturvapalveluissa käytettävän teknologian monimutkaisuus sekä tuotannon luonne massa- tai sarjatuotantona otetaan asianmukaisesti huomioon.”;

3) korvataan 19 ja 20 kohta seuraavasti:

”19. Vaatimustenmukaisuuden arviointilaitosten on täytettävä tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien taikka tietoturvapalvelujen sertifioinnista vastaavien vaatimustenmukaisuuden arviointilaitosten akkreditointia koskevan asiaankuuluvan, asetuksen (EY) N:o 765/2008 2 artiklan 9 alakohdassa määritellyn yhdenmukaistetun standardin vaatimukset.

20. Vaatimustenmukaisuuden arviointilaitosten on varmistettava, että vaatimustenmukaisuuden arvioinnissa käytettävät testilaboratoriot täyttävät testauksesta vastaavien laboratorioiden akkreditointia koskevan asiaankuuluvan, asetuksen (EY) N:o 765/2008 2 artiklan 9 alakohdassa määritellyn yhdenmukaistetun standardin vaatimukset.”.

Tästä säädöksestä on annettu lausuma, joka löytyy *Euroopan unionin virallisesta lehdestä* EUVL C, C/2025/307, 15.1.2025, ELI: http://data.europa.eu/eli/C/2025/307/oj.