Euroopan parlamentti
2019-2024

Teollisuus-, tutkimus- ja energiavaliokunta

2023/0108(COD)

21.9.2023

TARKISTUKSET
17 - 52

Mietintöluonnos
Josianne Cutajar
(PE752.802v01-00)

Ehdotus Euroopan parlamentin ja neuvoston asetukseksi asetuksen (EU) 2019/881 muuttamisesta tietoturvapalvelujen osalta

Ehdotus asetukseksi
(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Tarkistus 17
Evžen Tošenovský

Ehdotus asetukseksi
Johdanto-osan 2 kappale

Komission teksti	*Tarkistus*
(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) 2022/25558 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. 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.	(2) Tietoturvapalvelut ovat ***Euroopan parlamentin ja neuvoston direktiivin (EU) 2022/2555 6 artiklan 40 alakohdassa tarkoitettujen tietoturvapalveluntarjoajien tarjoamia*** palveluja***. Nämä palvelut koostuvat*** asiakkaiden kyberturvallisuusriskien hallintaan liittyvien toimien toteuttamisesta tai niissä avustamisesta, ja ne ovat tulleet yhä tärkeämmiksi kyberturvallisuuspoikkeamien ehkäisemisessä ja lieventämisessä. Näin ollen ***tietoturvapalveluntarjoajia*** pidetään ***direktiivin*** (EU) 2022/2555 ***liitteen I 10 alakohdan 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.
[8] Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason	[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).

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).

Or. en

Tarkistus 18
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Ehdotus asetukseksi
Johdanto-osan 2 kappale

Komission teksti	*Tarkistus*
(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. 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	(2) Tietoturvapalvelut ovat palveluja, jotka koostuvat asiakkaiden kyberturvallisuusriskien hallintaan liittyvien toimien toteuttamisesta tai niissä avustamisesta, ***myös poikkeamien ehkäisemisen, havaitsemisen, niihin reagoimisen ja niistä palautumisen osalta,*** 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. Tietoturvapalveluntarjoajat ovat kuitenkin myös itse olleet kyberhyökkäysten kohteena, ja ne muodostavat erityisen riskin, koska ne ovat tiiviisti integroituneet

ja tärkeiden toimijoiden olisi sen vuoksi noudatettava erityisen suurta huolellisuutta tietoturvapalveluntarjoajaa valitessaan.	asiakkaidensa toimintaan. Direktiivissä (EU) 2022/2555 tarkoitettujen keskeisten ja tärkeiden toimijoiden olisi sen vuoksi noudatettava erityisen suurta huolellisuutta tietoturvapalveluntarjoajaa valitessaan.
[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).	[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).

Or. en

Tarkistus 19
Evžen Tošenovský

Ehdotus asetukseksi
Johdanto-osan 3 kappale

Komission teksti	*Tarkistus*
(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	(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***.	reagoimista varten] annetulla asetuksella (EU) .../... säädetään prosessista, jolla ***luotettavat tietoturvapalveluntarjoajat*** valitaan EU:n kyberturvallisuusreserviin ja jossa olisi muun muassa otettava huomioon, ovatko kyseiset palveluntarjoajat saaneet eurooppalaisen tai kansallisen kyberturvallisuussertifioinnin. ***Lisäksi kun*** tietoturvapalveluja koskeva ***eurooppalainen kyberturvallisuuden sertifiointijärjestelmä, joka korvaisi myös kaikki kansalliset kyberturvallisuuden sertifiointijärjestelmät, on käytössä, kyseisen sertifiointijärjestelmän mukaista pakollista sertifiointia olisi sovellettava luotettavien tietoturvapalveluntarjoajien sisällyttämiseen EU:n kyberturvallisuusreserviin***.

Or. en

Tarkistus 20
Johan Nissinen

Ehdotus asetukseksi
Johdanto-osan 4 kappale

Komission teksti	*Tarkistus*
(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	(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. ***Näillä monilla asetuksen***

toimintaa.	***tavoitteilla olisi samalla saavutettava tasapaino sertifioinnin mahdollisen sääntelytaakan ja kustannusten välillä, kun otetaan huomioon, että sertifiointivaatimusten noudattamiseen liittyy lisäkustannuksia ja hallinnollisia toimia, joilla saattaa olla merkitystä pienemmille tarjoajille.***
	Or. en

Tarkistus 21
Ville Niinistö
Verts/ALE-ryhmän puolesta

Ehdotus asetukseksi
Johdanto-osan 4 a kappale (uusi)

Komission teksti	*Tarkistus*
	(4 a) Vaikka markkinat ja koulutusjärjestelmät tarjoavat erilaisia koulutusresursseja ja virallista koulutusta, on tärkeää painottaa, että osaamista hankitaan myös epävirallisen oppimisen kautta ja että taidot voidaan osoittaa myös muuten kuin pelkästään tutkinnoin ja todistuksin. Etenkin nykyisessä nopeasti muuttuvassa uhkaympäristössä jäsenvaltioiden ja tietoturvapalveluista hyötyvien toimijoiden olisi otettava huomioon ammattitaitoiset haavoittuvuuksien tutkijat. Lisäksi haavoittuvuuksia tutkivat yhteisöt ja luonnolliset henkilöt voivat joissakin jäsenvaltioissa joutua rikosoikeudelliseen ja siviilioikeudelliseen vastuuseen, joten jäsenvaltioita kannustetaan antamaan ohjeita tietoturvatutkimusta suorittavien syyttämättä jättämisestä ja vapauttamisesta siviilioikeudellisesta vastuusta tällaisen toiminnan osalta.
	Or. en

Perustelu

Turvallisuusammattilaisten toimintaympäristö vaihtelee osittain siksi, että heillä on erilaisia vakiintumattomia urapolkuja sekä erilaiset mahdollisuudet saada virallista koulutusta ja tulla sertifioiduiksi. Tästä syystä meidän on tuettava osaavien ihmisten työllistymistä ja varmistettava suotuisat puitteet kyberturvallisuutta parantavalle toiminnalle.

Tarkistus 22
Josianne Cutajar

Ehdotus asetukseksi
Johdanto-osan 4 a kappale (uusi)

Komission teksti	*Tarkistus*
	(4 a) Unionin tietoturvapalvelujen sertifiointijärjestelmällä olisi varmistettava, että saatavilla on turvallisia ja korkealaatuisia palveluja, jotka takaavat turvallisen digitaalisen siirtymän ja edistävät ”Polku digitaaliselle vuosikymmenelle” -politiikkaohjelmassa[8] [a] asetettujen tavoitteiden saavuttamista, erityisesti sen osalta, että 75 prosenttia EU:ssa sijaitsevista yrityksistä alkaa käyttää pilvipalveluja, tekoälyä tai massadataa, että yli 90 prosenttia pk-yrityksistä saavuttaa ainakin digitaalisen intensiteetin perustason ja että keskeiset julkiset palvelut ovat saatavilla verkossa.
	[8] [a] Euroopan parlamentin ja neuvoston päätös (EU) 2022/2481, annettu 14 päivänä joulukuuta 2022, digitaalinen vuosikymmen 2030 -ohjelman perustamisesta.

Or. en

Tarkistus 23
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Ehdotus asetukseksi
Johdanto-osan 4 a kappale (uusi)

Komission teksti	*Tarkistus*
	(4 a) Tietoturvapalvelujen eurooppalaisella sertifiointijärjestelmällä olisi helpotettava näiden palvelujen käyttöä erityisesti pienemmissä yhteisöissä, kuten paikallis- ja alueviranomaisissa tai pk-yrityksissä, joilta usein puuttuu taloudelliset ja henkilöresurssit toteuttaa näitä palveluja itse mutta jotka ovat haavoittuvaisia kyberhyökkäyksille, joilla saattaa olla merkittäviä seurauksia.

Or. en

Tarkistus 24
Josianne Cutajar

Ehdotus asetukseksi
Johdanto-osan 5 kappale

Komission teksti	*Tarkistus*
(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	(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. ***Tämän asetuksen mukaisesti perustetussa sertifiointijärjestelmässä olisi otettava myös huomioon asetuksen 67 artiklassa säädetyn arvioinnin ja***

lausuntonsa ***PP päivänä KKkuuta VVVV,***	***uudelleentarkastelun tulokset ja suositukset.*** 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,

Or. en

Tarkistus 25
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Ehdotus asetukseksi
Johdanto-osan 5 kappale

Komission teksti	*Tarkistus*
(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,	(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 ***ja luotettavuus***. 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,

Or. en

Tarkistus 26
Evžen Tošenovský

Ehdotus asetukseksi
Johdanto-osan 5 kappale

Komission teksti	*Tarkistus*
(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,	(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 ***erityinen*** 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,

Or. en

Tarkistus 27
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Ehdotus asetukseksi
Johdanto-osan 5 a kappale (uusi)

Komission teksti	*Tarkistus*
	(5 a) Kun otetaan huomioon, että eurooppalaisilla kyberturvallisuusjärjestelmillä olisi todistettava, että tietoturvapalveluja tarjoaa erittäin osaava henkilöstö, joka pystyy luotettavasti toimittamaan nämä palvelut ja varmistamaan mahdollisimman korkeatasoisten

kyberturvallisuusnormien noudattamisen, on tärkeää, että unionissa on saatavilla riittävästi erittäin pätevää henkilöstöä. Unionilla on osaamisvaje, mukaan lukien pätevien ammattilaisten puute, ja sen uhkaympäristö kehittyy nopeasti, kuten 18 päivänä huhtikuuta 2023 annetussa komission tiedonannossa kyberturvallisuusakatemiasta todetaan. On tärkeää kuroa tämä osaamisvaje umpeen vahvistamalla yhteistyötä ja koordinointia eri sidosryhmien välillä, mukaan lukien yksityissektori, korkeakoulut, jäsenvaltiot, komissio ja ENISA, synergioiden tehostamiseksi ja luomiseksi koulutukseen sijoittamista varten, julkisen ja yksityissektorin välisten kumppanuuksien kehittämiseksi, tutkimus- ja innovointialoitteiden tukemiseksi, yhteisten normien kehittämiseksi ja vastavuoroiseksi tunnustamiseksi ja kyberturvallisuustaitojen sertifioimiseksi, muun muassa eurooppalaisen kyberturvallisuustaitoja koskevan kehyksen avulla. Tämän olisi myös helpotettava kyberturvallisuusammattilaisten liikkuvuutta unionissa.

Or. en

Tarkistus 28
Johan Nissinen

Ehdotus asetukseksi
Johdanto-osan 5 a kappale (uusi)

Komission teksti	*Tarkistus*
	(5 a) Ottaen huomioon, että sertifiointijärjestelmät monimutkaistavat jo ennestään monimutkaista sääntely-ympäristöä, on kriittisen tärkeää estää mahdolliset päällekkäisyydet tai ristiriidat olemassa olevien kyberturvallisuutta koskevien asetusten ja vaatimusten

	kanssa. Painottaa edelleen tarvetta huolelliseen harkintaan ja suhteellisuuteen asetuksen täytäntöönpanossa, jotta voidaan vähentää markkinoiden vapauteen ja innovointiin kohdistuvia kielteisiä vaikutuksia.

Or. en

Tarkistus 29
Josianne Cutajar

Ehdotus asetukseksi
Johdanto-osan 5 a kappale (uusi)

Komission teksti	*Tarkistus*
	(5 a) ENISAlle tässä säädöksessä annettujen lisätehtävien tueksi olisi harkittava asianmukaista rahoitusta ja resursseja.

Or. en

Tarkistus 30
Evžen Tošenovský

Ehdotus asetukseksi
1 artikla – 1 kohta – 2 alakohta – a alakohta – johdantokappale

Komission teksti	*Tarkistus*
a) korvataan 9, 10 ja 11 alakohta seuraavasti:	a) korvataan ***7,*** 9, 10 ja 11 alakohta seuraavasti:

Or. en

Tarkistus 31
Evžen Tošenovský

Ehdotus asetukseksi
1 artikla – 1 kohta – 2 alakohta – a alakohta

Asetus (EU) 2019/881
2 artikla – 7 kohta

Komission teksti	*Tarkistus*
	7) 'poikkeamien käsittelyllä' direktiivin (EU) 2022/2555 6 artiklan 8 alakohdassa määriteltyä poikkeamien käsittelyä;

Or. en

Tarkistus 32
Evžen Tošenovský

Ehdotus asetukseksi
1 artikla – 1 kohta – 2 alakohta – b alakohta – johdantokappale

Komission teksti	*Tarkistus*
b) lisätään ***alakohta*** seuraavasti:	b) lisätään ***alakohdat*** seuraavasti:

Or. en

Tarkistus 33
Evžen Tošenovský

Ehdotus asetukseksi
1 artikla – 1 kohta – 2 alakohta – b alakohta
Asetus (EU) 2019/881
2 artikla – 7 a kohta

Komission teksti	*Tarkistus*
	7 A) 'riskillä' direktiivin (EU) 2022/2555 6 artiklan 9 alakohdassa määriteltyä 'riskiä';

Or. en

Tarkistus 34
Evžen Tošenovský

Ehdotus asetukseksi
1 artikla – 1 kohta – 2 alakohta – b alakohta
Asetus (EU) 2019/881
2 artikla – 14 a kohta

Komission teksti	*Tarkistus*
”14 a) ’tietoturvapalvelulla’ ***palvelua, joka koostuu kyberturvallisuusriskien hallintaan liittyvien toimien toteuttamisesta tai niissä avustamisesta, mukaan lukien poikkeamiin reagointi, tunkeutumisenestotestaus, turvallisuustarkastukset ja konsultointi***;***”***	”14 a) ’tietoturvapalvelulla’ ***direktiivin (EU) 2022/2555 6 artiklan 40 alakohdassa määriteltyä tietoturvapalvelua***;

Or. en

Tarkistus 35
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Ehdotus asetukseksi
1 artikla – 1 kohta – 2 alakohta – b alakohta
Asetus (EU) 2019/881
2 artikla – 14 a kohta

Komission teksti	*Tarkistus*
”14 a) ’tietoturvapalvelulla’ palvelua, joka koostuu kyberturvallisuusriskien hallintaan liittyvien toimien toteuttamisesta tai niissä avustamisesta, mukaan lukien poikkeamiin reagointi, ***tunkeutumisenestotestaus, turvallisuustarkastukset ja konsultointi***;”	”14 a) ’tietoturvapalvelulla’ palvelua, joka koostuu kyberturvallisuusriskien hallintaan liittyvien toimien toteuttamisesta tai niissä avustamisesta, mukaan lukien poikkeamien ***estäminen ja havainnointi*** sekä niihin reagoiminen tai niistä ***palautuminen***;”

Or. en

Tarkistus 36
Evžen Tošenovský

Ehdotus asetukseksi
1 artikla – 1 kohta – 2 alakohta – b alakohta
Asetus (EU) 2019/881
2 artikla – 14 aa kohta

Komission teksti	*Tarkistus*
	14 aa) 'tietoturvapalveluntarjoajalla' direktiivin (EU) 2022/2555 6 artiklan 40 alakohdassa määriteltyä tietoturvapalveluntarjoajaa;

Or. en

Tarkistus 37
Ville Niinistö
Verts/ALE-ryhmän puolesta

Ehdotus asetukseksi
1 artikla – 1 kohta – 6 alakohta
Asetus (EU) 2019/881
47 artikla – 2 kohta

Komission teksti	*Tarkistus*
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.	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. ***Mahdollisten vajeiden poistamiseen tarkoitettujen toimenpiteiden lisäksi käyttöön on otettava tukitoimia osaavien työntekijöiden tarpeiden, osaamisen ja nykyisten koulutuspolkujen arvioimiseksi.***

Or. en

Perustelu

Tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien tai niiden luokkien ja tietoturvapalvelujen määrittämistä on tuettava osaamisen arvioinnilla ja toimenpiteillä vajeiden poistamiseksi.

Tarkistus 38
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard

Ehdotus asetukseksi
1 artikla – 1 kohta – 6 alakohta
Asetus (EU) 2019/881
47 artikla – 3 kohta – a alakohta

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

Or. en

Perustelu

Unionin jatkuvassa työohjelmassa olisi arvioitava kansallisten järjestelmien kehittämisen lisäksi toimialan ja kansainvälisiä standardeja.

Tarkistus 39
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Ehdotus asetukseksi
1 artikla – 1 kohta – 7 alakohta
Asetus (EU) 2019/881
49 artikla – 7 kohta

Komission teksti	*Tarkistus*
7) Korvataan 49 artiklan 7 kohta seuraavasti:	***Poistetaan.***
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.”

Or. en

Tarkistus 40
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Ehdotus asetukseksi
1 artikla – 1 kohta – 7 alakohta
Asetus (EU) 2019/881
49 artikla – 7 kohta

Komission teksti	*Tarkistus*
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.”***	7. Komissio voi ENISAn valmisteleman ehdolla olevan järjestelmän pohjalta hyväksyä ***delegoituja*** säädöksiä tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sekä tietoturvapalvelujen eurooppalaisesta kyberturvallisuuden sertifiointijärjestelmästä, joka täyttää 51, 52 ja 54 artiklassa esitetyt vaatimukset. *(This amendment applies throughout the text. Adopting it will necessitate corresponding changes throughout.)*

Or. en

Tarkistus 41
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Ehdotus asetukseksi
1 artikla – 1 kohta – 7 alakohta
Asetus (EU) 2019/881
49 artikla – 7 a kohta (uusi)

Komission teksti	*Tarkistus*
	7 a. Ennen tällaisten delegoitujen säädösten hyväksymistä komissio suorittaa ja julkaisee yhteistyössä ENISAn kanssa vaikutustenarvioinnin ehdotetusta eurooppalaisesta kyberturvallisuuden sertifiointijärjestelmästä. Vaikutustenarviointia valmistellessaan komissio järjestää julkisia kuulemisia ja kuulemiset sidosryhmien kyberturvallisuuden sertifiointiryhmän (SCCG) ja Euroopan kyberturvallisuuden sertifiointiryhmän (ECCG) kanssa.

Or. en

Tarkistus 42
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Ehdotus asetukseksi
1 artikla – 1 kohta – 7 a alakohta (uusi)
Asetus (EU) 2019/881
49 artikla – 7 a kohta (uusi)

Komission teksti	*Tarkistus*
	7 a) Lisätään kohta seuraavasti:
	”7 a. Komissio voi ENISAn valmisteleman ehdolla olevan järjestelmän pohjalta hyväksyä delegoituja säädöksiä, joissa säädetään tietoturvallisuuspalveluja koskevasta eurooppalaisesta kyberturvallisuuden sertifiointijärjestelmästä, joka täyttää 51, 52 ja 54 artiklassa asetetut vaatimukset. Nämä delegoidut säädökset hyväksytään 66 a artiklassa tarkoitettua menettelyä noudattaen.”

Or. en

Tarkistus 43
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Ehdotus asetukseksi
1 artikla – 1 kohta – 9 alakohta
Asetus (EU) 2019/881
51 a artikla – 1 kohta – b alakohta

Komission teksti	*Tarkistus*
b) varmistetaan, että palveluntarjoajalla on käytössään asianmukaiset sisäiset menettelyt sen varmistamiseksi, että tarjotut tietoturvapalvelut ovat kaikkina aikoina erittäin korkealaatuisia;	b) varmistetaan, että palveluntarjoajalla on käytössään asianmukaiset sisäiset menettelyt sen varmistamiseksi, että tarjotut tietoturvapalvelut ovat kaikkina aikoina erittäin korkealaatuisia ***ja luotettavia***;

Or. en

Tarkistus 44
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Ehdotus asetukseksi
1 artikla – 1 kohta – 9 alakohta
Asetus (EU) 2019/881
51 a artikla – 1 kohta – g alakohta

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

Or. en

Tarkistus 45
Evžen Tošenovský

Ehdotus asetukseksi
1 artikla – 1 kohta – 9 alakohta
Asetus (EU) 2019/881
51 a artikla – 1 kohta – g alakohta

Komission teksti	*Tarkistus*
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.”	g) varmistetaan, että tietoturvapalveluiden tarjoamiseen käytettävät tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit ovat oletusarvoisesti ja sisäänrakennetusti turvallisia, että niissä ei ole tunnettuja haavoittuvuuksia ja että niihin on tehty uusimmat turvallisuuspäivitykset.”

Or. en

Tarkistus 46
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Ehdotus asetukseksi
1 artikla – 1 kohta – 13 alakohta – b alakohta – ii alakohta – a a alakohta
Asetus (EU) 2019/881
56 artikla – 3 kohta – kolmas alakohta – a alakohta

Komission teksti	*Tarkistus*
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;”	a) ottaa huomioon toimenpiteiden vaikutukset tällaisten tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien tai tietoturvapalvelujen valmistajiin tai tarjoajiin sekä käyttäjiin, ***mukaan lukien pk-yrityksiin***, kyseisten toimenpiteiden kustannusten ja kohteena olevien tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien tai tietoturvapalvelujen ennakoidusta parantuneesta turvallisuustasosta johtuvien yhteiskunnallisten tai taloudellisten hyötyjen osalta;” ***Komissio varmistaa, että pk-yrityksillä on mahdollisuus saada***

riittävästi taloudellista tukea toimenpiteiden täytäntöönpanoon unionin nykyisten ohjelmien kautta;

Or. en

Tarkistus 47
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Ehdotus asetukseksi
1 artikla – 1 kohta – 14 alakohta
Asetus (EU) 2019/881
57 artikla – 1 kohta

Komission teksti	*Tarkistus*
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.	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 ***delegoidussa säädöksessä***, 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. *(Muutos koskee koko tekstiä. Jos tarkistus hyväksytään, kaikkialle tekstiin on tehtävä vastaavat muutokset.)*

Or. en

Perustelu

Tämä pohjautuu 49 artiklan muutokseen.

Tarkistus 48
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Ehdotus asetukseksi
1 artikla – 1 kohta – 16 a alakohta (uusi)
Asetus (EU) 2019/881
66 a artikla (uusi)

Komission teksti	*Tarkistus*
	16 a) Lisätään artikla seuraavasti:
	66 a artikla (uusi)
	Siirretyn säädösvallan käyttäminen
	1. Komissiolle siirrettyä valtaa antaa delegoituja säädöksiä koskevat tässä artiklassa säädetyt edellytykset.
	2. Siirretään komissiolle ... päivästä ...kuuta ... [perussäädöksen voimaantulopäivä tai muu lainsäädäntövallan käyttäjien asettama päivä] viiden vuoden ajaksi 49 artiklan 7 a kohdassa tarkoitettu valta antaa delegoituja säädöksiä. Komissio laatii siirrettyä säädösvaltaa koskevan kertomuksen viimeistään yhdeksän kuukautta ennen tämän viiden vuoden kauden päättymistä. Säädösvallan siirtoa jatketaan ilman eri toimenpiteitä samanpituisiksi kausiksi, jollei Euroopan parlamentti tai neuvosto vastusta tällaista jatkamista viimeistään kolme kuukautta ennen kunkin kauden päättymistä.
	3. Euroopan parlamentti tai neuvosto voi milloin tahansa peruuttaa 49 artiklan 7 a kohdassa tarkoitetun säädösvallan siirron. Peruuttamispäätöksellä lopetetaan tuossa päätöksessä mainittu säädösvallan siirto. Peruuttaminen tulee voimaan sitä päivää seuraavana päivänä, jona sitä koskeva päätös julkaistaan

Euroopan unionin virallisessa lehdessä, tai jonakin myöhempänä, kyseisessä päätöksessä mainittuna päivänä. Peruuttamispäätös ei vaikuta jo voimassa olevien delegoitujen säädösten pätevyyteen.

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

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

6. Edellä olevan 49 artiklan 7 a kohdan nojalla annettu delegoitu säädös tulee voimaan ainoastaan, jos Euroopan parlamentti tai neuvosto ei ole kahden kuukauden kuluessa siitä, kun asianomainen säädös on annettu tiedoksi Euroopan parlamentille ja neuvostolle, ilmaissut vastustavansa sitä tai jos sekä Euroopan parlamentti että neuvosto ovat ennen mainitun määräajan päättymistä ilmoittaneet komissiolle, että ne eivät vastusta säädöstä. Euroopan parlamentin tai neuvoston aloitteesta tätä määräaikaa jatketaan [kahdella kuukaudella].

Or. en

Tarkistus 49
Evžen Tošenovský

Ehdotus asetukseksi
1 artikla – 1 kohta – 17 alakohta – johdantokappale
Asetus (EU) 2019/881
67 artikla

Komission teksti	*Tarkistus*
17) Korvataan 67 artiklan 2 ***ja*** 3 kohta	17) korvataan 67 artiklan 1**,** 2***, 3 ja 4***

seuraavasti:

kohta seuraavasti:

Or. en

Tarkistus 50
Evžen Tošenovský

Ehdotus asetukseksi
1 artikla – 1 kohta – 17 alakohta
Asetus (EU) 2019/881
67 artikla – 1 kohta

Komission teksti	*Tarkistus*
	1. Komissio arvioi viimeistään 28 päivänä kesäkuuta 2024 ja sen jälkeen neljän vuoden välein ENISAn ja sen työtapojen vaikutusta, tehokkuutta ja tuloksellisuutta sekä mahdollista tarvetta muuttaa ENISAn toimeksiantoa ja tällaisten muutosten taloudellisia vaikutuksia. Arvioinnissa otetaan huomioon ENISAn toiminnastaan mahdollisesti saama palaute. Jos komissio katsoo, ettei ENISAn toiminnan jatkaminen ole enää perusteltua sille asetettuihin tavoitteisiin, toimeksiantoon ja tehtäviin nähden, komissio voi ehdottaa, että tätä asetusta muutetaan ENISAa koskevien säännösten osalta.

Or. en

Tarkistus 51
Evžen Tošenovský

Ehdotus asetukseksi
1 artikla – 1 kohta – 17 alakohta
Asetus (EU) 2019/881
67 artikla – 2 kohta

Komission teksti	*Tarkistus*
2. Arvioinnissa arvioidaan myös tämän asetuksen III osaston säännösten	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.	vaikutusta, tehokkuutta ja tuloksellisuutta suhteessa tavoitteisiin varmistaa tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sekä tietoturvapalvelujen kyberturvallisuuden riittävä taso unionissa ja parantaa sisämarkkinoiden toimintaa, ***mukaan lukien ensimmäisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien valmisteluun ja hyväksymiseen johtavien menettelyjen ja määräaikojen arviointi sekä arviointi siitä, kuinka tätä menettelyä voitaisiin parantaa ja nopeuttaa tulevien sertifiointijärjestelmien osalta.***
	Or. en

Tarkistus 52
Evžen Tošenovský

Ehdotus asetukseksi
1 artikla – 1 kohta – 17 alakohta
Asetus (EU) 2019/881
67 artikla – 4 kohta

Komission teksti	*Tarkistus*
	4. Komissio toimittaa viimeistään 28 päivänä kesäkuuta 2024 ja joka neljäs vuosi sen jälkeen arviointikertomuksen ja päätelmänsä Euroopan parlamentille, neuvostolle ja johtokunnalle. Kyseisen kertomuksen tulokset julkistetaan. Kertomukseen liitetään tarvittaessa lainsäädäntöehdotus.
	Or. en