EUROOPAN UNIONI

EUROOPAN PARLAMENTTI **NEUVOSTO**

Bryssel, 27. maaliskuuta 2019
(OR. en)

2017/0225 (COD) **PE-CONS 86/18**

CYBER 330
TELECOM 491
COPEN 454
COPS 488
COSI 326
CSC 387
CSCI 179
IND 417
JAI 1315
JAIEX 174
POLMIL 231
RELEX 1115
CODEC 2380

SÄÄDÖKSET JA MUUT VÄLINEET

Asia:	EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus)

EUROOPAN PARLAMENTIN JA NEUVOSTON
ASETUS (EU) 2019/…,

annettu … päivänä …kuuta …,

Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus)

(ETA:n kannalta merkityksellinen teksti)

EUROOPAN PARLAMENTTI JA EUROOPAN UNIONIN NEUVOSTO, jotka

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

ottavat huomioon Euroopan komission ehdotuksen,

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

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

ottavat huomioon alueiden komitean lausunnon[2],

noudattavat tavallista lainsäätämisjärjestystä[3],

---

1 EUVL C 227, 28.6.2018, s. 86.
2 EUVL C 176, 23.5.2018, s. 29.
3 Euroopan parlamentin kanta, vahvistettu 12. maaliskuuta 2019 (ei vielä julkaistu virallisessa lehdessä), ja neuvoston päätös, annettu ….

sekä katsovat seuraavaa:

(1) Verkko- ja tietojärjestelmillä ja sähköisen viestinnän verkoilla ja palveluilla on yhteiskunnassa elintärkeä rooli, ja niistä on tullut talouskasvun selkäranka. Tieto- ja viestintätekniikka luo pohjaa monimutkaisille järjestelmille, jotka tukevat yhteiskunnan päivittäisiä toimintoja, pitävät talouden pyörät pyörimässä keskeisillä aloilla, kuten terveydenhuollossa, energia-alalla, rahoitusalalla ja liikenteessä, ja erityisesti tukevat sisämarkkinoiden toimintaa.

(2) Verkko- ja tietojärjestelmien käyttö on nykyisin laajalle levinnyttä kansalaisten, organisaatioiden ja yritysten piirissä kaikkialla unionissa. Digitalisoinnista ja verkkoyhteyksistä on tulossa keskeisiä ominaisuuksia yhä useammissa tuotteissa ja palveluissa, ja esineiden internetin myötä unionissa ennakoidaan otettavan käyttöön äärimmäisen suuri määrä verkkoon kytkettyjä digitaalisia laitteita seuraavan vuosikymmenen aikana. Yhä useammat laitteet liitetään internetiin huolehtimatta samalla siitä, että turvallisuus ja häiriönsietokyky ovat riittävällä tavalla sisäänrakennettuja, mikä johtaa puutteisiin kyberturvallisuudessa. Sertifioinnin vähäinen käyttö johtaa tässä yhteydessä siihen, että kansalaiset, organisaatiot ja yritykset eivät saa riittävästi tietoa tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien kyberturvallisuusominaisuuksista, mikä heikentää luottamusta digitaalisiin ratkaisuihin. Verkko- ja tietojärjestelmillä voidaan tukea kaikkia elämänaloja ja edistää unionin talouskasvua. Nämä järjestelmät ovat ratkaisevan tärkeitä digitaalisten sisämarkkinoiden toteuttamisen kannalta.

(3) Digitalisoinnin ja verkkoyhteyksien yleistyminen lisää kyberturvallisuuteen liittyviä riskejä, mikä tekee koko yhteiskunnasta alttiimman kyberuhkille ja pahentaa yksilöihin, myös heikommassa asemassa oleviin henkilöihin, kuten lapsiin, kohdistuvia vaaroja. Näiden riskien lieventämiseksi kyberturvallisuutta on tarpeen parantaa unionissa kaikin tarvittavin toimenpitein, jotta kansalaisten, organisaatioiden ja yritysten – pienistä ja keskisuurista yrityksistä, jäljempänä 'pk-yritykset', elintärkeiden infrastruktuureiden ylläpitäjiin – käyttämät verkko- ja tietojärjestelmät, televiestintäverkot, digitaaliset tuotteet, palvelut ja laitteet voidaan suojata paremmin kyberuhilta.

(4) Tuottamalla asiaa koskevaa tietoa ja asettamalla sitä yleisön saataville Euroopan parlamentin ja neuvoston asetuksella (EU) No 526/2013[1] perustettu Euroopan unionin verkko- ja tietoturvavirasto, jäljempänä 'ENISA', edistää kyberturvallisuusalan ja etenkin pk- ja startup-yritysten kehittymistä unionissa. ENISAn olisi pyrittävä tiiviimpään yhteistyöhän yliopistojen ja tutkimuslaitosten kanssa, jotta se voisi edistää osaltaan strategista lähestymistapaa, joka koskee riippuvuuden vähentämistä unionin ulkopuolelta peräisin olevista kyberturvallisuustuotteista ja -palveluista, ja vahvistaa unionin sisäisiä toimitusketjuja.

[1] Euroopan parlamentin ja neuvoston asetus (EU) N:o 526/2013, annettu 21 päivänä toukokuuta 2013, Euroopan unionin verkko- ja tietoturvavirastosta (ENISA) ja asetuksen (EY) N:o 460/2004 kumoamisesta (EUVL L 165, 18.6.2013, s. 41).

(5) Kyberhyökkäyksiä tapahtuu yhä enemmän, ja verkottunut talous ja yhteiskunta, joka on alttiimpi kyberuhille ja -hyökkäyksille, edellyttää vahvempaa puolustusvalmiutta. Vaikka kyberhyökkäykset ovat usein rajat ylittäviä, kyberturvallisuus- ja lainvalvontaviranomaisten toimivaltuudet ja poliittiset vastatoimet ovat enimmäkseen kansallisia. Laajamittaiset poikkeamat voivat häiritä keskeisten palvelujen tarjoamista koko unionissa. Tämä edellyttää kohdennettuihin politiikkoihin ja laaja-alaisempiin eurooppalaisen yhteisvastuun ja keskinäisen avunannon välineisiin perustuvia tehokkaita ja koordinoituja vastatoimia ja kriisinhallintaa unionin tasolla. Politiikan laatijoille, toimialalle ja käyttäjille on tärkeää, että kyberturvallisuuden ja häiriönsietokyvyn tilaa unionissa arvioidaan säännöllisesti luotettavan unionin tiedon pohjalta ja että laaditaan järjestelmällisesti ennusteita tulevista kehityskuluista, haasteista ja uhkista unionin tasolla ja maailmanlaajuisesti.

(6) Unioniin kohdistuvien kyberturvallisuushaasteiden lisääntymisen vuoksi tarvitaan kattava joukko toimenpiteitä, jotka pohjautuisivat aiempaan unionin toimintaan ja edistäisivät toisiaan vahvistavia tavoitteita. Näihin tavoitteisiin sisältyy tarve lisätä jäsenvaltioiden ja yritysten valmiuksia ja varautumiskykyä entisestään sekä parantaa yhteistyötä, tiedonjakamista ja koordinointia, jäsenvaltioiden ja unionin toimielinten, elinten ja laitosten välillä. Koska kyberuhkat ovat luonteeltaan rajattomia, on myös tarpeen lisätä valmiuksia unionin tasolla jäsenvaltioiden toimien täydentämiseksi erityisesti laajamittaisten rajat ylittävien poikkeamien ja kriisien tapauksessa ottaen samalla huomioon, että on tärkeää ylläpitää ja vahvistaa edelleen kansallisia valmiuksia vastata kaikenkokoisiin kyberuhkiin.

(7) Tarvitaan myös lisätoimia kansalaisorganisaatioiden ja yritysten tietoisuuden lisäämiseksi kyberturvallisuuteen liittyvistä kysymyksistä. Koska poikkeamat lisäksi vähentävät luottamusta digitaalisten palvelujen tarjoajiin ja digitaalisiin sisämarkkinoihin etenkin kuluttajien keskuudessa, luottamusta olisi edelleen vahvistettava tarjoamalla tieto- ja viestintätekniikan tuotteista, palveluista ja prosesseista avointa tietoa, jossa korostetaan, että korkeatasoinenkaan kyberturvallisuussertifiointi ei voi taata, että tieto- ja viestintätekniikan tuote, palvelu tai prosessi olisi täysin turvallinen. Luotettavuuden kasvua voidaan helpottaa unionin laajuisella sertifioinnilla, joka tuo käyttöön yhteiset kyberturvallisuusvaatimukset ja -arviointiperusteet kansallisille markkinoille ja aloille.

(8) Kyberturvallisuus ei ole ainoastaan teknologiaan liittyvä kysymys, vaan yhtä merkittävällä tavalla ihmisten käyttäytymiseen liittyvä kysymys. Sen vuoksi olisi voimakkaasti edistettävä 'kyberhygieniaa', eli yksinkertaisia rutiinitoimenpiteitä, jotka säännöllisesti toimeenpantuina ja toteutettuina minimoivat kansalaisten, organisaatioiden ja yritysten altistumisen kyberuhkien riskeille.

(9) Unionin kyberturvallisuuden rakenteiden vahvistamiseksi on tärkeää ylläpitää ja kehittää jäsenvaltioiden valmiuksia vastata kattavasti kyberuhkiin, myös rajat ylittävien poikkeamien tapauksessa.

(10) Yrityksillä ja yksittäisillä kuluttajilla olisi oltava tarkat tiedot varmuustasosta, jolla tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien turvallisuus on sertifioitu. Samalla mikään tieto- ja viestintätekniikan tuote tai palvelu ei ole täysin kyberturvallinen, ja kyberhygienian perussääntöjä olisi edistettävä ja ne olisi asetettava etusijalle. Koska esineiden internetin laitteita on yhä enemmän saatavilla, yksityissektori voi toteuttaa useita vapaaehtoisia toimenpiteitä vahvistaakseen luottamusta tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien turvallisuuteen.

(11) Nykyaikaiset tieto- ja viestintätekniikan tuotteet ja järjestelmät käsittävät usein yhden tai useamman kolmannen osapuolen teknologiaa ja komponentteja – kuten ohjelmistomoduuleja, ohjelmakirjastoja tai ohjelmointirajapintoja – ja ovat niistä riippuvaisia. Tämä riippuvuus voi aiheuttaa uusia kyberturvallisuusriskejä, koska kolmansien osapuolten komponenteissa olevat haavoittuvuudet voivat vaikuttaa myös tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien turvallisuuteen. Monissa tapauksissa riippuvuuksien tunnistaminen ja dokumentointi auttaa tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien loppukäyttäjiä parantamaan kyberturvallisuusriskien hallintatoimia parantamalla esimerkiksi käyttäjien toteuttamia kyberturvallisuuden haavoittuvuuden hallinta- ja korjaamismenettelyjä.

(12) Tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien suunnitteluun ja kehittämiseen osallistuvia organisaatioita, valmistajia tai tarjoajia olisi kannustettava ottamaan käyttöön suunnittelun ja kehittämisen mahdollisimman varhaisissa vaiheissa toimenpiteitä kyseisten tuotteiden, prosessien ja palvelujen turvallisuuden suojaamiseksi parhaalla mahdollisella tavalla siten, että kyberhyökkäyksiä oletetaan tapahtuvan ja niiden vaikutukset minimoidaan, jäljempänä 'sisäänrakennettu turvallisuus'. Turvallisuuteen olisi kiinnitettävä huomiota tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin koko elinkaaren ajan, käyttämällä suunnittelu- ja kehittämisprosesseja, jotka muuttuvat jatkuvasti ilkivallasta aiheutuvan haitan muodostaman riskin madaltamiseksi.

(13) Yritysten, organisaatioiden ja julkisen sektorin olisi konfiguroitava suunnittelemansa tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit tavalla, jolla varmistetaan korkeampi turvallisuuden taso, jonka ansiosta ensimmäinen käyttäjän pitäisi saada oletuskonfiguraatio, jossa on mahdollisimman turvalliset oletusasetukset, jäljempänä 'oletusarvoinen turvallisuus', ja siten kevennettäisiin rasitetta, joka käyttäjälle aiheutuu siitä, että hänen pitää muuttaa tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin asetuksia asianmukaisesti. Oletusarvoinen turvallisuus ei saisi edellyttää mittavaa konfigurointia eikä teknistä erityisosaamista tai muuta kuin ilmeistä käyttäytymistä käyttäjältä, ja sen olisi täytäntöönpantuna toimittava helposti ja luotettavasti. Jos riski- ja käytettävyysanalyysin perusteella voidaan tapauskohtaisesti päätellä, että tällainen asetus ei ole toteutettavissa oletusarvoisena, käyttäjiä olisi pyydettävä valitsemaan kaikkein turvallisin asetus.

(14) ENISA perustettiin Euroopan parlamentin ja neuvoston asetuksella (EY) N:o 460/2004[1], tavoitteena osaltaan varmistaa korkeatasoinen ja tehokas verkko- ja tietoturva unionissa ja luoda verkko- ja tietoturvakulttuuri, josta on hyötyä kansalaisille, kuluttajille, yrityksille ja julkishallinnoille. Euroopan parlamentin ja neuvoston asetuksella (EY) N:o 1007/2008[2], ENISAn toimikautta jatkettiin maaliskuuhun 2012. Euroopan parlamentin ja neuvoston asetuksella (EY) N:o 580/2011[3] ENISAn toimikautta jatkettiin edelleen 13 päivään syyskuuta 2013. Asetuksella (EU) N:o 526/2013 ENISAn toimikautta jatkettiin 19 päivään kesäkuuta 2020.

---

1 Euroopan parlamentin ja neuvoston asetus (EY) N:o 460/2004, annettu 10 päivänä maaliskuuta 2004, Euroopan verkko- ja tietoturvaviraston perustamisesta (EUVL L 77, 13.3.2004, s. 1).

2 Euroopan parlamentin ja neuvoston asetus (EY) N:o 1007/2008, annettu 24 päivänä syyskuuta 2008, Euroopan verkko- ja tietoturvaviraston perustamisesta annetun asetuksen (EY) N:o 460/2004 muuttamisesta sen toimikauden keston osalta (EUVL L 293, 31.10.2008, s. 1).

3 Euroopan parlamentin ja neuvoston asetus (EU) N:o 580/2011, annettu 8 päivänä kesäkuuta 2011, Euroopan verkko- ja tietoturvaviraston perustamisesta annetun asetuksen (EY) N:o 460/2004 muuttamisesta viraston toimikauden osalta (EUVL L 165, 24.6.2011, s. 3).

(15) Unioni on jo toteuttanut merkittäviä toimia varmistaakseen kyberturvallisuuden ja lisätäkseen luottamusta digitaaliteknologioihin. Vuonna 2013 hyväksyttiin Euroopan unionin kyberturvallisuusstrategia ohjaamaan unionin poliittisia vastatoimia kyberuhkiin ja -riskeihin. Tarjotakseen kansalaisille paremman suojan verkkoympäristössä unioni hyväksyi vuonna 2016 ensimmäisenä kyberturvallisuusalan säädöksenä Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/1148[1]. Direktiivillä (EU) 2016/1148 otettiin käyttöön vaatimukset kansallisista valmiuksista kyberturvallisuuden alalla, ensimmäiset mekanismit jäsenvaltioiden strategisen ja operatiivisen yhteistyön tehostamiseksi sekä velvoitteet toteuttaa turvallisuustoimenpiteitä ja tehdä ilmoitukset poikkeamista talouden ja yhteiskunnan kannalta olennaisilla aloilla, kuten energia, liikenne, juomaveden toimittaminen ja jakelu, pankkitoiminta, rahoitusmarkkinoiden infrastruktuurit, terveydenhuolto ja digitaalinen infrastruktuuri sekä keskeisten digitaalisten palvelujen (hakukoneet, pilvipalvelut ja verkossa toimivat markkinapaikat) tarjoajat.

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

ENISAlle annettiin keskeinen rooli tukea kyseisen direktiivin täytäntöönpanoa. Lisäksi kyberrikollisuuden torjunta on tärkeä prioriteetti Euroopan turvallisuusagendassa, joka tältä osin edistää yleistä tavoitetta saavuttaa kyberturvallisuuden korkea taso. Myös muut säädökset, kuten Euroopan parlamentin ja neuvoston asetus (EU) 2016/679[1] sekä Euroopan parlamentin ja neuvoston direktiivit 2002/58/EY[2] ja (EU) 2018/1972[3], edistävät kyberturvallisuuden korkeaa tasoa digitaalisilla sisämarkkinoilla.

---

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

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

3 Euroopan parlamentin ja neuvoston direktiivi (EU) 2018/1972, annettu 11 päivänä joulukuuta 2018, eurooppalaisesta sähköisen viestinnän säännöstöstä (EUVL L 321, 17.12.2018, s. 36).

(16) Sen jälkeen, kun Euroopan unionin kyberturvallisuusstrategia hyväksyttiin vuonna 2013 ja ENISAn toimeksiantoa viimeksi tarkistettiin, yleinen poliittinen tilanne on muuttunut merkittävästi, koska globaali toimintaympäristö on muuttunut epävarmemmaksi ja vähemmän turvatuksi. Tätä taustaa vasten ja ottaen huomioon ENISAn roolin myönteisen kehityksen neuvonnan ja asiantuntemuksen viitetahona, yhteistyön ja valmiuksien kehittämisen edistäjänä sekä osana uutta unionin kyberturvallisuuspolitiikkaa on tarpeen tarkistaa ENISAn toimeksiantoa, vahvistaa sen rooli muuttuneessa kyberturvallisuusekosysteemissä ja varmistaa, että se auttaa tehokkaasti unionia vastaamaan tästä perusteellisesti muuttuneesta kyberuhkaympäristöstä johtuviin kyberturvallisuushaasteisiin. Kuten ENISAn arvioinnissa todettiin, sen nykyinen toimeksianto ei ole riittävä näiden haasteiden kannalta.

(17) Tällä asetuksella perustetun ENISAn olisi jatkettava asetuksella (EU) N:o 526/2013 perustetun ENISAn toimintaa. ENISAn olisi hoidettava tehtäviä, jotka sille annetaan tässä asetuksessa ja muissa unionin säädöksissä kyberturvallisuuden alalla, muun muassa tarjoamalla neuvontaa ja asiantuntemusta ja toimimalla unionin tietokeskuksena. Sen olisi edistettävä parhaiden käytäntöjen vaihtoa jäsenvaltioiden ja yksityisten sidosryhmien välillä antamalla toimintapoliittisia ehdotuksia komissiolle ja jäsenvaltioille, toimimalla viitetahona unionin alakohtaisille toimintapoliittisille aloitteille kyberturvallisuuskysymyksissä ja edistämällä operatiivista yhteistyötä sekä jäsenvaltioiden välillä että jäsenvaltioiden ja unionin toimielinten, elinten ja laitosten välillä.

(18) Valtion- tai hallitusten päämiesten tasolla kokoontuneiden jäsenvaltioiden edustajien yhteisellä sopimuksella tehdyllä päätöksellä (2004/97/EY, Euratom[1]) jäsenvaltioiden edustajat päättivät, että ENISAn kotipaikaksi tulee Kreikan hallituksen myöhemmin nimeämä kaupunki Kreikassa. ENISAn isäntäjäsenvaltion olisi huolehdittava siitä, että ENISAlla on parhaat mahdolliset toimintaedellytykset. ENISAn tehtävien moitteettoman ja tehokkaan suorittamisen, henkilöstön palvelukseenoton ja sitouttamisen sekä verkostoitumisen tehokkuuden kannalta ENISAn on sijaittava soveltuvassa paikassa, jossa on muun muassa toimivat liikenneyhteydet ja palveluja ENISAn henkilöstön mukana tuleville puolisoille ja lapsille. Tarvittavat järjestelyt olisi vahvistettava ENISAn ja isäntäjäsenvaltion välisessä sopimuksessa, joka tehdään sen jälkeen kun ENISAn johtokunta on antanut hyväksyntänsä.

(19) Unioniin kohdistuvien kyberturvallisuusriskien ja -haasteiden lisääntyessä ENISAn määrärahoja ja henkilöresursseja olisi lisättävä siten, että ne vastaavat sen uutta roolia ja tehtäviä sekä sen keskeistä asemaa unionin digitaalista ekosysteemiä puolustavassa organisaatioiden ekosysteemissä, mikä antaisi ENISAlle mahdollisuuden toteuttaa tehokkaasti sille tällä asetuksella annetut tehtävät.

[1] Valtion- tai hallitusten päämiesten tasolla kokoontuneiden jäsenvaltioiden edustajien yhteisellä sopimuksella tehty päätös 2004/97/EY, Euratom, tehty 13 päivänä joulukuuta 2003, Euroopan unionin tiettyjen laitosten ja virastojen kotipaikan vahvistamisesta (EUVL L 29, 3.2.2004, s. 15).

(20) ENISAn olisi kehitettävä ja ylläpidettävä korkealaatuista asiantuntemusta ja toimittava viitetahona, joka vahvistaa uskoa ja luottamusta sisämarkkinoihin riippumattomuutensa, antamansa neuvonnan ja levittämänsä tiedon laadun, menettelyjensä ja toimintatapojensa avoimuuden sekä tehtäviensä suorittamisessa osoittamansa huolellisuuden ansiosta. ENISAn olisi aktiivisesti tuettava kansallisia toimia ja osaltaan proaktiivisesti edistettävä unionin toimia ja suoritettava tehtävänsä täydessä yhteistyössä unionin toimielinten, elinten ja laitosten sekä jäsenvaltioiden kanssa, vältettävä päällekkäistä työtä sekä edistettävä synergiaa. Lisäksi ENISAn olisi hyödynnettävä yksityisen sektorin ja muiden asiaankuuluvien sidosryhmien näkemyksiä ja niiden kanssa tehtävää yhteistyötä. ENISAn tehtävänannossa olisi vahvistettava, miten ENISAn on määrä saavuttaa tavoitteensa niin, että se pystyy toimimaan joustavasti.

(21) Jotta ENISA voisi tukea asianmukaisesti jäsenvaltioiden operatiivista yhteistyötä, sen olisi vahvistettava entisestään sen teknisiä ja henkilöstöön liittyviä valmiuksia ja taitoja. ENISAn olisi parannettava osaamistaan ja valmiuksiaan. ENISA ja jäsenvaltiot voisivat kehittää vapaaehtoisuuden pohjalta ohjelmia kansallisten asiantuntijoiden lähettämiseksi ENISAan, asiantuntijapoolien perustamiseksi ja henkilöstön vaihtamiseksi.

(22) ENISAn olisi avustettava komissiota antamalla neuvoja, lausuntoja ja analyysejä kaikista unionin asioista, jotka liittyvät kyberturvallisuusalaa ja sen alakohtaisia näkökohtia koskevan toimintapolitiikan ja lainsäädännön kehittämiseen, päivittämiseen ja uudelleentarkasteluun, jotta kyberturvallisuuteen liittyvistä unionin toimintapolitiikoista ja lainsäädännöstä saataisiin merkityksellisempiä ja kyseiset toimintapolitiikat ja lainsäädäntö voitaisiin panna yhdenmukaisesti täytäntöön kansallisella tasolla. ENISAn olisi toimittava neuvonnan ja asiantuntemuksen viitetahona unionin alakohtaisille toimintapoliittisille ja lainsäädännöllisille aloitteille, kun niihin liittyy kyberturvallisuuskysymyksiä. ENISAn olisi säännöllisesti tiedotettava toiminnastaan Euroopan parlamentille.

(23) Avoimen internetin julkinen ydin – eli sen tärkeimmät protokollat ja infrastruktuuri, jotka ovat globaali julkishyödyke – huolehtii koko internetin keskeisistä toiminnoista ja tukee sen normaalia toimintaa. ENISAn olisi tuettava muun muassa mutta ei pelkästään avoimen internetin julkisen ytimen keskeisten protokollien (erityisesti DNS:n, BGP:n ja iPv6:n) toiminnan turvallisuutta ja vakautta, verkkotunnusjärjestelmän toimintaa (mukaan lukien kaikkien aluetunnusten toiminta) sekä juurialueen toimintaa.

(24) ENISAn lähtökohtaisena tehtävänä on edistää asianomaisen lainsäädännön johdonmukaista täytäntöönpanoa ja erityisesti direktiivin (EU) 2016/1148 ja muiden asiaankuuluvien kyberturvallisuusnäkökohtia käsittelevien säädösten tehokasta täytäntöönpanoa, millä on olennainen merkitys kyberresilienssin lisäämisen kannalta. Koska kyberuhkaympäristö muuttuu nopeasti, on selvää, että jäsenvaltioita on tuettava omaksumalla kokonaisvaltaisempi, monialainen lähestymistapa kyberresilienssin rakentamiseen.

(25) ENISAn olisi avustettava jäsenvaltioita sekä unionin toimielimiä, elimiä ja laitoksia niiden pyrkimyksissä kehittää ja parantaa valmiuksia ja varautumiskykyä ehkäistä ja havaita kyberuhkia ja -poikkeamia ja reagoida niihin verkko- ja tietojärjestelmien turvallisuuden kannalta. ENISAn olisi erityisesti tuettava direktiivillä (EU) 2016/1148 perustettujen kansallisten ja unionin tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden, jäljempänä 'CSIRT-toimijat', kehittämistä ja tehostamista, jotta niiden kehitysaste olisi yhteisellä korkealla tasolla unionissa. Jäsenvaltioiden operatiivisiin valmiuksiin liittyvien ENISAn toimien olisi tuettava aktiivisesti toimia, joita jäsenvaltiot toteuttavat täyttääkseen direktiivistä (EU) 2016/1148 johtuvat velvoitteensa. ENISAn toimet eivät siksi saisi syrjäyttää jäsenvaltioiden toimia.

(26) ENISAn olisi myös autettava kehittämään ja päivittämään unionin ja pyynnöstä jäsenvaltioiden strategioita, jotka koskevat verkko- ja tietojärjestelmien turvallisuutta, erityisesti kyberturvallisuutta, ja sen olisi edistettävä tällaisten strategioiden levittämistä ja seurattava niiden täytäntöönpanon edistymistä. ENISAn olisi myös osallistuttava koulutusta ja koulutusmateriaalia koskevien tarpeiden kattamiseen, myös julkisten elinten tarpeiden osalta, ja tarvittaessa suuressa määrin 'koulutettava kouluttajia' kansalaisille tarkoitetun eurooppalaisen digitaalisten taitojen puitekehyksen pohjalta, jotta jäsenvaltioita sekä unionin toimielimiä, elimiä ja laitoksia voidaan auttaa kehittämään omia koulutusvalmiuksiaan.

(27) ENISAn olisi tuettava jäsenvaltioita kyberturvallisuutta koskevan tietoisuuden lisäämisen ja koulutuksen alalla helpottamalla tiiviimpää yhteistyötä ja parhaiden käytäntöjen vaihtoa jäsenvaltioiden välillä. Tällaiseen tukeen voisi kuulua muun muassa kansallisten koulutusalan yhteyspisteiden verkoston ja kyberturvallisuuden koulutusfoorumin kehittäminen. Kansallisten koulutusalan yhteyspisteiden verkosto voisi toimia kansallisten yhteyshenkilöiden verkostossa ja olla tulevan jäsenvaltioiden sisäisen koordinoinnin käynnistäjä.

(28) ENISAn olisi avustettava direktiivillä (EU) 2016/1148 perustettua yhteistyöryhmää sen tehtävien suorittamisessa erityisesti tarjoamalla asiantuntemusta ja neuvontaa sekä helpottamalla parhaiden käytäntöjen vaihtoa muun muassa jäsenvaltioiden toteuttamasta keskeisten palvelujen tarjoajien määrittämisestä, myös rajat ylittävien riippuvuussuhteiden osalta, siltä osin kuin kyse on riskeistä ja poikkeamista.

(29) Julkisen ja yksityisen sektorin välisen ja yksityisen sektorin sisäisen yhteistyön edistämiseksi ja erityisesti kriittisten infrastruktuurien suojelun tukemiseksi ENISAn olisi tuettava alojen sisäistä ja niiden välistä tietojen jakamista – erityisesti direktiivin (EU) 2016/1148 liitteessä II lueteltujen alojen osalta – tarjoamalla käyttöön parhaita käytäntöjä ja ohjeita käytettävissä olevista välineistä ja menettelyistä sekä ohjeita tietojen jakamiseen liittyvien sääntelykysymysten ratkaisemiseksi esimerkiksi helpottamalla tietojen jakamisen ja analysoinnin alakohtaisten keskusten perustamista.

(30) Koska tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien haavoittuvuuksien potentiaaliset kielteiset vaikutukset lisääntyvät jatkuvasti, tällaisten haavoittuvuuksien löytämisellä ja korjaamisella on merkittävä rooli kyberturvallisuuteen kohdistuvan kokonaisriskin pienentämisessä. Organisaatioiden, haavoittuvien tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien valmistajien tai tarjoajien sekä haavoittuvuuksia löytävien kyberturvallisuusalan tutkimusyhteisön jäsenten ja hallitusten välisen yhteistyön on todettu lisäävän merkittävästi tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien haavoittuvuuksien löytämistä ja korjaamista. Koordinoitu haavoittuvuuksien julkistaminen on jäsennelty yhteistyöprosessi, jossa haavoittuvuuksista raportoidaan tietojärjestelmän omistajalle, minkä ansiosta organisaatio voi diagnosoida ja korjata haavoittuvuuden ennen kuin sitä koskevat yksityiskohtaiset tiedot julkistetaan kolmansille osapuolille tai suurelle yleisölle. Prosessiin sisältyy myös löytäjän ja organisaation välinen koordinointi kyseisten haavoittuvuuksien julkaisemisen osalta. Koordinoiduilla haavoittuvuuksien julkistamisen hallintapolitiikalla voi olla merkittävä rooli kyberturvallisuuden lisäämiseen tähtäävissä jäsenvaltioiden toimissa.

(31) ENISAn olisi koottava ja analysoitava CSIRT-toimijoiden ja Euroopan parlamentin, Eurooppa-neuvoston, Euroopan unionin neuvoston, Euroopan komission, Euroopan unionin tuomioistuimen, Euroopan keskuspankin, Euroopan tilintarkastustuomioistuimen, Euroopan ulkosuhdehallinnon, Euroopan talous- ja sosiaalikomitean, Euroopan alueiden komitean ja Euroopan investointipankin välisellä järjestelyllä unionin toimielinten, elinten ja virastojen tietotekniikan kriisiryhmän (CERT-EU) organisaatiosta ja toiminnasta perustetun unionin toimielinten, elinten ja laitosten tietotekniikan kriisiryhmän, jäljempänä CERT-EU:n[1] vapaaehtoisesti toimittamat kansalliset raportit tietojenvaihdossa käytettävien yhteisten menettelyjen, kielen ja terminologian vahvistamista varten. Tässä yhteydessä ENISAn olisi myös otettava yksityinen sektori mukaan direktiivin (EU) 2016/1148 kehykseen, jossa vahvistettiin perusta vapaaehtoiselle teknisten tietojen vaihdolle operatiivisella tasolla kyseisellä direktiivillä perustetussa tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden välisessä verkostossa, jäljempänä 'CSIRT-verkosto'.

[1] EUVL C 12, 13.1.2018, s. 1.

(32) ENISAn olisi osallistuttava unionin tason reagointiin laajamittaisten rajat ylittävien kyberturvallisuuspoikkeamien ja -kriisien tapauksessa. Tämä tehtävä olisi täytettävä ENISAn tämän asetuksen mukaisen toimeksiannon ja sen toimintamallin mukaisesti, josta jäsenvaltiot sopivat komission suosituksen (EU) 2017/1584[1] ja EU:n koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin 26 päivänä kesäkuuta 2018 annettujen neuvoston päätelmien perusteella. Tähän tehtävään voisi kuulua tarvittavan tiedon keruu ja toimiminen välittäjänä CSIRT-verkoston ja tekniikan alan toimijoiden sekä kriisinhallinnasta vastaavien päätöksentekijöiden välillä. Lisäksi ENISAn olisi voitava yhden tai useamman jäsenvaltion pyynnöstä tukea jäsenvaltioiden välistä operatiivista yhteistyötä poikkeamien käsittelemisessä teknisestä näkökulmasta helpottamalla tarvittavaa ratkaisujen teknistä vaihtoa jäsenvaltioiden välillä ja osallistumalla julkiseen viestintään. ENISAn olisi tuettava tätä prosessia testaamalla tällaista yhteistyötä koskevia järjestelyjä säännöllisissä kyberturvallisuusharjoituksissa.

(33) ENISAn olisi operatiivista yhteistyötä tukiessaan hyödynnettävä saatavilla olevaa CERT-EU:n teknistä ja operatiivista asiantuntemusta jäsennellyssä yhteistyössä. Tällainen jäsennelty yhteistyö voisi kehittää ENISAn asiantuntemusta. Tarvittaessa tällaisen yhteistyön käytännön toteutus olisi määriteltävä erityisin järjestelyin näiden kahden yhteisön välillä päällekkäisiä tehtäviä välttäen.

---

[1] Komission suositus (EU) 2017/1584, annettu 13 päivänä syyskuuta 2017, koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin (EUVL L 239, 19.9.2017, s. 36).

(34) Operatiivista yhteistyötä CSIRT-verkostossa tukevia tehtäviänsä suorittaessaan ENISAn olisi voitava tarjota pyynnöstä tukea jäsenvaltioille esimerkiksi antamalla neuvoja siitä, miten nämä voivat kehittää valmiuksiaan ehkäistä ja havaita poikkeamia sekä reagoida niihin, helpottamalla vaikutukseltaan merkittävien poikkeamien teknistä käsittelyä tai varmistamalla, että kyberuhat ja poikkeamat analysoidaan. ENISAn olisi helpotettava vaikutukseltaan merkittävien poikkeamien teknistä käsittelyä erityisesti tukemalla teknisten ratkaisujen vapaaehtoista jakamista jäsenvaltioiden välillä tai tuottamalla yhdistettyjä teknisiä tietoja, kuten jäsenvaltioiden vapaaehtoisesti jakamia teknisiä ratkaisuja. Komission suosituksessa (EU) 2017/1584 suositellaan, että jäsenvaltiot tekisivät yhteistyötä vilpittömässä mielessä ja vaihtaisivat keskenään ja ENISAn kanssa tietoja laajamittaisista kyberturvallisuuspoikkeamista ja kyberturvallisuuskriiseihin liittyviä tietoja ilman aiheetonta viivytystä. Tällainen tieto auttaisi ENISAa sen operatiivisen yhteistyön tukemiseen liittyvien tehtävien suorittamisessa.

(35) ENISAn olisi osana unionin tilannetietoisuutta tukevaa säännöllistä teknisen tason yhteistyötä laadittava poikkeamista ja kyberuhkista säännöllisesti ja tiiviissä yhteistyössä jäsenvaltioiden kanssa perusteellisia unionin kyberturvallisuuden teknisiä tilanneraportteja, jotka perustuvat julkisesti saatavilla oleviin tietoihin, sen omaan analyysiin sekä raportteihin, joita se on saanut jäsenvaltioiden CSIRT-toimijoilta tai direktiivillä (EU) 2016/1148 perustetuilta verkko- ja tietojärjestelmien turvallisuudesta vastaavilta keskitetyiltä kansallisilta yhteyspisteiltä, jäljempänä 'keskitetyt yhteyspisteet', vapaehtoisuuteen perustuvassa tiedonvaihdossa taikka Europolissa toimivalta Euroopan kyberrikostorjuntakeskukselta, jäljempänä 'EC3', ja CERT-EU:lta sekä tarvittaessa Euroopan unionin tiedusteluanalyysikeskukselta (EU INTCEN) ja Euroopan ulkosuhdehallinnolta. Raportti olisi asetettava neuvoston, komission ja unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan asianomaisten yksiköiden ja CSIRT-verkoston saataville.

(36) ENISAn tuessa vaikutukseltaan merkittävien poikkeamien jälkikäteen tehtävälle tekniselle tutkinnalle, jota asianomaiset jäsenvaltiot ovat pyytäneet, olisi keskityttävä poikkeamien välttämiseen jatkossa. Kyseisten jäsenvaltioiden olisi toimitettava ENISAlle tarvittavat tiedot ja apu, jotta tämä voi tehokkaasti tukea jälkikäteen tehtävää teknistä tutkintaa.

(37) Jäsenvaltiot voivat pyytää yrityksiä, joita poikkeama koskee, tekemään yhteistyötä antamalla tarvittavan tiedon ja avun ENISAlle, sanotun kuitenkaan rajoittamatta niiden oikeutta suojata kaupallisesti arkaluonteiset tiedot ja yleisen turvallisuuden kannalta merkitykselliset tiedot.

(38) Ymmärtääkseen paremmin kyberturvallisuuden alaan liittyviä haasteita ja tarjotakseen strategista pitkän aikavälin neuvontaa jäsenvaltioille ja unionin toimielimille, elimille ja laitoksille ENISAn on tarpeen analysoida nykyisiä ja kehittymässä olevia kyberturvallisuusriskejä. Tätä varten ENISAn olisi yhteistyössä jäsenvaltioiden ja tarvittaessa tilastokeskusten ja muiden elinten kanssa kerättävä tarvittavaa julkisesti saatavilla olevaa tai vapaaehtoisesti toimitettua tietoa sekä tehtävä analyysejä uusista teknologioista ja aihekohtaisia arviointeja teknologisten innovaatioiden odotettavissa olevista yhteiskunnallisista, oikeudellisista, taloudellisista ja sääntelyyn liittyvistä vaikutuksista verkko- ja tietoturvallisuuden ja erityisesti kyberturvallisuuden kannalta. ENISAn olisi myös tuettava jäsenvaltioita ja unionin toimielimiä, elimiä ja laitoksia riskien kartoittamisessa ja poikkeamien ehkäisyssä tekemällä analyyseja kyberuhkista, haavoittuvuuksista ja poikkeamista.

(39) Unionin häiriönsietokyvyn lisäämiseksi ENISAn olisi kehitettävä erityisesti direktiivin (EU) 2016/1148 liitteessä II mainittuja aloja tukevien ja saman direktiivin liitteessä III mainittujen digitaalisten palvelujen tarjoajien hyödyntämien infrastruktuurien kyberturvallisuuteen liittyvää asiantuntemusta tarjoamalla neuvontaa, antamalla ohjeita ja vaihtamalla parhaita käytäntöjä. Jotta kyberturvallisuusriskeistä ja mahdollisista suojakeinoista saataisiin tietoa helpommin ja paremmin jäsennellyssä muodossa, ENISAn olisi kehitettävä unionin 'tietokeskus' ja ylläpidettävä sitä. Kyseessä on keskitetty verkkoportaali, josta yleisö saa unionin ja kansallisilta toimielimiltä, elimiltä ja laitoksilta peräisin olevaa tietoa kyberturvallisuudesta. Kyberturvallisuusriskejä ja mahdollisia suojakeinoja koskevien paremmin jäsenneltyjen tietojen saannin helpottaminen voi myös auttaa jäsenvaltioita kehittämään valmiuksiaan, yhdenmukaistamaan käytäntöjään ja siten parantamaan yleistä kyberhyökkäysten sietokykyä.

(40) ENISAn olisi autettava lisäämään yleisön tietoisuutta kyberturvallisuusriskeistä, myös unionin laajuisella tiedotuskampanjalla koulutusta edistämällä, ja antamaan kansalaisten, organisaatioiden ja yritysten käyttöön yksittäisille käyttäjille tarkoitettuja ohjeita hyvistä toimintatavoista. ENISAn olisi myös osaltaan edistettävä parhaita käytäntöjä ja ratkaisuja, kuten kyberhygieniaa ja kyberlukutaitoa, kansalaisten, organisaatioiden ja yritysten tasolla keräämällä ja analysoimalla julkisesti saatavilla olevia tietoja merkittävistä poikkeamista ja kokoamalla ja julkaisemalla raportteja ja ohjeita ohjeistuksen antamiseksi kansalaisille, organisaatioille ja yrityksille yleisen varautumis- ja häiriönsietokykytason parantamiseksi. ENISAn olisi myös pyrittävä tarjoamaan kuluttajille asiaa koskevia tietoa sovellettavista sertifiointijärjestelmistä esimerkiksi tarjoamalla ohjeistusta ja suosituksia. ENISAn olisi myös järjestettävä 17 päivänä tammikuuta 2018 annetun komission tiedonannon perusteella perustetun digitaalisen koulutuksen toimintasuunnitelman mukaisesti ja yhteistyössä jäsenvaltioiden sekä unionin toimielinten, elinten, ja laitosten kanssa säännöllisiä loppukäyttäjille suunnattuja tiedotus- ja valistuskampanjoita, jotta edistetään turvallisempaa verkkokäyttäytymistä yksilötasolla ja digitaalista lukutaitoa ja lisätään tietoisuutta kybertoimintaympäristössä piilevistä mahdollisista kyberuhkista, mukaan lukien verkkourkintayritysten, bottiverkkojen, talous- ja pankkipetosten sekä tietopetostapahtumien kaltainen kyberrikollisuus, sekä edistetään yleisluonteisen neuvonnan antamista monivaiheista aitouden todentamista, paikkausta, salaamista, anonymisointia ja tietosuojaa koskevissa kysymyksissä.

(41) ENISAlla olisi oltava keskeinen rooli pyrittäessä lisäämään loppukäyttäjien tietoisuutta laitteiden turvallisuudesta ja palvelujen turvallisesta käytöstä, ja sen olisi edistettävä unionin tasolla sisäänrakennettua turvallisuutta ja sisäänrakennettua yksityisyyttä. Tähän tavoitteeseen pyrkiessään ENISAn olisi hyödynnettävä mahdollisimman laajasti saatavilla olevia parhaita käytäntöjä ja kokemuksia, erityisesti akateemisilta laitoksilta sekä tietotekniikan turvallisuuden tutkijoilta.

(42) Kyberturvallisuuden alalla toimivien yritysten ja kyberturvallisuusratkaisujen käyttäjien tukemiseksi ENISAn olisi kehitettävä 'markkinoiden seurantakeskus' ja ylläpidettävä sitä tekemällä säännöllisiä analyyseja kyberturvallisuusmarkkinoiden tärkeimmistä suuntauksista sekä kysyntä- että tarjontapuolella ja levittämällä tietoa näistä suuntauksista.

(43) ENISAn olisi tuettava unionin toimia, joiden tavoitteena on edistää yhteistyötä kansainvälisten organisaatioiden kanssa sekä asianmukaisissa kansainvälisissä yhteistyöpuitteissa kyberturvallisuuden alalla. ENISAn olisi tarvittaessa tuettava erityisesti OECD:n, Etyjin ja Naton kaltaisten organisaatioiden kanssa tehtävää yhteistyötä. Yhteistyöhön voisi sisältyä muun muassa yhteisiä kyberturvallisuusharjoituksia ja yhteisen kyberturvallisuuspoikkeamiin reagoimisen koordinointia. Näissä toimissa on määrä noudattaa kaikilta osin osallistavuuden, vastavuoroisuuden ja unionin päätöksenteon riippumattomuuden periaatteita, vaikuttamatta yhdenkään jäsenvaltion turvallisuus- ja puolustuspolitiikan erityisluonteeseen.

(44) Varmistaakseen tavoitteidensa täysimittaisen saavuttamisen ENISAn olisi oltava yhteydessä asiaankuuluviin unionin valvontaviranomaisiin ja muihin toimivaltaisiin viranomaisiin unionissa, unionin toimielimiin, elimiin ja laitoksiin, mukaan lukien CERT-EU, EC3, Euroopan puolustusvirasto (EDA), Euroopan GNSS-virasto (GSA), Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelin (BEREC), laaja-alaisten tietojärjestelmien operatiivisesta hallinnoinnista vastaava eurooppalainen virasto (eu-LISA), Euroopan keskuspankki (EKP), Euroopan pankkiviranomainen (EPV), Euroopan tietosuojaneuvosto, Energia-alan sääntelyviranomaisten yhteistyövirasto (ACER), Euroopan unionin lentoturvallisuusvirasto (EASA) sekä muut kyberturvallisuuteen liittyviä kysymyksiä käsittelevät unionin virastot. ENISAn olisi oltava yhteydessä myös tietosuoja-asioita käsitteleviin viranomaisiin, jotta voidaan vaihtaa tietotaitoa ja parhaita käytäntöjä, ja annettava neuvontaa kyberturvallisuuskysymyksistä, joilla voi olla vaikutusta niiden toimintaan. Kansallisten ja unionin lainvalvonta- ja tietosuojaviranomaisten edustajien olisi voitava olla edustettuina ENISAn neuvoa-antavassa ryhmässä. Ollessaan yhteydessä lainvalvontaviranomaisiin sellaisissa verkko- ja tietoturvakysymyksissä, joilla voi olla vaikutusta niiden toimintaan, ENISAn olisi käytettävä olemassa olevia tietojenvaihtokanavia ja vakiintuneita verkostoja.

(45) Voitaisiin muodostaa kumppanuuksia sellaisten akateemisten laitosten kanssa, joilla on tutkimusaloitteita merkityksellisillä aloilla, ja olisi oltava sopivat kanavat kuluttajajärjestöiltä ja muilta järjestöiltä tuleville tiedoille, jotka olisi otettava huomioon

(46) ENISAn olisi asemassaan CSIRT-verkoston sihteeristönä tuettava jäsenvaltioiden CSIRT-toimijoita ja CERT-EU:ta operatiivisessa yhteistyössä kaikkien asiaankuuluvien CSIRT-verkoston tehtävien osalta, sellaisina kuin niihin viitataan direktiivissä (EU) 2016/1148. ENISAn olisi lisäksi edistettävä ja tuettava yhteistyötä asianomaisten CSIRT-toimijoiden välillä tapauksissa, joissa CSIRT-toimijoiden hallinnoimiin tai suojaamiin verkkoihin tai infrastruktuureihin kohdistuu poikkeamia, hyökkäyksiä tai häiriöitä, jotka koskevat tai mahdollisesti koskevat vähintään kahta CSIRT-toimijaa, ottaen asianmukaisesti huomioon CSIRT-verkoston menettelyohjeet.

(47) Jotta voidaan lisätä unionin varautumista kyberturvallisuuspoikkeamiin reagoimiseksi, ENISAn olisi järjestettävä säännöllisesti kyberturvallisuusharjoituksia unionin tasolla sekä tuettava jäsenvaltioita ja unionin toimielimiä, elimiä ja laitoksia niiden pyynnöstä harjoitusten järjestämisessä. Joka toinen vuosi olisi järjestettävä laajamittainen kattava harjoitus, joka sisältää teknisiä, operatiivisia ja strategisia osatekijöitä. Lisäksi ENISAn olisi voitava järjestää säännöllisesti vähemmän kattavia harjoituksia, joiden tavoitteena on samalla tavoin lisätä unionin varautumista poikkeamiin reagoimiseksi.

(48) ENISAn olisi kehitettävä edelleen ja ylläpidettävä asiantuntemustaan kyberturvallisuussertifioinnissa, jotta voidaan tukea unionin politiikkaa kyseisellä alalla. ENISAn olisi kehitettävä edelleen nykyisiä parhaita käytäntöjä ja edistettävä kyberturvallisuussertifioinnin käyttöä unionissa muun muassa osallistumalla kyberturvallisuuden sertifiointikehyksen perustamiseen ja ylläpitoon unionin tasolla (eurooppalainen kyberturvallisuuden sertifiointikehys), jotta voidaan lisätä avoimuutta tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien kyberturvallisuuden varmistuksessa ja tällä tavoin vahvistaa luottamusta digitaalisiin sisämarkkinoihin.

(49) Tehokkaan kyberturvallisuuspolitiikan olisi perustuttava kehittyneisiin riskinarviointimenetelmiin niin julkisella kuin yksityiselläkin sektorilla. Riskinarviointimenetelmiä käytetään eri tasoilla vailla yhteistä tehokasta soveltamiskäytäntöä. Riskinarvioinnin ja yhteentoimivien riskinhallintaratkaisujen parhaiden käytäntöjen edistäminen ja kehittäminen julkisen sektorin ja yksityisen sektorin organisaatioissa nostaa kyberturvallisuustasoa unionissa. Tätä varten ENISAn olisi tuettava sidosryhmien yhteistyötä unionin tasolla ja helpotettava niiden pyrkimyksiä laatia ja ottaa käyttöön eurooppalaisia ja kansainvälisiä standardeja riskinhallinnalle ja mitattavissa olevalle turvallisuudelle sähköisissä tuotteissa, järjestelmissä, verkoissa ja palveluissa, jotka yhdessä ohjelmistojen kanssa muodostavat verkko- ja tietojärjestelmät.

(50) ENISAn olisi kannustettava jäsenvaltioita, tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien valmistajia ja tarjoajia tiukentamaan yleisiä turvallisuusnormejaan, jotta kaikki internetin käyttäjät voivat toteuttaa tarvittavat toimenpiteet oman kyberturvallisuutensa varmistamiseksi, ja niille olisi luotava kannustimia tätä tarkoitusta varten. Erityisesti tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien tuottajien olisi järjestettävä tarpeelliset päivitykset, ja niiden olisi vedettävä pois markkinoilta, poistettava tuotannosta tai kierrätettävä tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit, jotka eivät täytä kyberturvallisuusstandardeja, ja samalla maahantuojien ja jakelijoiden olisi varmistettava, että niiden unionin markkinoille saattamat tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit täyttävät sovellettavat vaatimukset eivätkä aiheuta riskiä unionin kuluttajille.

(51) ENISAn olisi voitava yhteistyössä toimivaltaisten viranomaisten kanssa levittää tietoa sisämarkkinoilla tarjottavien tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien kyberturvallisuustasosta ja antaa varoituksia palveluntarjoajille ja valmistajille ja vaatia niitä parantamaan tieto- ja viestintätekniikan tuotteidensa, palvelujensa ja prosessiensa turvallisuutta, mukaan lukien kyberturvallisuus.

(52) ENISAn olisi otettava täysimääräisesti huomioon meneillään olevat tutkimus-, kehittämis- ja teknologian arvioimistoimet, erityisesti sellaiset, joita toteutetaan unionin eri tutkimusaloitteissa, antaakseen unionin toimielimille, elimille ja laitoksille sekä tarvittaessa jäsenvaltioille niiden pyynnöstä neuvoja kyberturvallisuusalan tutkimustarpeista ja -prioriteeteista. ENISAn olisi myös kuultava asianomaisia käyttäjäryhmiä, jotta se voi määritellä tutkimustarpeet ja -prioriteetit. Olisi erityisesti tehtävä yhteistyötä Euroopan tutkimusneuvoston ja Euroopan innovaatio- ja teknologiainstituutin sekä Euroopan unionin turvallisuusalan tutkimuslaitoksen kanssa.

(53) ENISAn olisi kuultava säännöllisesti standardointiorganisaatioita ja erityisesti eurooppalaisia standardointiorganisaatioita eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä valmistellessaan.

(54) Kyberuhat ovat maailmanlaajuisia. Tarvitaan tiiviimpää kansainvälistä yhteistyötä kyberturvallisuusstandardien parantamiseksi, mihin sisältyy myös tarve yhteisten käyttäytymisnormien määrittelemiseen, käytännesääntöjen hyväksymiseen ja kansainvälisten standardien käyttämiseen, sekä tietojenvaihtoa kansainvälisen yhteistoiminnan nopeuttamiseksi verkko- ja tietoturvakysymyksissä samoin kuin yhteisen maailmanlaajuisen lähestymistavan edistämistä tällaisten kysymysten osalta. Tätä varten ENISAn olisi tuettava unionin osallistumista yhä enemmän kolmansien maiden ja kansainvälisten organisaatioiden kanssa harjoitettavaan yhteistyöhön tarjoamalla asianomaisten unionin toimielinten, elinten ja laitosten mahdollisesti tarvitsemaa asiantuntemusta ja analysointivalmiuksia.

(55) ENISAn olisi voitava vastata tapauskohtaisiin neuvonta- ja avustamispyyntöihin, joita jäsenvaltiot ja unionin toimielimet, elimet ja laitokset esittävät ja jotka ovat ENISAn toimeksiannon mukaisia.

(56) On järkevää ja suositeltavaa panna täytäntöön tiettyjä ENISAn hallintoa koskevia periaatteita, jotta voidaan noudattaa unionin erillisvirastoja käsittelevässä toimielinten välisessä työryhmässä heinäkuussa 2012 hyväksyttyä yhteistä julkilausumaa ja yhteistä lähestymistapaa, joiden tarkoituksena on tehostaa hajautettujen virastojen toimintaa ja parantaa niiden tuloksellisuutta. Yhteisen julkilausuman ja yhteisen lähestymistavan ohjeistus olisi myös otettava huomioon asianmukaisella tavalla ENISAn työohjelmissa, ENISAn arvioinneissa ja ENISAn raportointi- ja hallintokäytännöissä tässä asetuksessa.

(57) Johtokunnan, jossa ovat edustettuna jäsenvaltiot ja komissio, olisi määriteltävä ENISAn toiminnan yleinen suunta ja varmistettava, että se hoitaa tehtäviään tämän asetuksen mukaisesti. Johtokunnalle olisi annettava tarvittavat valtuudet hyväksyä talousarvio, tarkastaa talousarvion toteuttamista, vahvistaa tarvittavat varainhoitoa koskevat säännöt, luoda avoimet menettelyt ENISAn päätöksentekoa varten, hyväksyä ENISAn yhtenäinen ohjelma-asiakirja, vahvistaa työjärjestyksensä, nimittää pääjohtaja sekä päättää tämän toimikauden jatkamisesta ja päättymisestä.

(58) ENISAn moitteettoman ja tehokkaan toiminnan takaamiseksi komission ja jäsenvaltioiden olisi varmistettava, että johtokunnan jäseniksi nimitettävillä henkilöillä on riittävä ammatillinen asiantuntemus ja asianmukainen kokemus. Johtokunnan työn jatkuvuuden varmistamiseksi komission ja jäsenvaltioiden olisi myös pyrittävä rajoittamaan johtokunnassa olevien edustajiensa vaihtuvuutta.

(59) ENISAn moitteeton toiminta edellyttää, että sen pääjohtaja nimitetään ansioiden ja todistuksin osoitettujen hallinnollisten taitojen ja johtamistaitojen sekä kyberturvallisuuden kannalta merkityksellisen pätevyyden ja kokemuksen perusteella. Pääjohtajan tehtäviä olisi hoidettava täysin riippumattomasti. Pääjohtajan olisi laadittava ehdotus ENISAn vuotuiseksi työohjelmaksi kuultuaan ensin komissiota ja toteutettava kaikki tarvittavat toimenpiteet varmistaakseen kyseisen työohjelman asianmukaisen toteuttamisen. Pääjohtajan olisi laadittava johtokunnalle esitettävä vuosikertomus, jossa käsitellään ENISAn vuotuisen työohjelman toteuttamista, sekä esitys ENISAn tuloja ja menoja koskevaksi ennakkoarvioksi ja vastattava talousarvion toteuttamisesta. Pääjohtajan olisi myös voitava perustaa tilapäisiä työryhmiä erityisesti tieteellisten, teknisten, oikeudellisten tai sosioekonomisten erityiskysymysten käsittelyä varten. Tilapäisen työryhmän perustamista pidetään tarpeellisena etenkin ehdolla olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän, jäljempänä 'ehdolla oleva järjestelmä', valmisteluun liittyen. Pääjohtajan olisi varmistettava, että tilapäisten työryhmien jäsenet valitaan huippuasiantuntemuksen perusteella ja siten, että pyritään varmistamaan sukupuolten tasapaino ja tarkasteltavien kysymysten edellyttämällä tavalla edustuksellinen tasapaino jäsenvaltioiden julkishallintojen, unionin toimielinten, elinten ja laitosten sekä yksityisen sektorin välillä, mukaan lukien toimiala, käyttäjät ja tiedeyhteisöä edustavat verkko- ja tietoturva-asiantuntijat.

(60) Hallituksen olisi edistettävä johtokunnan moitteetonta toimintaa. Osana johtokunnan päätöksiin liittyvää valmistelutyötään sen olisi tutkittava yksityiskohtaisesti asiaan liittyvät tiedot ja tarkasteltava käytettävissä olevia vaihtoehtoja sekä tarjottava neuvoja ja ratkaisuja johtokunnan päätösten valmistelemiseksi.

(61) ENISAlla olisi oltava neuvoa-antavana elimenä ENISAn neuvoa-antava ryhmä, jotta voitaisiin varmistaa säännöllinen vuoropuhelu yksityisen sektorin, kuluttajajärjestöjen ja muiden asianosaisten sidosryhmien kanssa. ENISAn neuvoa-antavan ryhmän, jonka johtokunta perustaa pääjohtajan ehdotuksesta, olisi keskityttävä sidosryhmiä koskeviin asioihin ja saatettava ne ENISAn tietoon. ENISAn neuvoa-antavan ryhmän kokoonpanossa ja tälle ryhmälle, jota kuullaan erityisesti työohjelmaluonnoksesta, annettavissa tehtävissä olisi varmistettava sidosryhmien riittävä edustus ENISAn työskentelyssä.

(62) Olisi perustettava sidosryhmien kyberturvallisuuden sertifiointiryhmä auttamaan ENISAa ja komissiota helpottamaan asianomaisten sidosryhmien kuulemista. Sidosryhmien kyberturvallisuuden sertifiointiryhmän jäsenten olisi edustettava oikeassa suhteessa toimialaa – sekä tieto- ja viestintätekniikan tuotteiden ja palvelujen kysyntä- että tarjontapuolta ja erityisesti pk-yrityksiä – digitaalisten palvelujen tarjoajia, eurooppalaisia ja kansainvälisiä standardointielimiä, kansallisia akkreditointielimiä, tietosuojaviranomaisia ja vaatimustenmukaisuuden arviointilaitoksia Euroopan parlamentin ja neuvoston asetuksen (EY) 765/2008[1] mukaisesti, tiedeyhteisöä sekä kuluttajajärjestöjä.

[1] Euroopan parlamentin ja neuvoston asetus (EY) N:o 765/2008, annettu 9 päivänä heinäkuuta 2008, tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja neuvoston asetuksen (ETY) N:o 339/93 kumoamisesta (EUVL L 218, 13.8.2008, s. 30).

(63) ENISAlla olisi oltava säännöt eturistiriitojen ehkäisemisestä ja hallinnasta. ENISAn olisi sovellettava asiakirjojen saamista yleisön tutustuttavaksi koskevia asiaankuuluvia unionin säännöksiä, sellaisina kuin ne on vahvistettu Euroopan parlamentin ja neuvoston asetuksessa (EY) N:o 1049/2001[1]. ENISAn suorittamassa henkilötietojen käsittelyssä olisi noudatettava Euroopan parlamentin ja neuvoston asetusta (EU) 2018/1725[2]. ENISAn olisi noudatettava tietojen käsittelyä koskevia unionin toimielimiin sovellettavia säännöksiä ja kansallista lainsäädäntöä, erityisesti kun on kyse arkaluonteisista turvallisuusluokittelemattomista tiedoista ja Euroopan unionin turvallisuusluokitelluista tiedoista (EUCI).

---

1 Euroopan parlamentin ja neuvoston asetus (EY) N:o 1049/2001, annettu 30 päivänä toukokuuta 2001, Euroopan parlamentin, neuvoston ja komission asiakirjojen saamisesta yleisön tutustuttavaksi (EYVL L 145, 31.5.2001, s. 43).

2 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).

(64) Jotta voidaan varmistaa ENISAn täydellinen itsemääräämisoikeus ja riippumattomuus ja jotta ENISA pystyy suorittamaan uusia ja täydentäviä tehtäviä, myös ennakoimattomia tehtäviä hätätilanteissa, ENISAlle olisi annettava riittävä ja itsenäinen talousarvio, jonka tulot muodostuisivat ensisijaisesti unionin rahoitusosuudesta ja ENISAn työhön osallistuvien kolmansien maiden rahoitusosuuksista. Asianmukaiset määrärahat ovat äärimmäisen tärkeät sen varmistamiseksi, että ENISAlla on riittävät valmiudet toteuttaa kaikki lisääntyvät tehtävänsä ja saavuttaa tavoitteensa. ENISAn henkilöstön enemmistön työtehtävien olisi liityttävä suoraan ENISAn toimeksiannon operatiiviseen täytäntöönpanoon. ENISAn isäntäjäsenvaltion ja minkä tahansa muun jäsenvaltion olisi voitava maksaa vapaaehtoisia rahoitusosuuksia ENISAlle. Unionin talousarviomenettelyä olisi sovellettava edelleen unionin yleisestä talousarviosta maksettaviin tukiin. Lisäksi tilintarkastustuomioistuimen olisi tarkastettava ENISAn tilit avoimuuden ja vastuuvelvollisuuden varmistamiseksi.

(65) Kyberturvallisuussertifioinnilla on tärkeä rooli lisättäessä tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien turvallisuutta ja luottamusta niitä kohtaan. Digitaaliset sisämarkkinat ja erityisesti datatalous ja esineiden internet voivat menestyä vain, jos vallitsee yleinen julkinen luottamus siihen, että tällaisissa tuotteissa, palveluissa ja prosesseissa varmistetaan tietyntasoinen kyberturvallisuus. Verkkoyhteyksillä varustetut ja automatisoidut autot, sähköiset terveyspalvelut, teollisuusautomaation ohjausjärjestelmät ja älykkäät sähköverkot ovat joitakin esimerkkejä aloista, joilla sertifiointi on jo laajalti käytössä tai tulee todennäköisesti käyttöön lähitulevaisuudessa. Direktiivillä (EU) 2016/1148 säännellyt alat ovat samalla aloja, joilla kyberturvallisuussertifioinnilla on ratkaiseva merkitys.

(66) Vuonna 2016 antamassaan tiedonannossa "Euroopan kyberresilienssijärjestelmän vahvistaminen sekä kilpailukykyisen ja innovatiivisen kyberturvallisuustoimialan tukeminen" komissio linjasi tarpeen ottaa käyttöön laadukkaita, kohtuuhintaisia ja yhteentoimivia kyberturvallisuustuotteita ja -ratkaisuja. Tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien tarjonta sisämarkkinoilla on edelleen maantieteellisesti hyvin hajanaista. Tämä johtuu siitä, että Euroopan kyberturvallisuusala on kehittynyt suurelta osin kansallisista valtiollisen kysynnän lähtökohdista. Kyberturvallisuuden alalla sisämarkkinoiden toimintapuutteisiin kuuluu lisäksi yhteentoimivien ratkaisujen (teknisten standardien), toimintatapojen ja unionin laajuisten sertifiointimekanismien puuttuminen. Tämä yhtäältä vaikeuttaa eurooppalaisten yritysten kilpailua niin kansallisella kuin Euroopan ja maailmanlaajuisellakin tasolla. Toisaalta se vähentää yksilöiden ja yritysten saatavilla olevan hyödyllisen ja käyttökelpoisen kyberturvallisuusteknologian valinnanvaraa. Samoin myös komission vuonna 2017 antamassaan tiedonannossa "Digitaalisten sisämarkkinoiden strategian täytäntöönpanon väliarviointi – Yhdennetyt digitaaliset sisämarkkinat kaikille" komissio korosti tarvetta huolehtia verkkoon liitettyjen tuotteiden ja järjestelmien turvallisuudesta ja totesi, että luomalla tieto- ja viestintätekniikan turvallisuudelle eurooppalaiset puitteet, joissa annetaan säännöt tieto- ja viestintäteknologian turvallisuussertifioinnin järjestämisestä unionissa, voitaisiin sekä ylläpitää luottamusta internetiin että puuttua sisämarkkinoiden nykyiseen hajanaisuuteen.

(67) Tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien kyberturvallisuussertifiointia käytetään tällä hetkellä vain vähäisessä määrin. Kun sitä käytetään, käyttö rajoittuu enimmäkseen jäsenvaltioiden tasolle tai teollisuuslähtöisten järjestelmien piiriin. Tässä yhteydessä yhden kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen myöntämää sertifikaattia ei periaatteessa tunnusteta muissa jäsenvaltioissa. Yritykset voivat näin ollen joutua sertifioimaan tieto- ja viestintätekniikan tuotteensa, palvelunsa ja prosessinsa useissa jäsenvaltioissa, joissa ne toimivat, esimerkiksi voidakseen osallistua kansallisiin hankintamenettelyihin, mikä aiheuttaa yrityksille lisäkustannuksia. Syntymässä on uusia järjestelmiä, mutta vaikuttaa siltä, ettei ole olemassa johdonmukaista ja kokonaisvaltaista lähestymistapaa laaja-alaisiin kyberturvallisuuskysymyksiin esimerkiksi esineiden internetin alalla. Nykyisissä järjestelmissä on merkittäviä puutteita ja eroja, jotka liittyvät niiden tuotekatteeseen, varmuustasoihin, aineellisiin edellytyksiin ja tosiasialliseen käyttöön, mikä haittaa vastavuoroisten tunnustamismekanismien toimintaa unionissa.

(68) Joillain toimilla on jo pyritty varmistamaan sertifikaattien vastavuoroinen tunnustaminen unionissa. Niiden tavoitteet on kuitenkin saavutettu vain osittain. Tärkein esimerkki tästä on johtavien virkamiesten tietoturvallisuusryhmän (SOG-IS) vastavuoroista tunnustamista koskeva sopimus (MRA). SOG-IS on tärkein malli yhteistyölle ja vastavuoroiselle tunnustamiselle turvallisuussertifioinnin alalla, mutta siihen kuuluu vain osa unionin jäsenvaltioista. Tämä seikka on rajoittanut SOG-ISia koskevan MRA-sopimuksen toimivuutta sisämarkkinoiden kannalta.

(69) Sen vuoksi on tarpeen omaksua yhteinen lähestymistapa ja perustaa eurooppalainen kyberturvallisuuden sertifiointikehys, jossa vahvistetaan tärkeimmät horisontaaliset vaatimukset kehitettäville eurooppalaisille kyberturvallisuuden sertifiointijärjestelmille ja jonka ansiosta tieto- ja viestintätekniikan tuotteita, palveluja ja prosesseja koskevat eurooppalaiset kyberturvallisuussertifikaatit ja EU-vaatimustenmukaisuusilmoitukset voidaan tunnustaa ja niitä voidaan käyttää kaikissa jäsenvaltioissa. Tässä yhteydessä on olennaista käyttää perustana nykyisiä kansallisia ja kansainvälisiä järjestelmiä sekä vastavuoroisen tunnustamisen järjestelmiä, erityisesti SOG-IS-järjestelmää, sekä mahdollistaa sujuva siirtyminen tällaisten järjestelmien piiriin kuuluvista nykyisistä järjestelmistä eurooppalaisen kehyksen mukaisiin uusiin järjestelmiin. Eurooppalaisen sertifiointikehyksen olisi palveltava kahta tarkoitusta. Ensinnäkin sen pitäisi lisätä luottamusta tieto- ja viestintätekniikan tuotteisiin, palveluihin ja prosesseihin, jotka on sertifioitu eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukaisesti. Toiseksi sen pitäisi auttaa välttämään tilanne, jossa käytössä on monia keskenään ristiriitaisia tai päällekkäisiä kansallisia kyberturvallisuussertifiointeja, ja auttaa siten vähentämään digitaalisilla sisämarkkinoilla yrityksille aiheutuvia kustannuksia. Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien olisi oltava syrjimättömiä ja eurooppalaisiin tai kansainvälisiin standardeihin perustuvia, paitsi jos kyseiset standardit ovat tehottomia tai epäasianmukaisia unionin oikeutettujen tavoitteiden saavuttamiseksi.

(70) Eurooppalaisen kyberturvallisuuden sertifiointikehyksen on oltava yhdenmukainen kaikissa jäsenvaltioissa, jotta vältetään ns. sertifiointishoppailu jäsenvaltioiden erilaisten vaatimustasojen vuoksi.

(71) Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien olisi perustettuttava siihen, mikä on jo käytössä kansainvälisellä ja kansallisella tasolla, ja tarvittaessa eri foorumeiden ja konsortioiden teknisiin eritelmiin, nykyisten vahvuuksien hyödyntämiseen sekä heikkouksien arviointiin ja korjaamiseen.

(72) Tarvitaan joustavia kyberturvallisuusratkaisuja, jotta toimialalla olisi etumatkaa kyberuhkiin nähden, joten sertifiointijärjestelmät olisi suunniteltava niin, että vältetään nopean vanhentumisen riski.

(73) Komissiolle olisi siirrettävä valta hyväksyä eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät yksittäisille tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien ryhmille. Kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten olisi vastattava näiden järjestelmien täytäntöönpanosta ja valvonnasta, ja näiden järjestelmien mukaisesti myönnettyjen sertifikaattien olisi oltava voimassa ja tunnustettuja kaikkialla unionissa. Toimialan tai muiden yksityisten organisaatioiden ylläpitämien sertifiointijärjestelmien ei tulisi kuulua tämän asetuksen soveltamisalaan. Tällaisia järjestelmiä ylläpitävien elinten olisi kuitenkin voitava ehdottaa, että komissio ottaa tällaiset järjestelmät lähtökohdaksi niiden hyväksymiseksi eurooppalaisena kyberturvallisuuden sertifiointijärjestelmänä.

(74) Tämän asetuksen säännökset eivät saisi vaikuttaa unionin lainsäädäntöön, jossa annetaan erityiset säännöt tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sertifioinnista. Erityisesti asetuksessa (EU) 2016/679 säädetään sertifiointimekanismeista sekä tietosuojasineteistä ja -merkeistä, joiden tarkoituksena on osoittaa, että rekisterinpitäjät ja henkilötietojen käsittelijät noudattavat kyseistä asetusta käsittelytoimia suorittaessaan. Rekisteröityjen olisi tällaisten sertifiointimekanismien ja tietosuojasinettien ja -merkkien avulla voitava nopeasti arvioida asianomaisten tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien tietosuojataso. Tämä asetus ei rajoita tietojenkäsittelytoimintojen sertifiointia asetuksen (EU) 2016/679 mukaisesti, ei myöskään silloin, kun nämä toimet on sisällytetty tieto- ja viestintätekniikan tuotteisiin, palveluihin ja prosesseihin.

(75) Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien tarkoituksena olisi oltava varmistaa, että tällaisissa järjestelmissä sertifioidut tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit täyttävät määritellyt vaatimukset, joiden tavoitteena on suojella tallennettujen, siirrettävien tai käsiteltävien tietojen tai niihin liittyvien, kyseisissä tuotteissa, palveluissa ja prosesseissa tarjottavien tai välitettävien tuotteiden, toimintojen ja palvelujen käytettävyyttä, aitoutta, eheyttä ja luottamuksellisuutta niiden koko elinkaaren ajan. Tässä asetuksessa ei ole mahdollista määritellä yksityiskohtaisesti kyberturvallisuusvaatimuksia kaikille tieto- ja viestintätekniikan tuotteille, palveluille ja prosesseille. Tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit ja näihin tuotteisiin, palveluihin ja prosesseihin liittyvät kyberturvallisuustarpeet ovat niin moninaiset, että on hyvin vaikeaa määritellä yleisiä kyberturvallisuusvaatimuksia, jotka olisivat voimassa kaikissa olosuhteissa. Siksi kyberturvallisuus olisi määriteltävä laajasti ja yleisesti sertifiointitarkoituksia varten, ja sitä olisi täydennettävä erityisillä kyberturvallisuustavoitteilla, jotka on tarpeen ottaa huomioon suunniteltaessa eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä. Järjestelyt, joilla tällaiset tavoitteet saavutetaan yksittäisissä tieto- ja viestintätekniikan tuotteissa, palveluissa ja prosesseissa, olisi täsmennettävä yksityiskohtaisemmin komission hyväksymien yksittäisten sertifiointijärjestelmien tasolla, esimerkiksi viittaamalla standardeihin tai teknisiin eritelmiin, jos asianmukaisia standardeja ei ole saatavilla.

(76) Eurooppalaisissa kyberturvallisuuden sertifiointijärjestelmissä käytettävien teknisten eritelmien olisi oltava Euroopan parlamentin ja neuvoston asetuksen (EU) 1025/2012[1] liitteessä II esitettyjen vaatimusten mukaiset. Poikkeuksia näihin periaatteisiin voidaan kuitenkin katsoa tarvittavan asianmukaisesti perustelluissa tapauksissa, joissa kyseisiä teknisiä eritelmiä käytetään eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän varmuustasolla "korkea". Tällaisten poikkeusten syyt olisi asetettava julkisesti saataville.

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

(77) Sertifiointiin kuuluva vaatimustenmukaisuuden arviointi on menettely, jossa arvioidaan, täyttyvätkö tieto- ja viestintätekniikan tuotteeseen, palveluun tai prosessiin liittyvät määritellyt vaatimukset. Arvioinnin tekee riippumaton kolmas osapuoli, joka ei ole arvioinnin kohteena olevien tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien valmistaja tai tarjoaja. Eurooppalainen kyberturvallisuussertifikaatti olisi myönnettävä, kun tieto- tai viestintätekniikan tuote, palvelu tai prosessi on läpäissyt arvioinnin. Eurooppalaista kyberturvallisuussertifikaattia olisi pidettävä vahvistuksena siitä, että kyseinen arviointi on tehty asianmukaisesti. Eurooppalaisessa kyberturvallisuusjärjestelmässä olisi varmuustasosta riippuen määritettävä, myöntääkö eurooppalaisen kyberturvallisuussertifikaatin yksityinen taho vai julkinen elin. Vaatimustenmukaisuuden arviointi ja sertifiointi eivät sinänsä takaa, että sertifioidut tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit ovat kyberturvallisia. Ne ovat pikemminkin menettelyjä ja teknisiä menetelmiä, jotka todistavat, että tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit on testattu ja että ne täyttävät tietyt kyberturvallisuusvaatimukset, jotka on vahvistettu muualla, esimerkiksi teknisissä standardeissa.

(78) Eurooppalaisten kyberturvallisuussertifikaattien käyttäjien olisi valittava asianmukainen sertifiointi ja siihen liittyvät turvallisuusvaatimukset tieto- ja viestintätekniikan tuotteeseen, palveluun tai prosessiin liittyvien riskien analyysin perusteella. Varmuustason olisi näin ollen vastattava tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin käyttötarkoitukseen liittyvän riskin tasoa.

(79) Eurooppalaisissa kyberturvallisuuden sertifiointijärjestelmissä voidaan määrätä, että vaatimustenmukaisuuden arviointi on pelkästään tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien valmistajan tai tarjoajan vastuulla, jäljempänä 'vaatimustenmukaisuuden itsearviointi'. Tällaisissa tapauksissa olisi riittävää, että tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin valmistaja tai tarjoaja tekee itse kaikki tarkastukset, joilla varmistetaan, että tieto- tai viestintätekniikan tuote, palvelu tai prosessi on eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukainen. Vaatimustenmukaisuuden itsearviointi olisi katsottava asianmukaiseksi sellaisten yksinkertaisten tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien yhteydessä, jotka aiheuttavat vain vähäisen riskin yleisölle, kuten esimerkiksi yksinkertaiset suunnittelu- ja tuotantomekanismit. Vaatimustenmukaisuuden itsearviointi olisi lisäksi sallittava vain varmuustasoltaan perustason tieto- ja viestintätekniikan tuotteille, palveluille ja prosesseille.

(80) Eurooppalaisissa kyberturvallisuuden sertifiointijärjestelmissä voidaan tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien yhteydessä käyttää sekä vaatimustenmukaisuuden itsearviointeja että sertifiointeja. Tällaisen tilanteen varalta järjestelmässä olisi määriteltävä selkeät ja ymmärrettävät käytännöt, joiden avulla kuluttajat ja muut käyttäjät erottavat, minkä tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien arvioinnista on vastannut valmistaja tai tarjoaja ja mitkä tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit on sertifioinut kolmas osapuoli.

(81) Tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien valmistajan tai tarjoajan, joka tekee vaatimustenmukaisuuden itsearvioinnin, olisi vaatimustenmukaisuuden arviointimenettelyn yhteydessä voitava antaa ja allekirjoittaa EU-vaatimustenmukaisuusilmoitus. EU-vaatimustenmukaisuusilmoitus on asiakirja, jossa todetaan, että tietty tieto- ja viestintätekniikan tuote, palvelu tai prosessi on järjestelmässä asetettujen vaatimusten mukainen. Antamalla ja allekirjoittamalla EU-vaatimustenmukaisuusilmoituksen valmistaja tai palveluntarjoaja ottaa vastuun siitä, että tieto- ja viestintätekniikan tuote, palvelu tai prosessi on eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä asetettujen oikeudellisten vaatimusten mukainen. Jäljennös EU-vaatimustenmukaisuusilmoituksesta olisi toimitettava kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle ja ENISAlle.

(82) Tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien valmistajan tai tarjoajan olisi asetettava EU-vaatimustenmukaisuusilmoitus, tekniset asiakirjat ja kaikki tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä asetettujen vaatimusten mukaisuutta koskevat muut tiedot toimivaltaisen kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen saataville asianomaisessa eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä määrätyn ajanjakson ajaksi. Teknisissä asiakirjoissa olisi eriteltävä sovellettavat järjestelmän mukaiset vaatimukset, ja niiden olisi katettava tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin suunnittelu, valmistus ja toiminta siinä määrin kuin se on olennaista itsearvioinnin noudattamisen kannalta. Tekniset asiakirjat olisi laadittava siten, että niiden perusteella voidaan arvioida, noudattaako tieto- ja viestintätekniikan tuote, palvelu tai prosessi kyseisen järjestelmän mukaan sovellettavia vaatimuksia.

(83) Eurooppalaisen kyberturvallisuuden sertifiontikehyksen hallinnossa otetaan huomioon jäsenvaltioiden osallistuminen sekä sidosryhmien asianmukainen osallistuminen ja vahvistetaan komission rooli eurooppalaisen kyberturvallisuuden sertifiointijärjestelmien suunnittelussa, ehdottamisessa, pyytämisessä, valmistelussa, hyväksymisessä ja uudelleentarkastelussa.

(84) Komission olisi valmisteltava Euroopan kyberturvallisuuden sertifiointiryhmän ja sidosryhmien kyberturvallisuuden sertifiointiryhmän tuella ja avoimen ja laajan kuulemisen jälkeen eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä koskeva unionin jatkuva työohjelma ja julkaistava se asiakirjana, joka ei ole oikeudellisesti sitova. Unionin jatkuvan työohjelman olisi oltava strateginen asiakirja, jonka ansiosta erityisesti toimiala, kansalliset viranomaiset ja standardointielimet voivat erityisesti valmistella tulevia eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä etukäteen. Unionin jatkuvan työohjelman olisi sisällettävä monivuotinen yleiskatsaus sellaisia ehdolla olevia järjestelmiä koskevista pyynnöistä, jotka komissio aikoo toimittaa ENISAlle valmisteltaviksi perusteltujen syiden pohjalta. Komission olisi otettava huomioon unionin jatkuva työohjelma laatiessaan tieto- ja viestintätekniikan standardointia koskevaa jatkuvaa suunnitelmaa sekä eurooppalaisille standardointiorganisaatioille osoitettuja standardointipyyntöjä. Ottaen huomioon uuden teknologian nopea käyttöönotto ja, aiemmin tuntemattomien kyberturvallisuusriskien ilmaantuminen ja lainsäädännön ja markkinoiden kehittyminen, komission tai Euroopan kyberturvallisuuden sertifiointiryhmän olisi voitava pyytää ENISAa valmistelemaan sellaisia ehdolla olevia järjestelmiä, jotka eivät sisälly unionin jatkuvaan työohjelmaan. Komission ja Euroopan kyberturvallisuuden sertifiointiryhmän olisi tällöin arvioitava myös tällaisten pyyntöjen tarpeellisuus ottamalla huomioon tämän asetuksen yleiset päämäärät ja tavoitteet sekä tarve varmistaa ENISAn suunnittelun ja resurssien käytön jatkuvuus.

Tällaisen pyynnön saatuaan ENISAn olisi valmisteltava tieto- ja viestintätekniikan tuotteita, palveluja tai prosesseja varten ehdolla olevat järjestelmät ilman aiheetonta viivytystä. Komission olisi arvioitava pyyntönsä kyseisiin markkinoihin kohdistuvia myönteisiä ja kielteisiä vaikutuksia etenkin pk-yritysten, innovoinnin, kyseisille markkinoille pääsyn esteiden sekä loppukuluttajille aiheutuvien kustannusten kannalta. Komissiolle olisi annettava valtuudet hyväksyä ENISAn valmisteleman ehdolla olevan järjestelmän pohjalta eurooppalainen kyberturvallisuuden sertifiointijärjestelmä täytäntöönpanosäädöksillä. Kun otetaan huomioon tämän asetuksen yleinen tarkoitus ja siinä määritellyt turvallisuustavoitteet, komission hyväksymissä eurooppalaisissa kyberturvallisuuden sertifiointijärjestelmissä olisi määritettävä tietyt vähimmäistekijät yksittäisen järjestelmän kohteen, soveltamisalan ja toiminnan osalta. Näihin tekijöihin olisi sisällyttävä muun muassa kyberturvallisuussertifioinnin soveltamisala ja kohde, mukaan lukien sertifioinnin kattamat tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien luokat, yksityiskohtainen eritelmä kyberturvallisuusvaatimuksista esimerkiksi viittaamalla standardeihin tai teknisiin eritelmiin, yksittäiset arviointiperusteet ja -menetelmät sekä tarkoitettu varmuustaso ("perustaso", "korotettu" tai "korkea") ja tarvittaessa arviointitasot. ENISAn olisi voitava asianmukaisesti perustelluissa tapauksissa hylätä Euroopan kyberturvallisuuden sertifiointiryhmän pyyntö. Johtokunnan olisi tehtävä tällaiset päätökset, ja ne olisi perusteltava.

(85) ENISAn olisi ylläpidettävä verkkosivustoa, jolla annetaan tietoa eurooppalaisista kyberturvallisuuden sertifiointijärjestelmistä ja tehdään niitä tunnetuiksi. Tietojen olisi sisällettävä muun muassa pyynnöt valmistella ehdolla oleva järjestelmä sekä palaute, jota ENISA on saanut valmisteluvaiheessa tehdyistä kuulemisista. Verkkosivustolla olisi annettava tietoa myös tämän asetuksen nojalla myönnetyistä eurooppalaisista kyberturvallisuuden sertifikaateista ja annetuista EU-vaatimustenmukaisuusilmoituksista, myös tällaisten eurooppalaisten kyberturvallisuuden sertifikaattien ja EU-vaatimustenmukaisuusilmoitusten peruuttamisesta tai vanhentumisesta. Verkkosivustolla olisi myös ilmoitettava ne kansalliset kyberturvallisuuden sertifiointijärjestelmät, jotka on korvattu eurooppalaisella kyberturvallisuuden sertifiointijärjestelmällä.

(86) Eurooppalaisen sertifiointijärjestelmän mukainen varmuustaso luo perustan sille, että tietty tieto- ja viestintätekniikan tuote, palvelu tai prosessi täyttää tietyn eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaiset turvallisuusvaatimukset. Sertifioituja tieto- ja viestintätekniikan tuotteita, palveluja ja prosesseja koskevan eurooppalaisessa kyberturvallisuuden sertifiointikehyksen yhdenmukaisuuden varmistamiseksi eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä olisi oltava mahdollista määrittää kyseisen järjestelmän nojalla myönnettyjen eurooppalaisten kyberturvallisuussertifikaattien ja EU-vaatimustenmukaisuusilmoitusten varmuustasot. Kussakin eurooppalaisessa kyberturvallisuuden sertifikaatissa viitattaisiin johonkin kolmesta varmuustasosta: "perustaso", "korotettu" tai "korkea". EU-vaatimustenmukaisuusilmoituksessa voitaisiin puolestaan viitata vain perustason varmuustasoon. Varmuustasot antaisivat tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin arvioinnille vastaavan tiukkuuden ja kattavuuden, ja ne määritettäisiin viittaamalla teknisiin eritelmiin, standardeihin ja niihin liittyviin menetelmiin (myös teknisiin tarkastuksiin), joiden tarkoituksena on lieventää tai ehkäistä poikkeamia. Kunkin varmuustason olisi oltava yhdenmukainen eri aloilla, joilla sertifiointeja käytetään.

(87) Eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voitaisiin määritellä useita arviointitasoja sen mukaan, miten tiukkoja ja kattavia arviointimenetelmiä käytetään. Arviointitasojen olisi vastattava varmuustasoja ja ne olisi määriteltävä asianmukaisten osatekijöiden perusteella. Tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin olisi kaikilla varmuustasoilla sisällettävä tietty määrä järjestelmässä määriteltyjä turvallisia toimintoja, joita voivat olla esimerkiksi ennalta turvalliseksi määritetty kokoonpano, allekirjoitettu koodi, suojatut päivitykset ja hyväksikäyttömenetelmien lieventäminen sekä koko pino- tai kekomuistin suojaukset. Näiden toimintojen kehitystyössä ja ylläpidossa olisi noudatettava turvallisuuskeskeistä toimintatapaa ja hyödynnettävä siihen liittyviä välineitä. Näin varmistetaan, että ohjelmistoon ja laitteistoon saadaan luotettavasti sisällytettyä toimivia mekanismeja.

(88) Varmuustason "perustaso" arvioinnissa olisi käsiteltävä vähintään seuraavat varmuuden osatekijät: arvioinnin olisi sisällettävä vähintään vaatimustenmukaisuuden arviointilaitoksen arvio tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin teknisistä asiakirjoista. Jos sertifiointiin sisältyy tieto- ja viestintätekniikan prosesseja, tekninen arviointi olisi tehtävä myös prosessille, jota käytetään tieto- ja viestintätekniikan tuotteen tai palvelun suunnitteluun, kehittämiseen ja ylläpitoon. Tapauksissa, joissa eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaan voidaan soveltaa vaatimustenmukaisuuden itsearviointia, olisi katsottava riittäväksi, että kyseinen valmistaja tai palveluntarjoaja tekee itsearvioinnin tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin vaatimustenmukaisuudesta sertifiointijärjestelmän suhteen.

(89) Varmuustason "korotettu" arvioinnissa olisi varmuustason "perustaso" vaatimusten lisäksi vähintään todennettava, noudattavatko tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin turvallisuustoiminnot sen teknisiä asiakirjoja.

(90) Varmuustason "korkea" arviointiin olisi varmuustason "korotettu" vaatimusten lisäksi vähintään sisällyttävä tehokkuustesti, jolla arvioidaan tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin turvallisuustoimintojen vastustuskykyä sellaisten henkilöiden suorittamia vaativia pitkälle kehittyneitä kyberhyökkäyksiä vastaan, joilla on huomattavaa osaamista ja resursseja.

(91) Eurooppalaisen kyberturvallisuussertifioinnin ja EU-vaatimustenmukaisuusilmoituksen käytön olisi oltava jatkossakin vapaaehtoista, jollei toisin säädetä unionin lainsäädännössä tai unionin oikeuden mukaisesti hyväksytyssä jäsenvaltioiden lainsäädännössä. Jos yhdenmukaista lainsäädäntöä ei ole, jäsenvaltiot voivat hyväksyä Euroopan parlamentin ja neuvoston direktiivin (EU) 2015/1535[1] mukaisia kansallisia teknisiä määräyksiä, joissa säädetään pakollisesta eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesta sertifioinnista. Jäsenvaltiot voivat myös käyttää eurooppalaista kyberturvallisuussertifiointia julkisissa hankinnoissa ja Euroopan parlamentin ja neuvoston direktiivin 2014/24/EU[2] yhteydessä.

---

1 Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/1535, annettu 9 päivänä syyskuuta 2015, teknisiä määräyksiä ja tietoyhteiskunnan palveluja koskevia määräyksiä koskevien tietojen toimittamisessa noudatettavasta menettelystä (EUVL L 241, 17.9.2015, s. 1).

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

(92) Joillakin aloilla saattaa myöhemmin olla tarpeen vahvistaa erityisiä kyberturvallisuusvaatimuksia ja tehdä tiettyjen tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien sertifioinnista pakollista kyberturvallisuuden tason parantamiseksi unionissa. Komission olisi säännöllisesti seurattava hyväksyttyjen eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien vaikutuksia turvallisten tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien saatavuuteen sisämarkkinoilla sekä säännöllisesti arvioitava, missä määrin tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien valmistajat tai tarjoajat käyttävät sertifiointijärjestelmiä unionissa. Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien tehokkuutta ja sitä, olisiko tietyt järjestelmät tehtävä pakollisiksi, olisi arvioitava kyberturvallisuuteen liittyvän unionin lainsäädännön ja erityisesti direktiivin (EU) 2016/1148 valossa ottaen huomioon keskeisten palvelujen tarjoajien käyttämien verkko- ja tietojärjestelmien turvallisuus.

(93) Eurooppalaisten kyberturvallisuussertifikaattien ja EU-vaatimustenmukaisuusilmoitusten olisi autettava loppukäyttäjiä tekemään tietoon perustuvia valintoja. Sen vuoksi tieto- ja viestintätekniikan tuotteiden, prosessien ja palvelujen, jotka on sertifioitu tai joista on annettu EU-vaatimustenmukaisuusilmoitus, mukana olisi oltava jäsennellyssä muodossa tietoja, jotka on mukautettu suunnitellun loppukäyttäjän odotettuun tekniseen tasoon. Kaikkien tällaisten tietojen olisi oltava saatavilla verkossa ja tapauksen mukaan fyysisessä muodossa. Loppukäyttäjän olisi voitava saada tiedot sertifiointijärjestelmän numerosta ja varmuustasosta, kuvaus tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin kyberturvallisuusriskeistä ja tieto sertifikaatin myöntävästä viranomaisesta tai elimestä tai heidän pitäisi voida saada kopio eurooppalaisesta kyberturvallisuussertifikaatista. Lisäksi loppukäyttäjälle olisi tiedotettava tieto- ja viestintätekniikan tuotteiden, prosessien tai palvelujen valmistajan tai tarjoajan noudattamasta kyberturvallisuuden tukemista koskevasta toimintapolitiikasta, eli siitä, kuinka kauan loppukäyttäjä voi odottaa saavansa kyberturvallisuuspäivityksiä tai -korjauksia. Tarvittaessa olisi annettava neuvontaa toimista tai asetuksista, joita loppukäyttäjä voi toteuttaa tieto- ja viestintätekniikan tuotteen, prosessin tai palvelun kyberturvallisuuden ylläpitämiseksi tai parantamiseksi, sekä yhteystiedot keskitetystä yhteyspisteestä, johon voi raportoida ja josta voi saada tukea kyberhyökkäysten tapauksissa (automaattisen raportoinnin lisäksi). Tiedot olisi päivitettävä säännöllisesti, ja niiden olisi saatettava saataville verkkosivustolla, joka tarjoaa tietoa eurooppalaisista kyberturvallisuuden sertifiointijärjestelmistä.

(94) Jotta voitaisiin saavuttaa tämän asetuksen tavoitteet ja välttää hajanaisuus sisämarkkinoilla, sellaisten kansallisten kyberturvallisuuden sertifiointijärjestelmien tai -menettelyjen, joiden kattamat tieto- ja viestintätekniikan tuotteet, palvelut tai prosessit kuuluvat jonkin eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan, olisi lakattava tuottamasta oikeusvaikutuksia alkaen päivästä, jonka komissio vahvistaa täytäntöönpanosäädöksillä. Jäsenvaltiot eivät myöskään saisi ottaa käyttöön uusia kansallisia kyberturvallisuuden sertifiointijärjestelmiä tieto- ja viestintätekniikan tuotteille, palveluille tai prosesseille, jotka kuuluvat jo jonkin olemassa olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan. Jäsenvaltioita ei kuitenkaan tulisi estää hyväksymästä tai pitämästä voimassa kansallisia kyberturvallisuussertifiointijärjestelmiä kansallisen turvallisuuden nimissä. Jäsenvaltioiden olisi toimitettava komissiolle ja Euroopan kyberturvallisuuden sertifiointiryhmälle tieto aikomuksestaan laatia uusia kansallisia kyberturvallisuuden sertifiointijärjestelmiä. Komission ja Euroopan kyberturvallisuuden sertifiointiryhmän olisi arvioitava uuden kansallisen kyberturvallisuuden sertifiointijärjestelmän vaikutuksia sisämarkkinoiden moitteettomaan toimintaan ja sitä, olisiko strategisesti asianmukaista pyytää käyttämään sen sijaan eurooppalaista kyberturvallisuuden sertifiointijärjestelmää.

(95) Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien tarkoituksena on auttaa yhdenmukaistamaan kyberturvallisuuskäytäntöjä unionissa. Niiden on tarpeen lisätä kyberturvallisuuden tasoa unionissa. Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien suunnittelussa olisi otettava huomioon myös kyberturvallisuusalan uusien innovaatioiden kehittäminen ja mahdollistettava ne.

(96) Eurooppalaisissa kyberturvallisuuden sertifiointijärjestelmissä olisi otettava huomioon olemassa olevat ohjelmien ja laitteistojen kehitysmenetelmät ja erityisesti usein tapahtuvien ohjelmisto- tai valmisohjelmistopäivitysten vaikutus yksittäisiin eurooppalaisiin kyberturvallisuussertifikaatteihin. Eurooppalaisissa kyberturvallisuuden sertifiointijärjestelmissä olisi täsmennettävä olosuhteet, joiden vallitessa päivitys voi edellyttää tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin sertifioimista uudelleen tai yksittäisen eurooppalaisen kyberturvallisuussertifikaatin kattavuuden supistamista ottaen huomioon päivityksen mahdolliset haitalliset vaikutukset kyseisen sertifikaatin turvallisuusvaatimusten mukaisuuteen.

(97) Kun eurooppalainen kyberturvallisuuden sertifiointijärjestelmä on hyväksytty, tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien valmistajien tai tarjoajien olisi voitava jättää tuotteidensa tai palvelujensa sertifiointia koskeva hakemus valitsemalleen vaatimustenmukaisuuden arviointilaitokselle kaikkialla unionissa. Kansallisten vaatimustenmukaisuuden arviointilaitosten olisi saatava akkreditointi kansalliselta akkreditointielimeltä, jos ne täyttävät tässä asetuksessa vahvistetut tietyt erityiset vaatimukset. Akkreditointi olisi myönnettävä enintään viideksi vuodeksi, ja se olisi uusittava samoin edellytyksin, jos vaatimustenmukaisuuden arviointilaitos edelleen täyttää vaatimukset. Kansallisten akkreditointielinten olisi rajoitettava vaatimustenmukaisuuden arviointilaitoksen akkreditointia, keskeytettävä sen voimassaolo tai peruutettava se, jos akkreditoinnin edellytykset eivät täyty tai eivät enää täyty tai jos vaatimustenmukaisuuden arviointilaitoksen toiminta rikkoo tätä asetusta.

(98) Kansallisessa lainsäädännössä olevat viittaukset kansallisiin standardeihin, jotka eivät ole enää voimassa eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän tultua voimaan, voivat mahdollisesti aiheuttaa. Jäsenvaltioiden olisi sen vuoksi otettava eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän hyväksyminen huomioon kansallisessa lainsäädännössään.

(99) Toisiaan vastaavien standardien soveltamiseksi koko unionissa, vastavuoroisen tunnustamisen helpottamiseksi sekä eurooppalaisten kyberturvallisuussertifikaattien ja EU-vaatimustenmukaisuusilmoitusten yleisen hyväksymisen edistämiseksi on perustettava kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten välinen vertaisarviointijärjestelmä. Vertaisarvioinnin olisi katettava menettelyt tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien eurooppalaisten kyberturvallisuussertifikaattien mukaisuuden valvontaa, itsearviointeja tekevien menettelyt tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien valmistajien tai tarjoajien velvoitteiden seurantaa ja vaatimustenmukaisuuden arviointilaitosten valvontaa varten sekä varmuustason "korkea" sertifikaatteja myöntävien elinten henkilöstön asiantuntemuksen asianmukaisuus. Komission olisi voitava täytäntöönpanosäädöksellä vahvistaa vertaisarviointeja varten vähintään viisivuotinen suunnitelma sekä säädettävä vertaisarviointijärjestelmän toimintaa koskevista kriteereistä ja menetelmistä.

(100) Sanotun vaikuttamatta perustettavan yleisen vertaisarviointijärjestelmän soveltamiseen, joka kattaa kaikki eurooppalaiseen kyberturvallisuuden sertifiointikehykseen kuuluvat kansalliset kyberturvallisuussertifioinnin myöntävät viranomaiset, tiettyihin eurooppalaiseen kyberturvallisuuden sertifiointijärjestelmiin voi sisältyä vertaisarviointimekanismi, joka kattaa varmuustason "korkea" eurooppalaisia kyberturvallisuussertifikaatteja näiden järjestelmien nojalla tieto- ja viestintätekniikan tuotteille, palveluille tai prosesseille myöntävät elimet. Eurooppalaisen kyberturvallisuuden sertifiointiryhmän olisi tuettava tällaisten vertaisarviointimekanismien täytäntöönpanoa. Vertaisarvioinneissa olisi arvioitava erityisesti sitä, hoitavatko kyseiset elimet tehtäviään yhdenmukaisella tavalla, ja niihin voi sisältyä muutoksenhakumekanismeja. Vertaisarviointien tulokset olisi julkistettava. Vertaisarvioinnin kohteena olevat elimet voivat toteuttaa aiheellisia toimenpiteitä, joilla ne mukauttavat käytäntöjään ja asiantuntemustaan vastaavasti.

(101) Jäsenvaltioiden olisi nimettävä yksi tai useampi kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen valvomaan tästä asetuksesta johtuvien velvoitteiden noudattamista. Kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen voi olla jo olemassa oleva tai uusi viranomainen. Jäsenvaltioiden olisi myös voitava päättää sovittuaan asiasta toisen jäsenvaltion kanssa yhden tai useamman kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen nimeämisestä kyseisen toisen jäsenvaltion alueelle.

(102) Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen olisi erityisesti saatettava voimaan kyseisen jäsenvaltion alueelle sijoittautuneiden tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien valmistajien tai tarjoajien velvollisuudet, jotka liittyvät EU-vaatimustenmukaisuusilmoitukseen, ja valvottava näiden velvollisuuksien noudattamista, avustettava kansallisia akkreditointielimiä niiden seuratessa ja valvoessa vaatimustenmukaisuuden arviointilaitosten toimintaa tarjoamalla niille asiantuntemusta ja asiaankuuluvia tietoja, valtuutettava vaatimustenmukaisuuden arviointilaitokset suorittamaan tehtävänsä, kun niihin kohdistuu järjestelmässä määriteltyjä Euroopan kyberturvallisuuden sertifiointijärjestelmässä esitettyjä lisävaatimuksia, ja seurattava merkityksellistä kehitystä kyberturvallisuussertifioinnin alalla. Kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten olisi myös käsiteltävä luonnollisten tai oikeushenkilöiden tekemät valitukset, jotka liittyvät näiden viranomaisten myöntämiin eurooppalaisiin kyberturvallisuussertifikaatteihin tai vaatimustenmukaisuuden arviointilaitosten myöntämiin, varmuustasoa "korkea" osoittaviin sertifikaatteihin, tutkittava asianmukaisessa määrin valituksen kohde ja ilmoitettava valituksen tekijälle tutkinnan etenemisestä ja tuloksesta kohtuullisessa ajassa. Lisäksi kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten olisi tehtävä yhteistyötä muiden kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten tai muiden viranomaisten kanssa esimerkiksi jakamalla tietoa mahdollisista tapauksista, joissa tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit eivät vastaa tämän asetuksen tai yksittäisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien vaatimuksia. Komission olisi helpotettava tätä tietojen jakamista asettamalla saataville yleinen sähköinen tietotukijärjestelmä, esimerkiksi markkinavalvontaa koskeva tieto- ja viestintäjärjestelmä (ICSMS) tai tuoteturvallisuutta koskeva unionin nopea tietojenvaihtojärjestelmä (RAPEX), joita markkinavalvontaviranomaiset jo käyttävät asetuksen (EY) N:o 765/2008 nojalla.

(103) Eurooppalaisen kyberturvallisuuden sertifiointikehyksen johdonmukaisen soveltamisen varmistamiseksi olisi perustettava Euroopan kyberturvallisuuden sertifiointiryhmä, joka koostuu kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten tai muiden asiaankuuluvien kansallisten viranomaisten edustajista. Eurooppalaisen kyberturvallisuuden sertifiointiryhmän päätehtävinä olisi neuvoa ja avustaa komissiota sen pyrkiessä varmistamaan eurooppalaisen kyberturvallisuuden sertifiointikehyksen yhdenmukaisen täytäntöönpanon ja soveltamisen, avustaa ENISAa ehdolla olevien kyberturvallisuuden sertifiointijärjestelmien valmistelussa tiiviissä yhteistyössä sen kanssa, asianmukaisesti perustelluissa tapauksissa pyytää ENISAa valmistelemaan ehdolla olevan järjestelmän, sekä antaa ENISAlle osoitettuja lausuntoja ehdolla olevista järjestelmistä ja komissiolle osoitettuja lausuntoja voimassa olevien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien ylläpitämisestä ja tarkistamisesta. Eurooppalaisen kyberturvallisuuden sertifiointiryhmän olisi helpotettava parhaiden käytäntöjen ja asiantuntemuksen vaihtoa erinäisten vaatimustenmukaisuuden arviointilaitosten valtuuttamisesta ja eurooppalaisten kyberturvallisuussertifikaattien myöntämisestä vastaavien kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten välillä.

(104) Tietoisuuden lisäämiseksi ja tulevien eurooppalaisten kyberturvallisuusjärjestelmien hyväksymisen helpottamiseksi komissio voi antaa yleisiä tai alakohtaisia kyberturvallisuutta koskevia suuntaviivoja esimerkiksi hyvistä kyberturvallisuuskäytännöistä tai vastuullisesta kyberturvallisuuskäyttäytymisestä korostaen sertifioitujen tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien käytön myönteistä vaikutusta.

(105) Tieto- ja viestintäalan toimitusketjut ovat maailmanlaajuisia, joten unioni voi Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 218 artiklan mukaisesti kaupankäyntiä edelleen helpottaakseen tehdä eurooppalaisia kyberturvallisuussertifikaatteja koskevia sopimuksia vastavuoroisesta tunnustamisesta. Komissio voi ENISAn ja Euroopan kyberturvallisuuden sertifiointiryhmän neuvot huomioiden suosittaa näitä koskevien neuvottelujen aloittamista. Kussakin eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä olisi määritettävä erikseen edellytykset tällaisille vastavuoroista tunnustamista koskeville sopimuksille kolmansien maiden kanssa.

(106) Jotta voidaan varmistaa tämän asetuksen yhdenmukainen täytäntöönpano, komissiolle olisi siirrettävä täytäntöönpanovaltaa. Tätä valtaa olisi käytettävä Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 182/2011[1] mukaisesti.

(107) Olisi sovellettava tarkastelumenettelyä hyväksyttäessä täytäntöönpanosäädöksiä, jotka koskevat tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä, ENISAn tutkimusten toteuttamista koskevia järjestelyjä, hyväksyttäessä täytäntöönpanosäädöksiä, jotka koskevat kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten vertaisarviointia koskevaa suunnitelmaa sekä hyväksyttäessä täytäntöönpanosäädöksiä, jotka koskevat kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten komissiolle tekemien, akkreditoituja vaatimustenmukaisuuden arviointilaitoksia koskevien ilmoitusten olosuhteita, muotoseikkoja ja menettelyjä.

---

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

(108) ENISAn toimintaa olisi arvioitava säännöllisesti ja riippumattomasti. Arvioinnissa olisi otettava huomioon ENISAn tavoitteet, sen toimintatavat ja sen tehtävien merkityksellisyys, erityisesti niiden tehtävien, jotka liittyvät unionin tasolla tapahtuvaan operatiiviseen yhteistyöhön. Tässä arvioinnissa olisi myös arvioitava eurooppalaisen kyberturvallisuuden sertifiointikehyksen vaikutusta, vaikuttavuutta ja tehokkuutta. Komission olisi uudelleentarkastelussaan arvioitava, miten ENISAn roolia neuvonnan ja asiantuntemuksen viitetahona voidaan vahvistaa, sekä arvioitava myös ENISAn mahdollista roolia sellaisten unionin markkinoille tulevien kolmansien maiden tieto- ja viestintätekniikan tuotteiden ja palvelujen arvioinnin tukemisessa, jos tällaiset tuotteet, palvelut ja prosessit eivät ole unionin sääntöjen mukaisia.

(109) Jäsenvaltiot eivät voi riittävällä tavalla saavuttaa tämän asetuksen tavoitteita, vaan ne voidaan saavuttaa paremmin unionin tasolla. Sen vuoksi unioni voi toteuttaa toimenpiteitä Euroopan unionista tehdyn sopimuksen (SEU) 5 artiklassa vahvistetun toissijaisuusperiaatteen mukaisesti. Mainitussa artiklassa vahvistetun suhteellisuusperiaatteen mukaisesti tässä asetuksessa ei ylitetä sitä, mikä on tarpeen näiden tavoitteiden saavuttamiseksi.

(110) Asetus (EU) N:o 526/2013 olisi kumottava,

OVAT HYVÄKSYNEET TÄMÄN ASETUKSEN:

I OSASTO
YLEISET SÄÄNNÖKSET

1 artikla

Kohde ja soveltamisala

1. Sisämarkkinoiden asianmukaisen toiminnan varmistamiseksi, pyrkien samalla saavuttamaan kyberturvallisuuden, kyberresilienssin ja luottamuksen korkean tason unionissa, tässä asetuksessa

   a) vahvistetaan Euroopan unionin kyberturvallisuusvirasto ENISAn tavoitteet, tehtävät ja organisatoriset näkökohdat; ja

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

   Edellä b alakohdassa tarkoitetun kehyksen soveltaminen ei rajoita niiden unionin muissa säädöksissä olevien erityisten säännösten soveltamista, jotka koskevat vapaaehtoista tai pakollista sertifiointia.

2. Tämä asetus ei rajoita jäsenvaltioiden toimivaltaa sellaisten toimien osalta, jotka koskevat yleistä turvallisuutta, puolustusta, kansallista turvallisuutta tai yksittäisen valtion toimia rikosoikeuden alalla.

2 artikla

Määritelmät

Tässä asetuksessa tarkoitetaan:

1) 'kyberturvallisuudella' toimia, joita tarvitaan verkko- ja tietojärjestelmien, tällaisten järjestelmien käyttäjien ja muiden asianosaisten henkilöiden suojaamiseksi kyberuhilta;

2) 'verkko- ja tietojärjestelmällä' direktiivin (EU) 2016/1148 4 artiklan 1 kohdassa määriteltyä verkko- ja tietojärjestelmää;

3) 'verkko- ja tietojärjestelmien turvallisuutta koskevalla kansallisella strategialla' direktiivin (EU) 2016/1148 4 artiklan 3 alakohdassa määriteltyä verkko- ja tietojärjestelmien turvallisuutta koskevaa kansallista strategiaa;

4) 'keskeisten palvelujen tarjoajalla' direktiivin (EU) N:o 2016/1148 4 artiklan 4 alakohdassa määriteltyä keskeisten palvelujen tarjoajaa;

5) 'digitaalisen palvelun tarjoajalla' direktiivin (EU) N:o 2016/1148 4 artiklan 6 alakohdassa määriteltyä digitaalisen palvelun tarjoajaa;

6) 'poikkeamalla' direktiivin (EU) N:o 2016/1148 4 artiklan 7 alakohdassa määriteltyä poikkeamaa;

7) 'poikkeamien käsittelyllä' direktiivin (EU) N:o 2016/1148 4 artiklan 8 alakohdassa määriteltyä poikkeamien käsittelyä;

8) 'kyberuhalla' potentiaalista tilannetta, tapahtumaa tai toimintaa, joka voi vahingoittaa tai häiritä verkko- ja tietojärjestelmiä, tällaisten järjestelmien käyttäjiä ja muita henkilöitä tai muulla tavoin vaikuttaa näihin haitallisesti;

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

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

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

12) 'tieto- ja viestintätekniikan tuotteella ' mitä tahansa verkko- ja tietojärjestelmien elementtiä tai elementtien ryhmää;

13) 'tieto- ja viestintätekniikan palvelulla' mitä tahansa palvelua, jonka sisältönä on kokonaan tai pääasiassa tiedon välittäminen, tallentaminen, hakeminen tai käsittely verkko- ja tietojärjestelmien avulla;

14) 'tieto- ja viestintätekniikan prosessilla' toimintaa, jonka tarkoituksena on suunnitella, kehittää, tarjota tai ylläpitää tieto- ja viestintätekniikan tuotetta tai palvelua;

15) 'akkreditoinnilla' asetuksen (EY) N:o 765/2008 2 artiklan 10 alakohdassa määriteltyä akkreditointia;

16) 'kansallisella akkreditointielimellä' asetuksen (EY) N:o 765/2008 2 artiklan 11 alakohdassa määriteltyä kansallista akkreditointielintä;

17) 'vaatimustenmukaisuuden arvioinnilla' asetuksen (EY) N:o 765/2008 2 artiklan 12 alakohdassa määriteltyä vaatimustenmukaisuuden arviointia;

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

19) 'standardilla' asetuksen (EU) N:o 1025/2012 2 artiklan 1 alakohdassa määriteltyä standardia;

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

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

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

II OSASTO
ENISA – EUROOPAN UNIONIN KYBERTURVALLISUUSVIRASTO

I luku
Toimeksianto ja tavoitteet

3 artikla

Toimeksianto

1. ENISA hoitaa sille tämän asetuksen nojalla kuuluvat tehtävät kyberturvallisuuden yhteisen korkean tason saavuttamiseksi koko unionissa, muun muassa tukemalla aktiivisesti jäsenvaltioita sekä unionin toimielimiä, elimiä ja laitoksia kyberturvallisuuden parantamisessa. ENISA toimii kyberturvallisuutta koskevan neuvonnan ja asiantuntemuksen viitetahona unionin toimielimille, elimille ja laitoksille sekä muille asiaankuuluville unionin sidosryhmille.

   Hoitamalla sille tässä asetuksessa annetut tehtävät ENISA osaltaan myötävaikuttaa sisämarkkinoiden hajanaisuuden vähentämiseen.

2. ENISA suorittaa tehtävät, jotka sille annetaan unionin säädöksissä, joissa vahvistetaan toimenpiteet jäsenvaltioiden lakien, asetusten ja hallinnollisten määräysten lähentämiseksi kyberturvallisuuden alalla.

3. ENISA toimii tehtävissään riippumattomasti ja pyrkii samalla välttämään päällekkäisyyttä jäsenvaltioiden toimien kanssa ja ottaa huomioon jäsenvaltioiden olemassa olevan asiantuntemuksen.

4. ENISA kehittää omia resurssejaan, kuten teknisiä ja henkilöstöön liittyviä valmiuksiaan ja taitojaan, jotka ovat tarpeen sille tässä asetuksessa osoitettujen tehtävien hoitamiseksi.

4 artikla

Tavoitteet

1. ENISA on kyberturvallisuuden osaamiskeskus riippumattomuutensa, antamansa neuvonnan ja avun ja tarjoamansa tiedon tieteellisen ja teknisen laadun, toimintatapojensa avoimuuden, menettelyjensä sekä tehtäviensä suorittamisessa osoittamansa huolellisuuden ansiosta.

2. ENISA auttaa unionin toimielimiä, elimiä ja laitoksia sekä jäsenvaltioita kehittämään ja panemaan täytäntöön kyberturvallisuutta koskevat unionin toimintapolitiikat, myös kyberturvallisuutta koskevat alakohtaiset politiikat.

3. ENISA tukee valmiuksien kehittämistä ja varautumista kaikkialla unionissa avustamalla unionin toimielimiä, elimiä ja laitoksia sekä jäsenvaltioita ja julkisia ja yksityisiä sidosryhmiä niiden verkko- ja tietojärjestelmien suojelun lisäämiseksi, kyberresilienssin ja toimintavalmiuksien kehittämiseksi ja parantamiseksi sekä taitojen ja osaamisen kehittämiseksi kyberturvallisuuden alalla.

4. ENISA edistää yhteistyötä, kuten tietojen jakamista ja koordinointia, unionin tasolla jäsenvaltioiden, unionin toimielinten, elinten ja laitosten sekä asiaankuuluvien yksityisten ja julkisten sidosryhmien välillä kyberturvallisuuteen liittyvissä kysymyksissä.

5. ENISA edistää kyberturvallisuusvalmiuksien lisäämistä unionin tasolla jäsenvaltioiden toimien tukemiseksi kyberuhkien ehkäisemisessä ja niihin vastaamisessa erityisesti rajat ylittävien poikkeamien tapauksessa.

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

7. ENISA edistää kyberturvallisuustietoisuuden, kuten kyberhygienian ja kyberlukutaidon, korkeaa tasoa kansalaisten, organisaatioiden ja yritysten keskuudessa.

II luku
Tehtävät

5 artikla

Unionin politiikan ja lainsäädännön kehittäminen ja täytäntöönpano

ENISA edistää unionin politiikan ja lainsäädännön kehittämistä ja täytäntöönpanoa tehtävänään

1) avustaa ja neuvoa erityisesti antamalla riippumattomia lausuntoja ja analyyseja sekä tekemällä valmistelutyötä unionin politiikan ja lainsäädännön kehittämisessä ja tarkistamisessa kyberturvallisuuden alalla sekä alakohtaisissa toimintapoliittisissa ja lainsäädännöllisissä aloitteissa, kun niihin liittyy kyberturvallisuuskysymyksiä;

2) auttaa jäsenvaltioita panemaan johdonmukaisesti täytäntöön erityisesti direktiiviin (EU) 2016/1148 liittyvää unionin kyberturvallisuuspolitiikkaa ja -lainsäädäntöä muun muassa antamalla lausuntoja, ohjeita ja neuvoja ja laatimalla parhaita käytäntöjä riskinhallinnan, poikkeamista raportoinnin ja tietojen jakamisen kaltaisista aiheista sekä helpottamalla parhaiden käytäntöjen vaihtoa toimivaltaisten viranomaisten välillä tältä osin;

3) auttaa jäsenvaltioita sekä unionin toimielimiä, elimiä ja laitoksia sellaisten kybertuvallisuuspolitiikkojen laatimisessa ja edistämisessä, joilla tuetaan avoimen internetin julkisen ytimen yleistä saatavuutta tai eheyttä;

4) osallistua yhteistyöryhmän työhön direktiivin (EU) 2016/1148 11 artiklan mukaisesti antamalla asiantuntemusta ja apua;

5) tukea

a) unionin politiikan kehittämistä ja täytäntöönpanoa sähköisen henkilöllisyyden ja sähköisten luottamuspalvelujen alalla erityisesti antamalla neuvoja ja teknisiä ohjeita sekä helpottamalla parhaiden käytäntöjen vaihtoa toimivaltaisten viranomaisten välillä;

b) sähköisen viestinnän turvallisuuden parantamista muun muassa tarjoamalla neuvontaa ja asiantuntemusta sekä helpottamalla parhaiden käytäntöjen vaihtoa toimivaltaisten viranomaisten välillä;

c) jäsenvaltioita tietosuojaa ja yksityisyyden suojaa koskevan unionin politiikan ja lainsäädännön kyberturvallisuuteen liittyvien erityisnäkökohtien täytäntöönpanossa sekä lausunnon antamisessa pyynnöstä Euroopan tietosuojaneuvostolle;

6) tukea unionin poliittisten toimien säännöllistä uudelleentarkastelua antamalla vuosiraportti asianomaisen lainsäädännön täytäntöönpanosta liittyen seuraaviin:

a) tiedot poikkeamista tehtävistä jäsenvaltioiden ilmoituksista, jotka keskitetyt yhteyspisteet toimittavat yhteistyöryhmälle direktiivin (EU) 2016/1148 10 artiklan 3 kohdan mukaisesti;

b) tiivistelmät luottamuspalvelun tarjoajilta saaduista tietoturvaloukkausta tai eheyden menetystä koskevista ilmoituksista, jotka valvontaelimet toimittavat ENISAlle Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014[1] 19 artiklan 3 kohdan mukaisesti;

c) yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajilta saadut turvapoikkeamia koskevat ilmoitukset, jotka toimivaltaiset viranomaiset toimittavat ENISAlle direktiivin (EU) 2018/1972 40 artiklan mukaisesti.

6 artikla

Valmiuksien kehittäminen

1. ENISA avustaa

a) jäsenvaltioita niiden pyrkiessä parantamaan kyberuhkien ja poikkeamien ennaltaehkäisyä, havaitsemista ja analysointia sekä valmiuksia reagoida näihin uhkiin ja poikkeamiin tarjoamalla jäsenvaltioille tietoa ja asiantuntemusta;

b) jäsenvaltioita ja unionin toimielimiä, elimiä ja laitoksia niiden vahvistaessa ja toteuttaessa haavoittuvuuksien julkistamista koskevia toimintaperiaatteita vapaaehtoisuuden pohjalta;

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

c) unionin toimielimiä, elimiä ja laitoksia niiden pyrkiessä parantamaan kyberuhkien ja poikkeamien ennaltaehkäisyä, havaitsemista ja analysointia sekä valmiuksiaan reagoida näihin uhkiin ja poikkeamiin erityisesti antamalla CERT-EU:lle asianmukaista tukea;

d) direktiivin (EU) 2016/1148 9 artiklan 5 kohdan mukaisesta pyynnöstä jäsenvaltioita niiden kehittäessä kansallisia CSIRT-toimijoita;

e) direktiivin (EU) 2016/1148 7 artiklan 2 kohdan mukaisesta pyynnöstä jäsenvaltioita niiden kehittäessä verkko- ja tietojärjestelmien turvallisuutta koskevia kansallisia strategioita ja edistää tiedon levittämistä kyseisistä strategioista ja panee merkille niiden täytäntöönpanon edistymisen kaikkialla unionissa parhaiden käytäntöjen edistämiseksi;

f) unionin toimielimiä niiden kehittäessä ja tarkastellessa uudelleen unionin strategioita kyberturvallisuuden alalla edistämällä niiden levittämistä ja seuraamalla niiden täytäntöönpanon edistymistä;

g) kansallisia ja unionin CSIRT-toimijoita niiden valmiuksien parantamisessa muun muassa edistämällä vuoropuhelua ja tiedonvaihtoa, jotta voidaan varmistaa, että viimeisimmän teknisen kehityksen huomioon ottaen jokaisella CSIRT-toimijalla on yhteisesti määritellyt vähimmäisvalmiudet ja että se toimii parhaita käytäntöjä noudattaen;

h) jäsenvaltioita järjestämällä säännöllisesti ja vähintään joka toinen vuosi 7 artiklan 5 kohdassa tarkoitettuja laajamittaisia kyberturvallisuusharjoituksia unionin tasolla ja antamalla poliittisia suosituksia harjoitusten arviointiprosessin ja niistä saatujen kokemusten pohjalta;

i) asianomaisia julkisia elimiä tarjoamalla kyberturvallisuuteen liittyvää koulutusta tarvittaessa yhteistyössä sidosryhmien kanssa;

j) yhteistyöryhmää parhaiden käytäntöjen vaihtamisessa erityisesti jäsenvaltioiden toteuttamasta keskeisten palvelujen tarjoajien määrittämisestä, myös rajat ylittävien riippuvuussuhteiden osalta, direktiivin (EU) 2016/1148 11 artiklan 3 kohdan l alakohdan mukaisesti siltä osin kuin kyse on riskeistä ja poikkeamista ja.

2. ENISA tukee tietojen jakamista alojen sisäisesti ja niiden välillä, erityisesti direktiivin (EU) 2016/1148 liitteessä II mainituilla toimialoilla tarjoamalla käyttöön parhaita käytäntöjä ja ohjeita käytettävissä olevista välineistä ja menettelyistä sekä ohjeita tietojen jakamiseen liittyvien sääntelykysymysten ratkaisemiseksi.

7 artikla

Unionin tasolla tehtävä operatiivinen yhteistyö

1. ENISA tukee operatiivista yhteistyötä jäsenvaltioiden, unionin toimielinten, elinten ja laitosten kesken sekä sidosryhmien välillä.

2. ENISA tekee yhteistyötä operatiivisella tasolla ja luo synergioita unionin toimielinten, elinten ja laitosten kanssa, mukaan lukien CERT-EU, kyberrikollisuutta käsittelevät yksiköt sekä yksityisyyden ja henkilötietojen suojaa käsittelevät valvontaviranomaiset, yhteiseen etuun liittyvien ongelmien ratkaisemiseksi muun muassa

   a) vaihtamalla tietotaitoa ja parhaita käytäntöjä;

   b) tarjoamalla neuvoja ja antamalla ohjeita asiaankuuluvista kyberturvallisuuteen liittyvistä kysymyksistä;

   c) ottamalla käyttöön komissiota kuultuaan käytännön järjestelyt erityisten tehtävien toteuttamiseksi.

3. ENISA toimii CSIRT-verkoston sihteeristönä direktiivin (EU) 2016/1148 12 artiklan 2 kohdan mukaisesti ja tukee tässä ominaisuudessa aktiivisesti tietojen jakamista ja yhteistyötä sen jäsenten kesken.

4. ENISA tukee jäsenvaltioita CSIRT-verkostossa tehtävässä operatiivisessa yhteistyössä tehtävänään

   a) antaa neuvoja siitä, miten ne voivat parantaa valmiuksiaan ehkäistä ja havaita poikkeamia ja reagoida niihin, sekä antaa yhden tai useamman jäsenvaltion pyynnöstä johonkin tiettyyn kyberuhkaan liittyviä neuvoja;

b) avustaa yhden tai useamman jäsenvaltion pyynnöstä vaikutukseltaan merkittävien poikkeamien arvioinnissa tarjoamalla asiantuntemustaan ja helpottamalla tällaisten poikkeamien teknistä käsittelyä, mukaan lukien erityisesti tukemalla asiaan liittyvien tietojen ja teknisten ratkaisujen vapaaehtoista jakamista jäsenvaltioiden välillä;

c) analysoida haavoittuvuuksia ja poikkeamia julkisesti saatavilla olevien tietojen tai jäsenvaltioiden tätä tarkoitusta varten vapaaehtoisesti toimittamien tietojen pohjalta; ja

d) tukea yhden tai useamman jäsenvaltion pyynnöstä direktiivissä (EU) 2016/1148 tarkoitettua vaikutukseltaan merkittävien poikkeamien jälkikäteen tehtävää teknistä tutkintaa.

Näiden tehtävien suorittamisessa ENISA ja CERT-EU tekevät jäsenneltyä yhteistyötä hyötyäkseen synergioista ja välttääkseen päällekkäiset toimet.

5. ENISA järjestää säännöllisesti kyberturvallisuusharjoituksia unionin tasolla ja tukee jäsenvaltioita ja unionin toimielimiä, elimiä ja laitoksia kyberturvallisuusharjoitusten järjestämisessä niiden pyynnöstä. Tällaisiin unionin tasolla järjestettäviin kyberturvallisuusharjoituksiin voi sisältyä teknisiä, operatiivisia tai strategisia osatekijöitä. Joka toinen vuosi ENISA järjestää laajamittaisen kattavan harjoituksen.

ENISA myös edistää ja auttaa tarvittaessa järjestämään alakohtaisia kyberturvallisuusharjoituksia yhdessä asiaankuuluvien organisaatioiden kanssa, jotka myös osallistuvat unionin tasolla järjestettäviin kyberturvallisuusharjoituksiin.

6. ENISA laatii poikkeamista ja kyberuhkista säännöllisesti ja tiiviissä yhteistyössä jäsenvaltioiden kanssa perusteellisen unionin kyberturvallisuuden teknisen tilanneraportin, joka perustuu julkisesti saatavilla oleviin tietolähteisiin, sen omaan analyysiin ja raportteihin, jotka on saatu muun muassa jäsenvaltioiden CSIRT-toimijoilta tai direktiivillä (EU) 2016/1148 perustetuilta keskitetyiltä yhteyspisteiltä vapaehtoisuuteen perustuvassa tiedonvaihdossa, EC3:lta sekä CERT-EU:lta.

7. ENISA edistää yhteistyöhön perustuvien vastatoimien kehittämistä unionin ja jäsenvaltioiden tasolla laajamittaisiin rajat ylittäviin kyberturvallisuuspoikkeamiin tai -kriiseihin pääasiallisesti

   a) kokoamalla ja analysoimalla yleisesti saatavilla olevia tai vapaaehtoisesti jaettuja raportteja kansallisista lähteistä, jotta voidaan edistää yhteisen tilannetietoisuuden luomista;

   b) varmistamalla tehokkaan tiedonkulun ja eskalointimekanismit CSIRT-verkoston sekä teknisten ja poliittisten päättäjien välillä unionin tasolla;

   c) helpottamalla pyynnöstä tällaisten poikkeamien tai kriisien teknistä käsittelyä, mukaan lukien erityisesti tukemalla teknisten ratkaisujen vapaaehtoista jakamista jäsenvaltioiden välillä;

d) tukemalla unionin toimielimiä, elimiä ja laitoksia sekä pyynnöstä jäsenvaltioita tällaisiin poikkeamiin tai kriiseihin liittyvässä julkisessa viestinnässä;

e) testaamalla tällaisiin poikkeamiin tai kriiseihin reagoimista varten laadittuja yhteistyösuunnitelmia unionin tasolla ja tukemalla jäsenvaltioita niiden pyynnöstä tällaisten suunnitelmien testaamisessa kansallisella tasolla.

8 artikla

Markkinat, kyberturvallisuussertifiointi ja standardointi

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

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

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

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

d) osallistua vertaisarviointeihin 59 artiklan 4 kohdan mukaisesti;

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

2. ENISA toimii sidosryhmien kyberturvallisuuden sertifiointiryhmän sihteeristönä 22 artiklan 4 kohdan mukaisesti;

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

4. ENISA edistää osaltaan arviointi- ja sertifiointiprosessien valmiuksien kehittämistä laatimalla ja antamalla ohjeita sekä tukemalla jäsenvaltioita näiden pyynnöstä;

5. ENISA helpottaa tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien riskinhallintaan ja turvallisuuteen liittyvien eurooppalaisten ja kansainvälisten standardien laatimista ja käyttöönottoa;

6. ENISA laatii yhteistyössä jäsenvaltioiden ja toimialan kanssa neuvoja ja suuntaviivoja keskeisten palvelujen tarjoajia ja digitaalisen palvelun tarjoajia koskeviin turvallisuusvaatimuksiin liittyvistä teknisistä aloista sekä jo olemassa olevista standardeista, mukaan lukien jäsenvaltioiden kansalliset standardit, direktiivin (EU) 2016/1148 19 artiklan 2 kohdan mukaisesti;

7. ENISA tekee säännöllisiä analyyseja kyberturvallisuusmarkkinoiden tärkeimmistä suuntauksista sekä kysyntä- että tarjontapuolella ja levittää näiden analyysien tuloksia kyberturvallisuusmarkkinoiden edistämiseksi unionissa.

9 artikla

Tietämys ja tiedotus

ENISA

a) tekee analyyseja uusista teknologioista ja aihekohtaisia arviointeja teknologisten innovaatioiden odotettavissa olevista yhteiskunnallisista, oikeudellisista, taloudellisista ja sääntelyyn liittyvistä vaikutuksista kyberturvallisuuden kannalta;

b) tekee pitkän aikavälin strategisia analyyseja kyberuhkista ja poikkeamista kyberturvallisuuteen liittyvien uusien kehityssuuntausten kartoittamiseksi ja poikkeamien ehkäisemiseksi;

c) tarjoaa yhteistyössä jäsenvaltioiden viranomaisten ja asiaankuuluvien sidosryhmien asiantuntijoiden kanssa neuvoja, ohjeita ja parhaita käytäntöjä, jotka koskevat verkko- ja tietojärjestelmien turvallisuutta sekä erityisesti direktiivin (EU) 2016/1148 liitteessä II mainittuja toimialoja tukevien ja kyseisen direktiivin liitteessä III lueteltujen digitaalisten palvelujen tarjoajien hyödyntämien infrastruktuurien turvallisuutta;

d) kokoaa, järjestää ja saattaa yleisön saataville tähän tarkoitetun portaalin kautta unionin toimielimiltä, elimiltä ja laitoksilta sekä vapaaehtoisuuteen perustuen jäsenvaltioilta ja yksityisiltä ja julkisilta sidosryhmiltä saatavaa tietoa kyberturvallisuudesta;

e) kerää ja analysoi julkisesti saatavilla olevia tietoja asiaa koskevista merkittävistä poikkeamista ja kokoaa raportteja ohjeiden antamiseksi kansalaisille, organisaatioille ja yrityksille kaikkialla unionissa.

10 artikla

Tietoisuuden lisääminen ja koulutus

ENISA

a) lisää suuren yleisön tietoisuutta kyberturvallisuusriskeistä ja antaa yksittäisille käyttäjille ohjeita hyvistä käytännöistä, kuten kyberhygieniasta ja kyberlukutaidosta, kansalaisten, organisaatioiden ja yritysten käyttöön;

b) järjestää yhteistyössä jäsenvaltioiden, unionin toimielinten, elinten ja laitosten sekä toimialan kanssa säännöllisiä tiedotuskampanjoita kyberturvallisuuden ja sen näkyvyyden parantamiseksi unionissa sekä laajan julkisen keskustelun aikaansaamiseksi;

c) avustaa jäsenvaltioita niiden työssä kyberturvallisuustietoisuuden lisäämiseksi ja kyberturvallisuuskoulutuksen edistämiseksi;

d) tukee jäsenvaltioiden välistä tiiviimpää koordinointia ja parhaiden käytäntöjen vaihtoa kyberturvallisuustietoisuuden ja -koulutuksen osalta.

11 artikla

Tutkimus ja innovointi

Tutkimuksen ja innovoinnin osalta ENISA

a) antaa unionin toimielimille, elimille ja laitoksille sekä jäsenvaltioille neuvoja kyberturvallisuusalan tutkimustarpeista ja -painopisteistä, jotta nykyisiin ja kehittyviin riskeihin ja kyberuhkiin, myös jos ne liittyvät uusiin ja kehittyviin tieto- ja viestintäteknologioihin, voitaisiin löytää toimivia ratkaisuja ja jotta riskinehkäisytekniikoita voitaisiin käyttää tehokkaasti;

b) osallistuu, jos komissio on siirtänyt sille toimivaltuudet, tutkimuksen ja innovoinnin rahoitusohjelmien täytäntöönpanovaiheeseen tai näiden ohjelmien rahoituksen saajana;

c) osallistuu kyberturvallisuusalalla strategisen tutkimus- ja innovointiohjelman laatimiseen unionin tasolla.

12 artikla

Kansainvälinen yhteistyö

ENISA edesauttaa unionin pyrkimyksiä yhteistoimintaan kolmansien maiden ja kansainvälisten organisaatioiden kanssa sekä asiaankuuluvissa kansainvälisissä yhteistyöpuitteissa kansainvälisen yhteistyön edistämiseksi kyberturvallisuuskysymyksissä muun muassa

a) toimimalla tarvittaessa tarkkailijana kansainvälisten harjoitusten järjestämisessä sekä analysoimalla harjoitusten tuloksia ja raportoimalla niistä johtokunnalle;

b) edistämällä komission pyynnöstä parhaiden käytäntöjen vaihtoa;

c) antamalla komission pyynnöstä asiantuntemusta sen käyttöön;

d) tarjoamalla neuvoja ja tukea komissiolle yhteistyössä 62 artiklan nojalla perustetun Euroopan kyberturvallisuuden sertifiointiryhmän kanssa kysymyksissä, jotka liittyvät kolmansien maiden kanssa tehtäviin kyberturvallisuussertifikaattien vastavuoroista tunnustamista koskeviin sopimuksiin.

III luku

ENISAn organisaatio

13 artikla

ENISAn rakenne

ENISAn hallinto- ja johtamisrakenne muodostuu seuraavista:

a) johtokunta;

b) hallitus;

c) pääjohtaja;

d) ENISAn neuvoa-antava ryhmä;

e) kansallisten yhteyshenkilöiden verkosto.

1 JAKSO

JOHTOKUNTA

14 artikla

Johtokunnan kokoonpano

1. Johtokuntaan kuuluu kustakin jäsenvaltiosta yksi jäsen ja kaksi komission nimittämää jäsentä. Kaikilla jäsenillä on äänioikeus.

2. Kullakin johtokunnan jäsenellä on varajäsen. Kyseinen varajäsen edustaa jäsentä tämän ollessa poissa.

3. Johtokunnan jäsenet ja varajäsenet nimitetään heidän kyberturvallisuusalaa koskevan tietämyksensä perusteella ottaen huomioon heidän asianmukaiset johtamis-, hallinto- ja varainhoitotaitonsa. Johtokunnan toiminnan jatkuvuuden varmistamiseksi komission ja jäsenvaltioiden on pyrittävä rajoittamaan edustajiensa vaihtuvuutta johtokunnassa. Komission ja jäsenvaltioiden on pyrittävä sukupuolten tasapuoliseen edustukseen johtokunnassa.

4. Johtokunnan jäsenten ja varajäsenten toimikausi on neljä vuotta. Toimikausi voidaan uusia.

15 artikla

Johtokunnan tehtävät

1. Johtokunta

a) vahvistaa ENISAn toiminnan yleiset suuntaviivat ja varmistaa, että ENISA toimii tässä asetuksessa vahvistettujen sääntöjen ja periaatteiden mukaisesti; se myös huolehtii ENISAn toiminnan johdonmukaisuudesta suhteessa jäsenvaltioiden toimintaan sekä unionin tason toimiin;

b) hyväksyy luonnoksen ENISAn yhtenäiseksi ohjelma-asiakirjaksi 24 artiklan mukaisesti ennen sen toimittamista komissiolle lausuntoa varten;

c) hyväksyy ENISAn yhtenäisen ohjelma-asiakirjan komission lausunnon huomioon ottaen;

d) valvoo yhtenäisen ohjelma-asiakirjan sisältämien monivuotisen ja vuotuisen ohjelmasuunnittelun toteutusta;

e) hyväksyy ENISAn vuotuisen talousarvion ja hoitaa muita tehtäviä, jotka liittyvät ENISAn talousarvioon, IV luvun mukaisesti;

f) arvioi ja hyväksyy ENISAn toimintaa koskevan vuotuisen konsolidoidun toimintakertomuksen ja toimittaa sen yhdessä sitä koskevan arviointinsa kanssa viimeistään seuraavan vuoden heinäkuun 1 päivänä Euroopan parlamentille, neuvostolle, komissiolle ja tilintarkastustuomioistuimelle; toimintakertomus sisältää tilinpäätöksen ja kuvauksen siitä, kuinka ENISA on saavuttanut tulosindikaattorinsa; toimintakertomus julkistetaan;

g) hyväksyy ENISAn varainhoitosäännöt 32 artiklan mukaisesti;

h) hyväksyy petostentorjuntastrategian, joka on oikeassa suhteessa petosriskeihin nähden, kun toteutettavien toimenpiteiden kustannus-hyötyanalyysi otetaan huomioon;

i) hyväksyy jäsentensä eturistiriitojen ehkäisemistä ja hallintaa koskevat säännöt;

j) huolehtii asianmukaisista jatkotoimista, joita toteutetaan Euroopan petostentorjuntaviraston (OLAF) tutkimuksiin ja erilaisiin sisäisen tai ulkoisen tarkastuksen raportteihin ja sisäisiin tai ulkoisiin arviointeihin perustuvien tulosten ja suositusten perusteella;

k) hyväksyy työjärjestyksensä, mukaan lukien yksittäisten tehtävien siirtämistä koskevia väliaikaisia päätöksiä koskevat säännöt 19 artiklan 7 kohdan mukaisesti;

l) käyttää ENISAn henkilöstön suhteen neuvoston asetuksella (ETY, EURATOM, EHTU) N:o 259/68[1] vahvistetuissa Euroopan unionin virkamiehiin sovellettavissa henkilöstösäännöissä, jäljempänä 'henkilöstösäännöt', nimittävälle viranomaiselle ja unionin muuta henkilöstöä koskevissa palvelussuhteen ehdoissa työsopimusten tekemiseen valtuutetulle viranomaiselle annettua toimivaltaa, jäljempänä 'nimittävän viranomaisen toimivalta', 2 kohdan mukaisesti;

m) vahvistaa henkilöstösääntöjen ja muuta henkilöstöä koskevien palvelussuhteen ehtojen täytäntöönpanoa koskevat säännöt henkilöstösääntöjen 110 artiklassa säädettyä menettelyä noudattaen;

n) nimittää pääjohtajan ja jatkaa tarvittaessa tämän toimikautta tai erottaa tämän 36 artiklan mukaisesti;

o) nimittää tilinpitäjän, joka voi olla komission tilinpitäjä ja joka hoitaa tehtäviään täysin riippumattomasti;

p) tekee kaikki päätökset viraston sisäisistä rakenteista ja tarvittaessa niiden muuttamisesta ottaen huomioon ENISAn toimintatarpeet ja moitteettoman varainhoidon;

[1] EYVL L 56, 4.3.1968, s. 1.

q) antaa luvan työjärjestelyjen vahvistamiseen 7 artiklan osalta;

r) antaa luvan työjärjestelyjen vahvistamiseen tai niistä sopimiseen 42 artiklan mukaisesti;

2. Johtokunta tekee henkilöstösääntöjen 110 artiklan mukaisesti henkilöstösääntöjen 2 artiklan 1 kohtaan ja muuta henkilöstöä koskevien palvelussuhteen ehtojen 6 artiklaan perustuvan päätöksen, jolla siirretään nimittävän viranomaisen toimivalta pääjohtajalle ja määritetään olosuhteet, joissa toimivallan siirto voidaan keskeyttää. Pääjohtaja voi siirtää tämän toimivallan edelleen.

3. Jos poikkeukselliset olosuhteet sitä edellyttävät, johtokunta voi tekemällään päätöksellä tilapäisesti keskeyttää pääjohtajalle siirretyn nimittävän viranomaisen toimivallan ja pääjohtajan edelleen siirtämän nimittävän viranomaisen toimivallan ja sen sijaan käyttää kyseistä toimivaltaa itse tai siirtää sen jollekin jäsenistään tai jollekulle henkilöstöön kuuluvalle, joka on muu kuin pääjohtaja.

16 artikla

Johtokunnan puheenjohtaja

Johtokunta valitsee keskuudestaan puheenjohtajan ja varapuheenjohtajan jäsentensä kahden kolmasosan enemmistöllä. Heidän toimikautensa on neljä vuotta, ja se voidaan uusia kerran. Jos heidän jäsenyytensä johtokunnassa kuitenkin päättyy heidän toimikautensa aikana, myös heidän toimikautensa päättyy tuona päivänä ilman eri toimenpiteitä. Varapuheenjohtaja toimii viran puolesta puheenjohtajan sijaisena tämän ollessa estynyt.

17 artikla

Johtokunnan kokoukset

1. Johtokunta kokoontuu puheenjohtajansa kutsusta.

2. Johtokunta pitää vähintään kaksi sääntömääräistä kokousta vuodessa. Johtokunta kokoontuu myös ylimääräisiin kokouksiin johtokunnan puheenjohtajan, komission tai vähintään yhden kolmasosan johtokunnan jäsenistä sitä pyytäessä.

3. Pääjohtaja osallistuu johtokunnan kokouksiin ilman äänioikeutta.

4. ENISAn neuvoa-antavan ryhmän jäsenet voivat osallistua puheenjohtajan kutsusta johtokunnan kokouksiin ilman äänioikeutta.

5. Johtokunnan jäsenillä ja varajäsenillä voi olla kokouksissa avustajinaan neuvonantajia tai asiantuntijoita, jollei johtokunnan työjärjestyksestä muuta johdu.

6. ENISA vastaa johtokunnan sihteeristön tehtävistä.

18 artikla

Johtokunnan äänestyssäännöt

1. Johtokunta tekee päätöksensä jäsentensä enemmistöllä.

2. Yhtenäisen ohjelma-asiakirjan ja vuotuisen talousarvion hyväksyminen sekä pääjohtajan nimittäminen, toimikauden jatkaminen ja erottaminen edellyttävät johtokunnan jäsenten kahden kolmasosan enemmistöä.

3. Kullakin jäsenellä on yksi ääni. Jäsenen poissa ollessa varajäsenellä on oikeus käyttää tämän äänioikeutta.

4. Johtokunnan puheenjohtaja osallistuu äänestykseen.

5. Pääjohtaja ei osallistu äänestykseen.

6. Johtokunnan työjärjestyksessä määritellään yksityiskohtaisemmat äänestystä koskevat järjestelyt, erityisesti olosuhteet, joissa jäsen voi toimia toisen jäsenen puolesta.

2 JAKSO

HALLITUS

19 artikla

Hallitus

1. Johtokuntaa avustaa hallitus.

2. Hallitus

a) valmistelee päätökset johtokunnan hyväksyttäviksi;

b) varmistaa yhdessä johtokunnan kanssa, että OLAFin tutkimuksissa sekä sisäisissä tai ulkoisissa tarkastuskertomuksissa ja arvioinneissa esitettyjen havaintojen ja suositusten johdosta toteutetaan asianmukaiset jatkotoimet:

c) avustaa ja neuvoo pääjohtajaa hallinnollisia ja talousarvioasioita koskevien johtokunnan päätösten täytäntöönpanossa 20 artiklan mukaisesti, sanotun kuitenkaan rajoittamatta 20 artiklassa säädettyjä pääjohtajan tehtäviä.

3. Hallitukseen kuuluu viisi jäsentä. Hallituksen jäsenet nimitetään johtokunnan jäsenten keskuudesta. Yksi hallituksen jäsenistä on johtokunnan puheenjohtaja, joka voi myös toimia hallituksen puheenjohtajana, ja toinen on komission edustaja. Hallituksen jäsenten nimityksissä on pyrittävä takaamaan tasapainoinen sukupuolijakauma hallituksessa. Pääjohtaja osallistuu hallituksen kokouksiin, mutta hänellä ei ole äänioikeutta.

4. Hallituksen jäsenten toimikausi on neljä vuotta. Toimikausi voidaan uusia.

5. Hallitus kokoontuu vähintään kerran kolmessa kuukaudessa. Hallituksen puheenjohtaja kutsuu kokoon ylimääräisiä kokouksia hallituksen jäsenten pyynnöstä.

6. Johtokunta vahvistaa hallituksen työjärjestyksen.

7. Hallitus voi tarvittaessa tehdä kiireellisissä tapauksissa tiettyjä väliaikaisia päätöksiä johtokunnan puolesta, erityisesti hallinnollisista kysymyksistä, mukaan lukien nimittävän viranomaisen toimivallan siirron keskeyttäminen, sekä talousarvioon liittyvistä kysymyksissä. Tällaisesta väliaikaisesta päätöksestä ilmoitetaan johtokunnalle ilman aiheetonta viivytystä. Johtokunta päättää päätöksen hyväksymisestä tai hylkäämisestä viimeistään kolmen kuukauden kuluttua päätöksen tekemisestä. Hallitus ei voi tehdä johtokunnan puolesta päätöksiä, joihin vaaditaan johtokunnan kahden kolmasosan enemmistö.

3 JAKSO

PÄÄJOHTAJA

20 artikla

Pääjohtajan tehtävät

1. ENISAa johtaa sen pääjohtaja, joka hoitaa tehtäväänsä riippumattomasti. Pääjohtaja on vastuussa johtokunnalle.

2. Pääjohtaja raportoi pyydettäessä Euroopan parlamentille tehtäviensä hoidosta. Neuvosto voi pyytää pääjohtajaa raportoimaan tehtäviensä hoidosta.

3. Pääjohtajan tehtävänä on

   a) ENISAn päivittäisen toiminnan hallinnointi;

   b) johtokunnan tekemien päätösten täytäntöönpano;

   c) yhtenäisen ohjelma-asiakirjan luonnoksen laatiminen ja sen toimittaminen johtokunnan hyväksyttäväksi ennen sen toimittamista komissiolle;

d) yhtenäisen ohjelma-asiakirjan täytäntöönpano ja siitä raportointi johtokunnalle;

e) ENISAn toimintaa koskevan vuotuisen konsolidoidun toimintakertomuksen, myös ENISAn vuotuisen työohjelman täytäntöönpanon osalta, laatiminen ja sen esittäminen johtokunnalle arvioitavaksi ja hyväksyttäväksi;

f) toimintasuunnitelman laatiminen jälkiarviointien päätelmien perusteella ja edistymiskertomuksen laatiminen komissiolle kahden vuoden välein;

g) toimintasuunnitelman laatiminen sisäisten tai ulkoisten tarkastuskertomusten päätelmiin sekä OLAFin tutkimuksiin perustuvia jatkotoimia varten ja suunnitelman edistymisestä raportointi kahdesti vuodessa komissiolle ja säännöllisesti johtokunnalle;

h) 32 artiklassa tarkoitettujen ENISAan sovellettavien varainhoitosääntöjen luonnoksen valmistelu;

i) ENISAn tuloja ja menoja koskevan ennakkoarvion luonnoksen laatiminen ja viraston talousarvion toteuttaminen;

j) unionin taloudellisten etujen suojeleminen toteuttamalla petosten, lahjonnan ja muun laittoman toiminnan torjuntatoimia ja tehokkaita tarkastuksia ja, jos väärinkäytöksiä ilmenee, perimällä takaisin väärin perustein maksetut määrät sekä soveltamalla tarvittaessa tehokkaita, oikeasuhteisia ja varoittavia hallinnollisia ja taloudellisia seuraamuksia;

k) petostentorjuntastrategian laatiminen ENISAlle ja sen esittäminen johtokunnalle hyväksyntää varten;

l) yhteyksien luominen ja ylläpito yritysmaailmaan ja kuluttajajärjestöihin säännöllisen vuoropuhelun varmistamiseksi asiaankuuluvien sidosryhmien kanssa;

m) säännöllinen näkemysten ja tietojen vaihto unionin toimielinten, elinten ja laitosten kanssa näiden kyberturvallisuuteen liittyvistä toimista, jotta varmistetaan johdonmukaisuus kehitettäessä ja pantaessa täytäntöön unionin politiikkaa;

n) muiden pääjohtajalle tällä asetuksella osoitettujen tehtävien hoito.

4. Tarpeen vaatiessa ja ENISAn tavoitteiden ja tehtävien puitteissa pääjohtaja voi perustaa muun muassa jäsenvaltioiden toimivaltaisten viranomaisten asiantuntijoista koostuvia tilapäisiä työryhmiä. Pääjohtajan on ilmoitettava tästä etukäteen johtokunnalle. Menettelyt, jotka koskevat erityisesti työryhmien kokoonpanoa, pääjohtajan suorittamaa työryhmien asiantuntijoiden nimeämistä ja työryhmien toimintaa, vahvistetaan ENISAn sisäisissä toimintasäännöissä.

5. Pääjohtaja voi asianmukaisen kustannus-hyötyanalyysin perusteella päättää perustaa ENISAlle yhden tai useamman paikallistoimiston yhteen tai useampaan jäsenvaltioon, jos hän katsoo sen tarpeelliseksi ENISAn tehtävien tehokkaan ja toimivan toteuttamisen kannalta. Ennen kuin pääjohtaja tekee päätöksen paikallistoimiston perustamisesta, hänen on kuultava asianomaisia jäsenvaltioita, myös jäsenvaltiota, jossa ENISAn toimipaikka sijaitsee, sekä hankittava ennakkosuostumus komissiolta ja johtokunnalta. Jos pääjohtajan toteuttamassa asianomaisten jäsenvaltioiden kuulemisessa ei päästä sopimukseen, asia on saatettava neuvoston käsiteltäväksi. Kaikkien paikallistoimistojen henkilöstön kokonaismäärä on pidettävä mahdollisimman vähäisenä, eikä se saa ylittää 40:tä prosenttia siihen jäsenvaltioon sijoitetun ENISAn henkilöstön kokonaismäärästä, jossa ENISAn toimipaikka sijaitsee. Yksittäisen paikallistoimiston henkilöstön määrä ei saa ylittää 10:tä prosenttia siihen jäsenvaltioon sijoitetun ENISAn henkilöstön kokonaismäärästä, jossa ENISAn toimipaikka sijaitsee.

Paikallistoimiston perustamista koskevassa päätöksessä on määriteltävä paikallistoimistossa toteutettavien toimien laajuus siten, että vältetään tarpeettomia kustannuksia ja ENISAn hallinnollisten tehtävien päällekkäisyyttä.

4 JAKSO

ENISAN NEUVOA-ANTAVA RYHMÄ,

SIDOSRYHMIEN KYBERTURVALLISUUDEN SERTIFIOINTIRYHMÄ

JA KANSALLISTEN YHTEYSHENKILÖIDEN VERKOSTO

21 artikla

ENISAn neuvoa-antava ryhmä

1. Johtokunta perustaa avoimella tavalla pääjohtajan esityksestä ENISAn neuvoa-antavan ryhmän, joka koostuu asiaan liittyviä sidosryhmiä, kuten tieto- ja viestintätekniikan alaa, sähköisten viestintäverkkojen tai yleisön saatavilla olevien sähköisten viestintäpalvelujen tarjoajia, pk-yrityksiä, keskeisten palvelujen tarjoajia ja kuluttajaryhmiä, edustavista tunnustetuista asiantuntijoista, tiedeyhteisöä edustavista kyberturvallisuusasiantuntijoista sekä direktiivin (EU) 2018/1972 mukaisesti ilmoitettujen toimivaltaisten viranomaisten, eurooppalaisten standardointiorganisaatioiden sekä lainvalvonta- ja tietosuojaviranomaisten edustajista. Johtokunta pyrkii varmistamaan asianmukaisen sukupuolten tasapuolisen edustuksen, maantieteellisen tasapainon sekä eri sidosryhmien tasapainoisen edustuksen.

2. ENISAn neuvoa-antavaa ryhmää koskevat menettelyt, jotka liittyvät erityisesti sen kokoonpanoon, 1 kohdassa tarkoitettuun pääjohtajan tekemään esitykseen, ryhmän jäsenten lukumäärään, sen jäsenten nimeämiseen sekä sen toimintaan, määritellään ENISAn sisäisissä toimintasäännöissä ja julkaistaan.

3. ENISAn neuvoa-antavan ryhmän puheenjohtajana toimii pääjohtaja tai pääjohtajan tähän tehtävään tapauskohtaisesti nimeämä henkilö.

4. ENISAn neuvoa-antavan ryhmän jäsenten toimikausi on kaksi ja puoli vuotta. Johtokunnan jäsenet eivät saa olla ENISAn neuvoa-antavan ryhmän jäseniä. Komission ja jäsenvaltioiden asiantuntijoilla on oikeus olla läsnä ENISAn neuvoa-antavan ryhmän kokouksissa ja osallistua sen työhön. Muiden pääjohtajan tärkeiksi katsomien elinten edustajia, jotka eivät ole ENISAn neuvoa-antavan ryhmän jäseniä, voidaan pyytää saapuville ENISAn neuvoa-antavan ryhmän kokouksiin ja osallistumaan sen työhön.

5. ENISAn neuvoa-antava ryhmä neuvoo ENISAa sen tehtävien hoidossa paitsi tämän asetuksen III osaston säännösten soveltamisessa. Erityisesti se neuvoo pääjohtajaa tämän laatiessa esitystä ENISAn vuotuiseksi työohjelmaksi sekä yhteydenpidossa asianmukaisten sidosryhmien kanssa vuotuiseen työohjelmaan liittyvissä kysymyksissä.

6. ENISAn neuvoa-antava ryhmä tiedottaa toiminnastaan johtokunnalle säännöllisesti.

22 artikla

Sidosryhmien kyberturvallisuuden sertifiointiryhmä

1. Perustetaan sidosryhmien kyberturvallisuuden sertifiointiryhmä.

2. Sidosryhmien kyberturvallisuuden sertifiointiryhmä koostuu jäsenistä, jotka valitaan asiaan liittyviä sidosryhmiä edustavien tunnustettujen asiantuntijoiden joukosta. Komissio valitsee sidosryhmien kyberturvallisuuden sertifiointiryhmän jäsenet ENISAn ehdotuksen perusteella läpinäkyvällä ja avoimella menettelyllä varmistaen eri sidosryhmien tasapainoisen edustuksen sekä asianmukaisen sukupuolten tasapuolisen edustuksen ja maantieteellisen tasapainon.

3. Sidosryhmien kyberturvallisuuden sertifiointiryhmän tehtävänä on

   a) neuvoa komissiota eurooppalaiseen kyberturvallisuuden sertifiointikehykseen liittyvien strategisten kysymysten osalta,

   b) neuvoa ENISAa pyynnöstä markkinoihin, kyberturvallisuussertifiointiin ja standardointiin liittyviä ENISAn tehtäviä koskevissa yleisissä ja strategisissa asioissa;

   c) avustaa komissiota 47 artiklassa tarkoitetun unionin jatkuvan työohjelman valmistelemisessa;

d) antaa lausunto unionin jatkuvasta työohjelmasta 47 artiklan 4 kohdan mukaisesti; ja

e) neuvoa kiireellisissä tapauksissa komissiota ja Euroopan kyberturvallisuuden sertifiointiryhmää sellaisten sertifiointijärjestelmien tarpeesta, jotka eivät sisälly 47 ja 48 artiklassa tarkoitettuun unionin jatkuvaan työohjelmaan.

4. Sidosryhmien kyberturvallisuuden sertifiointiryhmän puheenjohtajana toimivat komissio ja ENISA yhdessä, ja sen sihteeristönä toimii ENISA.

23 artikla

Kansallisten yhteyshenkilöiden verkosto

1. Johtokunta perustaa pääjohtajan esityksestä kansallisten yhteyshenkilöiden verkoston, joka koostuu jäsenvaltioiden edustajista. Kukin jäsenvaltio nimeää yhden edustajan kansallisten yhteyshenkilöiden verkostoon. Kansallisten yhteyshenkilöiden verkoston kokouksia voidaan järjestää vaihtelevissa asiantuntijakokoonpanoissa.

2. Kansallisten yhteyshenkilöiden verkoston tehtävänä on erityisesti helpottaa ENISAn ja jäsenvaltioiden välistä tietojenvaihtoa ja auttaa ENISAa levittämään toimintaansa, löydöksiään ja suosituksiaan asiaankuuluville sidosryhmille kaikkialla unionissa.

3. Kansalliset yhteyshenkilöt toimivat kansallisen tason yhteyspisteinä, jotka helpottavat ENISAn ja kansallisten asiantuntijoiden yhteistyötä ENISAn vuotuisen työohjelman täytäntöönpanossa.

4. Kansallisten yhteyshenkilöiden tiivis yhteistyö johtokunnassa toimivien jäsenvaltioidensa edustajien kanssa ei saa aiheuttaa sitä, että verkosto tekee päällekkäistä työtä johtokunnan tai muiden unionin foorumien kanssa.

5. Kansallisten yhteyshenkilöiden verkoston tehtävät ja menettelyt määritellään ENISAn sisäisissä toimintasäännöissä ja julkaistaan.

5 JAKSO
TOIMINTA

24 artikla
Yhtenäinen ohjelma-asiakirja

1. ENISA noudattaa toiminnassaan sen vuotuisen ja monivuotisen ohjelman suunnitelmat sisältävää yhtenäistä ohjelma-asiakirjaa, johon sisältyy kaikki sen suunniteltu toiminta.

2. Pääjohtaja laatii vuosittain luonnoksen yhtenäiseksi ohjelma-asiakirjaksi, joka sisältää vuotuisen ja monivuotisen ohjelman suunnitelmat ja vastaavan taloudellisia ja henkilöresursseja koskevan suunnittelun, komission delegoidun asetuksen (EU) N:o 1271/2013[1] 32 artiklan mukaisesti ja ottaen huomioon komission esittämät suuntaviivat.

3. Johtokunta hyväksyy viimeistään kunkin vuoden marraskuun 30 päivänä 1 kohdassa tarkoitetun yhtenäisen ohjelma-asiakirjan ja toimittaa sen Euroopan parlamentille, neuvostolle ja komissiolle viimeistään seuraavan vuoden tammikuun 31 päivänä, samoin kuin asiakirjan mahdolliset myöhemmät päivitetyt versiot.

4. Yhtenäisestä ohjelma-asiakirjasta tulee lopullinen, kun unionin yleinen talousarvio on lopullisesti vahvistettu, ja sitä on tarvittaessa mukautettava.

5. Vuotuisessa työohjelmassa on esitettävä yksityiskohtaiset tavoitteet ja odotetut tulokset, suoritusindikaattorit mukaan lukien. Siinä on myös esitettävä kuvaus rahoitettavista toimista ja mainittava kuhunkin toimeen osoitetut taloudelliset resurssit ja henkilöstöresurssit toimintoperusteisen budjetoinnin ja hallinnoinnin periaatteiden mukaisesti. Vuotuisen työohjelman on oltava yhdenmukainen 7 kohdassa tarkoitetun monivuotisen työohjelman kanssa. Siinä on selkeästi ilmoitettava, mitä tehtäviä on lisätty, muutettu tai poistettu edelliseen varainhoitovuoteen verrattuna.

[1] Komission delegoitu asetus (EU) N:o 1271/2013, annettu 30 päivänä syyskuuta 2013, Euroopan parlamentin ja neuvoston asetuksen (EU, Euratom) N:o 966/2012 208 artiklassa tarkoitettuja elimiä koskevasta varainhoidon puiteasetuksesta (EUVL L 328, 7.12.2013, s. 42).

6. Johtokunta muuttaa hyväksyttyä vuotuista työohjelmaa tarvittaessa, jos ENISAlle annetaan uusi tehtävä. Vuotuiseen työohjelmaan tehtävät olennaiset muutokset on hyväksyttävä samaa menettelyä noudattaen kuin alkuperäinen vuotuinen työohjelma. Johtokunta voi siirtää pääjohtajalle valtuudet tehdä vuotuiseen työohjelmaan muita kuin olennaisia muutoksia.

7. Monivuotisessa työohjelmassa on esitettävä yleinen strateginen ohjelma, mukaan lukien tavoitteet, odotetut tulokset ja suoritusindikaattorit. Siinä on esitettävä myös resursseja koskeva ohjelmasuunnittelu, mukaan lukien monivuotinen talousarvio ja henkilöstösuunnitelma.

8. Resursseja koskeva ohjelmasuunnittelu saatetaan ajan tasalle vuosittain. Strategista ohjelmaa päivitetään tarvittaessa ja erityisesti 67 artiklassa tarkoitetun arvioinnin tulosten huomioon ottamiseksi.

25 artikla

Etunäkökohtia koskeva ilmoitus

1. Jokaisen johtokunnan jäsenen, pääjohtajan sekä jokaisen toimihenkilön, joka on otettu palvelukseen jäsenvaltion tilapäisesti lähettämänä virkamiehenä, on tehtävä ilmoitus sitoumuksistaan sekä ilmoitus, jossa he toteavat, onko olemassa heidän riippumattomuuttaan mahdollisesti vaarantavia välittömiä tai välillisiä sidonnaisuuksia. Ilmoitusten on oltava tarkkoja ja täydellisiä, ne on tehtävä kirjallisesti vuosittain ja ne on tarvittaessa saatettava ajan tasalle.

2. Jokaisen johtokunnan jäsenen, pääjohtajan ja jokaisen tilapäisiin työryhmiin osallistuvan ulkopuolisen asiantuntijan on ilmoitettava viimeistään kunkin kokouksen alussa tarkasti ja täydellisesti mahdolliset sidonnaisuudet, jotka saattavat vaarantaa heidän riippumattomuutensa kokouksen esityslistalla olevien asioiden suhteen, sekä pidättäydyttävä osallistumasta kyseisiä kohtia koskevaan keskusteluun ja äänestykseen.

3. ENISA vahvistaa sisäisissä toimintasäännöissään 1 ja 2 kohdassa tarkoitettua sidonnaisuuksien ilmoittamista koskeviin sääntöihin liittyvät käytännön järjestelyt.

26 artikla

Avoimuus

1. ENISAn toiminnan on oltava mahdollisimman avointa sekä 28 artiklan mukaista.

2. ENISA varmistaa, että suuri yleisö ja kaikki asianomaiset tahot saavat asianmukaista, puolueetonta, luotettavaa ja helposti saatavissa olevaa tietoa erityisesti ENISAn työn tuloksista. Sen on myös julkistettava 25 artiklan mukaisesti tehdyt sidonnaisuuksia koskevat ilmoitukset.

3. Johtokunta voi pääjohtajan ehdotuksesta sallia asianomaisten tahojen seurata joidenkin ENISAn toimien käsittelyä.

4. ENISA vahvistaa sisäisissä toimintasäännöissään 1 ja 2 kohdassa tarkoitettujen avoimuussääntöjen täytäntöönpanoa koskevat käytännön järjestelyt.

27 artikla

Luottamuksellisuus

1. ENISA ei saa paljastaa kolmansille osapuolille käsittelemiään ja saamiaan tietoja, joiden käsittelystä luottamuksellisina on esitetty perusteltu pyyntö, sanotun kuitenkaan rajoittamatta 28 artiklan soveltamista.

2. Johtokunnan jäsenten, pääjohtajan, ENISAn neuvoa-antavan ryhmän jäsenten, tilapäisiin työryhmiin osallistuvien ulkopuolisten asiantuntijoiden sekä ENISAn henkilöstön, mukaan lukien ne toimihenkilöt, jotka on otettu palvelukseen jäsenvaltioiden tilapäisesti lähettäminä virkamiehinä, on noudatettava SEUT 339 artiklan mukaista salassapitovelvollisuutta myös tehtäviensä päätyttyä.

3. ENISA vahvistaa sisäisissä toimintasäännöissään 1 ja 2 kohdassa tarkoitettujen salassapitovelvollisuutta koskevien sääntöjen täytäntöönpanoa koskevat käytännön järjestelyt.

4. Johtokunta päättää antaa ENISAlle luvan käsitellä turvallisuusluokiteltua tietoa, jos ENISAn tehtävien suorittaminen sitä edellyttää. Tässä tapauksessa ENISAn on yhteisymmärryksessä komission yksiköiden kanssa vahvistettava turvallisuussäännöt soveltaen tietoturvan periaatteita, jotka on vahvistettu komission päätöksissä (EU, Euratom) 2015/443[1] ja 2015/444[2]. Nämä turvallisuussäännöt koskevat muun muassa turvallisuusluokiteltujen tietojen vaihtamista, käsittelyä ja tallentamista.

---

1 Komission päätös (EU, Euratom) 2015/443, annettu 13 päivänä maaliskuuta 2015, turvallisuudesta komissiossa (EUVL L 72, 17.3.2015, s. 41).

2 Komission päätös (EU, Euratom) 2015/444, annettu 13 päivänä maaliskuuta 2015, EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista säännöistä (EUVL L 72, 17.3.2015, s. 53).

28 artikla

Asiakirjojen julkisuus

1. ENISAn hallussaan pitämiin asiakirjoihin sovelletaan asetusta (EY) N:o 1049/2001.

2. Johtokunta vahvistaa järjestelyt asetuksen (EY) N:o 1049/2001 täytäntöön panemiseksi … viimeistään päivänä …kuuta … [kuusi kuukautta tämän asetuksen voimaantulon jälkeen].

3. Asetuksen (EY) N:o 1049/2001 8 artiklan nojalla tehdyistä ENISAn päätöksistä voidaan kannella oikeusasiamiehelle SEUT 228 artiklan nojalla tai nostaa kanne Euroopan unionin tuomioistuimessa SEUT 263 artiklan nojalla.

IV luku

ENISAn talousarvion laatiminen ja rakenne

29 artikla

ENISAn talousarvion laatiminen

1. Pääjohtaja laatii vuosittain esityksen ENISAn seuraavan varainhoitovuoden tuloja ja menoja koskevaksi ennakkoarvioksi ja toimittaa sen sekä siihen liitetyn henkilöstötaulukkoehdotuksen johtokunnalle. Tulojen ja menojen on oltava tasapainossa.

2. Johtokunta laatii ennakkoarvioesityksen pohjalta vuosittain ENISAn tulo- ja menoarvion seuraavaa varainhoitovuotta varten.

3. Johtokunta toimittaa tulo- ja menoarvion, joka on osa yhtenäisen ohjelma-asiakirjan luonnosta, vuosittain viimeistään 31 päivänä tammikuuta komissiolle ja niille kolmansille maille, joiden kanssa unioni on tehnyt sopimukset 42 artiklan 2 kohdan mukaisesti.

4. Komissio ottaa unionin talousarviota koskevaan esitykseen kyseiseen tulo- ja menoarvioon perustuvat arviot, joita se pitää henkilöstötaulukon ja unionin yleisestä talousarviosta suoritettavan rahoitusosuuden määrän osalta välttämättöminä, ja toimittaa talousarvioesityksen Euroopan parlamentille ja neuvostolle SEUT 314 artiklan mukaisesti.

5. Euroopan parlamentti ja neuvosto hyväksyvät ENISAlle annettavaa unionin rahoitusosuutta koskevat määrärahat.

6. Euroopan parlamentti ja neuvosto vahvistavat ENISAn henkilöstötaulukon.

7. Johtokunta vahvistaa ENISAn talousarvion yhdessä yhtenäisen ohjelma-asiakirjan kanssa. ENISAn talousarviosta tulee lopullinen, kun unionin yleinen talousarvio on lopullisesti vahvistettu. Johtokunta mukauttaa tarvittaessa ENISAn talousarviota ja yhtenäistä ohjelma-asiakirjaa unionin yleisen talousarvion mukaisesti.

30 artikla

ENISAn talousarvion rakenne

1. Sulkematta pois muita tulonlähteitä ENISAn tulot koostuvat seuraavista:

   a) rahoitusosuus unionin yleisestä talousarviosta;

   b) tiettyjen menoerien rahoittamiseen osoitettavat tulot sen 32 artiklassa tarkoitettujen varainhoitosääntöjen mukaisesti;

   c) unionin rahoitus, joka annetaan valtuutussopimusten tai kertaluonteisten avustusten muodossa 32 artiklassa tarkoitettujen varainhoitosääntöjen ja unionin politiikkoja tukeviin asianomaisiin välineisiin sovellettavien säännösten mukaisesti;

   d) ENISAn toimintaan 42 artiklan mukaisesti osallistuvien kolmansien maiden rahoitusosuudet;

   e) mahdolliset jäsenvaltioiden vapaaehtoiset rahoitusosuudet rahana tai luontoissuorituksina.

   Vapaaehtoisia rahoitusosuuksia ensimmäisen alakohdan e alakohdan mukaisesti suorittavat jäsenvaltiot eivät voi vaatia erityisoikeuksia tai -palveluja suorituksensa perusteella.

2. ENISAn menoihin kuuluvat henkilöstöstä, hallinnollisesta ja teknisestä tuesta, infrastruktuurista ja toiminnasta aiheutuvat menot sekä kolmansien osapuolten kanssa tehdyistä sopimuksista aiheutuvat menot.

31 artikla

Talousarvion toteuttaminen

1. Pääjohtaja vastaa ENISAn talousarvion toteuttamisesta.

2. Komission sisäinen tilintarkastaja käyttää ENISAan nähden samoja valtuuksia kuin komission yksiköihin.

3. ENISAn tilinpitäjä toimittaa alustavan tilinpäätöksen komission tilinpitäjälle ja tilintarkastustuomioistuimelle viimeistään varainhoitovuoden (vuosi N) päättymistä seuraavan varainhoitovuoden (vuosi N + 1) maaliskuun 1 päivänä.

4. Saatuaan ENISAn alustavaa tilinpäätöstä koskevat tilintarkastustuomioistuimen huomautukset Euroopan parlamentin ja neuvoston asetuksen (EU, Euratom) 2018/1046[1] 246 artiklan mukaisesti ENISAn tilinpitäjä laatii ENISAn lopullisen tilinpäätöksen omalla vastuullaan ja toimittaa sen johtokunnalle lausuntoa varten.

5. Johtokunta antaa lausunnon ENISAn lopullisesta tilinpäätöksestä.

[1] Euroopan parlamentin ja neuvoston asetus (EU, Euratom) 2018/1046, annettu 18 päivänä heinäkuuta 2018, unionin yleiseen talousarvioon sovellettavista varainhoitosäännöistä, asetusten (EU) N:o 1296/2013, (EU) N:o 1301/2013, (EU) N:o 1303/2013, (EU) N:o 1304/2013, (EU) N:o 1309/2013, (EU) N:o 1316/2013, (EU) N:o 223/2014, (EU) N:o 283/2014 ja päätöksen N:o 541/2014/EU muuttamisesta sekä asetuksen (EU, Euratom) N:o 966/2012 kumoamisesta (EUVL L 193, 30.7.2018, s. 1).

6. Pääjohtaja toimittaa selvityksen varainhoitovuoden talousarvio- ja varainhallinnosta Euroopan parlamentille, neuvostolle, komissiolle ja tilintarkastustuomioistuimelle viimeistään vuoden N + 1 maaliskuun 31 päivänä.

7. ENISAn tilinpitäjä toimittaa lopullisen tilinpäätöksen ja johtokunnan lausunnon Euroopan parlamentille, neuvostolle, komission tilinpitäjälle ja tilintarkastustuomioistuimelle viimeistään vuoden N + 1 heinäkuun 1 päivänä.

8. ENISAn tilinpitäjä toimittaa myös tilinpäätöstä koskevan vahvistuskirjeen tilintarkastustuomioistuimelle sekä jäljennöksen komission tilinpitäjälle samana päivänä kuin ENISAn lopullisen tilinpäätöksen.

9. ENISAn pääjohtaja julkistaa lopullisen tilinpäätöksen viimeistään vuoden N+1 marraskuun 15 päivänä *Euroopan unionin virallisessa lehdessä*.

10. Pääjohtaja lähettää tilintarkastustuomioistuimelle vastauksen sen huomautuksiin viimeistään vuoden N + 1 syyskuun 30 päivänä ja lähettää jäljennöksen tästä vastauksesta myös johtokunnalle ja komissiolle.

11. Pääjohtaja antaa asetuksen (EU, Euratom) 2018/1046 261 artiklan 3 kohdan mukaisesti Euroopan parlamentille tämän pyynnöstä kaikki asianomaista varainhoitovuotta koskevan vastuuvapausmenettelyn moitteettomaksi toteuttamiseksi tarvittavat tiedot.

12. Euroopan parlamentti myöntää neuvoston suosituksesta pääjohtajalle ennen vuoden N + 2 toukokuun 15 päivää vastuuvapauden vuoden N talousarvion toteuttamisen osalta.

32 artikla

Varainhoitosäännöt

Johtokunta hyväksyy ENISAan sovellettavat varainhoitoa koskevat säännöt komissiota kuultuaan. Varainhoitosäännöt voivat poiketa delegoidusta asetuksesta (EU) N:o 1271/2013 ainoastaan, jos ENISAn toiminta sitä erityisesti edellyttää ja jos komissio on antanut siihen ennalta suostumuksensa.

33 artikla

Petostentorjunta

1. Helpottaakseen Euroopan parlamentin ja neuvoston asetuksen (EU, Euratom) N:o 883/2013[1] soveltamisalaan kuuluvien petosten, lahjonnan ja muiden laittomien toimien torjuntaa ENISA liittyy viimeistään … päivänä …kuuta … [kuusi kuukautta tämän asetuksen voimaantulon jälkeen] OLAFin sisäisistä tutkimuksista 25 päivänä toukokuuta 1999 Euroopan parlamentin, Euroopan unionin neuvoston ja Euroopan yhteisöjen komission tekemään toimielinten väliseen sopimukseen[2]. ENISA antaa kaikkia sen työntekijöitä koskevat asiaan liittyvät määräykset käyttäen kyseisen sopimuksen liitteessä olevaa mallia.

2. Tilintarkastustuomioistuimella on valtuudet tehdä kaikkien ENISAlta unionin rahoitusta saaneiden avustuksensaajien, toimeksisaajien ja alihankkijoiden osalta asiakirjoihin perustuvia ja paikan päällä suoritettavia tarkastuksia.

---

[1] Euroopan parlamentin ja neuvoston asetus (EU, Euratom) N:o 883/2013, annettu 11 päivänä syyskuuta 2013, Euroopan petostentorjuntaviraston (OLAF) tutkimuksista sekä Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 1073/1999 ja neuvoston asetuksen (Euratom) N:o 1074/1999 kumoamisesta (EUVL L 248, 18.9.2013, s. 1).

[2] EYVL L 136, 31.5.1999, s. 15.

3. OLAF voi tehdä tarkastuksia, myös paikan päällä suoritettavia tarkastuksia ja todentamisia, Euroopan parlamentin ja neuvoston asetuksen (EU, Euratom) N:o 883/2013 ja neuvoston asetuksen (Euratom, EY) N:o 2185/96[1] säännösten ja niissä säädettyjen menettelyjen mukaisesti sen selvittämiseksi, onko ENISAn rahoittamaan avustukseen tai sopimukseen liittynyt unionin taloudellisia etuja vahingoittavia petoksia, lahjontaa tai muuta laitonta toimintaa.

4. ENISAn yhteistyösopimuksiin kolmansien maiden ja kansainvälisten järjestöjen kanssa, muihin sopimuksiin, avustussopimuksiin ja avustuspäätöksiin on sisällytettävä määräyksiä, joissa nimenomaisesti annetaan tilintarkastustuomioistuimelle ja OLAFille valtuudet tehdä tällaisia tarkastuksia ja tutkimuksia niiden oman toimivallan mukaisesti, sanotun kuitenkaan rajoittamatta 1, 2 ja 3 kohdan soveltamista.

V luku
Henkilöstö

34 artikla

Yleiset säännökset

ENISAn henkilöstöön sovelletaan henkilöstösääntöjä ja muuta henkilöstöä koskevia palvelussuhteen ehtoja sekä unionin toimielinten yhteisellä päätöksellä annettuja henkilöstösääntöjen ja muuta henkilöstöä koskevia palvelussuhteen ehtojen täytäntöönpanosäännöksiä.

[1] Neuvoston asetus (Euratom, EY) N:o 2185/96, annettu 11 päivänä marraskuuta 1996, komission paikan päällä suorittamista tarkastuksista ja todentamisista Euroopan yhteisöjen taloudellisiin etuihin kohdistuvien petosten ja muiden väärinkäytösten estämiseksi (EYVL L 292, 15.11.1996, s. 2).

35 artikla

Erioikeudet ja vapaudet

ENISAan ja sen henkilöstöön sovelletaan SEU- ja SEUT-sopimukseen liitettyä Euroopan unionin erioikeuksista ja vapauksista tehtyä pöytäkirjaa N:o 7.

36 artikla

Pääjohtaja

1. Pääjohtaja otetaan palvelukseen ENISAn väliaikaisena toimihenkilönä muuta henkilöstöä koskevien palvelussuhteen ehtojen 2 artiklan a alakohdan mukaisesti.

2. Johtokunta nimittää pääjohtajan ehdokaslistalta, jonka komissio esittää avoimen valintamenettelyn päätteeksi.

3. Johtokunnan puheenjohtaja tekee pääjohtajan työsopimuksen ENISAn puolesta.

4. Johtokunnan valitsema ehdokas kutsutaan ennen nimittämistä antamaan lausuma Euroopan parlamentin asiasta vastaavan valiokunnan kokouksessa ja vastaamaan Euroopan parlamentin jäsenten esittämiin kysymyksiin.

5. Pääjohtajan toimikausi on viisi vuotta. Toimikauden lopussa komissio laatii arvion pääjohtajan tehtävän hoidosta ja ENISAn tulevista tehtävistä ja haasteista.

6. Johtokunta tekee päätökset pääjohtajan nimittämisestä, toimikauden jatkamisesta tai erottamisesta 18 artiklan 2 kohdan mukaisesti.

7. Johtokunta voi komission ehdotuksesta, jossa otetaan huomioon 5 kohdassa tarkoitettu arviointi, jatkaa pääjohtajan toimikautta kerran viideksi vuodeksi.

8. Johtokunnan on ilmoitettava Euroopan parlamentille aikeestaan jatkaa pääjohtajan toimikautta. Pääjohtaja antaa toimikauden mahdollista jatkamista edeltävien kolmen kuukauden aikana pyydettäessä lausuman Euroopan parlamentin asiasta vastaavan valiokunnan kokouksessa ja vastaa Euroopan parlamentin jäsenten esittämiin kysymyksiin.

9. Pääjohtaja, jonka toimikautta on jatkettu, ei saa osallistua samaa tointa koskevaan valintamenettelyyn.

10. Pääjohtaja voidaan erottaa toimestaan ainoastaan johtokunnan päätöksellä, jonka se tekee komission ehdotuksen perusteella.

37 artikla

Kansalliset asiantuntijat ja muu henkilöstö

1. ENISA voi käyttää kansallisia asiantuntijoita tai muuta henkilöstöä, joka ei ole ENISAn palveluksessa. Näihin henkilöihin ei sovelleta henkilöstösääntöjä eikä muuta henkilöstöä koskevia palvelussuhteen ehtoja.

2. Johtokunta tekee päätöksen, jolla vahvistetaan säännöt kansallisten asiantuntijoiden tilapäisestä lähettämisestä ENISAn palvelukseen.

VI luku

ENISAn yleiset säännökset

38 artikla

ENISAn oikeudellinen asema

1. ENISA on unionin elin, ja se on oikeushenkilö.

2. ENISAlla on kussakin jäsenvaltiossa laajin kansallisen oikeuden mukainen oikeushenkilöllä oleva oikeus- ja oikeustoimikelpoisuus. Se voi erityisesti hankkia ja luovuttaa irtainta ja kiinteää omaisuutta sekä esiintyä kantajana ja vastaajana oikeudenkäynneissä.

3. ENISAa edustaa pääjohtaja.

39 artikla

ENISAn vastuu

1. Sopimukseen perustuva ENISAn vastuu määräytyy kyseessä olevaan sopimukseen sovellettavan lain mukaan.

2. Euroopan unionin tuomioistuimella on ENISAn tekemässä sopimuksessa olevaan välityslausekkeeseen perustuva tuomiovalta.

3. Sopimussuhteen ulkopuolisen vastuun osalta ENISAn on korvattava ENISAn tai sen henkilöstön tehtäviään suorittaessaan aiheuttamat vahingot jäsenvaltioiden lainsäädännön yhteisten yleisten periaatteiden mukaisesti.

4. Euroopan unionin tuomioistuimella on tuomiovalta 3 kohdassa tarkoitettujen vahinkojen korvaamista koskevissa riidoissa.

5. ENISAn henkilöstön henkilökohtaista vastuuta ENISAa kohtaan säännellään sen henkilöstöön sovellettavissa asiaa koskevissa määräyksissä.

40 artikla

Kielijärjestelyt

1. ENISAan sovelletaan neuvoston asetusta N:o 1[1]. Jäsenvaltiot ja niiden nimeämät muut elimet voivat kääntyä ENISAn puoleen ja saada siltä vastauksen valitsemallaan unionin toimielinten virallisella kielellä.

2. Euroopan unionin elinten käännöskeskus huolehtii ENISAn toiminnan edellyttämistä käännöspalveluista.

41 artikla

Henkilötietojen suoja

1. ENISAssa tapahtuvaan henkilötietojen käsittelyyn sovelletaan Euroopan parlamentin ja neuvoston asetusta (EU) 2018/1725.

2. Johtokunta hyväksyy asetuksen (EU) 2018/1725 45 artiklan 3 kohdassa tarkoitetut soveltamissäännöt. Johtokunta voi hyväksyä lisätoimenpiteitä, jotka ovat tarpeen ENISAn soveltaessa asetusta (EU) 2018/1725.

[1] Neuvoston asetus N:o 1 Euroopan talousyhteisössä käytettäviä kieliä koskevista järjestelyistä (EYVL 17, 6.10.1958, s. 385).

42 artikla

Yhteistyö kolmansien maiden ja kansainvälisten järjestöjen kanssa

1. Siinä määrin kuin on tarpeen tämän asetuksen tavoitteiden saavuttamiseksi ENISA voi tehdä yhteistyötä kolmansien maiden toimivaltaisten viranomaisten ja/tai kansainvälisten järjestöjen kanssa. ENISA voi tätä varten vahvistaa työjärjestelyt näiden kolmansien maiden viranomaisten ja kansainvälisten järjestöjen kanssa, edellyttäen että komissio antaa tähän ennakkohyväksynnän. Näistä työjärjestelyistä ei seuraa oikeudellisia velvoitteita unionille ja sen jäsenvaltioille.

2. ENISAn toimintaan voivat osallistua kolmannet maat, jotka ovat tehneet tästä sopimuksen unionin kanssa. Mainittujen sopimusten määräysten mukaisesti laaditaan järjestelyjä, joissa määritellään kyseisten maiden osalta erityisesti ENISAn toimintaan osallistumisen luonne, laajuus ja tapa, mukaan lukien ENISAn tekemiin aloitteisiin osallistumista, rahoitusosuuksia ja henkilöstöä koskevat säännöt. Henkilöstöasioiden osalta näiden työjärjestelyjen on kaikilta osin oltava henkilöstösääntöjen ja muuta henkilöstöä koskevien palvelussuhteen ehtojen mukaiset.

3. Johtokunta hyväksyy strategian, joka koskee ENISAn suhteita kolmansiin maihin tai kansainvälisiin järjestöihin asioissa, joissa ENISA on toimivaltainen. Komissio varmistaa, että ENISA toimii toimeksiantonsa ja olemassa olevien institutionaalisten puitteiden mukaisesti sopimalla asianmukaisesta työjärjestelystä pääjohtajan kanssa.

43 artikla

Arkaluonteisten turvallisuusluokittelemattomien tietojen ja turvallisuusluokiteltujen tietojen suojaamista koskevat turvallisuussäännöt

ENISA hyväksyy komissiota kuultuaan turvallisuussäännöt, joissa sovelletaan turvallisuutta koskevia periaatteita, jotka sisältyvät päätöksissä (EU, Euratom) 2015/443 ja 2015/444 vahvistettuihin arkaluonteisten turvallisuusluokittelemattomien tietojen ja Euroopan unionin turvallisuusluokiteltujen tietojen suojaamista koskeviin komission turvallisuussäännöksiin. ENISAn turvallisuussääntöihin sisältyy myös määräyksiä, jotka koskevat tällaisten tietojen vaihtamista, käsittelyä ja tallentamista.

44 artikla

Toimipaikkaa koskeva sopimus ja toimintaedellytykset

1. Isäntäjäsenvaltion ENISAlle tarjoamia tiloja ja palveluja koskevat järjestelyt sekä ENISAn pääjohtajaan, johtokunnan jäseniin, ENISAn henkilöstöön ja heidän perheenjäseniinsä isäntäjäsenvaltiossa sovellettavat erityissäännöt vahvistetaan ENISAn ja isäntäjäsenvaltion välisessä toimipaikkaa koskevassa sopimuksessa, joka tehdään sen jälkeen kun johtokunta on sen hyväksynyt.

2. ENISAn isäntäjäsenvaltion on tarjottava parhaat mahdolliset edellytykset ENISAn moitteettoman toiminnan varmistamiseksi, mukaan lukien toimivat liikenneyhteydet sijaintipaikalle, henkilöstön jäsenten lapsille soveltuvat koulunkäyntimahdollisuudet, puolisoiden mahdollisuudet päästä työmarkkinoille sekä riittävä sosiaaliturvan ja terveydenhuoltopalvelujen saatavuus henkilöstön jäsenten lapsille ja puolisoille.

45 artikla

Hallinnollinen valvonta

Euroopan oikeusasiamies valvoo ENISAn toimintaa SEUT 228 artiklan mukaisesti.

III OSASTO

KYBERTURVALLISUUDEN SERTIFIOINTIKEHYS

46 artikla

Eurooppalainen kyberturvallisuuden sertifiointikehys

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

2. Eurooppalaisessa kyberturvallisuuden sertifiointikehyksessä vahvistetaan mekanismi, jonka avulla laaditaan eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä ja annetaan vahvistus siitä, että tällaisten järjestelmien mukaisesti arvioidut tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit ovat niille määritettyjen turvallisuusvaatimusten mukaisia, jotta voidaan suojella tallennettavien, siirrettävien tai käsiteltävien tietojen tai kyseisissä tuotteissa, palveluissa ja prosesseissa tarjottavien tai välitettävien toimintojen tai palvelujen käytettävyyttä, aitoutta, eheyttä ja luottamuksellisuutta niiden koko elinkaaren ajan.

47 artikla

Eurooppalaista kyberturvallisuussertifiointia koskeva unionin jatkuva työohjelma

1. Komissio julkaisee eurooppalaista kyberturvallisuussertifiointia koskevan unionin jatkuvan työohjelman, jäljempänä 'unionin jatkuva työohjelma', jossa määritellään tulevien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien strategiset prioriteetit.

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

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

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

b) asiaa koskevat unionin tai jäsenvaltion politiikat tai lainsäädäntö;

c) markkinoiden kysyntä;

d) kyberuhkaympäristön kehitys;

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

4. Komissio ottaa asianmukaisesti huomioon Euroopan kyberturvallisuuden sertifiointiryhmän ja sidosryhmien sertifiointiryhmän toimittamat lausunnot luonnoksesta unionin jatkuvaksi työohjelmaksi.

5. Ensimmäinen unionin jatkuva työohjelma julkaistaan viimeistään … päivänä …kuuta … [kahdentoista kuukauden kuluttua tämän asetuksen voimaantulosta]. Unionin jatkuvaa työohjelmaa päivitetään ainakin kerran kolmessa vuodessa, ja tarvittaessa useammin.

48 artikla

Eurooppalaista kyberturvallisuuden sertifiointijärjestelmää koskeva pyyntö

1. Komissio voi unionin jatkuvan työohjelman pohjalta pyytää ENISAa valmistelemaan ehdolla olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän tai tarkistamaan voimassa olevaa eurooppalaista kyberturvallisuuden sertifiointijärjestelmää.

2. Asianmukaisesti perustelluissa tapauksissa komissio tai Euroopan kyberturvallisuuden sertifiointiryhmä voi pyytää ENISAa valmistelemaan ehdolla olevan järjestelmän tai tarkistamaan voimassa olevaa eurooppalaista kyberturvallisuuden sertifiointijärjestelmää, joka ei kuulu unionin jatkuvaan työohjelmaan. Unionin jatkuvaa työohjelmaa päivitetään tämän mukaisesti.

49 artikla

Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien valmistelu, hyväksyminen ja tarkistaminen

1. Kun komissio on esittänyt 48 artiklan mukaisen pyynnön, ENISAn on valmisteltava ehdolla oleva järjestelmä, joka täyttää 51, 52 ja 54 artiklassa esitetyt vaatimukset.

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

3. Valmistellessaan ehdolla olevia järjestelmiä ENISAn on kuultava kaikkia asiaankuuluvia sidosryhmiä virallisesti, avoimesti ja osallistavasti.

4. ENISAn on perustettava jokaista ehdolla olevaa järjestelmää varten 20 artiklan 4 kohdan mukaisesti tilapäinen työryhmä, jonka tarkoituksena on antaa ENISAlle erityistä neuvontaa ja asiantuntemusta

5. ENISAn on tehtävä tiivistä yhteistyötä Euroopan kyberturvallisuuden sertifiointiryhmän kanssa. Euroopan kyberturvallisuuden sertifiointiryhmän on annettava ENISAlle ehdolla olevan järjestelmän valmisteluun liittyvää apua ja asiantuntijaneuvontaa ja annettava ehdolla olevasta järjestelmästä lausunto.

6. ENISAn on otettava mahdollisimman tarkasti huomioon Euroopan kyberturvallisuuden sertifiointiryhmän lausunto, ennen kuin se toimittaa 3, 4 ja 5 kohdan mukaisesti valmistellun ehdolla olevan järjestelmän komissiolle. Euroopan kyberturvallisuuden sertifiointiryhmän lausunto ei ole sitova, eikä sen puuttuminen estä ENISAa toimittamasta ehdolla olevaa järjestelmää komissiolle.

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

8. ENISAn on vähintään joka viides vuosi arvioitava hyväksytyt eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät ja otettava tässä huomioon asianomaisten osapuolten palaute. Komissio tai Euroopan kyberturvallisuuden sertifiointiryhmä voi tarvittaessa pyytää ENISAa aloittamaan tarkistetun ehdolla olevan järjestelmän kehittämisen 48 artiklan ja tämän artiklan mukaisesti.

50 artikla

Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien verkkosivusto

1. ENISA ylläpitää erityistä verkkosivustoa, jolla annetaan tietoa eurooppalaisista kyberturvallisuuden sertifiointijärjestelmistä, eurooppalaisista kyberturvallisuussertifikaateista ja EU-vaatimustenmukaisuusilmoituksista, mukaan lukien tietoa eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien, jotka eivät ole enää voimassa, ja peruutettujen ja vanhentuneiden eurooppalaisten kyberturvallisuussertifikaattien ja EU-vaatimustenmukaisuusilmoitusten sekä sellaisten linkkikokoelmien osalta, jotka osoittavat 55 artiklan mukaisiin kyberturvallisuustietoihin, ja jolla niitä julkistetaan.

2. Edellä 1 kohdassa tarkoitetulla verkkosivustolla on tarvittaessa myös ilmoitettava ne kansalliset kyberturvallisuuden sertifiointijärjestelmät, jotka on korvattu eurooppalaisella kyberturvallisuuden sertifiointijärjestelmällä.

51 artikla

Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien turvallisuustavoitteet

Eurooppalainen kyberturvallisuuden sertifiointijärjestelmä olisi suunniteltava täyttämään soveltuvin osin vähintään seuraavat turvallisuustavoitteet:

a) tallennetut, siirretyt tai muulla tavoin käsitellyt tiedot suojataan vahingossa tapahtuvalta tai luvattomalta tallentamiselta, käsittelyltä, käytöltä tai luovuttamiselta tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin koko elinkaaren ajan;

b) tallennetut, siirretyt tai muulla tavoin käsitellyt tiedot suojataan vahingossa tapahtuvalta tai luvattomalta tuhoamiselta, katoamiselta tai muuttamiselta taikka puutteelliselta saatavuudelta tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin koko elinkaaren ajan;

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

d) tunnistetaan ja dokumentoidaan kaikki tunnetut riippuvuudet ja haavoittuvuudet;

e) järjestelmään tallentuu tieto siitä, mitä tietoja, palveluja tai toimintoja on käytetty, hyödynnetty tai muutoin käsitelty, sekä näiden toimien ajankohta ja tekijä;

f) on mahdollista tarkastaa, mitä tietoja, palveluja tai toimintoja on käytetty, hyödynnetty tai muutoin käsitelty, sekä näiden toimien ajankohta ja tekijä;

g) tarkistetaan, että tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit eivät sisällä tunnettuja haavoittuvuuksia;

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

i) tarkistetaan, että tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien suojaus on oletusarvoista ja sisäänrakennettua;

j) tieto- ja viestintätekniikan tuotteisiin, palveluihin ja prosesseihin sisältyy ajantasainen ohjelmisto ja laitteisto, jotka eivät sisällä julkisesti tiedossa olevia haavoittuvuuksia, ja mekanismit, joilla varmistetaan turvalliset päivitykset.

52 artikla

Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien varmuustasot

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

2. Eurooppalaisissa kyberturvallisuussertifikaateissa ja EU-vaatimustenmukaisuusilmoituksissa on viitattava varmuustasoon, joka määritetään siinä eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä, jonka nojalla kyseinen eurooppalainen kyberturvallisuussertifikaatti tai EU-vaatimustenmukaisuusilmoitus on annettu.

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

4. Sertifikaatissa tai EU-vaatimustenmukaisuusilmoituksessa viitataan siihen liittyviin teknisiin eritelmiin, standardeihin ja menettelyihin sekä teknisiin tarkastuksiin, joiden tarkoituksena on vähentää kyberturvallisuuspoikkeamien riskiä tai ehkäistä niitä.

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

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

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

8. Eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan määritellä useita arviointitasoja käytettävien arviointimenetelmien tiukkuuden ja kattavuuden mukaan. Kunkin arviointitason on vastattava yhtä varmuustasoa, ja arviointitasot on määriteltävä varmuuden osatekijöiden asianmukaisen yhdistelmän perusteella.

53 artikla

Vaatimustenmukaisuuden itsearviointi

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

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

3. Tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien valmistaja tai tarjoaja asettavat EU-vaatimustenmukaisuusilmoituksen, tekniset asiakirjat ja kaikki muut järjestelmässä määriteltyä tieto- ja viestintätekniikan tuotteiden ja palvelujen vaatimustenmukaisuutta koskevat asiaankuuluvat tiedot 58 artiklan 1 kohdassa tarkoitetun kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen saataville asiaankuuluvassa eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä määrätyn ajanjakson ajaksi. Jäljennös EU-vaatimustenmukaisuusilmoituksesta toimitetaan kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle ja ENISAlle.

4. EU-vaatimustenmukaisuusilmoituksen antaminen on vapaaehtoista, ellei unionin lainsäädännössä tai jäsenvaltioiden lainsäädännössä toisin säädetä.

5. EU-vaatimustenmukaisuusilmoitukset on tunnustettava kaikissa jäsenvaltioissa.

54 artikla

Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien osatekijät

1. Eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän on sisällettävä ainakin seuraavat osatekijät:

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

   b) selkeä kuvaus järjestelmän tarkoituksesta sekä siitä, miten valitut standardit, arviointimenetelmät ja varmuustasot vastaavat järjestelmän aiottujen käyttäjien tarpeisiin;

   c) viittaukset kansainvälisiin, eurooppalaisiin tai kansallisiin standardeihin, joita arvioinnissa on sovellettu, tai jos asianmukaisia standardeja ei ole saatavilla, teknisiin eritelmiin, jotka täyttävät asetuksen(EU) N:o 1025/2012 liitteessä II esitetyt vaatimukset, tai jos tällaisia eritelmiä ei ole saatavilla, viitataan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmässä määriteltyihin n teknisiin eritelmiin tai muihin kyberturvallisuusvaatimuksiin;

d) soveltuvin osin yksi tai useampi varmuustaso;

e) tieto siitä, sallitaanko järjestelmässä vaatimustenmukaisuuden itsearviointi;

f) soveltuvin osin erityiset vaatimukset tai lisävaatimukset, joita vaatimustenmukaisuuden arviointilaitoksiin sovelletaan, jotta varmistutaan siitä, että nämä ovat teknisesti päteviä arvioimaan kyberturvallisuusvaatimukset;

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

h) soveltuvin osin sertifioinnin edellyttämät tiedot, jotka hakijan on toimitettava vaatimustenmukaisuuden arviointilaitoksille tai jotka on muutoin asetettava näiden saataville;

i) jos järjestelmä tarjoaa käyttöön merkkejä tai merkintöjä, näiden merkkien tai merkintöjen käytön edellytykset;

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

k) soveltuvin osin ehdot eurooppalaisen kyberturvallisuussertifikaatin antamiselle, voimassa pitämiselle, jatkamiselle ja uusimiselle sekä sertifioinnin soveltamisalan laajentamiselle tai supistamiselle;

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

m) säännöt siitä, miten aiemmin tuntemattomat tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien kyberhaavoittuvuudet on määrä raportoida ja käsitellä;

n) tapauksen mukaan säännöt tietojen säilyttämisestä vaatimustenmukaisuuden arviointilaitoksissa;

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

p) myönnettävien eurooppalaisten kyberturvallisuussertifikaattien ja EU-vaatimustenmukaisuusilmoitusten sisältö ja muoto;

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

r) järjestelmän mukaisesti myönnettyjen Eurooppalaisten kyberturvallisuussertifikaattien enimmäisvoimassaoloaika;

s) järjestelmien mukaisesti myönnettyjä, muutettuja ja peruutettuja eurooppalaisia kyberturvallisuussertifikaatteja koskeva julkistamispolitiikka;

t) kolmansien maiden kanssa suoritettavan sertifiointijärjestelmien vastavuoroisen tunnustamisen edellytykset;

u) soveltuvin osin sellaista vertaisarviointimekanismia koskevat säännöt, joka on perustettu varmuustason "korkea" eurooppalaisia kyberturvallisuussertifikaatteja 56 artiklan 6 kohdan nojalla myöntäviä viranomaisia tai elimiä koskevan järjestelmän mukaisesti. Tämä mekanismi ei vaikuta vertaisarviointiin, josta säädetään 59 artiklassa;

v) muoto ja menettelyt, joita tieto- ja viestintätekniikan tuotteiden, palveluiden ja prosessien valmistajien ja tarjoajien on noudatettava, kun ne toimittavat ja päivittävät täydentäviä kyberturvallisuustietoja 55 artiklan mukaisesti;

2. Eurooppalaisen kyberturvallisuussertifioinnin sertifiointijärjestelmälle määritellyt vaatimukset eivät saa olla ristiriidassa sovellettavien oikeudellisten vaatimusten, erityisesti yhdenmukaistetusta unionin lainsäädännöstä johtuvien vaatimusten kanssa.

3. Jos unionin säädöksessä niin säädetään, eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaista sertifiointia tai annettua EU-vaatimustenmukaisuusilmoitusta voidaan käyttää osoittamaan, että kyseisen säädöksen vaatimusten suhteen vallitsee vaatimustenmukaisuusolettama.

4. Jos yhdenmukaistettua unionin lainsäädäntöä ei ole, myös jäsenvaltioiden lainsäädännössä voidaan säätää, että eurooppalaista kyberturvallisuuden sertifiointijärjestelmää voidaan käyttää luomaan vaatimustenmukaisuusolettama oikeudellisiin vaatimuksiin nähden.

55 artikla

Sertifioituja tieto- ja viestintätekniikan tuotteita, palveluja ja prosesseja koskevat täydentävät kyberturvallisuustiedot

1. Tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien, jotka on sertifioitu tai joista on annettu EU-vaatimustenmukaisuusilmoitus, valmistajan tai tarjoajan on asetettava julkisesti saataville seuraavat täydentävät tiedot:

   a) ohjeita ja suosituksia, jotka auttavat loppukäyttäjiä määrittämään, asentamaan, ottamaan käyttöön, käyttämään ja ylläpitämään tieto- ja viestintätekniikan tuotteita tai palveluja turvallisesti;

   b) loppukäyttäjille tarjottavan turvallisuustuen kesto, erityisesti kyberturvallisuutta koskevien päivitysten saatavuuden osalta;

   c) valmistajan tai tarjoajan yhteystiedot ja hyväksytyt tavat, joilla loppukäyttäjät ja tietoturvatutkijat voivat toimittaa tietoa haavoittuvuuksista;

d) viittaus verkkotietolähteisiin, joissa on luettelo tieto- ja viestintätekniikan tuotteeseen, palveluun tai prosessiin liittyvistä julkisesti tiedossa olevista haavoittuvuuksista ja niihin liittyvää kyberturvallisuusneuvontaa.

2. Edellä 1 kohdassa tarkoitetut tiedot on annettava sähköisessä muodossa, ja ne on pidettävä saatavilla ja tarpeen mukaan ajan tasalla vähintään vastaavan eurooppalaisen kyberturvallisuussertifikaatin tai EU-vaatimustenmukaisuusilmoituksen voimassaolon päättymiseen asti.

56 artikla

Kyberturvallisuussertifiointi

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

2. Kyberturvallisuussertifiointi on vapaaehtoista, jollei unionin lainsäädännössä tai jäsenvaltioiden lainsäädännössä toisin säädetä.

3. Komissio arvioi säännöllisesti hyväksyttyjen eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien tehokkuutta ja käyttöastetta sekä sitä, pitäisikö tietystä eurooppalaisesta kyberturvallisuuden sertifiointijärjestelmästä tehdä pakollinen asiaankuuluvan unionin lainsäädännön avulla, jotta varmistetaan, että tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien kyberturvallisuus on unionissa riittävällä tasolla, ja parannetaan sisämarkkinoiden toimintaa. Ensimmäinen tällainen arviointi on suoritettava viimeistään 31 päivänä joulukuuta 2023 ja sen jälkeen arvioinnit on suoritettava vähintään kahden vuoden välein.

Komissio määrittää kyseisten arvioinnin tulosten perusteella sellaiset voimassa olevan sertifiointijärjestelmän soveltamisalaan kuuluvat tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit, joiden olisi kuuluttava pakollisen sertifiointijärjestelmän soveltamisalaan.

Komissio keskittyy ensisijaisesti direktiivin (EU) 2016/1148 liitteessä II lueteltuihin aloihin, jotka arvioidaan viimeistään kahden vuoden kuluttua ensimmäisen eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän hyväksymisestä.

Arviointia valmistellessaan komissio

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

b) ottaa huomioon asiaankuuluvan jäsenvaltion lainsäädännön ja kolmannen maan lainsäädännön olemassaolon ja täytäntöönpanon;

c) kuulee kaikkia asiaankuuluvia sidosryhmiä ja jäsenvaltioita virallisesti, avoimesti ja osallistavasti;

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

e) ehdottaa nopeinta ja tehokkainta tapaa, jolla siirtyminen vapaaehtoisista pakollisiin sertifiointijärjestelmiin toteutetaan.

4. Tämän artiklan mukaisen, varmuustasoon "perustaso" tai "korotettu" viittaavan eurooppalaisen kyberturvallisuussertifikaatin myöntävät 60 artiklassa tarkoitetut vaatimustenmukaisuuden arviointilaitokset perustuen kriteereihin, jotka sisältyvät komission 49 artiklan mukaisesti hyväksymään eurooppalaiseen kyberturvallisuuden sertifiointijärjestelmään.

5. Poiketen siitä, mitä 4 kohdassa säädetään, asianmukaisesti perustelluissa tapauksissa yksittäisessä eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan määrätä, että järjestelmästä saatavan eurooppalaisen kyberturvallisuussertifikaatin myöntää vain julkinen elin. Tämän elimen on oltava joko

a) 58 artiklan 1 kohdassa tarkoitettu kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen; tai

b) 60 artiklan 1 kohdan nojalla vaatimustenmukaisuuden arviointilaitoksena akkreditoitu julkinen elin.

6. Jos 49 artiklan mukaisesti vahvistettu eurooppalainen kyberturvallisuuden sertifiointijärjestelmä edellyttää korkeaa varmuustasoa, eurooppalaisen kyberturvallisuussertifikaatin myöntää vain kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen tai seuraavissa tapauksissa vaatimustenmukaisuuden arviointilaitos:

a) kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen hyväksyy ennalta kunkin yksittäisen, vaatimustenmukaisuuden arviointilaitoksen myöntämän eurooppalaisen kyberturvallisuussertifikaatin; tai

b) kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen delegoi tämän eurooppalaisten kyberturvallisuussertifikaattien myöntämistä koskevan tehtävän ennalta yleisesti vaatimustenmukaisuuden arviointilaitokselle.

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

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

9. Eurooppalainen kyberturvallisuussertifikaatti myönnetään eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä määritellyksi ajaksi, ja se voidaan uusia, jos sovellettavat vaatimukset täyttyvät edelleen.

10. Tämän artiklan mukaisesti myönnetty eurooppalainen kyberturvallisuussertifikaatti on tunnustettava kaikissa jäsenvaltioissa.

57 artikla

Kansalliset kyberturvallisuuden sertifiointijärjestelmät ja sertifikaatit

1. Sellaisia tieto- ja viestintätekniikan tuotteita, palveluja ja prosesseja 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 varten voimassa olevat kansalliset kyberturvallisuuden sertifiointijärjestelmät ja niihin liittyvät menettelyt, jotka eivät kuulu jonkin eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan, pysyvät edelleen voimassa.

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

3. Kansallisissa kyberturvallisuuden sertifiointijärjestelmissä myönnetyt, eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän kattamat voimassa olevat sertifikaatit pysyvät voimassa niiden voimassaolon päättymispäivään asti.

4. Jäsenvaltioiden on ilmoitettava komissiolle ja Euroopan kyberturvallisuuden sertifiointiryhmälle kaikista aikeista laatia uusia kansallisia kyberturvallisuuden sertifiointijärjestelmiä, jotta voitaisiin välttää hajanaisuus sisämarkkinoilla.

58 artikla

Kansalliset kyberturvallisuussertifioinnin myöntävät viranomaiset

1. Kunkin jäsenvaltion on nimettävä yksi tai useampi kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen alueelleen tai sopimuksella toisen jäsenvaltion kanssa nimettävä yksi tai useampi tähän toiseen jäsenvaltioon sijoittautunut kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen vastaamaan valvontatehtävistä tämän nimeävän jäsenvaltion alueella.

2. Kunkin jäsenvaltion on ilmoitettava komissiolle nimeämänsä kansalliset kyberturvallisuussertifioinnin myöntävät viranomaiset. Jos jäsenvaltio nimeää useamman kuin yhden viranomaisen, sen on myös ilmoitettava komissiolle kyseisille viranomaisille osoitetut tehtävät.

3. Rajoittamatta 56 artiklan 5 kohdan a alakohdan ja 56 artiklan 6 kohdan soveltamista kunkin kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on organisaatioltaan, rahoituspäätöksiltään, oikeudelliselta rakenteeltaan ja päätöksenteoltaan oltava riippumaton yksiköistä, joita se valvoo.

4. Jäsenvaltioiden on varmistettava, että kansallisen kyberturvallisuussertifioinnin myöntävät viranomaisten toiminta, joka liittyy 56 artiklan 5 kohdan a alakohdan ja 56 artiklan 6 kohdan mukaiseen eurooppalaisten kyberturvallisuussertifikaattien myöntämiseen, on tiukasti erotettu tämän artiklan mukaisesta valvontatoiminnasta ja että nämä toiminnot suoritetaan toisistaan riippumattomasti.

5. Jäsenvaltioiden on varmistettava, että kansallisilla kyberturvallisuussertifioinnin myöntävillä viranomaisilla on riittävät resurssit käyttää valtuuksiaan ja suorittaa tuloksekkaasti ja tehokkaasti niille osoitetut tehtävät.

6. Tämän asetuksen tehokkaan täytäntöönpanon varmistamiseksi on aiheellista, että kansalliset kyberturvallisuussertifiointiviranomaiset osallistuvat Euroopan kyberturvallisuuden sertifiointiryhmään aktiivisella, tehokkaalla ja turvallisella tavalla.

7. Kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten on

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

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

c) aktiivisesti avustettava ja tuettava kansallisia akkreditointielimiä näiden seuratessa ja valvoessa vaatimustenmukaisuuden arviointilaitosten toimintaa tämän asetuksen soveltamiseksi, sanotun kuitenkaan rajoittamatta 60 artiklan 3 kohdan soveltamista;

d) seurattava ja valvottava 56 artiklan 5 kohdassa tarkoitettujen julkisten elinten toimintaa;

e) myönnettävä soveltuvin osin valtuudet vaatimustenmukaisuuden arviointilaitoksille 60 artiklan 3 kohdan mukaisesti ja rajoitettava myönnettyjä valtuutuksia taikka keskeytettävä tai peruutettava ne, jos vaatimustenmukaisuuden arviointilaitokset eivät noudata tämän asetuksen vaatimuksia;

f) käsiteltävä luonnollisten henkilöiden tai oikeushenkilöiden tekemät valitukset, jotka liittyvät kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten tai vaatimustenmukaisuuden arviointilaitosten 56 artiklan 6 kohdan mukaisesti myöntämiin eurooppalaisiin kyberturvallisuussertifikaatteihin tai 53 artiklan mukaisesti annettuihin EU-vaatimustenmukaisuusilmoituksiin, tutkittava asianmukaisessa määrin valituksen kohde ja ilmoitettava valituksen tekijälle tutkinnan etenemisestä ja tuloksesta kohtuullisessa ajassa;

g) toimitettava ENISAlle ja Euroopan kyberturvallisuuden sertifiointiryhmälle vuosittainen yhteenveto tämän kohdan b, c ja d alakohtien tai 8 kohdan nojalla toteutetuista toimista;

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

i) seurattava asiaa koskevaa kehitystä kyberturvallisuussertifioinnin alalla.

8. Kullakin kansallisella kyberturvallisuussertifioinnin myöntävällä viranomaisella on oltava ainakin valtuudet

a) pyytää vaatimustenmukaisuuden arviointilaitoksilta, eurooppalaisen kyberturvallisuussertifikaatin haltijoilta ja EU-vaatimustenmukaisuusilmoituksen antajilta kaikki tiedot, jotka se tarvitsee tehtävänsä suorittamiseksi;

b) tehdä tarkastusten avulla tutkimuksia vaatimustenmukaisuuden arviointilaitoksista, eurooppalaisen kyberturvallisuussertifikaatin haltijoista ja EU-vaatimustenmukaisuusilmoituksen antajista sen tarkastamiseksi, että ne noudattavat tämän osaston säännöksiä;

c) toteuttaa asianmukaisia toimenpiteitä kansallisen lainsäädännön mukaisesti varmistaakseen, että vaatimustenmukaisuuden arviointilaitokset, eurooppalaisen kyberturvallisuussertifikaatin haltijat ja EU-vaatimustenmukaisuusilmoitusten antajat noudattavat tämän asetuksen tai eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimuksia;

d) päästä vaatimustenmukaisuuden arviointilaitosten ja eurooppalaisen kyberturvallisuussertifikaatin haltijoiden tiloihin tutkimusten tekemiseksi unionin tai jäsenvaltion prosessioikeuden mukaisesti;

e) peruuttaa kansallisen lainsäädännön mukaisesti kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen tai 56 artiklan 6 kohdan mukaisesti vaatimustenmukaisuuden arviointilaitosten myöntämät eurooppalaiset kyberturvallisuussertifikaatit, jos ne eivät täytä tämän asetuksen tai eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimuksia;

f) määrätä seuraamuksia kansallisen lainsäädännön mukaisesti 65 artiklassa säädetyllä tavalla ja vaatia lopettamaan tässä asetuksessa säädettyjen velvoitteiden rikkominen välittömästi.

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 kyberturvallisuussertifioinnista ja niiden kyberturvallisuuteen liittyvistä teknisistä kysymyksistä.

59 artikla

Vertaisarviointi

1. Kansallisille kyberturvallisuussertifioinnin myöntäville viranomaisille on tehtävä vertaisarviointeja, jotta koko unionissa saadaan käyttöön toisiaan vastaavat standardit, jotka koskevat myönnettyjä eurooppalaisia kyberturvallisuussertifikaatteja ja EU-vaatimustenmukaisuusilmoituksia.

2. Vertaisarvioinnissa on käytettävä luotettavia ja avoimia arviointiperusteita ja -menettelyjä, erityisesti kun on kyse rakenteita, henkilöresursseja ja prosesseja koskevista vaatimuksista, luottamuksellisuudesta ja valituksista.

3. Vertaisarvioinnissa on arvioitava

   a) soveltuvin osin se, onko kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen toiminnot, jotka liittyvät 56 artiklan 5 kohdan a alakohdan ja 56 artiklan 6 kohdan mukaiseen eurooppalaisten kyberturvallisuussertifikaattien myöntämiseen, erotettu tiukasti 58 artiklan mukaisesta valvontatoiminnasta ja suoritetaanko molemmat toiminnot toisistaan riippumattomasti;

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

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

d) menettelyt, joilla seurataan, valtuutetaan ja valvotaan vaatimustenmukaisuuden arviointilaitosten toimintaa;

e) soveltuvin osin se, onko korkean varmuustason eurooppalaisia kyberturvallisuussertifikaatteja 56 artiklan 6 kohdan nojalla myöntävien viranomaisten tai elinten henkilökunnalla tarvittava asiantuntemus.

4. Vertaisarvioinnin tekevät vähintään kaksi muiden jäsenvaltioiden kansallista kyberturvallisuussertifioinnin myöntävää viranomaista ja komissio, ja se tehdään vähintään kerran viidessä vuodessa. ENISA voi osallistua vertaisarviointiin.

5. Komissio voi antaa täytäntöönpanosäädöksiä, joilla vahvistetaan vähintään viideksi vuodeksi vertaisarviointeja varten suunnitelma, jossa esitetään perusteet vertaisarviointiryhmän kokoonpanolle, vertaisarvioinnissa käytetyt menetelmät, aikataulu, arviointien suoritustiheys ja muut vertaisarviointiin liittyvät tehtävät. Tällaisia täytäntöönpanosäädöksiä antaessaan komissio ottaa asianmukaisesti huomioon Euroopan kyberturvallisuuden sertifiointiryhmän näkemykset. Nämä täytäntöönpanosäädökset hyväksytään 66 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

6. Euroopan kyberturvallisuuden sertifiointiryhmän on tarkasteltava vertaisarvioinnin tuloksia ja laadittava yhteenvetoja, jotka voidaan asettaa julkisesti saataville, sekä tarvittaessa annettava ohjeistusta tai suosituksia, jotka koskevat asianomaisten yksiköiden toteuttamia toimia tai toimenpiteitä.

60 artikla

Vaatimustenmukaisuuden arviointilaitokset

1. Asetuksen (EY) N:o 765/2008 mukaisesti nimettyjen kansallisten akkreditointielinten on akkreditoitava vaatimustenmukaisuuden arviointilaitokset. Tällainen akkreditointi annetaan vain, jos vaatimustenmukaisuuden arviointilaitos täyttää tämän asetuksen liitteessä esitetyt vaatimukset.

2. Jos kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen antaa eurooppalaisen kyberturvallisuussertifikaatin 56 artiklan 5 kohdan a alakohdan ja 56 artiklan 6 kohdan nojalla, kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen sertifiointielin akkreditoidaan tämän artiklan 1 kohdan nojalla vaatimustenmukaisuuden arviointilaitokseksi.

3. Jos eurooppalaisissa kyberturvallisuuden sertifiointijärjestelmissä vahvistetaan 54 artiklan 1 kohdan f alakohdan mukaisia erityisiä vaatimuksia tai lisävaatimuksia, kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen valtuuttaa ainoastaan sellaiset vaatimustenmukaisuuden arviointilaitokset, jotka täyttävät nämä vaatimukset.

4. Edellä 1 kohdassa tarkoitettu akkreditointi myönnetään enintään viideksi vuodeksi, ja se voidaan uusia samoin edellytyksin, jos vaatimustenmukaisuuden arviointilaitos edelleen täyttää tässä artiklassa säädetyt vaatimukset. Kansallisten akkreditointielinten on kaikin asianmukaisin toimin kohtuullisessa ajassa rajoitettava 1 kohdan nojalla myönnettyä vaatimustenmukaisuuden arviointilaitoksen akkreditointia taikka keskeytettävä tai peruttava se, jos akkreditoinnin edellytykset eivät täyty tai eivät enää täyty tai jos vaatimustenmukaisuuden arviointilaitoksen toiminta rikkoo tämän asetuksen säännöksiä.

61 artikla

Ilmoittaminen

1. Kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten on jokaisen eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän osalta ilmoitettava komissiolle vaatimustenmukaisuuden arviointilaitoksista, jotka on akkreditoitu ja soveltuvin osin 60 artiklan 3 kohdan nojalla valtuutettu myöntämään eurooppalaisia kyberturvallisuussertifikaatteja 52 artiklassa tarkoitetuilla määritellyillä varmuustasoilla. Kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten on ilman aiheetonta viivytystä ilmoitettava komissiolle kaikista niiden myöhemmistä muutoksista.

2. Vuoden kuluttua eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän voimaantulosta komissio julkaisee luettelon sertifiointijärjestelmän mukaisesti ilmoitetuista vaatimustenmukaisuuden arviointilaitoksista *Euroopan unionin virallisessa lehdessä*.

3. Jos komissio saa ilmoituksen 2 kohdassa tarkoitetun ajanjakson päättymisen jälkeen, se julkaisee *Euroopan unionin virallisessa lehdessä* muutokset ilmoitettuja vaatimustenmukaisuuden arviointilaitoksia koskevaan luetteloon kahden kuukauden kuluessa kyseisen ilmoituksen vastaanottamisesta.

4. Kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen voi esittää komissiolle pyynnön poistaa kyseisen viranomaisen ilmoittama vaatimustenmukaisuuden arviointilaitos 2 kohdassa tarkoitetusta luettelosta. Komissio julkaisee *Euroopan unionin virallisessa lehdessä* vastaavat tarkistukset luetteloon kuukauden kuluessa kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen pyynnön vastaanottamisesta.

5. Komissio voi hyväksyä täytäntöönpanosäädöksiä, joilla vahvistetaan olosuhteet, muotoseikat ja menettelyt tämän artiklan 1 kohdassa tarkoitetuille ilmoituksille. Nämä täytäntöönpanosäädökset hyväksytään 66 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

62 artikla

Euroopan kyberturvallisuuden sertifiointiryhmä

1. Perustetaan Euroopan kyberturvallisuuden sertifiointiryhmä.

2. Euroopan kyberturvallisuuden sertifiointiryhmä muodostetaan kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten tai muiden asiaankuuluvien kansallisten viranomaisten edustajista. Euroopan kyberturvallisuuden sertifiointiryhmän jäsen ei voi edustaa useampaa kuin kahta jäsenvaltiota.

3. Sidosryhmiä ja asiaankuuluvia kolmansia osapuolia voidaan kutsua Euroopan kyberturvallisuuden sertifiointiryhmän kokouksiin ja osallistumaan sen työhön.

4. Euroopan kyberturvallisuuden sertifiointiryhmän tehtävänä on

   a) neuvoa ja avustaa komissiota sen pyrkiessä varmistamaan tämän osaston johdonmukainen täytäntöönpano ja soveltaminen erityisesti unionin jatkuvan työohjelman osalta, kyberturvallisuussertifioinnin toimintapoliittisissa kysymyksissä, toimintaperiaatteiden yhteensovittamisessa ja eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien valmistelemisessa;

b) avustaa ja neuvoa ENISAa ja tehdä sen kanssa yhteistyötä ehdolla olevan järjestelmän valmistelemisessa 49 artiklan mukaisesti;

c) antaa ENISAn valmistelemasta ehdolla olevasta järjestelmästä lausunto 49 artiklan mukaisesti;

d) pyytää ENISAa valmistelemaan ehdolla olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän 48 artiklan 2 kohdan mukaisesti;

e) antaa komissiolle osoitettuja lausuntoja voimassa olevien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien ylläpitämisestä ja tarkistamisesta;

f) tarkastella merkityksellistä kehitystä kyberturvallisuussertifioinnin alalla ja vaihtaa tietoja ja hyviä käytäntöjä kyberturvallisuuden sertifiointijärjestelmistä;

g) helpottaa kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten välistä, tämän osaston mukaista yhteistyötä valmiuksien kehittämisen ja tietojenvaihdon avulla erityisesti ottamalla käyttöön menetelmiä tietojen vaihtamiseksi tehokkaasti kaikista kyberturvallisuussertifiointia koskevista kysymyksistä;

h) tukea vertaisarviointimekanismien täytäntöönpanoa 54 artiklan 1 kohdan u alakohdan nojalla perustetussa eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä vahvistettujen sääntöjen mukaisesti;

i) helpottaa eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukauttamista kansainvälisesti tunnustettuihin standardeihin muun muassa tarkastamalla nykyisiä eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä ja antamalla tarvittaessa ENISAlle suosituksia aloista, joilla sen olisi puututtava yhdessä asiaankuuluvien kansainvälisten standardointiorganisaatioiden kanssa saatavilla olevien kansainvälisesti tunnustettujen standardien puutteisiin tai aukkoihin.

5. Komissio toimii ENISAn avustuksella Euroopan kyberturvallisuuden sertifiointiryhmän puheenjohtajana ja sihteeristönä 8 artiklan 1 kohdan e alakohdan mukaisesti.

63 artikla

Valitusoikeus

1. Luonnollisilla henkilöillä ja oikeushenkilöillä on oikeus tehdä valitus eurooppalaisen kyberturvallisuussertifikaatin myöntäjälle tai asianmukaiselle kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle, jos valitus koskee vaatimustenmukaisuuden arviointilaitoksen 56 artiklan 6 kohdan mukaisesti myöntämää eurooppalaista kyberturvallisuussertifikaattia.

2. Viranomaisen tai elimen, jolle valitus on jätetty, on ilmoitettava valituksen tekijälle valituksen käsittelyn etenemisestä ja siitä tehdystä päätöksestä sekä 64 artiklassa tarkoitetusta oikeudesta tehokkaisiin oikeussuojakeinoihin.

64 artikla

Oikeus tehokkaisiin oikeussuojakeinoihin

1. Sen estämättä, mitä hallinnollisista tai muista kuin oikeudellisista oikeussuojakeinoista säädetään tai määrätään, luonnollisilla henkilöillä ja oikeushenkilöillä on oltava oikeus tehokkaisiin oikeussuojakeinoihin seuraavien osalta:

   a) edellä 63 artiklan 1 kohdassa tarkoitetun viranomaisen tai elimen päätökset, mukaan lukien soveltuvin osin eurooppalaisen kyberturvallisuussertifikaatin virheellistä myöntämistä koskevat päätökset, päätökset olla myöntämättä eurooppalaista kyberturvallisuussertifikaattia tai päätökset tunnustaa kyseisten luonnollisten henkilöiden ja oikeushenkilöiden hallussa oleva eurooppalainen kyberturvallisuussertifikaatti;

   b) edellä 63 artiklan 1 kohdassa tarkoitetulle viranomaiselle tai elimelle tehdyn valituksen käsittelemättä jättäminen.

2. Tämän artiklan mukaiset kanteet on nostettava sen jäsenvaltion tuomioistuimissa, johon kanteen kohteena oleva viranomainen tai elin on sijoittautunut.

65 artikla

Seuraamukset

Jäsenvaltioiden on annettava säännöt seuraamuksista, joita sovelletaan tämän osaston ja eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien säännösten rikkomiseen, ja toteutettava kaikki tarvittavat toimenpiteet sen varmistamiseksi, että ne pannaan täytäntöön. Säädettyjen seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia. Jäsenvaltioiden on ilmoitettava nämä säännöt ja toimenpiteet komissiolle viipymättä ja ilmoitettava sille niihin vaikuttavista myöhemmistä muutoksista.

IV OSASTO
LOPPUSÄÄNNÖKSET

66 artikla

Komiteamenettely

1. Komissiota avustaa komitea. Tämä komitea on asetuksessa (EU) N:o 182/2011 tarkoitettu komitea.

2. Kun viitataan tähän kohtaan, sovelletaan asetuksen (EU) N:o 182/2011 5 artiklan 4 kohdan b alakohtaa.

67 artikla

Arviointi ja uudelleentarkastelu

1. Komissio arvioi viimeistään … päivänä …kuuta … [viisi vuotta tämän asetuksen voimaantulosta] ja sen jälkeen viiden vuoden välein ENISAn ja sen työtapojen vaikutuksen, tehokkuuden ja tuloksellisuuden sekä mahdollisen tarpeen muuttaa ENISAn toimeksiantoa ja tällaisten muutosten taloudelliset vaikutukset. 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.

2. Arvioinnissa arvioidaan myös tämän asetuksen III osaston säännösten vaikutusta, tehokkuutta ja tuloksellisuutta suhteessa tavoitteisiin varmistaa tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien 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 pääsy unionin markkinoille, jotka eivät täytä kybertuvallisuuden perusvaatimuksia.

4. Komissio toimittaa viimeistään … päivänä …kuuta … [viisi vuotta tämän asetuksen voimaantulosta] ja joka viides vuosi sen jälkeen arviointikertomuksen ja päätelmänsä Euroopan parlamentille, neuvostolle ja johtokunnalle. Kyseisen kertomuksen tulokset julkistetaan.

68 artikla

Kumoaminen ja seuraanto

1. Kumotaan asetus (EU) N:o 526/2013 … päivästä …kuuta … [tämän asetuksen voimaantulopäivä] alkaen.

2. Viittaukset asetukseen (EU) N:o 526/2013 ja kyseisellä asetuksella perustettuun ENISAan katsotaan viittauksiksi tähän asetukseen ja tällä asetuksella perustettuun ENISAan.

3. Tällä asetuksella perustettu ENISA toimii kaikkien omistusten, sopimusten, oikeudellisten velvoitteiden, työsopimusten, taloudellisten sitoumusten ja vastuiden osalta asetuksella (EU) N:o 526/2013 perustetun ENISAn seuraajana. Kaikki johtokunnan ja hallituksen asetuksen (EU) N:o 526/2013 mukaisesti hyväksytyt päätökset pysyvät voimassa edellyttäen, että ne ovat tämän asetuksen mukaisia.

4. ENISA perustetaan määrittelemättömäksi toimiajaksi … päivästä …kuuta … [tämän asetuksen voimaantulopäivä].

5. Asetuksen (EU) N:o 526/2013 24 artiklan 4 kohdan mukaisesti nimitetty pääjohtaja toimii edelleen ENISAn pääjohtajana ja hoitaa tämän asetuksen 20 artiklassa tarkoitetut tehtävänsä jäljellä olevan toimikautensa ajan. Hänen työsopimuksensa muut ehdot pysyvät muuttumattomina.

6. Asetuksen (EU) N:o 526/2013 6 artiklan mukaisesti nimitetyt johtokunnan jäsenet ja varajäsenet toimivat edelleen ENISAn johtokunnan jäseninä ja varajäseninä ja hoitavat tämän asetuksen 15 artiklassa tarkoitetut tehtävänsä jäljellä olevan toimikautensa ajan.

69 artikla

Voimaantulo

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

2. Tätä asetusta sovelletaan ... päivästä ...kuuta ... lukuun ottamatta 58, 60, 61, 63, 64 ja 65 artiklaa, joita sovelletaan … päivästä …kuuta … [24 kuukautta tämän asetuksen voimaantulopäivästä].

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

Tehty …

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puhemies	*Puheenjohtaja*

LIITE

VAATIMUSTENMUKAISUUDEN ARVIOINTILAITOKSIA
KOSKEVAT VAATIMUKSET

Vaatimustenmukaisuuden arviointilaitokset akkreditoidaan vain, jos ne täyttävät seuraavat vaatimukset:

1. Vaatimustenmukaisuuden arviointilaitoksen on oltava perustettu kansallisen lainsäädännön mukaisesti ja sen on oltava oikeushenkilö.

2. Vaatimustenmukaisuuden arviointilaitoksen on oltava arvioimastaan organisaatiosta tai tieto- ja viestintätekniikan tuotteesta, palvelusta tai prosessista 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 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 vastaava henkilöstö eivät saa olla arvioitavan tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin suunnittelijoita, valmistajia, toimittajia, asentajia, ostajia, omistajia, käyttäjiä tai ylläpitäjiä taikka minkään tällaisen osapuolen valtuutettuja edustajia. Tämä 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 vastaava henkilöstö eivät myöskään saa olla suoranaisesti mukana arvioinnin kohteena olevien tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien suunnittelussa, valmistuksessa tai rakentamisessa, kaupan pitämisessä, asentamisessa, käytössä tai ylläpidossa eivätkä edustaa näissä 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 riippumattomuuden vaatimuksenmukaisuuden arviointitoimissa. Tämä kielto koskee erityisesti konsultointipalveluja.

6. Jos vaatimustenmukaisuuden arviointilaitoksen omistaa tai sen toimintaa harjoittaa julkinen taho tai laitos, riippumattomuus ja eturistiriidattomuus on varmistettava kansallisen sertifioinnin myöntävän viranomaisen ja vaatimustenmukaisuuden arviointilaitoksen välillä, ja se on dokumentoitava.

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

8. Vaatimustenmukaisuuden arviointilaitosten ja niiden henkilöstön on suoritettava vaatimustenmukaisuuden arviointitoimet moitteetonta ammattietiikkaa ja kyseisellä erityisalalla vaadittavaa teknistä pätevyyttä osoittaen, eikä arviointilaitoksiin ja niiden henkilöstöön saa kohdistua mitään sellaista painostusta tai johdattelua – mukaan lukien taloudellista painostusta tai johdattelua – joka saattaisi vaikuttaa arviointilaitosten ja niiden henkilöstön harkintaan tai vaatimustenmukaisuuden arviointitoimien tuloksiin, erityisesti sellaisten henkilöiden tai henkilöryhmien osalta, joille näiden toimien tuloksilla on merkitystä.

9. Vaatimustenmukaisuuden arviointilaitoksen on kyettävä suorittamaan kaikki vaatimustenmukaisuuden arviointitehtävät, jotka sille on tässä asetuksessa osoitettu, siitä riippumatta, suorittaako vaatimustenmukaisuuden arviointilaitos kyseiset tehtävät itse vai suoritetaanko ne sen puolesta ja sen vastuulla. Kaikki alihankinta tai ulkopuolisen henkilöstön kuuleminen on dokumentoitava asianmukaisesti, siihen ei saa osallistua välittäjiä, ja siitä on laadittava kirjallinen sopimus, jossa sovitaan muun muassa luottamuksellisuudesta ja eturistiriidoista. Kyseisen vaatimustenmukaisuuden arviointilaitoksen on kannettava täysi vastuu suoritetuista tehtävistä.

10. Vaatimustenmukaisuuden arviointilaitoksella on kaikissa tapauksissa ja kunkin sellaisen vaatimustenmukaisuuden arviointimenettelyn ja kunkin tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien tyypin, luokan tai alaluokan osalta, jota varten se on ilmoitettu, oltava käytössään

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

b) tarvittavat kuvaukset menettelyistä, joiden mukaisesti vaatimustenmukaisuuden arviointi suoritetaan siten, että varmistetaan näiden menettelyiden avoimuus ja toistettavuus. Sen käytössä on oltava asianmukaiset toimintatavat ja menettelyt, joilla erotetaan toisistaan ilmoitettuna sen laitoksena 61 artiklan nojalla suorittamat tehtävät ja sen muu toiminta;

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

11. Vaatimustenmukaisuuden arviointilaitoksella on oltava käytössään tarvittavat keinot niiden teknisten ja hallinnollisten tehtävien suorittamiseen, joita vaatimustenmukaisuuden arviointitoimien asianmukainen hoitaminen edellyttää, ja sillä on oltava käytettävissään kaikki tarvittavat laitteet ja välineet.

12. Vaatimustenmukaisuuden arviointitoimien suorittamisesta vastaavalla henkilöllä on oltava:

a) vankka tekninen ja ammatillinen koulutus, joka kattaa kaikki vaatimustenmukaisuuden arviointitoimet;

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

c) tarvittavat tiedot ja ymmärrys sovellettavista vaatimuksista ja testausstandardeista;

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

13. Vaatimustenmukaisuuden arviointilaitosten, niiden ylimmän johdon, vaatimustenmukaisuuden arviointitoimien suorittamisesta vastaavan henkilöstön ja alihankkijoiden puolueettomuus on taattava.

14. Ylimmän johdon ja vaatimustenmukaisuusarviointitoiminnasta vastaavien henkilöiden palkka ei saa olla riippuvainen suoritettujen vaatimustenmukaisuusarviointien määrästä eikä arviointien tuloksista.

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

16. Vaatimustenmukaisuuden arviointilaitoksen ja sen henkilöstön, komiteoiden, tytäryhtiöiden, alihankkijoiden ja laitokseen yhteydessä olevien elinten tai ulkoisten elinten henkilöstön on ylläpidettävä luottamuksellisuutta ja niillä on vaitiolovelvollisuus kaikkien niiden tietojen suhteen, joita ne saavat suorittaessaan vaatimustenarviointiin liittyviä tehtäviään tämän asetuksen tai sen täytäntöön panemiseksi annetun kansallisen lainsäädännön säännösten mukaisesti, paitsi kun näihin sovelletaan unionin tai jäsenvaltion lainsäädäntöä, jossa edellytetään niiden julkistamista ja lukuun ottamatta niiden jäsenvaltioiden toimivaltaisten viranomaisten osalta, joissa laitoksen toimet suoritetaan. Teollis- ja tekijänoikeudet on suojattava. Vaatimustenmukaisuuden arviointilaitoksella on oltava käytössä tämän kohdan vaatimusten mukaiset dokumentoidut menettelyt.

17. Edellä olevaa 16 kohtaa lukuun ottamatta tämän liitteen vaatimukset eivät estä millään tavalla teknisten tietojen ja sääntelyohjeistuksen vaihtoa vaatimustenmukaisuuden arviointilaitoksen ja sertifiointia hakevan tai sitä harkitsevan henkilön välillä.

18. Vaatimustenmukaisuuden arviointilaitosten on toimittava johdonmukaisilla, oikeudenmukaisilla ja kohtuullisilla ehdoilla ja edellytyksillä ja otettava huomioon pk-yritysten maksuihin liittyvät edut.

19. Vaatimustenmukaisuuden arviointilaitosten on täytettävä sellaisen asiaankuuluvan standardin vaatimukset, joka on yhdenmukaistettu asetuksessa (EY) N:o 765/2008 tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien sertifioinnista vastaavien vaatimustenmukaisuuden arviointilaitosten akkreditointia varten.

20. Vaatimustenmukaisuuden arviointilaitosten on varmistettava, että vaatimustenmukaisuuden arvioinnissa käytettävät testilaboratoriot täyttävät sellaisen asiaankuuluvan standardin vaatimukset, joka on yhdenmukaistettu asetuksessa (EY) N:o 765/2008 testauksesta vastaavien laboratorioiden akkreditointia varten.