Euroopan unionin neuvosto

Bryssel, 29. toukokuuta 2018
(OR. en)

9350/18

Toimielinten välinen asia:
2017/0225 (COD)

CYBER 115
TELECOM 152
CODEC 860
COPEN 163
COPS 175
COSI 129
CSC 170
CSCI 80
IND 143
JAI 514
JAIEX 55
POLMIL 61
RELEX 463

ILMOITUS

Lähettäjä:	Puheenjohtajavaltio
Vastaanottaja:	Neuvosto
Ed. asiak. nro:	8834/18
Kom:n asiak. nro:	12183/17
Asia:	Ehdotus EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUKSEKSI EU:n kyberturvallisuusvirastosta ENISAsta ja asetuksen (EU) 526/2013 kumoamisesta sekä tieto- ja viestintätekniikan kyberturvallisuussertifioinnista ("kyberturvallisuusasetus") – Yleisnäkemys

I JOHDANTO

1. Komissio hyväksyi ja toimitti neuvostolle ja Euroopan parlamentille 13. syyskuuta 2017 edellä mainitun ehdotuksen[1], joka on osa komission digitaalisten sisämarkkinoiden strategiaa. Ehdotuksen oikeusperusta on SEUT 114 artikla. Ehdotus kuuluu ns. kyberturvallisuuspakettiin, ja sillä pyritään kyberturvallisuuden, kyberresilienssin ja luottamuksen korkeaan tasoon unionissa. Tavoitteena on varmistaa, että sisämarkkinat toimivat asianmukaisesti.

2. Ehdotetussa asetuksessa esitetään EU:n kyberturvallisuusvirasto ENISAn tavoitteet, tehtävät ja organisatoriset näkökohdat. Lisäksi siinä vahvistetaan kehys eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien perustamiselle, jotta voidaan varmistaa riittäväntasoinen kyberturvallisuus tieto- ja viestintätekniikan tuotteille ja palveluille unionissa. Komission ehdotukseen liittyy vaikutustenarviointi. Siinä käsitellään kahdeksaa toimintapoliittista vaihtoehtoa, ja se kattaa ENISAn ja tieto- ja viestintätekniikan kyberturvallisuuden sertifioinnin arvioinnin.

3. Ehdotetussa asetuksessa on kaksi pääosiota:

   - viraston pysyvä toimeksianto, jonka soveltamisala on rajattu uusiin poliittisiin painopisteisiin ja välineisiin liittyvien tarpeiden perusteella, sekä viraston uudistetut tehtävät ja toiminnot, joiden avulla se voi tehokkaasti tukea jäsenvaltioiden, EU:n toimielinten ja muiden sidosryhmien työtä turvallisen kybertoimintaympäristön varmistamiseksi;

   - tieto- ja viestintätekniikan tuotteita ja palveluja koskeva eurooppalainen kyberturvallisuuden sertifiointikehys, jonka avulla hallinnoidaan eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä ja kyseisten järjestelmien puitteissa myönnetyt sertifikaatit voidaan katsoa kelvollisiksi ja tunnustaa kaikissa jäsenvaltioissa, mikä korjaisi markkinoiden nykyistä hajanaisuutta.

[1] Asiak. 12183/17; 12183/1/17 REV 1; 12183/2/17 REV 2.

4. Eurooppa-neuvosto kehotti lokakuussa 2017[2], että komissio laatisi kyberturvallisuutta koskevat ehdotuksensa kokonaisvaltaisella tavalla ja toimittaisi ne oikea-aikaisesti ja että niitä tarkasteltaisiin viipymättä neuvoston laatiman toimintasuunnitelman pohjalta.

5. Yleisten asioiden neuvosto hyväksyi 12. joulukuuta 2017 toimintasuunnitelman[3] Euroopan parlamentille ja neuvostolle annettua yhteistä tiedonantoa[4] "Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle" koskevien neuvoston päätelmien[5] täytäntöönpanoa varten. Toimintasuunnitelmasta kävi ilmi neuvoston tavoite muodostaa ehdotuksesta yleisnäkemys kesäkuuhun 2018 mennessä.

6. Euroopan parlamentissa ehdotuksen esittelijäksi on nimetty Angelika NIEBLER (teollisuus-, tutkimus ja energiavaliokunta – EPP). Teollisuus-, tutkimus- ja energiavaliokunnan on tarkoitus äänestää mietinnöstään 19. kesäkuuta 2018.

7. Euroopan talous- ja sosiaalikomitea antoi lausuntonsa 14. helmikuuta 2018.

II ASIAN KÄSITTELY NEUVOSTOSSA

8. Komissio esitti 26. syyskuuta 2017 tämän ehdotuksen ja siihen liittyvän vaikutustenarvioinnin kyberkysymysten horisontaaliselle työryhmälle (jäljempänä 'työryhmä'), minkä jälkeen työryhmä tarkasteli vaikutustenarviointia 20. lokakuuta 2017. Tätä seuranneissa keskusteluissa käsiteltiin pääasiassa viraston operatiivisia valmiuksia ja toimivaltaisten kansallisten viranomaisten kanssa tapahtuvan vuorovaikutuksen laajuutta sekä sertifiointikehyksen vaikutusta markkinoihin ja yritysten kilpailukykyyn. Yleisesti ottaen valtuuskunnat suhtautuivat myönteisesti sekä vaikutustenarviointiin että ehdotukseen.

---

2 EUCO 14/17, 11 kohta.
3 Asiak. 15748/17.
4 Asiak. 12211/17.
5 Asiak. 14435/17.

9. Itse ehdotuksen käsittely työryhmässä alkoi Viron puheenjohtajakaudella marraskuussa 2017, ja sitä jatkettiin Bulgarian puheenjohtajakaudella. Ehdotusta käsitteleviä kokouksia pidettiin 12. Niiden tuloksena saatiin kahdeksan peräkkäistä tarkistettua ehdotusta, ja tavoitteena on muodostaa ehdotuksesta yleisnäkemys 8. kesäkuuta 2018 pidettävässä TTE-neuvoston (televiestintä) istunnossa.

10. Työryhmässä 14. ja 15. toukokuuta 2018 käytyjen keskustelujen tulokset ja puheenjohtajavaltion tarkistettu kompromissiteksti ovat tämän ilmoituksen liitteenä. Johdanto-osa on mukautettu artiklaosan säännöksiin tehtyihin muutoksiin. Komission ehdotukseen tehdyt muutokset on **lihavoitu** tai merkitty hakasulkein [...]. Viimeisimpään työryhmän laatimaan asiakirjaan (8834/18) tehdyt muutokset on **lihavoitu ja alleviivattu**, ja poistot on merkitty alleviivatuin hakasulkein **[...]**.

III LOPUKSI

11. Liitteenä olevassa puheenjohtajavaltion kompromissitekstissä on otettu huomioon puheenjohtajavaltion ja jäsenvaltioiden pyrkimykset saada teksti hyvään tasapainoon.

12. Pysyvien edustajien komitea pääsi 25. toukokuuta 2018 puheenjohtajavaltion kompromissitekstistä yhteisymmärrykseen liitteessä olevin, 19 artiklan 5 kohtaa ja 48 artiklan 5 kohtaa koskevin muutoksin.

13. Neuvostoa pyydetään näin ollen istunnossaan 8. kesäkuuta 2018 hyväksymään yleisnäkemys ja valtuuttamaan puheenjohtajavaltio aloittamaan neuvottelut tästä asiasta Euroopan parlamentin ja Euroopan komission edustajien kanssa.

LIITE

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS

***[...] Euroopan Unionin kyberturvallisuusvirastosta* ENISAsta ja asetuksen (EU) 526/2013 kumoamisesta sekä tieto- ja viestintätekniikan kyberturvallisuussertifioinnista (''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[6],

ottavat huomioon alueiden komitean lausunnon[7],

noudattavat tavallista lainsäätämisjärjestystä,

[6] EUVL C , , s. .
[7] EUVL C , , s. .

sekä katsovat seuraavaa:

(1) Verkko- ja tietojärjestelmillä ja televiestintäverkoilla ja -palveluilla on yhteiskunnassa elintärkeä rooli, ja niistä on tullut talouskasvun selkäranka. Tieto- ja viestintätekniikka luo pohjaa monimutkaisille järjestelmille, jotka tukevat yhteiskunnan 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 laajalla levinnyttä kansalaisten, yritysten ja julkishallinnon piirissä kaikkialla unionissa. Digitoinnista ja verkkoyhteyksistä on tulossa keskeisiä ominaisuuksia yhä useammissa tuotteissa ja palveluissa, ja esineiden internetin myötä EU:ssa ennakoidaan otettavan käyttöön miljoonia, ellei miljardeja, verkkoon kytkettyjä digitaalisia laitteita seuraavan vuosikymmenen aikana. Yhä useammat laitteet liitetään internetiin huolehtimatta samalla siitä, että turvallisuus ja resilienssi ovat riittävällä tavalla sisäänrakennettuja, mikä johtaa puutteisiin kyberturvallisuudessa. Sertifioinnin vähäinen käyttö johtaa tässä yhteydessä siihen, että organisaatiot ja yksittäiset käyttäjät eivät saa riittävästi tietoa tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuusominaisuuksista, mikä heikentää luottamusta digitaalisiin ratkaisuihin.

(3) Digitalisoinnin ja verkkoyhteyksien yleistyminen lisää kyberturvallisuuteen liittyviä riskejä, jolloin koko yhteiskunta on haavoittuvampi kyberuhkille, ja pahentaa yksilöihin, myös heikommassa asemassa oleviin henkilöihin, kuten lapsiin, kohdistuvia vaaroja. Tämän yhteiskuntaan kohdistuvan riskin lieventämiseksi kyberturvallisuutta on tarpeen parantaa EU:ssa kaikin tarvittavin toimenpitein, jotta kansalaisten, hallintojen ja yritysten – pk-yrityksistä elintärkeiden infrastruktuureiden ylläpitäjiin – käyttämät verkko- ja tietojärjestelmät, televiestintäverkot, digitaaliset tuotteet, palvelut ja laitteet voidaan suojata paremmin kyberuhilta.

(4) Kyberhyökkäyksiä tapahtuu yhä enemmän, ja verkottunut talous ja yhteiskunta, jotka ovat alttiimpia kyberuhille ja -hyökkäyksille, edellyttävät vahvempaa puolustusvalmiutta. Vaikka kyberhyökkäykset ovat usein rajatylittäviä, kyberturvallisuusviranomaisten poliittiset vastatoimet ja lainvalvontavaltuudet ovat enimmäkseen kansallisia. Laajamittaiset kyberturvallisuuspoikkeamat voivat häiritä keskeisten palvelujen tarjoamista koko EU:ssa. Tämä edellyttää tehokasta EU-tason reagointia ja kriisinhallintaa, jossa nojaudutaan kohdennettuihin politiikkoihin ja laaja-alaisempiin eurooppalaisen yhteisvastuun ja keskinäisen avunannon välineisiin. Politiikan laatijoille, toimialalle ja käyttäjille on tärkeää, että kyberturvallisuuden ja resilienssin tilaa unionissa arvioidaan säännöllisesti luotettavan unionin tiedon pohjalta ja että laaditaan järjestelmällisesti ennusteita tulevista kehityskuluista, haasteista ja uhkista sekä unionin tasolla että maailmanlaajuisesti.

(5) Unioniin kohdistuvien kyberturvallisuushaasteiden lisääntymisen vuoksi tarvitaan kattava joukko toimenpiteitä, jotka pohjautuvat aiempaan unionin toimintaan ja edistävät toisiaan vahvistavia tavoitteita. Tähän sisältyy tarve lisätä jäsenvaltioiden ja yritysten valmiuksia ja varautumiskykyä sekä parantaa yhteistyötä ja koordinointia jäsenvaltioiden ja EU:n toimielinten, virastojen ja elinten välillä. Koska kyberuhkat ovat luonteeltaan rajattomia, on myös tarpeen lisätä valmiuksia unionin tasolla jäsenvaltioiden toimien täydentämiseksi erityisesti laajamittaisten rajatylittävien kyberturvallisuuspoikkeamien ja -kriisien tapauksessa. Tarvitaan myös lisätoimia kansalaisten ja yritysten tietoisuuden lisäämiseksi kyberturvallisuuteen liittyvistä kysymyksistä. Lisäksi digitaalisiin sisämarkkinoihin tunnettua luottamusta olisi edelleen parannettava tarjoamalla avointa tietoa tieto- ja viestintätekniikan tuotteiden ja palvelujen turvallisuustasosta. Tätä voidaan helpottaa EU:n laajuisella sertifioinnilla, joka tuo käyttöön yhteiset kyberturvallisuusvaatimukset ja arviointiperusteet kansallisille markkinoille ja sektoreille.

(6) Euroopan parlamentti ja neuvosto antoivat vuonna 2004 ENISAn perustamisesta asetuksen (EY) N:o 460/2004[8], jolla pyrittiin osaltaan varmistamaan korkeatasoinen verkko- ja tietoturva unionissa ja luomaan verkko- ja tietoturvakulttuuri, josta on hyötyä kansalaisille, kuluttajille, yrityksille ja julkishallinnoille. Vuonna 2008 Euroopan parlamentti ja neuvosto antoivat asetuksen (EY) N:o 1007/2008[9], jolla viraston toimikautta jatkettiin maaliskuuhun 2012. Asetuksella (EY) N:o 580/2011[10] viraston toimikautta jatkettiin edelleen 13 päivään syyskuuta 2013. Vuonna 2013 Euroopan parlamentti ja neuvosto antoivat ENISAsta ja asetuksen (EY) N:o 460/2004 kumoamisesta asetuksen (EU) N:o 526/2013[11], jolla viraston toimikautta jatkettiin kesäkuuhun 2020 saakka.

---

8 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).

9 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).

10 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).

11 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).

(7) Unioni on jo toteuttanut merkittäviä toimia kyberturvallisuuden varmistamiseksi ja luottamuksen lisäämiseksi digitaaliteknologioihin. Vuonna 2013 hyväksyttiin EU:n kyberturvallisuusstrategia ohjaamaan unionin poliittisia vastatoimia kyberturvallisuusuhkiin ja -riskeihin. Tarjotakseen eurooppalaisille paremman suojan verkkoympäristössä unioni hyväksyi vuonna 2016 ensimmäisenä kyberturvallisuusalan säädöksenä direktiivin (EU) 2016/1148 toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa, jäljempänä 'verkko- ja tietoturvadirektiivi'. Verkko- ja tietoturvadirektiivillä 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, vesihuolto, pankkitoiminta, rahoitusmarkkinoiden infrastruktuurit, terveydenhuolto ja digitaalinen infrastruktuuri sekä keskeisten digitaalisten palvelujen (hakukoneet, pilvipalvelut ja verkossa toimivat markkinapaikat) tarjoajat. ENISAlle annettiin keskeinen rooli tukea direktiivin täytäntöönpanoa. Lisäksi kyberrikollisuuden tehokas torjunta on tärkeä prioriteetti Euroopan turvallisuusagendassa, joka tältä osin edistää yleistä tavoitetta saavuttaa kyberturvallisuuden korkea taso.

(8) Yleisesti tunnustetaan, että sen jälkeen, kun EU:n kyberturvallisuusstrategia hyväksyttiin vuonna 2013 ja viraston toimeksiantoa viimeksi tarkistettiin, yleinen poliittinen tilanne on muuttunut merkittävästi, myös epävarmemman ja vähemmän turvatun globaalin toimintaympäristön vuoksi. Tässä yhteydessä ja osana uutta unionin kyberturvallisuuspolitiikkaa on tarpeen tarkistaa ENISAn toimeksiantoa, jotta voidaan määritellä sen rooli muuttuneessa kyberturvallisuuden toimintaympäristössä ja varmistaa, että se auttaa tehokkaasti unionia vastaamaan tästä perusteellisesti muuttuneesta uhkaympäristöstä johtuviin kyberturvallisuushaasteisiin. Kuten viraston arvioinnissa todetaan, sen nykyinen toimeksianto ei ole riittävä näiden haasteiden kannalta.

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

(10) Eurooppa-neuvoston kokouksessa 13 päivänä joulukuuta 2003 hyväksytyllä päätöksellä 2004/97/EY, Euratom, jäsenvaltioiden edustajat päättivät, että ENISAn kotipaikaksi tulee Kreikan hallituksen myöhemmin nimeämä kaupunki Kreikassa. Viraston isäntäjäsenvaltion olisi huolehdittava siitä, että virastolla on parhaat mahdolliset toimintaedellytykset. Viraston tehtävien moitteettoman ja tehokkaan suorittamisen, henkilöstön palvelukseenoton ja sitouttamisen sekä verkostoitumisen tehokkuuden kannalta on ehdottoman tärkeää, että virasto sijaitsee soveltuvassa paikassa, jossa on muun muassa toimivat liikenneyhteydet ja palveluja viraston henkilöstön mukana tuleville puolisoille ja lapsille. Tarvittavat järjestelyt olisi vahvistettava viraston ja isäntäjäsenvaltion välisessä sopimuksessa, joka tehdään sen jälkeen kun viraston johtokunta on antanut hyväksyntänsä.

(11) Unioniin kohdistuvien kyberturvallisuushaasteiden lisääntyessä viraston määrärahoja ja henkilöresursseja olisi lisättävä siten, että ne vastaavat sen uutta roolia ja tehtäviä sekä sen keskeistä asemaa eurooppalaista digitaalista toimintaympäristöä puolustavassa organisaatioiden ekosysteemissä.

(12) Viraston 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. Viraston olisi **tuettava** [...] kansallisia toimia ja **osaltaan proaktiivisesti edistettävä** unionin toimia ja suoritettava tehtävänsä täydessä yhteistyössä unionin toimielinten, [...] virastojen **ja elinten** sekä jäsenvaltioiden kanssa. Lisäksi viraston olisi hyödynnettävä yksityisen sektorin ja muiden asiaankuuluvien sidosryhmien näkemyksiä ja niiden kanssa tehtävää yhteistyötä. Viraston tehtävänannossa olisi vahvistettava, miten viraston on määrä saavuttaa tavoitteensa niin, että se pystyy toimimaan joustavasti.

(13) Viraston 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 EU:n toimintapolitiikoista ja lainsäädännöstä saataisiin merkityksellisempiä ja ne voitaisiin panna yhdenmukaisesti täytäntöön kansallisella tasolla**[...]. Viraston olisi toimittava neuvonnan ja asiantuntemuksen viitetahona unionin alakohtaisille toimintapoliittisille ja lainsäädännöllisille aloitteille, kun niihin liittyy kyberturvallisuuskysymyksiä.

(14) Viraston lähtökohtaisena tehtävänä on edistää asianomaisen lainsäädännön johdonmukaista täytäntöönpanoa ja erityisesti verkko- ja tietoturvadirektiivin 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.

(15) Viraston olisi avustettava jäsenvaltioita sekä unionin toimielimiä, [...] virastoja **ja elimiä** niiden pyrkimyksissä kehittää ja parantaa valmiuksia ja varautumiskykyä ehkäistä ja havaita [...] **kyberuhkia** ja -poikkeamia ja reagoida niihin verkko- ja tietojärjestelmien turvallisuuden kannalta. Viraston olisi erityisesti tuettava kansallisten CSIRT-toimijoiden kehittämistä ja tehostamista, jotta niiden kypsyys olisi yhteisellä korkealla tasolla unionissa. **Jäsenvaltioiden operatiivisiin valmiuksiin liittyvien ENISAn toimien olisi oltava pelkästään täydentäviä siihen nähden, mitä omia toimia jäsenvaltiot toteuttavat täyttääkseen verkko- ja tietoturvadirektiivistä johtuvat velvoitteensa. ENISAn toimet eivät siis saa syrjäyttää jäsenvaltioiden omia toimia** [...].

(15 a) Viraston olisi myös autettava kehittämään ja päivittämään unionin ja pyynnöstä jäsenvaltioiden strategioita, jotka koskevat verkko- ja tietojärjestelmien turvallisuutta, erityisesti kyberturvallisuutta, sekä edistettävä niiden levittämistä ja seurattava niiden täytäntöönpanoa. Viraston olisi myös tarjottava koulutusta ja koulutusmateriaalia julkisille elimille ja tarvittaessa "koulutettava kouluttajia", jotta voidaan auttaa jäsenvaltioita kehittämään omia koulutusvalmiuksia.

(16) Viraston olisi avustettava verkko- ja tietoturvadirektiivillä perustettua yhteistyöryhmää sen tehtävien suorittamisessa erityisesti tarjoamalla asiantuntemusta ja neuvontaa sekä helpotettava parhaiden käytäntöjen vaihtoa muun muassa keskeisten palvelujen tarjoajien yksilöimisestä, myös rajat ylittävien riippuvuussuhteiden osalta, siltä osin kuin kyse on riskeistä ja poikkeamista.

(17) Julkisen ja yksityisen sektorin välisen ja yksityisen sektorin sisäisen yhteistyön edistämiseksi [...] **viraston 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 (ISAC) perustamista. [...].

(18) Viraston olisi koottava ja analysoitava CSIRT-toimijoiden ja CERT-EU:n **vapaaehtoisesti toimittamat** kansalliset raportit, **jotta se voi avustaa jäsenvaltioita**, kun ne laativat tiedonvaihtoa varten yhteiset [...] **menettelyt**, kielen ja terminologian. Viraston olisi myös otettava yksityinen sektori mukaan verkko- ja tietoturvadirektiivin kehykseen, jossa vahvistettiin perusta vapaaehtoiselle teknisten tietojen vaihdolle operatiivisella tasolla [...] **CSIRT-verkostossa**.

(19) Viraston olisi osallistuttava EU:n tason vastaukseen laajamittaisten rajatylittävien kyberturvallisuuspoikkeamien ja -kriisien tapauksessa. Tämä tehtävä olisi **täytettävä viraston tässä asetuksessa määritetyn toimeksiannon ja sen toimintamallin mukaisesti, josta jäsenvaltiot sopivat koordinoitua reagointia laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin koskevan komission suosituksen perusteella. Siihen voi kuulua** tarvittavan tiedon keruu ja toimiminen välittäjänä CSIRT-verkoston ja tekniikan alan toimijoiden sekä kriisinhallinnasta vastaavien päätöksentekijöiden välillä. Lisäksi virasto voisi tukea poikkeamien käsittelyä teknisestä näkökulmasta helpottamalla tarvittavien ratkaisujen teknistä vaihtoa jäsenvaltioiden välillä ja osallistumalla julkiseen viestintään. Viraston olisi tuettava tätä prosessia testaamalla tällaisen yhteistyön menettelyjä [...] **säännöllisissä** kyberturvallisuusharjoituksissa.

(20) [...] Viraston olisi **operatiivista yhteistyötä tukiessaan** hyödynnettävä saatavilla olevaa CERT-EU:n **teknistä ja operatiivista** asiantuntemusta jäsennellyssä yhteistyössä [...]. Tarvittaessa tällaisen yhteistyön käytännön toteutus olisi määriteltävä erityisin järjestelyin näiden kahden organisaation välillä **päällekkäisiä tehtäviä välttäen**.

(21) [...] **Operatiivista yhteistyötä CSIRT-verkostossa tukevien** tehtäviensä mukaisesti viraston 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 analyysit uhkista ja poikkeamista. **[...] Vaikutukseltaan merkittävien poikkeamien teknisen käsittelyn helpottamisen yhteydessä ENISAn olisi erityisesti tuettava teknisten ratkaisujen vapaaehtoista jakamista jäsenvaltioiden välillä tai tuotettava yhdistettyjä teknisiä tietoja, kuten jäsenvaltioiden vapaaehtoisesti jakamia teknisiä ratkaisuja.** Komission suosituksessa koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin suositellaan, että jäsenvaltiot tekisivät yhteistyötä vilpittömässä mielessä ja vaihtaisivat keskenään ja ENISAn kanssa tietoja laajamittaisista kyberturvallisuuspoikkeamista ja -kriiseistä ilman aiheetonta viivytystä. Tällainen tieto auttaisi ENISAa [...] **tukemaan operatiivista yhteistyötä**.

(22) Viraston olisi osana unionin tilannetietoisuutta tukevaa säännöllistä teknisen tason yhteistyötä laadittava poikkeamista ja uhkista säännöllisesti **ja tiiviissä yhteistyössä jäsenvaltioiden kanssa** EU:n kyberturvallisuuden tekninen tilanneraportti, joka perustuu julkisesti saatavilla oleviin tietoihin, sen omaan analyysiin sekä raportteihin, joita se on saanut jäsenvaltioiden CSIRT-toimijoilta [...] tai verkko- ja tietoturvadirektiivillä perustetuilta keskitetyiltä yhteyspisteiltä **(molemmat perustuvat vapaaehtoisuuteen)**, Europolissa toimivalta Euroopan kyberrikostorjuntakeskukselta (EC3) ja CERT-EU:lta sekä tarvittaessa EU:n tiedusteluanalyysikeskukselta (INTCEN) ja Euroopan ulkosuhdehallinnolta (EUH). Raportti olisi asetettava neuvoston, komission ja unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan asianomaisten yksiköiden ja CSIRT-verkoston saataville.

(23) **Viraston tuessa** [...] merkittävästi vaikuttaneiden poikkeamien jälkikäteen tehtäville teknisille **tutkinnoille**, joita [...] **asianomaiset** jäsenvaltiot ovat pyytäneet, olisi keskityttävä poikkeamien välttämiseen jatkossa [...]. **Kyseisten jäsenvaltioiden olisi toimitettava virastolle tarvittavat tiedot, jotta tämä voi tehokkaasti tukea teknistä tutkintaa.**

(24) [...]

(25) Jäsenvaltiot voivat pyytää yrityksiä, joita poikkeama koskee, tekemään yhteistyötä antamalla tarvittavan tiedon ja avun virastolle, sanotun kuitenkaan rajoittamatta niiden oikeutta suojata kaupallisesti arkaluonteiset tiedot.

(26) Ymmärtääkseen paremmin kyberturvallisuuteen liittyviä haasteita ja tarjotakseen strategista pitkän aikavälin neuvontaa jäsenvaltioille ja unionin toimielimille viraston on tarpeen analysoida nykyisiä ja kehittymässä olevia riskejä. Tätä varten viraston 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. Viraston olisi myös tuettava jäsenvaltioita ja unionin toimielimiä, virastoja ja elimiä kyberturvallisuuteen liittyvien uusien kehityssuuntausten kartoittamisessa ja **kyberturvallisuuspoikkeamien** [...] ehkäisyssä tekemällä analyyseja uhkista ja poikkeamista.

(27) Unionin resilienssin lisäämiseksi viraston olisi kehitettävä **erityisesti verkko- ja tietoturvadirektiivin liitteessä II mainittuja aloja tukevien ja saman direktiivin liitteessä III mainittujen digitaalisten palvelujen tarjoajien hyödyntämien infrastruktuurien kyberturvallisuuteen** liittyvää huippuosaamista tarjoamalla neuvontaa, ohjeita ja parhaita käytäntöjä. Jotta kyberturvallisuusriskeistä ja mahdollisista suojakeinoista saataisiin tietoa helpommin ja paremmin jäsennellyssä muodossa, viraston olisi kehitettävä unionin "tietokeskus" ja ylläpidettävä sitä. Kyseessä on keskitetty verkkoportaali, josta yleisö saa EU:n ja kansallisilta toimielimiltä, virastoilta ja laitoksilta peräisin olevaa tietoa kyberturvallisuudesta.

(28) Viraston olisi autettava lisäämään yleisön tietoisuutta kyberturvallisuuteen liittyvistä riskeistä ja annettava yksittäisille käyttäjille ohjeita hyvistä toimintatavoista kansalaisten ja organisaatioiden käyttöön. Viraston pitäisi osaltaan edistää parhaita käytäntöjä ja ratkaisuja yksilöiden ja organisaatioiden tasolla keräämällä ja analysoimalla julkisesti saatavilla olevia tietoja merkittävistä poikkeamista ja kokoamalla raportteja ohjeistuksen antamiseksi yrityksille ja kansalaisille ja yleisen varautumis- ja resilienssitason parantamiseksi. Viraston olisi myös järjestettävä yhteistyössä jäsenvaltioiden sekä unionin toimielinten, [...] virastojen **ja elinten** kanssa säännöllisiä loppukäyttäjille suunnattuja tiedotus- ja valistuskampanjoita, joiden tarkoituksena on edistää turvallisempaa verkkokäyttäytymistä yksilötasolla ja lisätä tietoisuutta verkossa piilevistä mahdollisista uhkista, mukaan lukien verkkourkintayritysten, bottiverkkojen sekä talous- ja pankkipetosten kaltainen kyberrikollisuus, sekä edistää yleisluonteisen neuvonnan antamista aitouden todentamista ja tietosuojaa koskevissa kysymyksissä. Virastolla olisi oltava keskeinen rooli pyrittäessä lisäämään loppukäyttäjien tietoisuutta laitteiden turvallisuudesta.

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

(30) Varmistaakseen tavoitteidensa täysimittaisen saavuttamisen viraston olisi oltava yhteydessä asiaankuuluviin toimielimiin, virastoihin ja elimiin, mukaan lukien CERT-EU, Europolissa toimiva Euroopan kyberrikostorjuntakeskus (EC3), Euroopan puolustusvirasto (EDA), laaja-alaisten tietojärjestelmien operatiivisesta hallinnoinnista vastaava eurooppalainen virasto (eu-LISA), Euroopan lentoturvallisuusvirasto (EASA)**, Euroopan GNSS-virasto (GSA)** sekä muut kyberturvallisuuteen liittyviä kysymyksiä käsittelevät EU:n virastot. Sen olisi oltava yhteydessä myös tietosuoja-asioita käsitteleviin viranomaisiin, jotta voidaan vaihtaa tietotaitoa ja parhaita käytäntöjä ja antaa neuvontaa kyberturvallisuusnäkökohdista, joilla voi olla vaikutusta niiden toimintaan. Kansallisten ja unionin lainvalvonta- ja tietosuojaviranomaisten edustajien olisi voitava olla edustettuina viraston pysyvässä sidosryhmässä. Ollessaan yhteydessä lainvalvontaviranomaisiin sellaisissa verkko- ja tietoturvakysymyksissä, joilla voi olla vaikutusta niiden toimintaan, viraston olisi käytettävä olemassa olevia tiedonvaihtokanavia ja vakiintuneita verkostoja.

(31) Viraston olisi **asemassaan** CSIRT-verkoston sihteeristönä [...] tuettava jäsenvaltioiden CSIRT-toimijoita ja CERT-EU:ta operatiivisessa yhteistyössä kaikkien asiaankuuluvien CSIRT-verkoston tehtävien lisäksi, sellaisina kuin ne määritellään verkko- ja tietoturvadirektiivissä. Viraston 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 CERT-toimijaa, ottaen asianmukaisesti huomioon CSIRT-verkoston menettelyohjeet.

(32) Jotta voidaan lisätä unionin varautumista kyberturvallisuuspoikkeamiin vastaamisessa, viraston olisi järjestettävä [...] **säännöllisesti** kyberturvallisuusharjoituksia unionin tasolla sekä tuettava jäsenvaltioita ja EU:n toimielimiä, virastoja ja elimiä niiden pyynnöstä harjoitusten järjestämisessä.

(33) Viraston olisi kehitettävä ja ylläpidettävä asiantuntemustaan kyberturvallisuussertifioinnissa, jotta voidaan tukea unionin politiikkaa tällä alalla. Viraston olisi edistettävä kyberturvallisuussertifioinnin käyttöä unionissa muun muassa osallistumalla kyberturvallisuuden sertifiointikehyksen perustamiseen ja ylläpitoon unionin tasolla, jotta voidaan lisätä avoimuutta tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuuden varmistuksessa ja tällä tavoin vahvistaa luottamusta digitaalisiin sisämarkkinoihin.

(34) 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 ja yksityisen sektorin organisaatioissa nostaa kyberturvallisuustasoa unionissa. Tätä varten viraston 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.

(35) Viraston olisi kannustettava jäsenvaltioita ja palveluntarjoajia tiukentamaan yleisiä turvallisuusnormejaan, jotta kaikki internetin käyttäjät voivat toteuttaa tarvittavat toimenpiteet oman kyberturvallisuutensa varmistamiseksi. Erityisesti palveluntarjoajien ja tuotteiden valmistajien olisi poistettava tuotannosta tai kierrätettävä tuotteet ja palvelut, jotka eivät täytä kyberturvallisuusnormeja. ENISA voi yhteistyössä toimivaltaisten viranomaisten kanssa levittää tietoa sisämarkkinoilla tarjottavien tuotteiden ja palvelujen kyberturvallisuustasosta ja antaa varoituksia palveluntarjoajille ja valmistajille ja vaatia niitä parantamaan tuotteidensa ja palvelujensa turvallisuutta, mukaan lukien kyberturvallisuus.

(36) Viraston olisi otettava täysimääräisesti huomioon meneillään olevat tutkimus-, kehittämis- ja teknologian arvioimistoimet, erityisesti sellaiset, joita toteutetaan unionin eri tutkimusaloitteissa, antaakseen unionin toimielimille, [...] virastoille **ja elimille** sekä tarvittaessa jäsenvaltioille, näiden sitä pyytäessä, neuvoja [...] kyberturvallisuusalan tutkimustarpeista. **Viraston olisi myös kuultava asianomaisia käyttäjäryhmiä, jotta se voi määritellä tutkimustarpeet ja -prioriteetit.**

(37) **Kyberturvallisuusuhat** [...] ovat maailmanlaajuisia. Tarvitaan tiiviimpää kansainvälistä yhteistyötä **kyberturvallisuusstandardien** parantamiseksi, mihin sisältyy myös yhteisten käyttäytymisnormien määrittely, sekä tiedonvaihtoa kansainvälisen yhteistoiminnan nopeuttamiseksi verkko- ja tietoturvakysymyksissä samoin kuin yhteistä maailmanlaajuista lähestymistapaa näihin kysymyksiin. Tätä varten viraston olisi tuettava unionin osallistumista kolmansien maiden ja kansainvälisten organisaatioiden kanssa harjoitettavaan yhteistyöhön ja tämän yhteistyön lisäämistä tarjoamalla käyttöön asianomaisten unionin toimielinten, [...] virastojen **ja elinten** mahdollisesti tarvitsemaa asiantuntemusta ja analysointivalmiuksia.

(38) Viraston olisi voitava vastata tapauskohtaisiin neuvonta- ja avustamispyyntöihin, joita jäsenvaltiot ja EU:n toimielimet, virastot ja elimet esittävät ja jotka ovat viraston tavoitteiden mukaisia.

(39) On tarpeen panna täytäntöön tiettyjä viraston hallintoa koskevia periaatteita, jotta voidaan noudattaa EU:n erillisvirastoja käsittelevässä toimielinten välisessä työryhmässä heinäkuussa 2012 hyväksyttyä yhteistä julkilausumaa ja yhteistä lähestymistapaa, joiden tarkoituksena on tehostaa virastojen toimintaa ja parantaa niiden tuloksellisuutta. Yhteisen julkilausuman ja yhteisen lähestymistavan tulisi näkyä asianmukaisella tavalla myös viraston työohjelmissa, viraston arvioinneissa ja viraston raportointi- ja hallintokäytännöissä.

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

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

(42) Viraston moitteeton toiminta edellyttää, että sen pääjohtaja nimitetään ansioiden ja todistuksin osoitettujen hallinnollisten taitojen ja johtamistaitojen sekä kyberturvallisuuden kannalta merkityksellisen pätevyyden ja kokemuksen perusteella ja että pääjohtajan tehtäviä hoidetaan täysin riippumattomasti. Pääjohtajan olisi laadittava ehdotus viraston työohjelmaksi kuultuaan ensin komissiota ja toteutettava kaikki tarvittavat toimenpiteet varmistaakseen viraston työohjelman asianmukaisen toteuttamisen. Pääjohtajan olisi laadittava johtokunnalle esitettävä vuosikertomus**, jossa käsitellään myös viraston vuotuisen työohjelman toteuttamista,** sekä esitys viraston tuloja ja menoja koskevaksi ennakkoarvioksi ja vastattava talousarvion toteuttamisesta. Pääjohtajan olisi voitava perustaa tilapäisiä työryhmiä erityisesti tieteellisiä, teknisiä, oikeudellisia tai sosioekonomisia erityiskysymyksiä varten. Pääjohtajan olisi varmistettava, että tilapäisten työryhmien jäsenet valitaan huippuasiantuntemuksen perusteella ja ottaen asianmukaisesti huomioon tarkasteltavan kysymyksen edellyttämällä tavalla edustuksellinen tasapaino jäsenvaltioiden julkishallintojen, unionin toimielinten ja yksityisen sektorin välillä, mukaan lukien toimiala, käyttäjät ja tiedeyhteisöä edustavat verkko- ja tietoturva-asiantuntijat.

(43) 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.

(44) Virastolla olisi oltava neuvoa-antavana elimenä pysyvä sidosryhmä, jotta voitaisiin varmistaa säännöllinen yhteydenpito yksityisen sektorin, kuluttajajärjestöjen ja muiden asianosaisten sidosryhmien kanssa. Pysyvän sidosryhmän, jonka johtokunta perustaa pääjohtajan ehdotuksesta, olisi keskityttävä sidosryhmiä koskeviin asioihin ja saatettava ne viraston tietoon. Pysyvän sidosryhmän kokoonpanossa ja tälle ryhmälle, jotka kuullaan erityisesti työohjelmaluonnoksesta, annettavissa tehtävissä olisi varmistettava sidosryhmien riittävä edustus viraston työskentelyssä.

(45) Virastolla olisi oltava säännöt eturistiriitojen ehkäisemisestä ja hallinnasta. Viraston 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[12]. Viraston suorittamassa henkilötietojen käsittelyssä olisi noudatettava yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 18 päivänä joulukuuta 2000 annettua Euroopan parlamentin ja neuvoston asetusta (EY) N:o 45/2001[13]. Viraston olisi noudatettava tietojen käsittelyä koskevia unionin toimielimiin sovellettavia määräyksiä ja kansallista lainsäädäntöä, erityisesti kun on kyse arkaluonteisista turvallisuusluokittelemattomista ja EU:n turvallisuusluokitelluista tiedoista.

---

12 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).

13 EYVL L 8, 12.1.2001, s. 1.

(46) Jotta voidaan varmistaa viraston täydellinen itsemääräämisoikeus ja riippumattomuus ja jotta virasto pystyy suorittamaan uusia ja täydentäviä tehtäviä, myös ennakoimattomia tehtäviä hätätilanteissa, virastolle olisi annettava riittävä ja itsenäinen talousarvio, jonka tulot koostuvat ensisijaisesti unionin rahoitusosuudesta ja viraston työhön osallistuvien kolmansien maiden rahoitusosuuksista. Viraston henkilöstön enemmistön työtehtävien olisi liityttävä suoraan viraston toimeksiannon operatiiviseen täytäntöönpanoon. Viraston isäntäjäsenvaltion tai minkä tahansa muun jäsenvaltion olisi voitava maksaa vapaaehtoisia rahoitusosuuksia virastolle. Unionin talousarviomenettelyä olisi sovellettava edelleen unionin yleisestä talousarviosta maksettaviin tukiin. Lisäksi tilintarkastustuomioistuimen olisi tarkastettava viraston tilit avoimuuden ja vastuuvelvollisuuden varmistamiseksi.

(47) [...]

(48) Kyberturvallisuussertifioinnilla on tärkeä rooli lisättäessä tieto- ja viestintätekniikan tuotteiden ja palvelujen turvallisuutta ja niihin tunnettua luottamusta. Digitaaliset sisämarkkinat ja erityisesti datatalous ja esineiden internet voivat menestyä vain, jos vallitsee yleinen julkinen luottamus siihen, että tuotteissa ja palveluissa varmistetaan kyberturvallisuus tietyllä tasolla. Verkkoyhteyksillä varustetut ja automatisoidut autot, sähköiset terveyspalvelut, teollisuusautomaation ohjausjärjestelmät ja älykkäät verkot ovat joitakin esimerkkejä aloista, joilla sertifiointi on jo laajalti käytössä tai tulee todennäköisesti käyttöön lähitulevaisuudessa. Verkko- ja tietoturvadirektiivillä säännellyt alat ovat samalla aloja, joilla kyberturvallisuussertifioinnilla on ratkaiseva merkitys.

(49) 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 ja -palvelujen tarjonta sisämarkkinoilla on edelleen maantieteellisesti hyvin hajanaista. Tämä johtuu siitä, että Euroopan kyberturvallisuusala on kehittynyt suurelta osin kansallisista valtiollisen kysynnän lähtökohdista. Kyberturvallisuuden sisämarkkinoiden toimintapuutteisiin kuuluu lisäksi yhteentoimivien ratkaisujen (teknisten standardien), toimintatapojen ja EU:n 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 digitaalisten sisämarkkinoiden strategian täytäntöönpanon väliarvioinnissa 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 ja puuttua kyberturvallisuuden markkinoiden nykyiseen hajanaisuuteen.

(50) Tieto- ja viestintätekniikan **prosessien,** tuotteiden ja palvelujen kyberturvallisuussertifiointia käytetään tällä hetkellä vain vähäisessä määrin. Kun sitä käytetään, käyttö rajoittuu enimmäkseen jäsenvaltioiden tasolle tai teollisuuslähtöisten järjestelmien piiriin. Tässä yhteydessä yhden kansallisen kyberturvallisuusviranomaisen myöntämää sertifikaattia ei periaatteessa tunnusteta muissa jäsenvaltioissa. Yritykset voivat näin ollen joutua sertifioimaan tuotteensa ja palvelunsa useissa jäsenvaltioissa, joissa ne toimivat, esimerkiksi voidakseen osallistua kansallisiin hankintamenettelyihin. 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.

(51) Joillain toimilla on jo pyritty sertifikaattien vastavuoroiseen tunnustamiseen Euroopassa. Niiden tavoitteet on kuitenkin saavutettu vain osittain. Tärkein esimerkki tästä on johtavien virkamiesten tietoturvallisuusryhmän (SOGIS) vastavuoroista tunnustamista koskeva sopimus (MRA). SOGIS [...] on tärkein malli yhteistyölle ja vastavuoroiselle tunnustamiselle turvallisuussertifioinnin alalla, mutta siihen kuuluu vain osa unionin jäsenvaltioista. Tämä on rajoittanut SOGISia koskevan MRA-sopimuksen toimivuutta sisämarkkinoiden kannalta.

(52) Edellä esitetyn perusteella on tarpeen perustaa eurooppalainen kyberturvallisuuden sertifiointikehys, jossa vahvistetaan tärkeimmät horisontaaliset vaatimukset kehitettäville eurooppalaisille kyberturvallisuuden sertifiointijärjestelmille ja jonka ansiosta tieto- ja viestintätekniikan tuotteita ja palveluja koskevat sertifikaatit **ja EU-vaatimustenmukaisuusilmoitukset** voidaan tunnustaa ja ottaa käyttöön kaikissa jäsenvaltioissa. Eurooppalaisen sertifiointikehyksen tulisi palvella kahta tarkoitusta. Yhtäältä sen pitäisi lisätä luottamusta tieto- ja viestintätekniikan tuotteisiin ja palveluihin, jotka on sertifioitu tällaisten järjestelmien mukaisesti. Toisaalta sen avulla pitäisi välttää tilanne, jossa käytössä on monia keskenään ristiriitaisia tai päällekkäisiä kansallisia kyberturvallisuussertifiointeja, ja vähentää siten digitaalisilla sisämarkkinoilla yrityksille aiheutuvia kustannuksia. Järjestelmien olisi oltava syrjimättömiä ja kansainvälisiin ja/tai [...] **eurooppalaisiin** standardeihin perustuvia, paitsi jos kyseiset standardit ovat tehottomia tai epäasianmukaisia EU:n oikeutettujen tavoitteiden saavuttamiseksi.

(53) Komissiolle olisi siirrettävä valta hyväksyä eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät yksittäisille tieto- ja viestintätekniikan **prosessien,** tuotteiden ja palvelujen ryhmille. Kansallisten [...] **kyberturvallisuussertifioinnin myöntävien viranomaisten** olisi vastattava näiden järjestelmien täytäntöönpanosta ja valvonnasta, ja näissä järjestelmissä myönnettyjen sertifikaattien olisi oltava voimassa ja tunnustettuja kaikkialla unionissa. Toimialan tai muiden yksityisten organisaatioiden ylläpitämien sertifiointijärjestelmien ei tulisi kuulua tämän asetuksen soveltamisalaan. Tällaisia järjestelmiä ylläpitävät elimet voivat kuitenkin ehdottaa, että komissio ottaa tällaiset järjestelmät lähtökohdaksi niiden hyväksymiseksi eurooppalaisena järjestelmänä.

(54) Tämän asetuksen säännökset eivät saisi vaikuttaa unionin lainsäädäntöön, jossa annetaan erityiset säännöt tieto- ja viestintätekniikan tuotteiden ja palvelujen sertifioinnista. Erityisesti yleisessä tietosuoja-asetuksessa 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 tuotteiden ja palvelujen tietosuojataso. Tämä asetus ei rajoita tietojenkäsittelytoimintojen sertifiointia yleisen tietosuoja-asetuksen mukaisesti, ei myöskään silloin, kun nämä toimet on sisällytetty tuotteisiin ja palveluihin.

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

(55 a) Eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä käytettävät tekniset eritelmät olisi määriteltävä asetuksen (EU) 1025/2012 liitteessä II vahvistettujen periaatteiden mukaisesti. Poikkeuksia näihin periaatteisiin voidaan kuitenkin katsoa tarvittavan asianmukaisesti perustelluissa tapauksissa, joissa kyseisiä teknisiä eritelmiä käytetään eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän korkealla varmuustasolla. Tällaisten poikkeusten syyt on asetettava julkisesti saataville.

(55 b) Sertifioidun vaatimustenmukaisuuden arvioinnissa arvioidaan, täyttyvätkö tieto- ja viestintätekniikan prosessiin, tuotteeseen tai palveluun liittyvät määritellyt vaatimukset. Arvioinnin tekee riippumaton kolmas osapuoli – ei siis tuotteen valmistaja tai palvelun tarjoaja. Kun tieto- tai viestintätekniikan prosessi, tuote tai palvelu on läpäissyt arvioinnin, sille voidaan myöntää sertifikaatti. Tämän olisi katsottava vahvistavan, että kyseinen arviointi on tehty asianmukaisesti. Eurooppalaisessa kyberturvallisuusjärjestelmässä olisi varmuustasosta riippuen määritettävä, myöntääkö sertifikaatin yksityinen taho vai julkinen elin. Vaatimustenmukaisuuden arviointi ja sertifiointi ei sinänsä takaa, että sertifioidut tieto- ja viestintätekniikan tuotteet ja palvelut ovat kyberturvallisia. Se on pikemminkin menettely ja tekninen menetelmä todistaa, että tieto- ja viestintätekniikan tuotteet ja palvelut on testattu ja että ne täyttävät tietyt kyberturvallisuusvaatimukset, jotka on vahvistettu muualla, esimerkiksi teknisissä standardeissa.

(55 c) Sertifikaattien käyttäjien olisi valittava asianmukainen sertifioinnin taso ja siihen liittyvät turvallisuusvaatimukset tieto- ja viestintätekniikan prosessin, tuotteen tai palvelun käytöstä tehdyn riskianalyysin perusteella. Varmuustason olisi näin ollen vastattava tieto- ja viestintätekniikan prosessin, tuotteen tai palvelun aiottuun käyttöön liittyvän riskin tasoa.

(55 d) Eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan määrätä, että vaatimustenmukaisuuden arviointi on pelkästään tieto- ja viestintätekniikan tuotteiden ja palvelujen valmistajan tai tarjoajan vastuulla (vaatimustenmukaisuuden itsearviointi). Tällaisissa tapauksissa riittää, että valmistaja tai palveluntarjoaja tekee itse kaikki tarkastukset, joilla varmistetaan, että tieto- tai viestintätekniikan prosessi, tuote tai palvelu on sertifiointijärjestelmässä asetettujen vaatimusten mukainen. Tämäntyyppinen vaatimustenmukaisuuden arviointi olisi katsottava asianmukaiseksi yksinkertaisten tieto- ja viestintätekniikan tuotteiden ja palvelujen yhteydessä, jotka aiheuttavat vain vähäisen yleistä etua koskevan riskin. Tällaisia voivat olla esimerkiksi tuotteet tai palvelut, joiden suunnittelu- ja tuotantomekanismit ovat yksinkertaiset. Vaatimustenmukaisuuden itsearviointia voidaan soveltaa vain varmuustasoltaan perustason tieto- ja viestintätekniikan tuotteisiin ja palveluihin.

(55 e) Eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan tieto- ja viestintätekniikan tuotteiden ja palveluiden yhteydessä käyttää sekä sertifiointia että vaatimustenmukaisuuden itsearviointia. Tällaisen tilanteen varalta järjestelmässä olisi määriteltävä selkeät ja ymmärrettävät käytännöt, joiden avulla kuluttajat ja muut käyttäjät erottavat, minkä tuotteiden ja palvelujen arvioinnista on vastannut valmistaja tai palveluntarjoaja ja mitkä kolmas osapuoli on sertifioinut.

(55 f) Tieto- ja viestintätekniikan tuotteiden ja palvelujen valmistajan tai tarjoajan, joka tekee vaatimustenmukaisuuden itsearvioinnin, olisi vaatimustenmukaisuuden arviointimenettelyn yhteydessä laadittava ja allekirjoitettava EU-vaatimustenmukaisuusilmoitus. EU-vaatimustenmukaisuusilmoitus on asiakirja, jossa todetaan, että tietty tieto- ja viestintätekniikan tuote tai palvelu on järjestelmässä asetettujen vaatimusten mukainen. Laatimalla ja allekirjoittamalla EU-vaatimustenmukaisuusilmoituksen valmistaja tai palveluntarjoaja ottaa vastuun siitä, että tieto- ja viestintätekniikan tuote tai palvelu on järjestelmässä asetettujen oikeudellisten vaatimusten mukainen. Jäljennös EU-vaatimustenmukaisuusilmoituksesta olisi toimitettava kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle ja ENISAlle.

(55 g) Tieto- ja viestintätekniikan tuotteiden ja palvelujen valmistajan tai tarjoajan olisi pidettävä EU-vaatimustenmukaisuusilmoitus ja kaikkia tieto- ja viestintätekniikan tuotteiden ja palvelujen järjestelmässä määriteltyä vaatimustenmukaisuutta koskevia tietoja sisältävät tekniset asiakirjat toimivaltaisen kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen saatavilla asiaankuuluvassa eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä määritetyn ajanjakson ajan. Teknisissä asiakirjoissa olisi eriteltävä sovellettavat vaatimukset, ja niiden olisi katettava tieto- ja viestintätekniikan tuotteen tai palvelun suunnittelu, valmistus ja toiminta siinä määrin kuin se on olennaista arvioinnin kannalta. Tekniset asiakirjat olisi laadittava siten, että niiden perusteella voidaan arvioida, onko tieto- ja viestintätekniikan tuote tai palvelu sovellettavien vaatimusten mukainen.

(55 h) Jäsenvaltioiden ja kiinnostuneita sidosryhmiä edustavien organisaatioiden olisi voitava esittää Euroopan kyberturvallisuuden sertifiointiryhmälle ehdotus sertifiointijärjestelmäksi. Kiinnostuneita sidosryhmiä edustavat organisaatiot ovat teollisuuden toimijoita tai kuluttajia edustavat organisaatiot, myös pk-yrityksiä edustavat organisaatiot, joilla on pätevä syy olla kiinnostuneita erityisen eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän kehittämisestä. Tällaisia ehdotuksia olisi tarkasteltava Euroopan kyberturvallisuuden sertifiointiryhmän kehittämien perusteiden pohjalta. Perusteet on laadittu läpinäkyvyyden, avoimuuden, puolueettomuuden, yhteisymmärryksen, tehokkuuden, merkityksellisyyden ja yhtenäisyyden periaatteita noudattaen.

(56) Komissiolle **ja sertifiointiryhmälle** olisi annettava valtuudet pyytää ENISAa valmistelemaan **ilman aiheetonta viivytystä** yksittäisiä tieto- ja viestintätekniikan **prosesseja,** tuotteita tai palveluja varten ehdolla olevat järjestelmät. Edelleen 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 määriteltävä tietyt vähimmäistekijät yksittäisen järjestelmän kohteen, soveltamisalan ja toiminnan osalta. Näihin olisi sisällyttävä muun muassa kyberturvallisuussertifioinnin soveltamisala ja kohde, mukaan lukien sertifioinnin kattamat tieto- ja viestintätekniikan **prosessien,** tuotteiden ja palvelujen luokat, yksityiskohtainen eritelmä kyberturvallisuusvaatimuksista esimerkiksi viittaamalla standardeihin tai teknisiin eritelmiin, yksittäiset arviointiperusteet ja -menetelmät sekä aiottu varmuustaso (perustaso, korotettu ja/tai korkea taso) **ja tarvittaessa arviointitasot**.

(56 a) Eurooppalaisen sertifiointijärjestelmän mukainen varmuustaso luo perustan luottamukselle siihen, että tietty tieto- ja viestintätekniikan prosessi, tuote tai palvelu täyttää tietyn eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaiset turvallisuusvaatimukset. Sertifioituja tieto- ja viestintätekniikan prosesseja, tuotteita ja palveluja koskevan kehyksen yhdenmukaisuuden varmistamiseksi eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan määrittää kyseisen järjestelmän nojalla myönnettyjen eurooppalaisten kyberturvallisuussertifikaattien ja EU-vaatimustenmukaisuusilmoitusten varmuustasot. Sertifikaateissa voidaan viitata johonkin kolmesta varmuustasosta: perustaso, korotettu taso tai korkea taso. EU-vaatimustenmukaisuusilmoituksessa voidaan puolestaan viitata vain perustasoon. Varmuustasot kertovat, miten tarkka arvio prosessille, tuotteelle tai palvelulle on tehty. Niissä viitataan teknisiin eritelmiin, standardeihin ja niihin liittyviin menetelmiin (myös teknisiin tarkastuksiin), joiden tarkoituksena on lieventää tai ehkäistä kyberturvallisuuspoikkeamia. Kunkin varmuustason tulisi olla yhdenmukainen eri aloilla, joilla sertifiointeja käytetään.

(56 b) Eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan 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 tai palvelun 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. Tällaisten toimintojen kehitystyössä ja ylläpidossa olisi noudatettava turvallisuuskeskeistä toimintatapaa ja hyödynnettävä siihen liittyviä välineitä. Näin varmistetaan, että sekä ohjelmistoon että laitteistoon saadaan luotettavasti sisällytettyä toimivia mekanismeja. Varmuustasoista perustason arvioinnissa olisi käsiteltävä vähintään seuraavat osatekijät: arvioinnin olisi sisällettävä vähintään vaatimustenmukaisuuden arviointilaitoksen arvio tieto- ja viestintätekniikan tuotteen tai palvelun 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 valmistaja tai palveluntarjoaja tekee sertifiointijärjestelmän mukaisen itsearvioinnin tieto- ja viestintätekniikan prosessin, tuotteiden tai palvelujen vaatimustenmukaisuudesta. Korotetun varmuustason arvioinnissa olisi perustason arvioinnin lisäksi todennettava, vastaavatko tieto- ja viestintätekniikan tuotteen tai palvelun turvallisuustoiminnot sen teknisiä asiakirjoja. Korkean varmuustason arvioinnissa olisi korotetun tason arvioinnin lisäksi tehtävä tehokkuustesti, jolla arvioidaan tieto- ja viestintätekniikan tuotteen tai palvelun turvallisuustoimintojen vastustuskykyä huomattavaa osaamista ja resursseja vaativia pitkälle kehittyneitä kyberhyökkäyksiä vastaan.

(56 c) Ehdolla olevaa järjestelmää valmistellessaan ENISAn olisi kuultava kaikkia asiaankuuluvia sidosryhmiä, joita ovat esimerkiksi eurooppalaiset standardointiorganisaatiot, asiaankuuluvat kansalliset viranomaiset, vastavuoroista tunnustamista koskeviin sopimuksiin perustuvat organisaatiot (kuten SOGIS MRA), pk-yritykset, kuluttajajärjestöt sekä ympäristöalan sidosryhmät ja sosiaaliset sidosryhmät.

(56 d) ENISAn olisi ylläpidettävä verkkosivustoa, jolla annetaan tietoa eurooppalaisista kyberturvallisuuden sertifiointijärjestelmistä ja tehdään niitä tunnetuiksi. Tietojen olisi sisällettävä muun muassa pyynnöt valmistella ehdolla oleva eurooppalainen kyberturvallisuuden sertifiointijärjestelmä sekä palaute, jota ENISA on saanut valmisteluvaiheessa tehdyistä kuulemisista. Verkkosivustolla olisi annettava tietoa myös tämän asetuksen nojalla myönnetyistä sertifikaateista ja annetuista EU-vaatimustenmukaisuusilmoituksista.

(57) Eurooppalaisen kyberturvallisuussertifioinnin **ja EU-vaatimustenmukaisuusilmoituksen** käytön tulisi edelleen olla vapaaehtoista, jollei toisin säädetä unionin lainsäädännössä tai **unionin lainsäädännön mukaisesti hyväksytyssä** kansallisessa lainsäädännössä. **Jos yhdenmukaista lainsäädäntöä ei ole, jäsenvaltiot voivat hyväksyä direktiivin (EU) 2015/1535 mukaisia kansallisia teknisiä määräyksiä, joissa säädetään pakollisesta eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesta sertifioinnista. Jäsenvaltiot voivat myös käyttää eurooppalaista kyberturvallisuussertifiointia julkisissa hankinnoissa ja direktiivin 2014/214/EU yhteydessä**. [...]

(57 a) Jotta voitaisiin saavuttaa tämän asetuksen tavoitteet ja välttää hajanaisuus sisämarkkinoilla, sellaisten kansallisten kyberturvallisuuden sertifiointijärjestelmien tai -menettelyjen, joiden kattamat tieto- ja viestintätekniikan tuotteet ja palvelut kuuluvat jonkin eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan, olisi lakattava tuottamasta oikeusvaikutuksia alkaen päivästä, jonka komissio vahvistaa täytäntöönpanosäädöksessä. Jäsenvaltiot eivät myöskään saisi ottaa käyttöön uusia kansallisia kyberturvallisuuden sertifiointijärjestelmiä tieto- ja viestintätekniikan tuotteille ja palveluille, jotka kuuluvat jo jonkin olemassa olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan. Jäsenvaltioita ei kuitenkaan tulisi estää hyväksymästä tai pitämästä voimassa kansallisia sertifiointijärjestelmiä kansallisen turvallisuuden nimissä.

(58) Kun eurooppalainen kyberturvallisuuden sertifiointijärjestelmä on hyväksytty, tieto- ja viestintätekniikan tuotteiden valmistajien tai tieto- ja viestintätekniikan palvelujen tarjoajien olisi voitava jättää tuotteidensa tai palvelujensa sertifiointia koskeva hakemus valitsemalleen vaatimustenmukaisuuden arviointilaitokselle. Vaatimustenmukaisuuden arviointilaitosten olisi saatava akkreditointi akkreditointielimeltä, jos ne täyttävät tässä asetuksessa vahvistetut tietyt erityiset vaatimukset. Akkreditointi olisi myönnettävä enintään viideksi vuodeksi, ja se voidaan uusia samoin edellytyksin, jos vaatimustenmukaisuuden arviointilaitos täyttää vaatimukset. Akkreditointielimen 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 tämän asetuksen säännöksiä.

(59) [...] Jäsenvaltioiden [...] **olisi** nimettävä **ainakin** yksi [...] **kyberturvallisuussertifioinnin myöntävä viranomainen** valvomaan **tästä asetuksesta johtuvien velvoitteiden noudattamista. Nämä tehtävät voidaan osoittaa myös nykyisille viranomaisille, jos jäsenvaltio pitää tätä asianmukaisena. Jäsenvaltioiden olisi myös voitava päättää keskinäisellä sopimuksella toisen jäsenvaltion kanssa yhden tai useamman valvontaviranomaisen nimeämisestä kyseisen toisen jäsenvaltion alueelle. Viranomaisen olisi erityisesti seurattava kyseisen jäsenvaltion alueelle sijoittautuneiden tieto- ja viestintätekniikan tuotteiden ja palvelujen valmistajien tai tarjoajien velvollisuuksia, 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 uusia vaatimuksia, ja seurattava merkityksellistä kehitystä kyberturvallisuussertifioinnin alalla**[...]. Kansallisten [...] **kyberturvallisuussertifioinnin myöntävien viranomaisten** olisi käsiteltävä luonnollisten tai oikeushenkilöiden tekemät valitukset, jotka liittyvät **niiden** myöntämiin sertifikaatteihin **tai vaatimustenmukaisuuden arviointilaitosten myöntämiin, korkeaa varmuustasoa koskeviin sertifikaatteihin** [...], tutkittava asianmukaisessa määrin valituksen kohde ja ilmoitettava valituksen tekijälle tutkinnan etenemisestä ja tuloksesta kohtuullisessa ajassa. Lisäksi niiden olisi tehtävä yhteistyötä muiden kansallisten [...] **kyberturvallisuussertifioinnin myöntävien viranomaisten** tai muiden viranomaisten kanssa esimerkiksi jakamalla tietoa mahdollisista tapauksista, joissa tieto- ja viestintätekniikan tuotteet ja palvelut eivät vastaa tämän asetuksen tai yksittäisten kyberturvallisjärjestelmien vaatimuksia.

(60) Eurooppalaisen kyberturvallisuuden sertifiointikehyksen johdonmukaisen soveltamisen varmistamiseksi olisi perustettava Euroopan kyberturvallisuuden sertifiointiryhmä (jäljempänä 'sertifiointiryhmä'), joka koostuu kansallisten [...] **kyberturvallisuussertifioinnin myöntävien** viranomaisten **tai muiden asiaankuuluvien kansallisten viranomaisten edustajista**. Ryhmän päätehtävinä tulisi olla neuvoa ja avustaa komissiota sen pyrkiessä varmistamaan eurooppalaisen kyberturvallisuuden sertifiointikehyksen yhdenmukaisen täytäntöönpanon ja soveltamisen, avustaa virastoa ehdolla olevien kyberturvallisuuden sertifiointijärjestelmien valmistelussa tiiviissä yhteistyössä sen kanssa, suosittaa, että komissio pyytää virastoa valmistelemaan ehdolla olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän, sekä antaa **virastolle osoitettuja lausuntoja ehdolla olevista järjestelmistä ja** komissiolle osoitettuja lausuntoja voimassa olevien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien ylläpitämisestä ja tarkistamisesta.

(60 a) Ryhmän olisi helpotettava parhaiden käytäntöjen ja asiantuntemuksen vaihtoa vaatimustenmukaisuuden arviointilaitosten valtuuttamisesta ja sertifikaattien myöntämisestä vastaavien kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten välillä. Ryhmän olisi tuettava vertaisarviointimekanismin kehittämistä korkean varmuustason eurooppalaisia kyberturvallisuussertifikaatteja myöntäville elimille ehdolla olevien järjestelmien valmistelua sekä niiden täytäntöönpanoa varten. Tällaisissa vertaisarvioinneissa olisi erityisesti arvioitava sitä, onko kyseisillä elimillä käytettävissään asianmukaista asiantuntemusta ja suorittavatko ne tehtävänsä yhdenmukaisesti. Vertaisarviointien tulokset olisi julkistettava. Arvioitavat elimet voivat toteuttaa aiheellisia toimenpiteitä, joilla ne mukauttavat käytäntöjään ja asiantuntemustaan.

(61) Tietoisuuden lisäämiseksi ja tulevien EU:n kyberturvallisuusjärjestelmien hyväksymisen helpottamiseksi Euroopan komissio voi antaa yleisiä tai alakohtaisia kyberturvallisuutta koskevia suuntaviivoja esimerkiksi hyvistä kyberturvallisuuskäytännöistä tai vastuullisesta kyberturvallisuuskäyttäytymisestä korostaen sertifioitujen tieto- ja viestintätekniikan tuotteiden ja palvelujen käytön myönteistä vaikutusta.

(61 a) Tieto- ja viestintäalan toimitusketjut ovat maailmanlaajuisia, joten unioni voi SEUT 218 artiklan mukaisesti kaupankäyntiä edelleen helpottaakseen tehdä eurooppalaisen kyberturvallisuuden sertifiointikehyksen pohjalta perustetuissa järjestelmissä myönnettyjä sertifikaatteja koskevia sopimuksia vastavuoroisesta tunnustamisesta. Komissio voi ENISAn ja Euroopan kyberturvallisuuden sertifiointiryhmän neuvot huomioiden suosittaa näitä koskevien neuvottelujen aloittamista. Järjestelmissä olisi määriteltävä erikseen edellytykset vastavuoroiselle tunnustamiselle kolmansien maiden kanssa.

(62) [...]

(63) [...]

(64) Jotta voidaan varmistaa tämän asetuksen yhdenmukainen täytäntöönpano, komissiolle olisi siirrettävä täytäntöönpanovaltaa tässä asetuksessa säädetyn mukaisesti. Tätä valtaa olisi käytettävä asetuksen (EU) N:o 182/2011 mukaisesti.

(65) Olisi sovellettava tarkastusmenettelyä hyväksyttäessä täytäntöönpanosäädöksiä, jotka koskevat tieto- ja viestintätekniikan tuotteiden ja palvelujen eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä, viraston tutkimusten toteuttamista koskevia yksityiskohtaisia sääntöjä sekä kansallisten [...] **kyberturvallisuussertifioinnin myöntävien viranomaisten** komissiolle tekemien, akkreditoituja vaatimustenmukaisuuden arviointilaitoksia koskevien ilmoitusten olosuhteita, muotoseikkoja ja menettelyjä.

(66) Viraston toimintaa olisi arvioitava riippumattomasti. Arvioinnissa olisi otettava huomioon viraston tavoitteiden saavuttaminen, sen toimintatavat ja sen tehtävien merkityksellisyys. Arvioinnissa olisi myös arvioitava eurooppalaisen kyberturvallisuuden sertifiointikehyksen vaikutusta, vaikuttavuutta ja tehokkuutta.

(67) Asetus (EU) N:o 526/2013 olisi kumottava.

(68) 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 5 artiklassa vahvistetun toissijaisuusperiaatteen mukaisesti. Mainitussa artiklassa vahvistetun suhteellisuusperiaatteen mukaisesti tässä asetuksessa ei ylitetä sitä, mikä on tarpeen tämän tavoitteen saavuttamiseksi,

OVAT HYVÄKSYNEET TÄMÄN ASETUKSEN:

I OSASTO
YLEISET SÄÄNNÖKSET

1 artikla

Kohde ja soveltamisala

1. Sisämarkkinoiden asianmukaisen toiminnan varmistamiseksi, pyrkien samalla kyberturvallisuuden, kyberresilienssin ja luottamuksen korkeaan tasoon unionissa, tässä asetuksessa

a) vahvistetaan "[...] **Euroopan unionin kyberturvallisuusviraston**" ENISAn (jäljempänä 'virasto') tavoitteet, tehtävät ja organisatoriset näkökohdat ja

b) vahvistetaan kehys eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien perustamiselle, jotta voidaan varmistaa riittäväntasoinen kyberturvallisuus tieto- ja viestintätekniikan **prosesseille,** tuotteille ja palveluille unionissa. Tämän kehyksen soveltaminen ei rajoita niiden erityisten säännösten soveltamista, jotka koskevat vapaaehtoista tai pakollista sertifiointia muiden unionin säädösten nojalla.

2. **Tämä asetus ei rajoita kyberturvallisuutta koskevaa jäsenvaltioiden toimivaltaa eikä missään tapauksessa toimia, jotka koskevat yleistä turvallisuutta, puolustusta, kansallista turvallisuutta tai yksittäisen valtion toimia rikosoikeuden alalla.**

2 artikla

Määritelmät

Tässä asetuksessa tarkoitetaan:

1) 'kyberturvallisuudella' kaikkia toimia, joita tarvitaan verkko- ja tietojärjestelmien, niiden käyttäjien ja asianosaisten henkilöiden suojaamiseksi kyberuhilta;

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

3) 'verkko- ja tietojärjestelmien turvallisuutta koskevalla kansallisella strategialla' direktiivin (EU) 2016/1148 4 artiklan 3 kohdassa tarkoitettua kehystä;

4) 'keskeisten palvelujen tarjoajalla' direktiivin (EU) N:o 2016/1148 4 artiklan 4 kohdassa määriteltyä julkista tai yksityistä toimijaa;

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

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

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

8) 'kyberuhalla' potentiaalista tilannetta tai tapahtumaa, joka voi **vahingoittaa tai häiritä** verkko- ja tietojärjestelmiä, niiden käyttäjiä ja asianosaisia henkilöitä **tai muulla tavoin** vaikuttaa näihin haitallisesti;

9) 'eurooppalaisella kyberturvallisuuden sertifiointijärjestelmällä' unionin tasolla määriteltyjä kattavia sääntöjä, teknisiä vaatimuksia, standardeja ja menettelyjä, joita sovelletaan kyseisen erityisen järjestelmän kattamien tieto- ja viestintätekniikan **prosessien,** tuotteiden ja palvelujen sertifiointiin tai **vaatimustenmukaisuuden arviointiin**;

9 a) 'kansallisella kyberturvallisuuden sertifiointijärjestelmällä' kansallisen viranomaisen kehittämiä ja käyttöön ottamia kattavia sääntöjä, teknisiä vaatimuksia, standardeja ja menettelyjä, joita sovelletaan kyseisen erityisen järjestelmän kattamien tieto- ja viestintätekniikan prosessien, tuotteiden ja palvelujen sertifiointiin tai vaatimustenmukaisuuden arviointiin;

10) 'eurooppalaisella kyberturvallisuussertifikaatilla' [...] asiakirjaa, jolla todistetaan, että tietty tieto- ja viestintätekniikan **prosessi,** tuote tai palvelu [...] **on arvioitu** eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä vahvistettujen erityisten **turvallisuusvaatimusten** mukaiseksi;

11) 'tieto- ja viestintätekniikan tuotteella [...]' mitä tahansa verkko- ja tietojärjestelmien elementtiä tai elementtien ryhmää;

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

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

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

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

14) 'vaatimustenmukaisuuden arvioinnilla' vaatimustenmukaisuuden arviointia sellaisena kuin se on määritelty asetuksen (EY) N:o 765/2008 2 artiklan 12 kohdassa;

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

16) 'standardilla' asetuksen (EU) N:o 1025/2012 2 artiklan 1 kohdassa määriteltyä standardia**;**

16 a) 'teknisellä eritelmällä' asiakirjaa, jossa määrätään tekniset vaatimukset, jotka tieto- ja viestintätekniikan prosessin, tuotteen tai palvelun on täytettävä;

16 b) 'varmuustasolla' sitä, että tietty tieto- ja viestintätekniikan prosessi, tuote tai palvelu täyttää tietyn eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaiset turvallisuusvaatimukset; varmuustaso ilmaisee myös, millä tasolla tätä on arvioitu; varmuustaso ei ilmaise itse tieto- ja viestintätekniikan prosessin, tuotteen tai palvelun turvallisuutta.

II OSASTO

ENISA – "*[...] Euroopan unionin kyberturvallisuusvirasto*"

I LUKU

TOIMEKSIANTO JA TAVOITTEET *[...]*

3 artikla

Toimeksianto

1. Virasto hoitaa sille tämän asetuksen mukaisesti kuuluvia tehtäviä kyberturvallisuuden korkean tason edistämiseksi [...] **koko** unionissa**, erityisesti tukemalla jäsenvaltioita sekä unionin toimielimiä, virastoja ja elimiä kyberturvallisuuden parantamisessa**. **Virasto toimii kyberturvallisuutta koskevan neuvonnan ja asiantuntemuksen viitetahona unionin toimielimille, virastoille ja elimille.**

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

2 a. Virasto toimii tehtävissään riippumattomasti ja ottaa mahdollisimman tarkasti huomioon jäsenvaltioiden asiaankuuluvien viranomaisten kansallisen asiantuntemuksen sekä pyrkii välttämään päällekkäisiä toimia.

3. [...]

4 artikla

Tavoitteet

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

2. Virasto auttaa unionin toimielimiä, virastoja ja elimiä sekä jäsenvaltioita kehittämään ja panemaan täytäntöön kyberturvallisuutta koskevat **unionin** toimintapolitiikat**, myös kyberturvallisuutta koskevat alakohtaiset politiikat**.

3. Virasto tukee valmiuksien kehittämistä ja varautumista kaikkialla unionissa avustamalla unionin **toimielimiä, virastoja ja elimiä sekä** jäsenvaltioita ja julkisia ja yksityisiä sidosryhmiä niiden verkko- ja tietojärjestelmien suojelun lisäämiseksi, **kyberresilienssin ja toimintavalmiuksien** kehittämiseksi **ja parantamiseksi [...] sekä** ammattitaidon ja osaamisen **kehittämiseksi** kyberturvallisuuden alalla.

4. Virasto edistää yhteistyötä ja koordinointia unionin tasolla jäsenvaltioiden, unionin toimielinten, virastojen ja elinten sekä asiaankuuluvien **yksityisten ja julkisten** sidosryhmien välillä [...] kyberturvallisuuteen liittyvissä kysymyksissä.

5. Virasto [...] **parantaa osaltaan** kyberturvallisuusvalmiuksia unionin tasolla jäsenvaltioiden [...] **avustamiseksi** kyberuhkien ehkäisemisessä ja niihin vastaamisessa erityisesti rajat ylittävien poikkeamien tapauksessa.

6. Virasto edistää sertifioinnin käyttöä, **jotta voidaan välttää EU:n sertifiointijärjestelmien hajanaisuus. Virasto edistää erityisesti** [...] kyberturvallisuuden sertifiointikehyksen perustamista ja ylläpitoa unionin tasolla tämän asetuksen III osaston mukaisesti, jotta voidaan lisätä avoimuutta tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuuden varmistuksessa ja tällä tavoin vahvistaa luottamusta digitaalisiin sisämarkkinoihin.

7. Virasto edistää tietoisuuden korkeaa tasoa kansalaisten ja yritysten keskuudessa kyberturvallisuuteen liittyvissä kysymyksissä.

IA LUKU
TEHTÄVÄT

5 artikla

*Unionin politiikan ja lainsäädännön **kehittäminen ja täytäntöönpano** [...]*

Virasto edistää unionin politiikan ja lainsäädännön kehittämistä ja täytäntöönpanoa tehtävänään

1. avustaa ja neuvoa erityisesti antamalla riippumattomia lausuntoja ja 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. edesauttaa yhteistyöryhmän työtä direktiivin (EU) 2016/1148 11 artiklan mukaisesti antamalla asiantuntemusta ja apua;

4. tukea

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

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

5. tukea unionin poliittisten toimien säännöllistä uudelleentarkastelua antamalla vuosiraportti asianomaisen lainsäädännön täytäntöönpanosta liittyen seuraaviin:

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

    b) luottamuspalvelun tarjoajiin liittyvät tietoturvaloukkausta tai eheyden menetystä koskevat ilmoitukset, jotka valvontaelimet toimittavat virastolle asetuksen (EU) N:o 910/2014 19 artiklan 3 kohdan mukaisesti;

    c) yleisiä viestintäverkkoja tai yleisesti saatavilla olevia sähköisiä viestintäpalveluja tarjoavilta yrityksiltä saadut [...] **turvallisuuspoikkeamia** koskevat ilmoitukset, jotka toimivaltaiset viranomaiset toimittavat virastolle [eurooppalaisesta sähköisen viestinnän säännöstöstä annetun direktiivin] 40 artiklan mukaisesti.

6 artikla

[...] ***Valmiuksien kehittäminen***

1. Virasto avustaa

a) jäsenvaltioita niiden pyrkiessä parantamaan [...] **kyberuhkien** ja -poikkeamien ennaltaehkäisyä, havaitsemista ja analysointia sekä valmiuksia reagoida näihin uhkiin ja poikkeamiin tarjoamalla jäsenvaltioille tarvittavaa osaamista ja asiantuntemusta;

b) unionin toimielimiä, [...] virastoja **ja elimiä** niiden pyrkiessä parantamaan [...] **kyberuhkien** ja -poikkeamien ennaltaehkäisyä, havaitsemista ja analysointia sekä valmiuksia reagoida näihin uhkiin ja poikkeamiin **erityisesti** antamalla CERTille asianmukaista tukea unionin toimielimiä, virastoja ja elimiä varten (CERT-EU);

c) pyynnöstä jäsenvaltioita niiden kehittäessä kansallisia tietoturvaloukkauksiin reagoivia ja niitä tutkivia yksiköitä (CSIRT-toimijoita) direktiivin (EU) 2016/1148 9 artiklan 5 kohdan mukaisesti;

d) pyynnöstä jäsenvaltioita niiden kehittäessä verkko- ja tietojärjestelmien turvallisuutta koskevia kansallisia strategioita direktiivin (EU) 2016/1148 7 artiklan 2 kohdan mukaisesti; virasto myös edistää tiedon levittämistä kyseisistä strategioista ja seuraa niiden **täytäntöönpanoa** [...] kaikkialla unionissa parhaiden käytäntöjen edistämiseksi;

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

f) kansallisia ja unionin CSIRT-toimijoita niiden valmiustason nostamisessa 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;

g) jäsenvaltioita järjestämällä **säännöllisesti** [...] 7 artiklan 6 kohdassa tarkoitettuja laajamittaisia kyberturvallisuusharjoituksia unionin tasolla ja antamalla poliittisia suosituksia harjoitusten arviointiprosessin ja niistä saatavien kokemusten pohjalta;

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

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

2. Virasto **tukee tietojen jakamista alojen sisäisesti ja niiden välillä** [...], erityisesti direktiivin (EU) 2016/1148 liitteessä II mainituilla aloilla 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. Virasto tukee operatiivista yhteistyötä [...] **jäsenvaltioiden, unionin toimielinten, virastojen ja elinten kesken** sekä sidosryhmien välillä.

2. Virasto tekee yhteistyötä operatiivisella tasolla ja luo synergioita unionin toimielinten, [...] virastojen **ja elinten** 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 ohjeita asiaankuuluvista kyberturvallisuuteen liittyvistä kysymyksistä;

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

3. Virasto toimii CSIRT-verkoston sihteeristönä direktiivin (EU) 2016/1148 12 artiklan 2 kohdan mukaisesti ja **tässä ominaisuudessa** [...] helpottaa tietojen jakamista ja yhteistyötä sen jäsenten kesken.

4. Virasto **tukee** [...] operatiivista yhteistyötä CSIRT-verkostossa tukemalla jäsenvaltioita **näiden pyynnöstä** tehtävänään

a) antaa neuvoja siitä, miten ne voivat parantaa valmiuksiaan ehkäistä ja havaita poikkeamia ja reagoida niihin;

b) [...] **helpottaa** vaikutukseltaan merkittävien poikkeamien teknistä **käsittelyä** [...]**, mukaan lukien erityisesti** tukemalla **teknisten ratkaisujen vapaaehtoista jakamista jäsenvaltioiden välillä**;

c) analysoi haavoittuvuuksia [...] ja poikkeamia**;**

c a) tukee direktiivin (EU) 2016/1148 mukaisesti vaikutukseltaan merkittävien poikkeamien jälkikäteen tehtävää teknistä tutkintaa.

Näiden tehtävien suorittamisessa virasto ja CERT-EU tekevät jäsenneltyä yhteistyötä hyötyäkseen synergioista **ja välttääkseen toiminnan päällekkäisyyden** [...].

5. [...]

[...]

6. Virasto järjestää **säännöllisesti** [...] kyberturvallisuusharjoituksia unionin tasolla ja tukee jäsenvaltioita ja EU:n toimielimiä, virastoja ja elimiä harjoitusten järjestämisessä niiden pyynnöstä. **Tällaisiin unionin tasolla järjestettäviin harjoituksiin voi sisältyä teknisiä, operatiivisia ja strategisia osatekijöitä** [...]. **Joka toinen vuosi järjestetään laajamittainen harjoitus, joka sisältää kaikki nämä osatekijät.** Virasto myös edistää ja auttaa tarvittaessa järjestämään alakohtaisia kyberturvallisuusharjoituksia yhdessä [...] **asiaankuuluvien organisaatioiden** kanssa**, jotka voivat osallistua** [...] myös unionin tasolla järjestettäviin kyberturvallisuusharjoituksiin.

7. Virasto laatii poikkeamista ja uhkista säännöllisesti ja **tiiviissä yhteistyössä jäsenvaltioiden kanssa** EU:n kyberturvallisuuden teknisen tilanneraportin, joka perustuu julkisiin tietolähteisiin, sen omaan analyysiin ja raportteihin, jotka on saatu muun muassa jäsenvaltioiden CSIRT-toimijoilta [...] tai verkko- ja tietoturvadirektiivillä perustetuilta keskitetyiltä yhteyspisteiltä (**molemmat perustuvat vapaaehtoisuuteen** [...]); Europolissa toimivalta Euroopan kyberrikostorjuntakeskukselta (EC3) sekä CERT-EU:lta.

8. Virasto edistää yhteistyöhön perustuvan vastauksen kehittämistä unionin ja jäsenvaltioiden tasolla laajamittaisiin rajatylittäviin kyberturvallisuuspoikkeamiin tai -kriiseihin pääasiallisesti

   a) kokoamalla **vapaaehtoisesti toimitettuja** raportteja kansallisista lähteistä, jotta voidaan edistää yhteistä tilannetietoisuutta;

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

c) [...] **helpottamalla jäsenvaltioiden pyynnöstä** poikkeaman tai kriisin teknistä käsittelyä, mukaan lukien **erityisesti** [...] **tukemalla** teknisten ratkaisujen **vapaaehtoista** jakamista jäsenvaltioiden välillä;

d) tukemalla **EU:n toimielimiä, virastoja ja elimiä sekä pyynnöstä jäsenvaltioita** poikkeamaan tai kriisiin [...] **liittyvässä julkisessa viestinnässä**;

e) [...] **tukemalla jäsenvaltioita näiden pyynnöstä** tällaisiin poikkeamiin tai kriiseihin **vastaamista varten laadittujen yhteistyösuunnitelmien testaamisessa**.

8 artikla

*[...] **Markkinat, kyberturvallisuussertifiointi ja standardointi***

Virasto

a) tukee ja edistää tieto- ja viestintätekniikan **prosessien,** tuotteiden ja palvelujen kyberturvallisuussertifiointiin liittyvän, tämän asetuksen III osastolla käyttöön otettavan unionin politiikan kehittämistä ja täytäntöönpanoa tehtävänään

1) valmistella ehdolla olevat eurooppalaiset [...] **kyberturvallisuuden** sertifiointijärjestelmät tieto- ja viestintätekniikan **prosesseille,** tuotteille ja palveluille **yhteistyössä toimialan kanssa ja** tämän asetuksen 44 artiklan mukaisesti;

2) avustaa komissiota toimimalla Euroopan kyberturvallisuuden sertifiointiryhmän sihteeristönä tämän asetuksen 53 artiklan mukaisesti;

3) koota ja julkaista ohjeita ja laatia hyviä käytäntöjä, jotka koskevat tieto- ja viestintätekniikan tuotteiden ja palvelujen kyberturvallisuusvaatimuksia, yhteistyössä kansallisten [...] **kyberturvallisuussertifioinnin myöntävien viranomaisten** ja toimialan kanssa;

3 a) suositella asianmukaisia teknisiä eritelmiä käytettäväksi eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien kehittämisessä 47 artiklan 1 kohdan b alakohdassa tarkoitetulla tavalla tapauksissa, joissa standardeja ei ole saatavilla;

3 b) edistää osaltaan riittävien arviointiin ja sertifiointiin liittyvien valmiuksien kehittämistä laatimalla ja julkaisemalla ohjeita sekä tukemalla jäsenvaltioita näiden pyynnöstä;

b) helpottaa tieto- ja viestintätekniikan **prosessien,** tuotteiden ja palvelujen riskinhallintaan ja turvallisuuteen liittyvien eurooppalaisten ja kansainvälisten standardien laatimista ja käyttöönottoa [...]**;**

b a) laatii yhteistyössä jäsenvaltioiden 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;

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

9 artikla

[...] ***Tietämys*** **ja** ***tiedotus*** [...]

Virasto

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 kyberturvallisuusuhista ja -poikkeamista kyberturvallisuuteen liittyvien uusien kehityssuuntausten kartoittamiseksi ja [...] **kyberturvallisuuspoikkeamien** ehkäisemiseksi;

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

d) kokoaa, järjestää ja saattaa yleisön saataville erityisen portaalin kautta unionin toimielimiltä, virastoilta ja elimiltä **sekä vapaaehtoisuuteen perustuen jäsenvaltioilta ja yksityisiltä ja julkisilta sidosryhmiltä** saatavaa ja jäsenvaltioiden ja julkisten ja yksityisten sidosryhmien saataville asettamaa tietoa [...] **kyberturvallisuudesta**;

e) [...]

f) kerää ja analysoi julkisesti saatavilla olevia tietoja merkittävistä poikkeamista ja kokoaa raportteja ohjeiden antamiseksi yrityksille ja kansalaisille kaikkialla unionissa.

g) [...].

9 a artikla

Tietoisuuden lisääminen ja koulutus

Virasto

a) lisää suuren yleisön tietoisuutta kyberturvallisuuteen liittyvistä riskeistä ja antaa yksittäisille käyttäjille ohjeita hyvistä käytännöistä kansalaisten ja organisaatioiden käyttöön;

b) järjestää yhteistyössä jäsenvaltioiden, unionin toimielinten, elinten ja virastojen sekä toimialan kanssa säännöllisiä tiedotuskampanjoita kyberturvallisuuden ja sen näkyvyyden parantamiseksi unionissa;

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

d) tukee entistä tiiviimpää kyberturvallisuuskoulutusta ja -tietoisuutta koskevaa yhteistyötä ja parhaiden käytäntöjen vaihtoa jäsenvaltioiden välillä helpottamalla kansallisten koulutusalan yhteyspisteiden verkoston luomista ja ylläpitoa.

10 artikla

[...] ***Tutkimus ja innovointi***

Tutkimuksen ja innovoinnin osalta virasto

a) antaa unionille ja jäsenvaltioille neuvoja kyberturvallisuusalan tutkimustarpeista ja -painopisteistä, jotta nykyisiin ja kehittyviin riskeihin ja uhkiin, 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 on näiden ohjelmien rahoituksen saajana.

11 artikla

[...] ***Kansainvälinen yhteistyö***

Virasto edesauttaa unionin pyrkimyksiä yhteistoimintaan kolmansien maiden ja kansainvälisten organisaatioiden kanssa kansainvälisen yhteistyön edistämiseksi kyberturvallisuuskysymyksissä muun muassa

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

b) helpottamalla parhaiden käytäntöjen vaihtoa [...] **asiaankuuluvissa kansainvälisissä yhteistyöverkostoissa**;

c) antamalla pyynnöstä asiantuntemusta komission käyttöön**;**

c a) tarjoamalla yhteistyössä 53 artiklan nojalla perustetun Euroopan kyberturvallisuuden sertifiointiryhmän kanssa neuvoja ja tukea komissiolle kysymyksissä, jotka liittyvät kolmansien maiden kanssa tehtäviin kyberturvallisuussertifikaattien vastavuoroista tunnustamista koskeviin sopimuksiin.

II LUKU
VIRASTON ORGANISAATIO

12 artikla

Rakenne

Viraston hallinto- ja johtamisrakenne muodostuu seuraavista:

a) johtokunta, jonka tehtävät vahvistetaan 14 artiklassa;

b) hallitus, jonka tehtävät vahvistetaan 18 artiklassa;

c) pääjohtaja, jonka velvollisuudet vahvistetaan 19 artiklassa; [...]

d) pysyvä sidosryhmä, jonka tehtävät vahvistetaan 20 artiklassa**;**

d a) kansallisten yhteyshenkilöiden verkosto, jonka tehtävät vahvistetaan 20 a artiklassa.

1 JAKSO
JOHTOKUNTA

13 artikla

Johtokunnan kokoonpano

1. Johtokuntaan kuuluu kustakin jäsenvaltiosta yksi edustaja ja kaksi komission nimittämää edustajaa. Kaikilla edustajilla on äänioikeus.

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

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

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

14 artikla

Johtokunnan tehtävät

1. Johtokunta

a) määrittelee viraston toiminnan yleiset suuntaviivat ja varmistaa, että virasto toimii tässä asetuksessa vahvistettujen sääntöjen ja periaatteiden mukaisesti; Se myös huolehtii viraston toiminnan johdonmukaisuudesta suhteessa jäsenvaltioiden toimintaan sekä unionin tason toimiin.

b) hyväksyy luonnoksen viraston yhtenäiseksi ohjelma-asiakirjaksi 21 artiklan mukaisesti ennen sen toimittamista komissiolle lausuntoa varten;

c) komission lausunnon huomioon ottaen hyväksyy viraston yhtenäisen ohjelma-asiakirjan jäsentensä kahden kolmasosan enemmistöllä ja 17 artiklan mukaisesti;

c a) valvoo yhtenäisen ohjelma-asiakirjan sisältämien monivuotisen ja vuotuisen ohjelman toteutusta;

d) hyväksyy jäsentensä kahden kolmasosan enemmistöllä viraston vuotuisen talousarvion ja hoitaa muita tehtäviä, jotka liittyvät viraston talousarvioon, III luvun mukaisesti;

e) arvioi ja hyväksyy viraston toimintaa koskevan vuotuisen konsolidoidun toimintakertomuksen ja toimittaa sen yhdessä arviointinsa kanssa seuraavan vuoden heinäkuun 1 päivään mennessä Euroopan parlamentille, neuvostolle, komissiolle ja tilintarkastustuomioistuimelle. Toimintakertomus sisältää tilinpäätöksen ja kuvauksen siitä, kuinka virasto on saavuttanut tulosindikaattorinsa. Toimintakertomus julkistetaan;

f) hyväksyy viraston varainhoitosäännöt 29 artiklan mukaisesti;

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

h) hyväksyy jäsentensä eturistiriitojen ehkäisemistä ja hallintaa koskevat säännöt;

i) 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;

j) hyväksyy työjärjestyksensä;

k) käyttää 2 kohdan mukaisesti viraston henkilöstön suhteen Euroopan unionin virkamiehiin sovellettavissa henkilöstösäännöissä nimittävälle viranomaiselle ja unionin muuta henkilöstöä koskevissa palvelussuhteen ehdoissa työsopimusten tekemiseen valtuutetulle viranomaiselle annettuja valtuuksia, jäljempänä 'nimittävän viranomaisen valtuudet';

l) vahvistaa henkilöstösääntöjen ja muuhun henkilöstöön sovellettavien palvelussuhteen ehtojen täytäntöönpanoa koskevat säännökset henkilöstösääntöjen 110 artiklassa säädettyä menettelyä noudattaen;

m) nimittää pääjohtajan ja jatkaa tarvittaessa tämän toimikautta tai erottaa tämän asetuksen 33 artiklan mukaisesti;

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

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

p) hyväksyy työjärjestelyistä sopimisen 7 ja 39 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 määritellään olosuhteet, joissa toimivallan siirto voidaan keskeyttää. Pääjohtajalla on valtuudet siirtää tämä toimivalta edelleen.

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

15 artikla

Johtokunnan puheenjohtaja

Johtokunta valitsee keskuudestaan puheenjohtajan ja varapuheenjohtajan jäsentensä kahden kolmasosan enemmistöllä neljän vuoden toimikaudeksi, joka 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.

16 artikla

Johtokunnan kokoukset

1. Johtokunta kokoontuu puheenjohtajansa kutsusta.

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

3. Pääjohtaja osallistuu johtokunnan kokouksiin ilman äänioikeutta.

4. Pysyvän sidosryhmän jäsenet voivat osallistua puheenjohtajan kutsusta johtokunnan kokouksiin ilman äänioikeutta.

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

6. Virasto vastaa johtokunnan sihteeristön tehtävistä.

17 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 kaikkien johtokunnan jäsenten kahden kolmasosan enemmistöä.

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

4. 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

18 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 19 artiklan mukaisesti, sanotun kuitenkaan rajoittamatta 19 artiklassa säädettyjä pääjohtajan tehtäviä.

3. Hallitukseen kuuluu viisi jäsentä, jotka nimitetään johtokunnan jäsenten keskuudesta ja joista yksi on johtokunnan puheenjohtaja, joka voi myös toimia hallituksen puheenjohtajana, ja yksi on komission edustaja. Pääjohtaja osallistuu hallituksen kokouksiin ilman 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. [...]

3 JAKSO
PÄÄJOHTAJA

19 artikla

Pääjohtajan tehtävät

1. Virastoa 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) viraston 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) viraston toimintaa koskevan vuotuisen konsolidoidun toimintakertomuksen **– myös 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 Euroopan petostentorjuntaviraston (OLAF) tutkimuksiin perustuvia jatkotoimia varten ja suunnitelman edistymisestä raportointi kahdesti vuodessa komissiolle ja säännöllisesti johtokunnalle;

h) virastoon sovellettavien varainhoitosääntöjen luonnoksen valmistelu;

i) viraston 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 virastolle ja sen esittäminen johtokunnalle hyväksyntää varten;

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

l a) säännöllinen tietojenvaihto unionin toimielinten, virastojen ja elinten kanssa näiden kyberturvallisuutta koskevista toimista, jotta varmistetaan johdonmukaisuus kehitettäessä ja pantaessa täytäntöön EU:n toimintapolitiikkaa;

m) muiden pääjohtajalle tällä asetuksella osoitettujen tehtävien hoito.

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

5. Pääjohtaja **voi asianmukaisen kustannus-hyötyanalyysin perusteella** päättää [...] **perustaa virastolle yhden tai useamman paikallistoimiston yhteen tai useampaan jäsenvaltioon, jos hän katsoo sen tarpeelliseksi viraston tehtävien tehokkaan ja toimivan toteuttamisen kannalta**. Ennen kuin pääjohtaja tekee päätöksen paikallistoimiston perustamisesta, hänen on **kuultava asianomaisia jäsenvaltioita, myös jäsenvaltiota, jossa viraston toimipaikka sijaitsee, sekä** hankittava ennakkosuostumus komissiolta **ja** johtokunnalta. **Jos pääjohtajan toteuttamassa asianomaisten jäsenvaltioiden kuulemisessa ei päästä sopimukseen, asia on saatettava neuvoston käsiteltäväksi.** Päätöksessä on määriteltävä paikallistoimistossa toteutettavien toimien laajuus siten, että vältetään tarpeettomia kustannuksia ja viraston hallinnollisten tehtävien päällekkäisyyttä.[...] **Kaikkien paikallistoimistojen henkilöstön kokonaismäärä [...] olisi pidettävä mahdollisimman vähäisenä, [...] eikä se saa ylittää [...] 40 prosenttia siihen jäsenvaltioon sijoitetun henkilöstön määrästä, jossa viraston toimipaikka sijaitsee. Yksittäisen paikallistoimiston henkilöstön määrä ei saa ylittää 10 prosenttia [...] siihen jäsenvaltioon sijoitetun henkilöstön määrästä, jossa viraston toimipaikka sijaitsee.**

4 JAKSO
PYSYVÄ SIDOSRYHMÄ

20 artikla

Pysyvä sidosryhmä

1. Johtokunta perustaa pääjohtajan esityksestä pysyvän sidosryhmän, joka koostuu asiaan liittyviä sidosryhmiä, kuten tieto- ja viestintätekniikan alaa, sähköisten viestintäverkkojen tai yleisön saatavilla olevien palvelujen tarjoajia**, keskeisten palvelujen tarjoajia** ja kuluttajajärjestöjä, edustavista tunnustetuista asiantuntijoista, tiedeyhteisöä edustavista kyberturvallisuusasiantuntijoista sekä [eurooppalaisesta sähköisen viestinnän säännöstöstä annetun direktiivin] mukaisesti ilmoitettujen toimivaltaisten viranomaisten sekä lainvalvonta- ja tietosuojaviranomaisten edustajista.

2. Pysyvän sidosryhmän menettelyt, jotka koskevat erityisesti ryhmän jäsenten lukumäärää, sen kokoonpanoa, johtokunnan suorittamaa ryhmän jäsenten nimeämistä, pääjohtajan tekemää esitystä sekä ryhmän toimintaa, määritellään viraston sisäisissä toimintasäännöissä ja julkaistaan.

3. Pysyvän sidosryhmän puheenjohtajana toimii pääjohtaja tai pääjohtajan tähän tehtävään tapauskohtaisesti nimeämä henkilö.

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

5. Pysyvä sidosryhmä neuvoo virastoa sen tehtävien hoidossa. Erityisesti se neuvoo pääjohtajaa tämän laatiessa esitystä viraston työohjelmaksi sekä yhteydenpidossa asianmukaisten sidosryhmien kanssa kaikissa työohjelmaan liittyvissä kysymyksissä.

5 a. Pysyvä sidosryhmä tiedottaa toiminnastaan johtokunnalle säännöllisesti.

4 A JAKSO
KANSALLISTEN YHTEYSHENKILÖIDEN VERKOSTO

20 a artikla

Kansallisten yhteyshenkilöiden verkosto

1. Johtokunta perustaa pääjohtajan esityksestä kansallisten yhteyshenkilöiden verkoston, joka koostuu jäsenvaltioiden edustajista.

2. Kansallisten yhteyshenkilöiden verkosto koostuu kaikkien jäsenvaltioiden edustajista. Kukin jäsenvaltio nimeää yhden edustajan. Verkoston kokouksia voidaan järjestää vaihtelevissa asiantuntijakokoonpanoissa.

3. Kansallisten yhteyshenkilöiden verkosto helpottaa ENISAn ja jäsenvaltioiden välistä tietojen vaihtoa. Erityisesti se tukee ENISAa levittämään toimintaansa, löydöksiään ja suosituksiaan asiaankuuluville sidosryhmille kaikkialle EU:hun.

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

5. Kansallisten yhteyshenkilöiden tiivis yhteistyö johtokunnassa toimivien maidensa edustajien kanssa ei saisi aiheuttaa sitä, että verkosto tekee päällekkäistä työtä johtokunnan tai muiden EU:n foorumien kanssa.

6. Kansallisten yhteyshenkilöiden verkoston tehtävät ja menettelyt määritellään viraston sisäisissä toimintasäännöissä ja julkaistaan.

5 JAKSO
TOIMINTA

21 artikla

Yhtenäinen ohjelma-asiakirja

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

2. Pääjohtaja laatii vuosittain luonnoksen yhtenäiseksi ohjelma-asiakirjaksi, joka sisältää monivuotisen ja vuotuisen ohjelman suunnitelmat ja vastaavan henkilöstö- ja resurssisuunnittelun, komission delegoidun asetuksen (EU) N:o 1271/2013[14] 32 artiklan mukaisesti ja ottaen huomioon komission esittämät ohjeet.

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

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

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 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.

---

[14] 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 virastolle 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 56 artiklassa tarkoitetun arvioinnin tulosten huomioon ottamiseksi.

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

23 artikla

Avoimuus

1. Viraston toiminnan on oltava mahdollisimman avointa sekä 25 artiklan mukaista.

2. Virasto varmistaa, että suuri yleisö ja kaikki asianomaiset tahot saavat asianmukaista, puolueetonta, luotettavaa ja helposti saatavissa olevaa tietoa erityisesti viraston työn tuloksista. Sen on myös julkistettava 22 artiklan mukaisesti tehdyt sidonnaisuuksia koskevat ilmoitukset.

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

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

24 artikla

Luottamuksellisuus

1. Virasto ei saa paljastaa kolmansille osapuolille käsittelemiään ja saamiaan tietoja, joiden käsittelystä osittain tai kokonaisuudessaan luottamuksellisina on esitetty perusteltu pyyntö, sanotun kuitenkaan rajoittamatta 25 artiklan soveltamista.

2. Johtokunnan jäsenten, pääjohtajan, pysyvän sidosryhmän jäsenten, tilapäisiin työryhmiin osallistuvien ulkopuolisten asiantuntijoiden sekä viraston henkilöstön, mukaan lukien ne toimihenkilöt, jotka on otettu palvelukseen jäsenvaltioiden tilapäisesti lähettäminä virkamiehinä, on myös tehtäviensä päätyttyä noudatettava Euroopan unionin toiminnasta tehdyn sopimuksen 339 artiklan mukaista salassapitovelvollisuutta.

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

4. Johtokunta päättää antaa virastolle luvan käsitellä turvallisuusluokiteltua tietoa, jos viraston tehtävien suorittaminen sitä edellyttää. Tässä tapauksessa johtokunnan on yhteisymmärryksessä komission yksiköiden kanssa vahvistettava sisäiset toimintasäännöt soveltaen tietoturvan periaatteita, jotka on vahvistettu komission päätöksissä (EU, Euratom) 2015/443[15] ja 2015/444[16]. Nämä säännöt koskevat muun muassa turvallisuusluokiteltujen tietojen vaihtamista, käsittelyä ja tallentamista.

---

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

16 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).

25 artikla

Asiakirjojen julkisuus

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

2. Johtokunta vahvistaa järjestelyt asetuksen (EY) N:o 1049/2001 täytäntöönpanemiseksi kuuden kuukauden kuluessa viraston perustamisesta.

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

III LUKU
TALOUSARVION LAATIMINEN JA RAKENNE

26 artikla

Talousarvion laatiminen

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

2. Johtokunta laatii 1 kohdassa tarkoitetun tuloja ja menoja koskevan ennakkoarvioesityksen pohjalta vuosittain viraston tulo- ja menoarvion seuraavaa varainhoitovuotta varten.

3. Johtokunta toimittaa 2 kohdassa tarkoitetun tulo- ja menoarvion, joka on osa yhtenäisen ohjelma-asiakirjan luonnosta, vuosittain viimeistään tammikuun 31 päivänä komissiolle ja niille kolmansille maille, joiden kanssa unioni on tehnyt sopimukset 39 artiklan mukaisesti.

4. Komissio ottaa unionin talousarviota koskevaan esitykseen kyseiseen tulo- ja menoarvioon perustuvat arviot, joita se pitää henkilöstötaulukon ja yleisestä talousarviosta suoritettavan rahoitusosuuden määrän osalta välttämättöminä, ja toimittaa talousarvioesityksen Euroopan parlamentille ja neuvostolle Euroopan unionin toiminnasta tehdyn sopimuksen 313 ja 314 artiklan mukaisesti.

5. Euroopan parlamentti ja neuvosto hyväksyvät virastolle annettavaa rahoitusosuutta koskevat määrärahat.

6. Euroopan parlamentti ja neuvosto vahvistavat viraston henkilöstötaulukon.

7. Johtokunta vahvistaa yhtenäisen ohjelma-asiakirjan ohella viraston talousarvion. Siitä tulee lopullinen, kun unionin yleinen talousarvio on lopullisesti vahvistettu. Johtokunta mukauttaa tarvittaessa viraston talousarviota ja yhtenäistä ohjelma-asiakirjaa unionin yleisen talousarvion mukaisesti.

27 artikla

Talousarvion rakenne

1. Sulkematta pois muita tulonlähteitä viraston tulot koostuvat seuraavista:

   a) rahoitusosuus unionin talousarviosta;

   b) tiettyjen menoerien rahoittamiseen osoitettavat tulot 29 artiklassa tarkoitettuja varainhoitosääntöjä noudattaen;

   c) unionin rahoitus, joka annetaan valtuutussopimusten tai kertaluonteisten avustusten muodossa 29 artiklassa tarkoitettujen varainhoitosääntöjen ja unionin politiikkoja tukeviin asianomaisiin välineisiin sovellettavien säännösten mukaisesti;

d) viraston toimintaan 39 artiklan mukaisesti osallistuvien kolmansien maiden rahoitusosuudet;

e) mahdolliset jäsenvaltioiden vapaaehtoiset rahoitusosuudet rahana tai luontoissuorituksina. Vapaaehtoisia rahoitusosuuksia suorittavat jäsenvaltiot eivät voi vaatia erityisoikeuksia tai -palveluja suorituksensa perusteella.

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

28 artikla

Talousarvion toteuttaminen

1. Pääjohtaja vastaa viraston talousarvion toteuttamisesta.

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

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

4. Saatuaan viraston alustavaa tilinpäätöstä koskevat tilintarkastustuomioistuimen huomautukset viraston tilinpitäjä laatii viraston lopullisen tilinpäätöksen omalla vastuullaan.

5. Pääjohtaja toimittaa lopullisen tilinpäätöksen johtokunnalle lausuntoa varten.

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

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

8. Tilinpitäjä toimittaa myös tilinpäätöstä koskevan vahvistuskirjeen tilintarkastustuomioistuimelle sekä tiedoksi komission tilinpitäjälle samana päivänä kuin lopullisen tilinpäätöksen.

9. Pääjohtaja julkistaa lopullisen tilinpäätöksen viimeistään seuraavan vuoden marraskuun 15 päivänä.

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 varainhoitoasetuksen 165 artiklan 3 kohdan mukaisesti Euroopan parlamentille tämän pyynnöstä kaikki kyseistä varainhoitovuotta koskevan vastuuvapausmenettelyn moitteettoman toteuttamisen edellyttämät tiedot.

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

29 artikla

Varainhoitosäännöt

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

30 artikla

Petostentorjunta

1. Helpottaakseen Euroopan parlamentin ja neuvoston asetuksen (EU, Euratom) N:o 883/2013[17] soveltamisalaan kuuluvien petosten, lahjonnan ja muiden laittomien toimien torjuntaa virasto liittyy kuuden kuukauden kuluessa päivästä, jona se aloittaa toimintansa, Euroopan petostentorjuntaviraston (OLAF) sisäisistä tutkimuksista 25 päivänä toukokuuta 1999 tehtyyn toimielinten väliseen sopimukseen ja antaa kaikkia viraston työntekijöitä koskevat asiaan liittyvät määräykset käyttäen kyseisen sopimuksen liitteessä olevaa mallia.

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

[17] 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).

3. OLAF voi tehdä tarkastuksia, myös paikalla suoritettavia tarkastuksia ja todentamisia, Euroopan parlamentin ja neuvoston asetuksen (EU, Euratom) N:o 883/2013 ja komission paikan päällä suorittamista tarkastuksista ja todentamisista Euroopan yhteisöjen taloudellisiin etuihin kohdistuvien petosten ja muiden väärinkäytösten estämiseksi 11 päivänä marraskuuta 1996 annetun neuvoston asetuksen (Euratom, EY) N:o 2185/96[18] säännösten ja niissä säädettyjen menettelyjen mukaisesti sen selvittämiseksi, onko viraston rahoittamaan avustukseen tai sopimukseen liittynyt unionin taloudellisia etuja vahingoittavia petoksia, lahjontaa tai muuta laitonta toimintaa.

4. Viraston 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.

IV LUKU
VIRASTON HENKILÖSTÖ

31 artikla

Yleiset säännökset

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

---

18 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).

32 artikla

Erioikeudet ja vapaudet

Virastoon ja sen henkilöstöön sovelletaan Euroopan unionista tehtyyn sopimukseen ja Euroopan unionin toiminnasta tehtyyn sopimukseen liitettyä Euroopan unionin erioikeuksista ja vapauksista tehtyä pöytäkirjaa N:o 7.

33 artikla

Pääjohtaja

1. Pääjohtaja otetaan palvelukseen viraston 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 viraston 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 **neljä** [...] vuotta. Toimikauden lopussa komissio laatii arvion, jossa otetaan huomioon pääjohtajan tehtävän hoidon arviointi ja viraston tulevat tehtävät ja haasteet.

6. Johtokunta tekee päätökset pääjohtajan nimittämisestä, toimikauden jatkamisesta tai erottamisesta äänivaltaisten jäsentensä kahden kolmasosan enemmistöllä.

7. Johtokunta voi komission ehdotuksesta, jossa otetaan huomioon 5 kohdassa tarkoitettu arviointi, jatkaa pääjohtajan toimikautta kerran enintään **neljäksi** [...] 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 ainoastaan johtokunnan päätöksellä [...].

34 artikla

Kansalliset asiantuntijat ja muu henkilöstö

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

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

V LUKU
YLEISET SÄÄNNÖKSET

35 artikla

Viraston oikeudellinen asema

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

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

3. Virastoa edustaa sen pääjohtaja.

36 artikla

Viraston vastuu

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

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

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

4. Euroopan unionin tuomioistuimella on tuomiovalta tällaisten vahinkojen korvaamista koskevissa riidoissa.

5. Viraston toimihenkilöiden henkilökohtaista vastuuta virastoa kohtaan säännellään sen henkilöstöön sovellettavissa asiaa koskevissa määräyksissä.

37 artikla

Kielijärjestelyt

1. Virastoon sovelletaan neuvoston asetusta N:o 1[19]. Jäsenvaltiot ja niiden nimeämät muut elimet voivat kääntyä viraston puoleen ja saada siltä vastauksen valitsemallaan unionin toimielinten virallisella kielellä.

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

38 artikla

Henkilötietojen suoja

1. Virastossa tapahtuvaan henkilötietojen käsittelyyn sovelletaan Euroopan parlamentin ja neuvoston asetusta (EY) N:o 45/2001[20].

2. Johtokunta hyväksyy asetuksen (EY) N:o 45/2001 24 artiklan 8 kohdassa tarkoitetut täytäntöönpanotoimenpiteet. Johtokunta voi hyväksyä lisätoimenpiteitä, jotka ovat tarpeen viraston soveltaessa asetusta (EY) N:o 45/2001.

---

19 Asetus N:o 1 Euroopan atomienergiayhteisössä käytettäviä kieliä koskevista järjestelyistä (EYVL 17, 6.10.1958, s. 401).

20 Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001, annettu 18 päivänä joulukuuta 2000, yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (EYVL L 8, 12.1.2001, s. 1).

39 artikla

Yhteistyö kolmansien maiden ja kansainvälisten järjestöjen kanssa

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

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

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

40 artikla

Turvallisuusluokiteltujen ja arkaluonteisten turvallisuusluokittelemattomien tietojen suojaamista koskevat turvallisuussäännöt

Virasto hyväksyy komissiota kuullen turvallisuussääntönsä, joissa sovelletaan turvallisuutta koskevia periaatteita, jotka sisältyvät komission päätöksissä (EU, Euratom) 2015/443 ja 2015/444 vahvistettuihin Euroopan unionin turvallisuusluokiteltujen tietojen ja arkaluonteisten turvallisuusluokittelemattomien tietojen suojaamista koskeviin komission turvallisuussäännöksiin. Tämä koskee muun muassa tällaisten tietojen vaihtamista, käsittelyä ja tallentamista.

41 artikla

Päätoimipaikkaa koskeva sopimus ja toimintaedellytykset

1. Vastaanottavan jäsenvaltion virastolle tarjoamia tiloja ja palveluja koskevat tarvittavat järjestelyt sekä pääjohtajaan, johtokunnan jäseniin, viraston henkilöstöön ja heidän perheenjäseniinsä vastaanottavassa jäsenvaltiossa sovellettavat erityissäännöt vahvistetaan viraston ja vastaanottavan jäsenvaltion välisessä toimipaikkaa koskevassa sopimuksessa, joka tehdään sen jälkeen kun johtokunta on sen hyväksynyt ja viimeistään [2 vuotta tämän asetuksen voimaantulon jälkeen].

2. Viraston vastaanottavan jäsenvaltion on tarjottava [...] edellytykset viraston moitteettomalle toiminnalle, mukaan lukien toimivat liikenneyhteydet sijaintipaikalle, henkilöstön jäsenten lapsille soveltuvat koulunkäyntimahdollisuudet, puolisoiden mahdollisuudet päästä työmarkkinoille sekä riittävä sosiaaliturvan ja terveydenhuoltopalvelujen saatavuus lapsille ja puolisoille.

42 artikla

Hallinnollinen valvonta

Oikeusasiamies valvoo viraston toimintaa Euroopan unionin toiminnasta tehdyn sopimuksen 228 artiklan mukaisesti.

III OSASTO
KYBERTURVALLISUUDEN SERTIFIOINTIKEHYS

43 artikla

Eurooppalainen kyberturvallisuuden sertifiointikehys […]

1. **Eurooppalainen kyberturvallisuuden sertifiointikehys perustetaan, jotta voidaan nostaa kyberturvallisuustasoa unionissa ja siten parantaa sisämarkkinoiden toimintaedellytyksiä. Siinä määritellään hallintotapa, jonka avulla voidaan yhdenmukaistaa eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät EU:n tasolla. Tavoitteena on luoda tieto- ja viestintätekniikan prosesseille, tuotteille ja palveluille digitaaliset sisämarkkinat.**

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

44 artikla

Eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän valmistelu ja hyväksyminen

1. Kun komissio **tai 53 artiklan nojalla perustettu Euroopan kyberturvallisuuden sertifiointiryhmä, jäljempänä 'sertifiointiryhmä',** on esittänyt asiaa koskevan pyynnön, ENISA valmistelee ehdolla olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän, joka täyttää tämän asetuksen 45, 46 ja 47 artiklassa esitetyt vaatimukset.[...]

1 a. Jäsenvaltiot tai asianomaisia sidosryhmiä edustavat organisaatiot voivat esittää sertifiointiryhmälle ehdolla olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän valmistelemista. Sertifiointiryhmä arvioi ehdotuksia 53 artiklan 3 kohdan c a alakohdassa annettujen ohjeiden mukaisesti määrittelemiensä perusteiden pohjalta ja voi pyytää ENISAa valmistelemaan ehdolla olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän.

2. Valmistellessaan tämän artiklan 1 kohdassa tarkoitettuja ehdolla olevia järjestelmiä ENISA kuulee kaikkia asiaankuuluvia sidosryhmiä **avoimesti** ja tekee tiivistä yhteistyötä sertifiointiryhmän kanssa. Sertifiointiryhmä antaa ENISAlle ehdolla olevan järjestelmän valmisteluun liittyvää apua ja asiantuntijaneuvontaa [...] **ja antaa ehdolla olevasta järjestelmästä lausunnon, ennen kuin ehdotus toimitetaan komissiolle** [...]. **ENISA varmistaa, että ehdolla olevat järjestelmät ovat yhdenmukaisia vaatimustenmukaisuuden arviointilaitoksen akkreditointiin sovelletun yhdenmukaistetun standardin kanssa.**

3. ENISA **ottaa mahdollisimman tarkasti huomioon sertifiointiryhmän kannan, ennen kuin se toimittaa** tämän artiklan 2 kohdan mukaisesti valmistellun [...] ehdolla olevan [...] järjestelmän komissiolle.

4. Komissio voi ENISAn valmisteleman ehdolla olevan järjestelmän pohjalta hyväksyä 55 artiklan 2 kohdan mukaisesti täytäntöönpanosäädöksiä tieto- ja viestintätekniikan **prosessien,** tuotteiden ja palvelujen eurooppalaisista kyberturvallisuuden sertifiointijärjestelmistä, jotka täyttävät tämän asetuksen 45, 46 ja 47 artiklan vaatimukset.

5. [...]

44 a artikla

Eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän ylläpito

1. Virasto ylläpitää erityistä verkkosivustoa, jolla annetaan tietoa eurooppalaisista kyberturvallisuuden sertifiointijärjestelmistä, sertifikaateista ja 47 a artiklan nojalla myönnetyistä EU-vaatimustenmukaisuusilmoituksista ja tehdään niitä tunnetuiksi.

2. Viraston olisi tiiviissä yhteistyössä sertifiointiryhmän kanssa vähintään joka viides vuosi tarkistettava hyväksytyt eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät ja otettava tässä huomioon asianomaisten osapuolten palaute. Komissio tai sertifiointiryhmä voi tarvittaessa pyytää virastoa aloittamaan tarkistetun ehdolla olevan järjestelmän kehittämisen 44 artiklan 2 ja 3 kohdan mukaisesti.

45 artikla

Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien turvallisuustavoitteet

Eurooppalainen kyberturvallisuuden sertifiointijärjestelmä olisi suunniteltava siten, että se täyttää [...] soveltuvin osin seuraavat turvallisuustavoitteet:

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

b)

tallennetut, siirretyt tai muulla tavoin käsitellyt tiedot suojataan vahingossa tapahtuvalta tai luvattomalta tuhoamiselta, [...] katoamiselta tai muuttamiselta **taikka huonolta saatavuudelta prosessin, tuotteen tai palvelun koko elinkaaren ajan**;

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

d) **järjestelmään tallentuu** tieto siitä, [...] **mitä tietoja, toimintoja tai palveluja on käytetty, hyödynnetty tai muutoin käsitelty, sekä näiden toimien** ajankohta ja tekijä;

e) [...] on mahdollista tarkastaa, mitä tietoja, palveluja tai toimintoja on käytetty [...]**, hyödynnetty tai muutoin käsitelty, sekä näiden toimien ajankohta ja tekijä**;

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

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

g a) tieto- ja viestintätekniikan prosessit, tuotteet ja palvelut kehitetään, valmistetaan ja toimitetaan niitä koskevassa järjestelmässä esitettyjen turvallisuusvaatimusten mukaisesti.

46 artikla

Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien varmuustasot

1. Eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan määritellä tieto- ja viestintätekniikan **prosesseille,** tuotteille ja palveluille yksi tai useampi varmuustaso: perustaso, korotettu ja/tai korkea [...]. **Varmuustason on vastattava tieto- ja viestintätekniikan prosessin, tuotteen tai palvelun aiottuun käyttöön liittyvän riskin tasoa.**

2. Varmuustasot perustaso, korotettu ja korkea [...]**viittaavat eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän perusteella myönnettyyn sertifikaattiin tai EU-vaatimustenmukaisuusilmoitukseen. Järjestelmässä määritellään kunkin varmuustason turvallisuusvaatimukset, mukaan lukien turvallisuustoiminnot, ja niitä vastaava tieto- ja viestintätekniikan prosessin, tuotteen tai palvelun arvioinnin tarkkuus. Sertifikaattia tai EU-vaatimustenmukaisuusilmoitusta luonnehditaan suhteessa siihen liittyviin teknisiin eritelmiin, standardeihin ja menettelyihin sekä teknisiin tarkastuksiin, joiden tarkoituksena on vähentää kyberturvallisuuspoikkeamien riskiä tai ehkäistä niitä seuraavasti:**

a) varmuustasoon "perustaso" **viittaava eurooppalainen kyberturvallisuussertifikaatti tai EU-vaatimustenmukaisuusilmoitus antaa varmuuden siitä, että tieto- ja viestintätekniikan prosessit, tuotteet ja palvelut täyttävät vastaavat turvallisuusvaatimukset, myös turvallisuustoimintojen osalta, ja että ne on arvioitu tasolla, jolla pyritään vähentämään tunnettuja perustason kyberturvallisuuspoikkeamien ja kyberhyökkäysten riskejä. Arvioinnissa on vähintään arvioitava tekniset asiakirjat, tai jos tätä ei voida soveltaa, arvioinnin on sisällettävä vaikutukseltaan vastaavat korvaavat toimet** [...];

b) varmuustasoon "korotettu" **viittaava eurooppalainen kyberturvallisuussertifikaatti antaa varmuuden siitä, että tieto- ja viestintätekniikan prosessit, tuotteet ja palvelut täyttävät vastaavat turvallisuusvaatimukset, myös turvallisuustoimintojen osalta, ja että ne on arvioitu tasolla, jolla pyritään vähentämään tunnettuja kyberriskejä, kyberturvallisuuspoikkeamia ja sellaisten tahojen tekemien kyberhyökkäysten vaikutuksia, joilla on niukat kyvyt ja resurssit. Arvioinnissa on vähintään arvioitava julkisesti tiedossa olevien haavoittuvuuksien soveltumattomuus ja testattava, toteuttavatko tieto- ja viestintätekniikan prosessit, tuotteet tai palvelut välttämättömät turvallisuustoiminnot oikein; jos tätä ei voida soveltaa, arvioinnin on sisällettävä vaikutukseltaan vastaavat korvaavat toimet** [...];

c) varmuustasoon "korkea" **viittaava eurooppalainen kyberturvallisuussertifikaatti antaa varmuuden siitä, että tieto- ja viestintätekniikan prosessit, tuotteet ja palvelut täyttävät vastaavat turvallisuusvaatimukset, myös turvallisuustoimintojen osalta, ja että ne on arvioitu tasolla, jolla pyritään vähentämään sellaisten tahojen tekemien uusinta tekniikkaa hyödyntävien kyberhyökkäysten riskiä, joilla on merkittävät kyvyt ja resurssit. Arvioinnissa on vähintään arvioitava julkisesti tiedossa olevien haavoittuvuuksien soveltumattomuus; testattava, toteuttavatko tieto- ja viestintätekniikan prosessit, tuotteet tai palvelut välttämättömät turvallisuustoiminnot oikein ja hyödynnetäänkö niissä uusinta tekniikkaa; sekä arvioitava penetraatiotestauksen avulla kyseisten prosessien, tuotteiden tai palveluiden kykyä vastustaa kyvykkäitä hyökkääjiä; jos tätä ei voida soveltaa, arvioinnin on sisällettävä vaikutukseltaan vastaavat korvaavat toimet** [...].

2 a. Eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan määritellä useita arviointitasoja arviointimenetelmien tiukkuuden ja kattavuuden mukaan. Kunkin arviointitason tulee vastata yhtä varmuustasoa, ja arviointitasot on määriteltävä varmuuden osatekijöiden asianmukaisen yhdistelmän perusteella.

47 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 **prosessien,** tuotteiden, ja palvelujen tyyppi tai luokat **sekä selostus siitä, miten sertifiointijärjestelmä soveltuu oletettujen kohderyhmien tarpeisiin**;

b) [...] viittaus [...] kansainvälisiin**, eurooppalaisiin tai kansallisiin** standardeihin, **joita arvioinnissa on noudatettu. Jos standardeja ei ole saatavilla, viitataan** [...] teknisiin eritelmiin, **jotka täyttävät asetuksen 1025/2012 liitteen II vaatimukset, tai jos tällaisiakaan ei ole saatavilla, viitataan järjestelmässä määriteltyihin teknisiin eritelmiin tai muihin kyberturvallisuusvaatimuksiin**;

c) soveltuvin osin yksi tai useampi varmuustaso;

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

d) yksittäiset arvioinnissa käytettävät perusteet ja menetelmät, mukaan lukien arvioinnin tyypit, jotta voidaan osoittaa, että 45 artiklassa tarkoitetut erityiset tavoitteet saavutetaan;

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

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

g) [...] säännöt sertifikaattien **tai EU-vaatimustenmukaisuusilmoituksen** vaatimustenmukaisuuden seurantaa varten ja mekanismit, joilla voidaan osoittaa, että määriteltyjä kyberturvallisuusvaatimuksia noudatetaan jatkuvasti;

h) **soveltuvin osin** ehdot **sertifikaatin** myöntämiselle **ja uusimiselle sekä** sertifioinnin soveltamisalan voimassa pitämiselle, jatkamiselle, laajentamiselle **tai** supistamiselle;

i) säännöt seurauksista tapauksissa, joissa sertifioidut **tai itsearvioidut** tieto- ja viestintätekniikan tuotteet ja palvelut eivät vastaa [...] **järjestelmässä määriteltyjä** vaatimuksia;

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

k) **soveltuvin osin** säännöt tietojen säilyttämisestä vaatimustenmukaisuuden arviointilaitoksissa;

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

m) myönnetyn sertifikaatin **tai EU-vaatimustenmukaisuusilmoituksen** sisältö;

m a) EU-vaatimustenmukaisuusilmoituksen ja kaikki tieto- ja viestintätekniikan tuotteiden ja palveluiden valmistajan tai tarjoajan toimittamat asiaan liittyvät tiedot sisältävien teknisten asiakirjojen säilytysaika;

m b[...]) sertifikaattien enimmäisvoimassaoloaika;

m c[...]) myönnettyjä, muutettuja ja peruutettuja sertifikaatteja koskeva julkistamispolitiikka;

m d[...]) kolmansien maiden kanssa suoritettavan sertifiointijärjestelmien vastavuoroisen tunnustamisen edellytykset;

m e[...]) soveltuvin osin säännöt, jotka koskevat korkean varmuustason [...] eurooppalaisia kyberturvallisuussertifikaatteja 48 artiklan 4 a kohdan nojalla myöntäville elimille tarkoitettua vertaisarviointimekanismia.

2. Järjestelmälle 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 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.

47 a artikla

Vaatimustenmukaisuuden itsearviointi

1. Eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan sallia, että vaatimustenmukaisuuden arviointi on pelkästään tieto- ja viestintätekniikan tuotteiden ja palvelujen valmistajan tai tarjoajan vastuulla. Tällaista vaatimustenmukaisuuden arviointia voidaan soveltaa vain varmuustasoltaan perustason tieto- ja viestintätekniikan tuotteisiin ja palveluihin, joihin liittyvät riskit ovat vähäiset.

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

3. Tieto- ja viestintätekniikan tuotteiden ja palvelujen valmistaja tai tarjoaja pitää EU-vaatimustenmukaisuusilmoituksen ja kaikkia järjestelmässä määriteltyä tieto- ja viestintätekniikan tuotteiden ja palvelujen vaatimustenmukaisuutta koskevia tietoja sisältävät tekniset asiakirjat 50 artiklan 1 kohdassa tarkoitetun kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen saatavilla asiaankuuluvassa eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä määritetyn ajanjakson ajan. Jäljennös EU-vaatimustenmukaisuusilmoituksesta toimitetaan kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle ja ENISAlle.

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

5. Tämän artiklan nojalla myönnetty EU-vaatimustenmukaisuusilmoitus on tunnustettava kaikissa jäsenvaltioissa.

48 artikla

Kyberturvallisuussertifiointi

1. Tieto- ja viestintätekniikan **prosessit,** tuotteet ja palvelut, jotka on sertifioitu jossain 44 artiklan mukaisesti hyväksytyssä eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä, katsotaan kyseisen järjestelmän vaatimusten mukaisiksi.

2. Sertifiointi on vapaaehtoinen, jollei unionin **tai jäsenvaltioiden** lainsäädännössä toisin säädetä.

3. Tämän artiklan mukaisen**, varmuustasoon perustaso tai korotettu viittaavan** eurooppalaisen kyberturvallisuussertifikaatin antavat 51 artiklassa tarkoitetut vaatimustenmukaisuuden arviointilaitokset perustuen kriteereihin, jotka sisältyvät 44 artiklan mukaisesti hyväksyttyyn eurooppalaiseen kyberturvallisuuden sertifiointijärjestelmään.

4. Poiketen siitä, mitä 3 kohdassa säädetään, asianmukaisesti perustelluissa tapauksissa yksittäisessä eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan määrätä, että järjestelmästä saatavan eurooppalaisen kyberturvallisuussertifikaatin voi myöntää vain julkinen elin. Tämän [...] elimen on oltava joko

a) 50 artiklan 1 kohdassa tarkoitettu kansallinen [...] **kyberturvallisuussertifioinnin myöntävä viranomainen tai**

b) 51 artiklan 1 kohdan nojalla vaatimustenmukaisuuden arviointilaitoksena akkreditoitu **julkinen** elin [...].

c) [...]

4 a. Tapauksissa, joissa 44 artiklan mukainen eurooppalainen kyberturvallisuuden sertifiointijärjestelmä edellyttää varmuustasoa korkea, sertifikaatin voi myöntää vain 50 artiklan 1 kohdassa tarkoitettu kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen tai seuraavin edellytyksin 51 artiklassa tarkoitettu vaatimustenmukaisuuden arviointilaitos:

a) kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen hyväksyy ennalta kunkin yksittäisen, vaatimustenmukaisuuden arviointilaitoksen myöntämän sertifikaatin tai

b) kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen delegoi tämän tehtävän ennalta yleisesti vaatimustenmukaisuuden arviointilaitokselle.

5. Luonnollisen henkilön tai oikeushenkilön, joka jättää tieto- ja viestintätekniikan **prosessinsa,** tuotteensa tai palvelunsa sertifioitavaksi, on [...] **asetettava** 51 artiklassa tarkoitetun vaatimustenmukaisuuden arviointilaitoksen **tai 50 artiklassa tarkoitetun kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen, jos sertifikaatin myöntää kyseinen viranomainen,** saataville [...] kaikki sertifiointimenettelyn suorittamiseen tarvittavat tiedot.

5 a. Sertifikaatin haltija ilmoittaa sertifikaatin myöntävälle elimelle, jos myöhemmin ilmenee sertifioidun tieto- ja viestintätekniikan prosessin, tuotteen tai palvelun turvallisuutta koskevia haavoittuvuuksia tai epäsäännönmukaisuuksia, jotka saattavat vaikuttaa sertifiointiin liittyviin vaatimuksiin. Elin välittää tällaiset tiedot ilman aiheetonta viivytystä kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle.

6. Sertifikaatit myönnetään [...] **niitä koskevassa sertifiointijärjestelmässä määritellyksi ajaksi**, ja ne voidaan uusia [...], jos sovellettavat vaatimukset täyttyvät edelleen.

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

49 artikla

Kansalliset kyberturvallisuuden sertifiointijärjestelmät ja sertifikaatit

1. Sellaisia tieto- ja viestintätekniikan **prosesseja,** tuotteita ja palveluja varten voimassa olevat kansalliset kyberturvallisuuden sertifiointijärjestelmät ja niihin liittyvät menettelyt, jotka kuuluvat jonkin eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan, lakkaavat tuottamasta oikeusvaikutuksia alkaen päivästä, joka vahvistetaan 44 artiklan 4 kohdan nojalla hyväksytyssä täytäntöönpanosäädöksessä, sanotun kuitenkaan rajoittamatta 3 kohdan soveltamista. Sellaisia tieto- ja viestintätekniikan **prosesseja,** tuotteita ja palveluja **koskevat** 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 **prosesseille,** tuotteille ja palveluille, jotka kuuluvat 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.

50 artikla

Kansalliset [...] ***kyberturvallisuussertifioinnin myöntävät viranomaiset***

1. Kukin jäsenvaltio **nimeää vähintään yhden** kansallisen [...] **kyberturvallisuussertifioinnin myöntävän viranomaisen alueelleen tai keskinäisellä sopimuksella toisen jäsenvaltion kanssa nimeää vähintään yhden tähän toiseen jäsenvaltioon sijoittautuneen viranomaisen vastaamaan valvontatehtävistä omalla alueellaan**.

2. Kukin jäsenvaltio ilmoittaa komissiolle [...] **nimeämänsä viranomaisen ja tälle osoitetut tehtävät**.

3. **Rajoittamatta 48 artiklan 4 kohdan a alakohdan ja 48 artiklan 4 a kohdan soveltamista** [...] **kukin** kansallinen [...] **kyberturvallisuussertifioinnin myöntävä viranomainen** on organisaatioltaan, rahoituspäätöksiltään, oikeudelliselta rakenteeltaan ja päätöksenteoltaan riippumaton yksiköistä, joita ne valvovat.

3 a. Jäsenvaltiot varmistavat, että kansallisen kyberturvallisuussertifioinnin myöntävät viranomaiset noudattavat toiminnassaan, joka liittyy 48 artiklan 4 kohdan a alakohdan ja 48 artiklan 4 a kohdan mukaiseen sertifikaattien myöntämiseen, tehtävien ja vastuualueiden tiukkaa erottamista tämän artiklan mukaisesta valvontatoiminnasta ja että molemmat toiminnot ovat toisistaan riippumattomia.

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

5. Tämän asetuksen tehokkaan täytäntöönpanon varmistamiseksi on aiheellista, että kyseiset viranomaiset osallistuvat 53 artiklan nojalla perustettuun Euroopan kyberturvallisuuden sertifiointiryhmään aktiivisella, tehokkaalla ja turvallisella tavalla.

6. Kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten on

a) [...]

a a) seurattava tieto- ja viestintätekniikan tuotteiden ja palvelujen valmistajien tai tarjoajien velvollisuuksia, jotka on vahvistettu 47 a artiklan 2 ja 3 kohdassa sekä vastaavassa eurooppalaisen kyberturvallisuuden sertifiointijärjestelmässä, sekä valvottava näiden velvollisuuksien noudattamista;

b) [...] **51 artiklan 1 b kohdan soveltamista rajoittamatta avustettava kansallisia akkreditointielimiä näiden seuratessa ja valvoessa** vaatimustenmukaisuuden arviointilaitosten toimintaa tämän asetuksen soveltamiseksi [...];

b a) seurattava ja valvottava 48 artiklan 4 kohdassa tarkoitettujen elinten toimintaa;

b b) myönnettävä valtuudet 51 artiklan 1 b kohdassa tarkoitetuille vaatimustenmukaisuuden arviointilaitoksille ja rajoitettava myönnettyjä valtuutuksia taikka keskeytettävä tai peruttava ne, jos tässä asetuksessa vahvistetut vaatimukset eivät täyty;

c) käsiteltävä luonnollisten henkilöiden tai oikeushenkilöiden tekemät valitukset, jotka liittyvät kansallisten [...] **kyberturvallisuussertifioinnin myöntävien viranomaisten tai 48 artiklan 4 a kohdan mukaisesti vaatimustenmukaisuuden arviointilaitosten** myöntämiin sertifikaatteihin, tutkittava asianmukaisessa määrin valituksen kohde ja ilmoitettava valituksen tekijälle tutkinnan etenemisestä ja tuloksesta kohtuullisessa ajassa;

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

e) seurattava merkityksellistä kehitystä kyberturvallisuussertifioinnin alalla.

7. Kullakin kansallisella [...] **kyberturvallisuussertifioinnin myöntävällä viranomaisella** on oltava ainakin valtuudet

a) pyytää vaatimustenmukaisuuden arviointilaitoksilta**,** [...] eurooppalaisten 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-vaatimustenmukaisuusilmoitusten antajista** III osaston säännösten noudattamisen valvomiseksi;

c) toteuttaa asianmukaisia toimenpiteitä kansallisen lainsäädännön mukaisesti varmistaakseen, että vaatimustenmukaisuuden arviointilaitokset**,** [...] sertifikaattien 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 48 artiklan 4 a kohdan mukaisesti vaatimustenmukaisuuden arviointilaitoksen myöntämät** sertifikaatit, jotka eivät täytä tämän asetuksen tai eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaatimuksia;

f) määrätä seuraamuksia 54 artiklassa säädetyllä tavalla kansallisen lainsäädännön mukaisesti ja vaatia lopettamaan tässä asetuksessa säädettyjen velvoitteiden rikkominen välittömästi.

8. Kansallisten [...] **kyberturvallisuussertifioinnin myöntävien viranomaisten** on tehtävä yhteistyötä keskenään ja komission kanssa ja erityisesti vaihdettava tietoja, kokemuksia ja hyviä käytäntöjä tieto- ja viestintätekniikan **prosessien,** tuotteiden ja palvelujen kyberturvallisuussertifioinnista ja niiden kyberturvallisuuteen liittyvistä teknisistä kysymyksistä.

51 artikla

Vaatimustenmukaisuuden arviointilaitokset

1. Asetuksen (EY) N:o 765/2008 mukaisesti nimetyn kansallisen akkreditointielimen on akkreditoitava vaatimustenmukaisuuden arviointilaitokset vain, jos ne täyttävät tämän asetuksen liitteessä esitetyt vaatimukset.

1 a. Tilanteissa, joissa kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen antaa eurooppalaisen kyberturvallisuussertifikaatin 48 artiklan 4 kohdan a alakohdan ja 48 artiklan 4 a kohdan nojalla, kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen sertifiointielin akkreditoidaan tämän artiklan 1 kohdan nojalla vaatimustenmukaisuuden arviointilaitokseksi.

1 b. Kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen valtuuttaa soveltuvissa tapauksissa vaatimustenmukaisuuden arviointilaitokset suorittamaan tehtävänsä, jos ne täyttävät 47 artiklan 1 kohdan c a alakohdan mukaisessa eurooppalaisessa sertifiointijärjestelmässä annetut erityiset tai lisävaatimukset.

2. Akkreditointi myönnetään enintään viideksi vuodeksi, ja se voidaan uusia samoin edellytyksin, jos vaatimustenmukaisuuden arviointilaitos täyttää tässä artiklassa säädetyt vaatimukset. Akkreditointielimen on **kaikin asianmukaisin toimin kohtuullisessa ajassa rajoitettava tämän artiklan 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.

52 artikla

Ilmoittaminen

1. Kansallisten [...] **kyberturvallisuussertifioinnin myöntävien viranomaisten** on jokaisen 44 artiklan mukaisesti hyväksytyn eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän osalta ilmoitettava komissiolle [...] vaatimustenmukaisuuden arviointilaitoksista, jotka on akkreditoitu **ja soveltuvin osin 51 artiklan 1 b kohdan nojalla valtuutettu** myöntämään sertifikaatteja 46 artiklassa tarkoitetuilla määritellyillä varmuustasoilla, ja ilman aiheetonta viivytystä kaikista niiden myöhemmistä muutoksista.

2. Vuoden kuluttua eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän voimaantulosta komissio julkaisee luettelon 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 2 kohdassa tarkoitettuun luetteloon kahden kuukauden kuluessa kyseisen ilmoituksen vastaanottamisesta.

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

5. Komissio voi täytäntöönpanosäädöksillä määritellä olosuhteet, muotoseikat ja menettelyt tämän artiklan 1 kohdassa tarkoitetuille ilmoituksille. Nämä täytäntöönpanosäädökset hyväksytään 55 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

53 artikla

Euroopan kyberturvallisuuden sertifiointiryhmä

1. Perustetaan Euroopan kyberturvallisuuden sertifiointiryhmä, jäljempänä 'sertifiointiryhmä'.

2. Ryhmä muodostetaan kansallisten [...] **kyberturvallisuussertifioinnin myöntävien viranomaisten tai muiden asiaankuuluvien kansallisten viranomaisten edustajista**. [...]**Kukin ryhmän jäsen voi edustaa enintään yhtä jäsenvaltiota**.

3. Sertifiointiryhmän tehtävänä on

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

b) avustaa ja neuvoa ENISAa ja tehdä sen kanssa yhteistyötä ehdolla olevan järjestelmän valmistelemisessa tämän asetuksen 44 artiklan mukaisesti;

b a) antaa ehdolla olevasta järjestelmästä lausunto tämän asetuksen 44 artiklan mukaisesti;

c) [...] pyytää virastoa valmistelemaan ehdolla olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän tämän asetuksen 44 artiklan mukaisesti;

c a) kehittää ja ottaa käyttöön ohjeita, jotka koskevat sertifiointiryhmälle 44 artiklan 1 a kohdan nojalla toimitettujen ehdolla olevien järjestelmien valmisteluehdotusten arviointiperusteita;

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

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

f) helpottaa kansallisten [...] **kyberturvallisuussertifioinnin myöntävien viranomaisten** välistä, tämän osaston mukaista yhteistyötä **valmiuksien kehittämisen ja** tiedonvaihdon avulla erityisesti ottamalla käyttöön menetelmiä tietojen vaihtamiseksi tehokkaasti kaikista kyberturvallisuussertifiointia koskevista kysymyksistä**;**

f a) tukea vertaisarviointimekanismin täytäntöönpanoa tämän asetuksen 47 artiklan 1 kohdan m d alakohdan nojalla perustetussa eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä vahvistettujen sääntöjen mukaisesti.

4. Sertifiointiryhmän puheenjohtajana **(keskustelun vetäjänä)** ja sihteeristönä toimii komissio ENISAn avustuksella siten kuin 8 artiklan a alakohdassa säädetään.

53 a artikla

Oikeus tehdä valitus kansalliselle [...] kyberturvallisuussertifioinnin myöntävälle viranomaiselle

1. Luonnollisilla henkilöillä ja oikeushenkilöillä on oikeus tehdä kansalliselle kyberturvallisuussertifioinnin myöntävälle viranomaiselle valitus, joka liittyy kyseisen viranomaisen myöntämään sertifikaattiin tai vaatimustenmukaisuuden arviointilaitoksen 48 artiklan 4 a kohdan nojalla myöntämään sertifikaattiin.

2. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen, jolle valitus on jätetty, on ilmoitettava valituksen tekijälle valituksen etenemisestä ja ratkaisusta, mukaan lukien 53 b artiklan mukaisten oikeussuojakeinojen mahdollisuudesta.

53 b artikla

Oikeus tehokkaisiin oikeussuojakeinoihin

1. Luonnollisilla henkilöillä ja oikeushenkilöillä on oikeus tehokkaisiin oikeussuojakeinoihin itseään koskevaa kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen oikeudellisesti sitovaa päätöstä vastaan.

2. Luonnollisilla henkilöillä ja oikeushenkilöillä on oikeus tehokkaisiin oikeussuojakeinoihin, kun kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen ei käsittele valitusta.

3. Kanne kansallista kyberturvallisuussertifioinnin myöntävää viranomaista vastaan on nostettava sen jäsenvaltion tuomioistuimissa, johon viranomainen on sijoittautunut.

54 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 [viimeistään ... / viipymättä] ja ilmoitettava sille niihin vaikuttavista myöhemmistä muutoksista.

IV OSASTO
LOPPUSÄÄNNÖKSET

55 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**.

56 artikla

Arviointi ja uudelleentarkastelu

1. Komissio arvioi viimeistään viiden vuoden kuluttua 58 artiklassa tarkoitetusta päivämäärästä ja sen jälkeen viiden vuoden välein viraston ja sen työtapojen vaikutuksen, tehokkuuden ja tuloksellisuuden sekä mahdollisen tarpeen muuttaa viraston toimeksiantoa ja tällaisten muutosten taloudelliset vaikutukset. Arvioinnissa otetaan huomioon viraston toiminnastaan mahdollisesti saama palaute. Jos komissio katsoo, ettei viraston toiminnan jatkaminen ole enää perusteltua sille asetettuihin tavoitteisiin, toimeksiantoon ja tehtäviin nähden, se voi ehdottaa, että tätä asetusta muutetaan virastoa koskevien säännösten osalta.

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

3. Komissio toimittaa arviointikertomuksen ja päätelmänsä Euroopan parlamentille, neuvostolle ja johtokunnalle. Arvioinnin tulokset julkistetaan.

57 artikla

Kumoaminen ja seuraanto

1. Kumotaan asetus (EY) N:o 526/2013 [...] alkaen.

2. Viittaukset asetukseen (EY) N:o 526/2013 ja ENISAan katsotaan viittauksiksi tähän asetukseen ja virastoon.

3. Virasto toimii kaikkien omistusten, sopimusten, oikeudellisten velvoitteiden, työsopimusten, taloudellisten sitoumusten ja vastuiden osalta asetuksella (EY) N:o 526/2013 perustetun viraston seuraajana. Kaikki johtokunnan ja hallituksen voimassa olevat päätökset pysyvät voimassa edellyttäen, että ne eivät ole ristiriidassa tämän asetuksen säännösten kanssa.

4. Virasto perustetaan määrittelemättömäksi toimiajaksi [...] alkaen.

5. Asetuksen (EY) N:o 526/2013 24 artiklan 4 kohdan mukaisesti nimitetty pääjohtaja toimii viraston pääjohtajana jäljellä olevan toimikautensa ajan.

6. Asetuksen (EY) N:o 526/2013 6 artiklan mukaisesti nimitetyt johtokunnan jäsenet ja varajäsenet toimivat viraston johtokunnan jäseninä ja varajäseninä jäljellä olevan toimikautensa ajan.

58 artikla

Voimaantulo

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

1 a. Tätä asetusta sovelletaan [... päivästä ...kuuta ...] lukuun ottamatta 50–52, 53 a, 53 b ja 54 artiklaa, joita sovelletaan [24 kuukauden kuluttua siitä, kun asetus on julkaistu Euroopan unionin virallisessa lehdessä].

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

Tehty Brysselissä

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puhemies	*Puheenjohtaja*

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 viestintäteknisestä tuotteesta tai palvelusta riippumaton kolmas osapuoli.

3. Elintä, joka kuuluu yrittäjäjärjestöön tai ammattialajärjestöön, joka edustaa yrityksiä, jotka ovat osallisina elimen arvioimien tieto- ja viestintäteknisten tuotteiden tai palveluiden suunnittelussa, valmistuksessa, toimittamisessa, kokoamisessa, käytössä tai huoltamisessa, voidaan pitää vaatimustenmukaisuuden arviointilaitoksena sillä ehdolla, että osoitetaan sen riippumattomuus ja välttyminen eturistiriidoilta.

4. Vaatimustenmukaisuuden arviointilaitos, sen ylin johto ja vaatimustenmukaisuuden arviointitehtävien suorittamisesta vastaava henkilöstö eivät saa olla arvioitavien tieto- ja viestintäteknisten tuotteiden tai palveluiden suunnittelijoita, valmistajia, toimittajia, asentajia, ostajia, omistajia, käyttäjiä tai ylläpitäjiä taikka minkään tällaisen osapuolen valtuutettuja edustajia. Tämä ei sulje pois sellaisten arvioitujen tuotteiden käyttöä, jotka ovat vaatimustenmukaisuuden arviointilaitoksen toimien kannalta tarpeellisia, tai tällaisten tuotteiden käyttöä henkilökohtaisiin tarkoituksiin.

5. Vaatimustenmukaisuuden arviointilaitos, sen ylin johto ja vaatimustenmukaisuusarviointitehtävien suorittamisesta vastaava henkilöstö eivät myöskään saa olla suoranaisesti mukana näiden tieto- ja viestintäteknisten tuotteiden tai palveluiden suunnittelussa, valmistuksessa tai rakentamisessa, kaupan pitämisessä, asentamisessa, käytössä tai ylläpidossa eivätkä edustaa näissä toiminnoissa mukana olevia osapuolia. Ne eivät saa osallistua mihinkään toimintaan, joka voi olla ristiriidassa sen kanssa, että ne ovat arvioissaan riippumattomia, tai joka voi vaarantaa niiden riippumattomuuden niissä vaatimuksenmukaisuuden arviointitoimissa, joita varten ne on ilmoitettu. Tämä koskee erityisesti konsultointipalveluja.

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

7. 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.

8. 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.

9. Vaatimustenmukaisuuden arviointilaitoksella on kaikissa tapauksissa ja kunkin sellaisen vaatimustenmukaisuuden arviointimenettelyn ja kunkin tieto- ja viestintäteknisten tuotteiden tai palveluiden 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) 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 laitoksena suoritetut tehtävät ja muu toiminta;

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

10. 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.

11. Vaatimustenmukaisuuden arviointitoimien suorittamisesta vastaavalla henkilöstöllä on oltava:

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

b) riittävät tiedot suoritettavia 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 arvioinnit on suoritettu.

12. Vaatimustenmukaisuuden arviointilaitosten, niiden ylimmän johdon ja arviointihenkilöstön puolueettomuus on taattava.

13. Vaatimustenmukaisuuden arviointilaitoksen ylimmän johdon ja arviointihenkilöstön palkka ei saa olla riippuvainen suoritettujen arviointien määrästä eikä arviointien tuloksista.

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

15. Vaatimustenmukaisuuden arviointilaitosten henkilöstöllä on vaitiolovelvollisuus kaikkien niiden tietojen suhteen, joita se saa suorittaessaan tehtäviään tämän asetuksen tai sen täytäntöön panemiseksi annetun kansallisen lainsäädännön säännösten mukaisesti, paitsi niiden jäsenvaltioiden toimivaltaisiin viranomaisiin nähden, joissa laitoksen toimet suoritetaan.

16. Vaatimustenmukaisuuden arviointilaitosten on täytettävä **sellaisen asiaankuuluvan** standardin vaatimukset, **joka on yhdenmukaistettu asetuksessa (EY) 765/2008 prosessien, tuotteiden tai palvelujen sertifioinnista vastaavien vaatimustenmukaisuuden arviointilaitosten akkreditointia varten**[...].

17. Vaatimustenmukaisuuden arviointilaitosten on varmistettava, että vaatimustenmukaisuuden arvioinnissa käytettävät laboratoriot täyttävät **sellaisen asiaankuuluvan** standardin vaatimukset, **joka on yhdenmukaistettu asetuksessa (EY) 765/2008 testauksesta vastaavien laboratorioiden akkreditointia varten**[...].