



**2020/0359(COD)**

14.7.2021

## **LAUSUNTO**

sisämarkkina- ja kuluttajansuojavaliokunnalta

teollisuus-, tutkimus- ja energiavaliokunnalle

ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi toimenpiteistä yhteisen korkean kyberturvaston varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta (COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Valmistelija: Morten Løkkegaard

PA\_Legam

## LYHYET PERUSTELUT

Valmistelija suhtautuu yleisesti ottaen myönteisesti lainsäädäntöehdotukseen direktiiviksi toimenpiteistä korkean kyberturvatason varmistamiseksi koko unionissa (NIS 2). Valmistelija katsoo, että yhä digitalisoituneemmassa maailmassa verkkoturvallisuus on avainasemassa, jotta voidaan taata turvallinen digitaalinen ympäristö ja sisämarkkinoiden toiminta sekä kuluttajien ja talouden toimijoiden mahdollisuudet toimia niillä vapaasti.

NIS 2 -ehdotus on merkittävä parannus toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annettuun direktiiviin (EU) 2016/1148 (NIS 1) verrattuna. Siinä luetellaan NIS 1 -direktiivin keskeiset puutteet, kuten yritysten ja toimialojen heikko kyberuhkien sietokyky sekä erot häiriönsietokyvyssä ja heikko yhteinen tilannetietoisuus ja kyky yhteiseen reagointiin jäsenvaltioissa ja niiden välillä. Valmistelija suhtautuu myönteisesti pyrkimykseen korjata nämä puutteet NIS 2 -direktiivillä.

### **Soveltamisala**

Valmistelija arvostaa soveltamisalan laajentamista NIS 2 -ehdotuksessa ja erityisesti uusien alojen, kuten julkishallinnon, sisällyttämistä. Nimenomainen luettelo soveltamisalaan sisällytetyistä aloista ja palveluista vähentää varmasti jäsenvaltioiden harkintavaltaa direktiivin soveltamisalaan kuuluvien konkreettisten toimijoiden määrittelyssä ja vähentää siten sisämarkkinoiden hajanaisuutta.

Komissio ehdotti, että direktiivin soveltamisalaan kuuluvien alojen ja palvelujen sisällä sovelletaan kokokattosääntöä yhdenmukaisena kriteerinä, jolla määritetään direktiivin soveltamisalaan kuuluvat toimijat. Tämän kriteerin etuna on epäilemättä oikeusvarmuuden takaaminen ja jäsenvaltioiden välisten erojen vähentäminen.

Valmistelija suhtautuu myönteisesti laajennettuun alakohtaiseen soveltamisalaan mutta katsoo, että tähän yleiseen kriteeriin olisi yhdistettävä kunkin alan toimijoiden kriittisyyden arviointi. Näin keskisuuret ja suuret toimijat, joiden kriittisyyden tason katsotaan riskinarvioinnin perusteella olevan alhainen ja riippuvuuden muutoin kriittisistä toimijoista vähäinen, voitaisiin jättää direktiivin soveltamisalan ulkopuolelle.

Valmistelija korostaa, että tämän ei pitäisi katsoa avaavan oven jäsenvaltioiden välisille eriävillä tulkinnoille. Jotta tämä ei lisäisi täytäntöönpanon hajanaisuutta jäsenvaltioiden välillä, komissiota kannustetaan antamaan asiasta selkeitä ohjeita.

Valmistelija on tyytyväinen siihen, että mikro- ja pienyritykset on jätetty soveltamisalan ulkopuolelle, mutta katsoo, että on tarpeen kannustaa niiden vapaaehtoiseen sisällyttämiseen, sillä myös mikro- ja pientoimijat joutuvat kyberhyökkäysten kohteeksi ja niiden vaikutuspiiriin.

### **Koordinoidut kyberturvallisuuden sääntelykehykset**

Valmistelija panee tyytyväisenä merkille luvun, jossa määritellään kansallisten kyberturvallisuusstrategioiden ja niiden kriisinhallintavälineiden eri osatekijät. Ehdotetaan, että jäsenvaltiot ottavat osana kansallista kyberturvallisuusstrategiaansa käyttöön toimintaperiaatteet salaustekniikoiden ja salauksen käytön edistämiseksi erityisesti pk-yrityksissä.

Valmistelija pitää myönteisenä, että ENISA kehittää eurooppalaisen haavoittuvuusrekisterin, mutta pitää tärkeänä, että rekisteröinnissä noudatetaan liikesalaisuuksien luottamuksellisuutta eikä sillä rasiteta toimijoita tarpeettomasti.

### **Jäsenvaltioiden yhteistyö**

Erityisen tervetullutta NIS 2 -direktiivissä on jäsenvaltioiden jäsennellympi yhteistyö yhteistyöryhmässä, CSIRT-verkostossa ja vastaperustetussa laajamittaisia poikkeamia käsittelevässä ryhmässä. On kuitenkin tarpeen varmistaa, että jäsenvaltioiden luottamus toisiinsa ja halukkuus vaihtaa tietoja keskenään kasvaa, koska yhteistyön tehokkuus on keskeisessä asemassa varmistettaessa kyberturvallisuuden korkea taso EU:ssa.

Tämän kannan mukaisesti on laadittu tarkistuksia verkostojen roolin vahvistamiseksi. Valmistelija pitää erityisesti vertaisarviointeja hedelmällisenä tapana lisätä jäsenvaltioiden keskinäistä luottamusta ja kannattaa sitä, että niillä olisi oltava ratkaiseva rooli arvioitaessa yksittäisten jäsenvaltioiden kyberturvallisuushallinnan vaikuttavuutta.

### **Kyberturvallisuusriskien hallinta**

Valmistelija arvostaa riskinarvioinnin ulottamista koko toimitusketjuun (18 ja 19 artikla) mutta korostaa, että asiaa koskevaa kohtaa on selvennettävä, jotta voidaan antaa selkeitä ohjeita toimijoille, joita tämä vaatimus koskee, ja jäsenvaltioille, kun ne toteuttavat erityisen kriittisten alojen tai toimitusketjujen koordinoitua turvallisuusriskien arviointia.

### **Raportointivelvoitteet**

Valmistelija katsoo, että tarkistetun direktiivin tiettyjä kohtia olisi selkeytettävä. Ne koskevat pääasiassa joitakin NIS 2 -direktiivin soveltamisalaan kuuluville yrityksille asetettavia velvoitteita. Valmistelija on pyrkinyt vähentämään byrokratiaa ja helpottamaan uusien sääntöjen noudattamista yrityksissä pitäen mielessä lopullisen tavoitteen eli direktiivin tehokkaan täytäntöönpanon.

Valmistelija ehdottaa ensimmäisiä ilmoituksia koskevissa raportointivelvoitteissa ehdotetun 24 tunnin määräajan pidentämistä 72 tuntiin, jotta yritykset voivat puuttua tuloksellisesti meneillään olevaan kyberturvallisuushyökkäykseen ennen ilmoittamista. Lisäksi ehdotetaan, että poistetaan kaikki viittaukset ”mahdollisten poikkeamien” pakolliseen ilmoittamiseen.

## **TARKISTUKSET**

Sisämarkkina- ja kuluttajansuojavaliokunta pyytää asiasta vastaavaa teollisuus-, tutkimus- ja energiavaliokuntaa ottamaan huomioon seuraavat tarkistukset:

### **Tarkistus 1**

#### **Ehdotus direktiiviksi**

#### **Johdanto-osan 5 kappale**

*Komission teksti*

(5) Kaikki nämä erot aiheuttavat sisämarkkinoiden pirstoutumista ja voivat haitata niiden toimintaa, mikä vaikuttaa erityisesti rajat ylittävään palveluntarjontaan ja kyberturvatasoon, kun käytössä on toisistaan poikkeavia standardeja. Tällä direktiivillä pyritään poistamaan näitä suuria eroja jäsenvaltioiden välillä erityisesti vahvistamalla vähimmäissäännöt koordinoitun sääntelykehyksen toiminnalle, vahvistamalla mekanismit kunkin jäsenvaltion vastuuviranomaisten toimivaa yhteistyötä varten, päivittämällä luettelo aloista ja toiminnoista, joihin sovelletaan kyberturvavelvoitteita, ja säätämällä tehokkaista oikeussuojakeinoista ja seuraamuksista, jotka ovat olennaisen tärkeitä velvoitteiden tehokkaan täytäntöönpanon kannalta. Sen vuoksi direktiivi (EU) 2016/1148 olisi kumottava ja korvattava tällä direktiivillä.

*Tarkistus*

(5) Kaikki nämä erot aiheuttavat sisämarkkinoiden pirstoutumista ja voivat haitata niiden toimintaa, mikä vaikuttaa erityisesti rajat ylittävään palveluntarjontaan ja kyberturvatasoon, kun käytössä on toisistaan poikkeavia standardeja. Tällä direktiivillä pyritään poistamaan näitä suuria eroja jäsenvaltioiden välillä **ja lujittamaan sisämarkkinoita** erityisesti vahvistamalla vähimmäissäännöt koordinoitun sääntelykehyksen toiminnalle, vahvistamalla mekanismit kunkin jäsenvaltion vastuuviranomaisten toimivaa yhteistyötä varten, päivittämällä luettelo aloista ja toiminnoista, joihin sovelletaan kyberturvavelvoitteita, ja säätämällä tehokkaista oikeussuojakeinoista ja seuraamuksista, jotka ovat olennaisen tärkeitä velvoitteiden tehokkaan täytäntöönpanon kannalta. Sen vuoksi direktiivi (EU) 2016/1148 olisi kumottava ja korvattava tällä direktiivillä.

**Tarkistus 2**

**Ehdotus direktiiviksi**

**Johdanto-osan 6 a kappale (uusi)**

*Komission teksti*

*Tarkistus*

**(6 a) Tällä direktiivillä ei rajoiteta unionin lainsäädännössä vahvistettujen, henkilötietojen suojaa koskevien sääntöjen soveltamista.**

**Tarkistus 3**

**Ehdotus direktiiviksi**

**Johdanto-osan 9 kappale**

*Komission teksti*

*Tarkistus*

(9) Tämän direktiivin olisi kuitenkin katettava myös sellaiset pienet tai

(9) Tämän direktiivin olisi kuitenkin katettava myös sellaiset pienet tai

mikrotoimijat, jotka täyttävät tietyt kriteerit, jotka osoittavat niiden olevan avainasemassa jäsenvaltion taloudessa tai yhteiskunnassa tai tietyllä alalla tai tietäntyyppisissä palveluissa. Jäsenvaltioiden olisi vastattava tällaisten toimijoiden luettelon laatimisesta ja toimitettava se komissiolle.

mikrotoimijat, jotka täyttävät tietyt kriteerit, jotka osoittavat niiden olevan avainasemassa jäsenvaltion taloudessa tai yhteiskunnassa tai tietyllä alalla tai tietäntyyppisissä palveluissa. Jäsenvaltioiden olisi vastattava tällaisten toimijoiden luettelon laatimisesta ja toimitettava se komissiolle. **Komission olisi annettava selkeät ohjeet kriteereistä, joilla määritetään, mitkä pienet tai mikrotoimijat olisivat keskeisiä tai tärkeitä, erityisesti sellaisten toimijoiden osalta, jotka tarjoavat palveluja useissa jäsenvaltioissa.**

**Tarkistus 4**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 10 kappale**

*Komission teksti*

(10) **Komissio voi** yhteistyössä yhteistyöryhmän kanssa **antaa** ohjeita mikro- ja pienyrityksiin sovellettavien kriteerien käytöstä.

*Tarkistus*

(10) **Komission olisi** yhteistyössä yhteistyöryhmän kanssa **annettava** ohjeita mikro- ja pienyrityksiin sovellettavien kriteerien käytöstä.

**Tarkistus 5**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 12 a kappale (uusi)**

*Komission teksti*

(12 a) **Tämän direktiivin soveltamisalan laajentaminen johtaa alakohtaisen sääntelyn piiriin kuuluvien toimijoiden sisällyttämiseen siihen. Jotta vältetään kaikenlainen sääntelyn päällekkäisyys tai sääntelytaakka, komission olisi varmistettava, että alakohtaiset säädökset, joissa vaaditaan keskeisiä tai tärkeitä toimijoita joko hyväksymään kyberturvallisuusriskien hallintatoimenpiteitä tai ilmoittamaan poikkeamista tai merkittävistä kyberuhista, ovat tämän direktiivin mukaisia.**

*Tarkistus*

(12 a) **Tämän direktiivin soveltamisalan laajentaminen johtaa alakohtaisen sääntelyn piiriin kuuluvien toimijoiden sisällyttämiseen siihen. Jotta vältetään kaikenlainen sääntelyn päällekkäisyys tai sääntelytaakka, komission olisi varmistettava, että alakohtaiset säädökset, joissa vaaditaan keskeisiä tai tärkeitä toimijoita joko hyväksymään kyberturvallisuusriskien hallintatoimenpiteitä tai ilmoittamaan poikkeamista tai merkittävistä kyberuhista, ovat tämän direktiivin mukaisia.**

**Tarkistus 6**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 12 b kappale (uusi)**

*Komission teksti*

*Tarkistus*

**(12 b) Komission olisi julkaistava selkeät ohjeet tämän direktiivin ohessa, jotta autetaan varmistamaan täytäntöönpanon yhdenmukaistaminen kaikissa jäsenvaltioissa ja vältetään hajanaisuus.**

**Tarkistus 7**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 12 c kappale (uusi)**

*Komission teksti*

*Tarkistus*

**(12 c) Komission olisi myös laadittava ohjeistusta jäsenvaltioiden tukemiseksi soveltamisalaa koskevien säännösten asianmukaisessa täytäntöönpanossa ja tässä direktiivissä asetettujen velvoitteiden oikeasuhteisuuden arvioimisessa siten, että otetaan huomioon soveltamisalaan kuuluvien toimijoiden kriittisyys, erityisesti kun velvoitteita sovelletaan toimijoihin, joiden liiketoimintamallit tai toimintaympäristöt ovat monimutkaisia, jolloin toimija voi samanaikaisesti täyttää sekä keskeisille että tärkeille toimijoille asetetut kriteerit tai voi samanaikaisesti toteuttaa toimia, joista jotkut kuuluvat tämän direktiivin soveltamisalaan ja toiset eivät kuulu. Tapauksissa, joissa toimijoiden pääasiallinen toiminta ei kuulu tämän direktiivin soveltamisalaan mutta niiden toissijainen toiminta kuuluu, säännöksiä olisi sovellettava vain toimijan siihen toimintaan tai yksikköön, joka kuuluu tämän direktiivin soveltamisalaan.**

**Tarkistus 8**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 14 kappale**

*Komission teksti*

(14) Kyberturvallisuuden ja toimijoiden fyysisen turvallisuuden välisten yhteyksien vuoksi olisi varmistettava johdonmukainen lähestymistapa Euroopan parlamentin ja neuvoston direktiivin (EU) XXX/XXX<sup>17</sup> ja tämän direktiivin välillä. Tämän saavuttamiseksi jäsenvaltioiden olisi varmistettava, että direktiivin (EU) XXX/XXX mukaisia kriittisiä toimijoita ja vastaavia toimijoita pidetään tämän direktiivin mukaisina keskeisinä toimijoina. Jäsenvaltioiden olisi myös varmistettava, että niiden kyberturvallisuusstrategiat sisältävät puitteet tämän direktiivin ja direktiivin (EU) XXX/XXX mukaisen toimivaltaisen viranomaisen välisen koordinoinnin tehostamiselle poikkeamia ja kyberuhkia koskevan tietojenvaihdon ja valvontatehtävien hoitamisen yhteydessä. Molempien direktiivien nojalla nimettyjen viranomaisten olisi tehtävä yhteistyötä ja vaihdettava tietoja erityisesti kriittisten toimijoiden, kyberuhkien, kyberturvariskien ja kriittisiin toimijoihin vaikuttavien poikkeamien tunnistamisen sekä kriittisten toimijoiden kyberturvatoimenpiteiden suhteen. Direktiivin (EU) XXX/XXX mukaisten toimivaltaisten viranomaisten pyynnöstä tämän direktiivin mukaisten toimivaltaisten viranomaisten olisi voitava käyttää valvonta- ja täytäntöönpanovaltuuksiaan kriittiseksi määritellyn keskeisen toimijan osalta. Molempien viranomaisten olisi tehtävä yhteistyötä ja vaihdettava tietoja tätä tarkoitusta varten.

---

<sup>17</sup> [lisätään koko nimi ja EUVL:n julkaisuviite, kun ne ovat tiedossa]

*Tarkistus*

(14) Kyberturvallisuuden ja toimijoiden fyysisen turvallisuuden välisten yhteyksien vuoksi olisi varmistettava johdonmukainen lähestymistapa Euroopan parlamentin ja neuvoston direktiivin (EU) XXX/XXX<sup>17</sup> ja tämän direktiivin välillä. Tämän saavuttamiseksi jäsenvaltioiden olisi varmistettava, että direktiivin (EU) XXX/XXX mukaisia kriittisiä toimijoita ja vastaavia toimijoita pidetään tämän direktiivin mukaisina keskeisinä toimijoina. Jäsenvaltioiden olisi myös varmistettava, että niiden **kansalliset** kyberturvallisuusstrategiat sisältävät puitteet tämän direktiivin ja direktiivin (EU) XXX/XXX mukaisen toimivaltaisen viranomaisen välisen koordinoinnin tehostamiselle **poikkeamista raportoinnin**, poikkeamia, **läheltä piti -tilanteiden** ja kyberuhkia koskevan tietojenvaihdon ja valvontatehtävien hoitamisen yhteydessä. Molempien direktiivien nojalla nimettyjen viranomaisten olisi tehtävä yhteistyötä ja vaihdettava tietoja erityisesti kriittisten toimijoiden, kyberuhkien, kyberturvariskien ja kriittisiin toimijoihin vaikuttavien poikkeamien tunnistamisen sekä kriittisten toimijoiden kyberturvatoimenpiteiden suhteen. Direktiivin (EU) XXX/XXX mukaisten toimivaltaisten viranomaisten pyynnöstä tämän direktiivin mukaisten toimivaltaisten viranomaisten olisi voitava käyttää valvonta- ja täytäntöönpanovaltuuksiaan kriittiseksi määritellyn keskeisen toimijan osalta. Molempien viranomaisten olisi tehtävä yhteistyötä ja vaihdettava tietoja tätä tarkoitusta varten.

---

<sup>17</sup> [lisätään koko nimi ja EUVL:n julkaisuviite, kun ne ovat tiedossa]



**Tarkistus 9**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 15 kappale**

*Komission teksti*

(15) Luotettavan, häiriönsietokykyisen ja turvallisen verkkotunnusjärjestelmän (DNS) ylläpitäminen ja säilyttäminen on keskeinen tekijä internetin eheyden kannalta, ja olennaisen tärkeää internetin jatkuvan ja vakaan toiminnan kannalta, mistä koko digitaalitalous ja -yhteiskunta ovat riippuvaisia. Sen vuoksi tätä direktiiviä olisi sovellettava kaikkiin DNS-palvelujen tarjoajiin DNS-selvitysketjussa, mukaan lukien juuripalvelinten ylläpitäjät, ylätasen tunnusten nimipalvelimet (TLD), verkkotunnuksia vastaavia IP-osoitteita selvittävät auktoritatiiviset nimipalvelimet ja osoitteita ensin sisäisesti selvittävät rekursiiviset nimipalvelimet.

**Tarkistus 10**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 20 kappale**

*Komission teksti*

(20) Nämä kasvavat keskinäiset riippuvuussuhteet ovat tulosta yhä useammin rajat ylittävästä ja keskinäisriippuvaisesta palveluntarjontaverkostosta, jossa käytetään keskeisiä infrastruktuureja eri puolilla unionia energian, liikenteen, digitaalisen infrastruktuurin, juoma- ja jäteveden, terveyden, julkishallinnon tiettyjen näkökohtien alalla sekä

*Tarkistus*

(15) Luotettavan, häiriönsietokykyisen ja turvallisen verkkotunnusjärjestelmän (DNS) ylläpitäminen ja säilyttäminen on keskeinen tekijä internetin eheyden kannalta, ja olennaisen tärkeää internetin jatkuvan ja vakaan toiminnan kannalta, mistä koko digitaalitalous ja -yhteiskunta **sekä sisämarkkinat** ovat riippuvaisia. Sen vuoksi tätä direktiiviä olisi sovellettava kaikkiin DNS-palvelujen tarjoajiin DNS-selvitysketjussa, mukaan lukien juuripalvelinten ylläpitäjät, ylätasen tunnusten nimipalvelimet (TLD), verkkotunnuksia vastaavia IP-osoitteita selvittävät auktoritatiiviset nimipalvelimet ja osoitteita ensin sisäisesti selvittävät rekursiiviset nimipalvelimet **sekä yksityisyys- tai välityspalvelujen rekisteröintipalvelujen tarjoajat, verkkotunnusten välittäjät tai jälleenmyyjät ja kaikki muut palvelut, jotka liittyvät verkkotunnusten rekisteröintiin.**

*Tarkistus*

(20) Nämä kasvavat keskinäiset riippuvuussuhteet ovat tulosta yhä useammin rajat ylittävästä ja keskinäisriippuvaisesta palveluntarjontaverkostosta, jossa käytetään keskeisiä infrastruktuureja eri puolilla unionia energian, liikenteen, digitaalisen infrastruktuurin, juoma- ja jäteveden, terveyden, julkishallinnon tiettyjen näkökohtien alalla sekä

avaruustoiminnassa siltä osin kuin on kyse tiettyjen sellaisten palvelujen tarjoamisesta, jotka riippuvat joko jäsenvaltioiden tai yksityisten osapuolten omistamasta, hallinnoimasta ja käyttämästä maassa sijaitsevasta infrastruktuurista, eli lukuun ottamatta infrastruktuureja, jotka ovat unionin omistamia, hallinnoimia tai sen puolesta hallinnoituja osana sen avaruusohjelmia. Nämä keskinäiset riippuvuussuhteet merkitsevät sitä, että kaikilla häiriöillä, vaikka ne alun perin rajoittuisivatkin yhteen toimijaan tai yhteen toimialaan, voi olla ketjureaktiovaikutuksia, jotka voivat johtaa kauaskantoisiin ja pitkäaikaisiin kielteisiin vaikutuksiin palvelujen tarjontaan sisämarkkinoilla. Covid-19-pandemia on osoittanut yhä voimakkaammin keskinäisriippuvaisten yhteiskuntiemme haavoittuvuuden kohdatessamme alhaisen todennäköisyyden riskejä.

avaruustoiminnassa siltä osin kuin on kyse tiettyjen sellaisten palvelujen tarjoamisesta, jotka riippuvat joko jäsenvaltioiden tai yksityisten osapuolten omistamasta, hallinnoimasta ja käyttämästä maassa sijaitsevasta infrastruktuurista, eli lukuun ottamatta infrastruktuureja, jotka ovat unionin omistamia, hallinnoimia tai sen puolesta hallinnoituja osana sen avaruusohjelmia. Nämä keskinäiset riippuvuussuhteet merkitsevät sitä, että kaikilla häiriöillä, vaikka ne alun perin rajoittuisivatkin yhteen toimijaan tai yhteen toimialaan, voi olla ketjureaktiovaikutuksia, jotka voivat johtaa kauaskantoisiin ja pitkäaikaisiin kielteisiin vaikutuksiin palvelujen tarjontaan sisämarkkinoilla. Covid-19-pandemia on osoittanut yhä voimakkaammin keskinäisriippuvaisten yhteiskuntiemme haavoittuvuuden kohdatessamme alhaisen todennäköisyyden riskejä **ja tarpeen suojella sisämarkkinoita unionin tasolla yhteisten strategioiden ja toimien avulla.**

## **Tarkistus 11**

### **Ehdotus direktiiviksi**

### **Johdanto-osan 23 kappale**

#### *Komission teksti*

(23) Toimivaltaisten viranomaisten tai CSIRT-yksiköiden olisi saatava ilmoitukset poikkeamista toimijoilta toimivalla ja tehokkaalla tavalla. Keskitetyille yhteyspisteille olisi annettava tehtäväksi toimittaa poikkeamailmoitukset edelleen muiden asianomaisten jäsenvaltioiden keskitettyihin yhteyspisteisiin.

**Jäsenvaltioiden viranomaisten tasolla** sen varmistamiseksi, että jokaisessa jäsenvaltiossa on yksi keskitetty asiointipiste, yhteyspisteiden olisi myös oltava toimivaltaisten viranomaisten asetuksen XXXX/XXXX mukaisesti toimittamien, finanssialan yhteisöjä koskevia turvapoikkeamia koskevien asiaankuuluvien tietojen vastaanottajia,

#### *Tarkistus*

(23) Toimivaltaisten viranomaisten tai CSIRT-yksiköiden olisi saatava ilmoitukset poikkeamista toimijoilta **standardoidulla**, toimivalla ja tehokkaalla tavalla. Keskitetyille yhteyspisteille olisi annettava tehtäväksi toimittaa poikkeamailmoitukset edelleen muiden asianomaisten jäsenvaltioiden keskitettyihin yhteyspisteisiin. Sen varmistamiseksi, että jokaisessa jäsenvaltiossa on yksi keskitetty asiointipiste, yhteyspisteiden olisi myös oltava toimivaltaisten viranomaisten asetuksen XXXX/XXXX mukaisesti toimittamien, finanssialan yhteisöjä koskevia turvapoikkeamia koskevien asiaankuuluvien tietojen vastaanottajia, jotta ne voisivat tarvittaessa toimittaa nämä

jotta ne voisivat tarvittaessa toimittaa nämä tiedot eteenpäin tämän direktiivin mukaisille asiaankuuluville kansallisille toimivaltaisille viranomaisille tai CSIRT-yksiköille.

tiedot eteenpäin tämän direktiivin mukaisille asiaankuuluville kansallisille toimivaltaisille viranomaisille tai CSIRT-yksiköille.

**Tarkistus 12**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 25 kappale**

*Komission teksti*

(25) **Henkilötietojen osalta** CSIRT-yksiköiden olisi voitava Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679<sup>19</sup> mukaisesti tarjota tämän direktiivin nojalla tahon puolesta ja pyynnöstä **ennakoiva** skannaus verkko- ja tietojärjestelmistä, joita kyseinen taho käyttää palvelujensa tarjontaan. Jäsenvaltioiden olisi pyrittävä varmistamaan, että kaikilla toimialakohtaisilla CSIRT-yksiköillä on yhtäläiset tekniset valmiudet. Jäsenvaltiot voivat pyytää kansallisten CSIRT-yksiköiden kehittämisessä apua Euroopan unionin kyberturvallisuusvirastolta (ENISA).

---

<sup>19</sup> Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuojasetus) (EUVL L 119, 4.5.2016, s. 1).

**Tarkistus 13**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 26 a kappale (uusi)**

*Tarkistus*

(25) **Henkilötietoihin kohdistuvien erityisten uhkien tunnistamiseksi, lieventämiseksi tai ehkäisemiseksi** CSIRT-yksiköiden olisi voitava Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679<sup>19</sup> mukaisesti tarjota tämän direktiivin nojalla tahon puolesta ja pyynnöstä skannaus verkko- ja tietojärjestelmistä, joita kyseinen taho käyttää palvelujensa tarjontaan. Jäsenvaltioiden olisi pyrittävä varmistamaan, että kaikilla toimialakohtaisilla CSIRT-yksiköillä on yhtäläiset tekniset valmiudet. Jäsenvaltiot voivat pyytää kansallisten CSIRT-yksiköiden kehittämisessä apua Euroopan unionin kyberturvallisuusvirastolta (ENISA).

---

<sup>19</sup> Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuojasetus) (EUVL L 119, 4.5.2016, s. 1).

*(26 a) Jäsenvaltioiden olisi kansallisten kyberturvallisuusstrategioidensa yhteydessä hyväksyttävä toimintapolitiikkoja, jotka koskevat älykkäiden järjestelmien edistämistä ja integrointia kyberturvallisuuspoikkeamien ja -uhkien ennaltaehkäisyyn ja havaitsemiseen. Jäsenvaltioiden olisi kansallisten kyberturvallisuusstrategioidensa mukaisesti otettava käyttöön tietoisuutta kyberturvallisuudesta ja kyberlukutaitoa koskevia toimintapolitiikkoja kuluttajien suojelemiseksi. Hyväksyessään kansallisia kyberturvallisuusstrategioita jäsenvaltioiden olisi varmistettava laillista pääsyä tietoihin koskevien toimintapoliittisten kehysten käyttöönotto ja soveltaminen.*

**Tarkistus 14**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 27 kappale**

(27) Koordinoitua reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin annetun komission suosituksen (EU) 2017/1548<sup>20</sup> liitteen mukaisesti laajamittaisella poikkeamalla olisi tarkoitettava poikkeamaa, jolla on merkittävä vaikutus vähintään kahteen jäsenvaltioon tai jonka aiheuttama häiriö ylittää yksittäisen jäsenvaltion valmiudet reagoida siihen. Laajamittaiset poikkeamat voivat niiden syistä ja vaikutuksista riippuen kärjistyä ja muuttua todellisiksi kriiseiksi, jotka estävät sisämarkkinoiden moitteettoman toiminnan. Kun otetaan huomioon tällaisten poikkeamien laaja vaikuttavuus ja useimmissa tapauksissa rajat ylittävä luonne, jäsenvaltioiden ja asiaankuuluvien unionin toimielinten,

(27) Koordinoitua reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin annetun komission suosituksen (EU) 2017/1548<sup>20</sup> liitteen mukaisesti laajamittaisella poikkeamalla olisi tarkoitettava poikkeamaa, jolla on merkittävä vaikutus vähintään kahteen jäsenvaltioon tai jonka aiheuttama häiriö ylittää yksittäisen jäsenvaltion valmiudet reagoida siihen, **mikä vaarantaa sisämarkkinoiden toiminnan**. Laajamittaiset poikkeamat voivat niiden syistä ja vaikutuksista riippuen kärjistyä ja muuttua todellisiksi kriiseiksi, jotka estävät sisämarkkinoiden moitteettoman toiminnan. Kun otetaan huomioon tällaisten poikkeamien laaja vaikuttavuus ja useimmissa tapauksissa rajat ylittävä

elinten ja virastojen olisi tehtävä yhteistyötä teknisellä, operatiivisella ja poliittisella tasolla, jotta reagointia voidaan koordinoita asianmukaisesti kaikkialla unionissa.

---

<sup>20</sup> Komission suositus (EU) 2017/1584, annettu 13 päivänä syyskuuta 2017, koordinoitusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin (EUVL L 239, 19.9.2017, s. 36).

## **Tarkistus 15**

### **Ehdotus direktiiviksi**

### **Johdanto-osan 28 kappale**

#### *Komission teksti*

(28) Koska verkko- ja tietojärjestelmien haavoittuvuuksien hyödyntäminen voi aiheuttaa merkittäviä häiriöitä ja haittoja, näiden haavoittuvuuksien nopea tunnistaminen ja korjaaminen on tärkeä tekijä kyberturvallisuusriskin vähentämisessä. Tällaisia järjestelmiä kehittävien tahojen olisi sen vuoksi otettava käyttöön asianmukaiset menettelyt haavoittuvuuksien käsittelemiseksi, kun niitä havaitaan. Koska haavoittuvuuksia havaitsevat ja ilmoittavat (julkistavat) usein kolmannet osapuolet (raportoivat tahot), tieto- ja viestintätekniiikan tuotteiden tai palvelujen valmistajan tai tarjoajan olisi myös otettava käyttöön tarvittavat menettelyt haavoittuvuustietojen saamiseksi kolmansilta osapuolilta. Tältä osin kansainvälisissä standardeissa ISO/IEC 30111 ja ISO/IEC 29417 annetaan ohjeita haavoittuvuuksien käsittelystä ja haavoittuvuuksien havaitsemisesta. Haavoittuvuuksien julkistamisen osalta on erityisen tärkeää koordinoita toimia raportoivien tahojen ja tieto- ja viestintätekniiikan tuotteiden tai palvelujen valmistajien tai tarjoajien välillä. Koordinoitussa haavoittuvuuksien

luonne, jäsenvaltioiden ja asiaankuuluvien unionin toimielinten, elinten ja virastojen olisi tehtävä yhteistyötä teknisellä, operatiivisella ja poliittisella tasolla, jotta reagointia voidaan koordinoita asianmukaisesti kaikkialla unionissa.

---

<sup>20</sup> Komission suositus (EU) 2017/1584, annettu 13 päivänä syyskuuta 2017, koordinoitusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin (EUVL L 239, 19.9.2017, s. 36).

#### *Tarkistus*

(28) Koska verkko- ja tietojärjestelmien haavoittuvuuksien hyödyntäminen voi aiheuttaa merkittäviä häiriöitä ja haittoja **yrityksille ja kuluttajille**, näiden haavoittuvuuksien nopea tunnistaminen ja korjaaminen on tärkeä tekijä kyberturvallisuusriskin vähentämisessä. Tällaisia järjestelmiä kehittävien tahojen olisi sen vuoksi otettava käyttöön asianmukaiset menettelyt haavoittuvuuksien käsittelemiseksi, kun niitä havaitaan. Koska haavoittuvuuksia havaitsevat ja ilmoittavat (julkistavat) usein kolmannet osapuolet (raportoivat tahot), tieto- ja viestintätekniiikan tuotteiden tai palvelujen valmistajan tai tarjoajan olisi myös otettava käyttöön tarvittavat menettelyt haavoittuvuustietojen saamiseksi kolmansilta osapuolilta. Tältä osin kansainvälisissä standardeissa ISO/IEC 30111 ja ISO/IEC 29417 annetaan ohjeita haavoittuvuuksien käsittelystä ja haavoittuvuuksien havaitsemisesta. Haavoittuvuuksien julkistamisen osalta on erityisen tärkeää koordinoita toimia raportoivien tahojen ja tieto- ja viestintätekniiikan tuotteiden tai palvelujen valmistajien tai tarjoajien

ilmaisemisessa määritellään jäsenelty prosessi, jonka avulla haavoittuvuuksista ilmoitetaan organisaatiolle siten, että se voi diagnosoida haavoittuvuuden ja korjata sen ennen kuin yksityiskohtaiset haavoittuvuustiedot paljastetaan kolmansille osapuolille tai yleisölle. Koordinoituun haavoittuvuuksien ilmaisemiseen olisi kuuluttava myös raportoivan tahon ja organisaation välinen koordinointi korjaamisen ajoituksen ja haavoittuvuuksien julkistamisen osalta.

välillä. Koordinoidussa haavoittuvuuksien ilmaisemisessa määritellään jäsenelty prosessi, jonka avulla haavoittuvuuksista ilmoitetaan organisaatiolle siten, että se voi diagnosoida haavoittuvuuden ja korjata sen ennen kuin yksityiskohtaiset haavoittuvuustiedot paljastetaan kolmansille osapuolille tai yleisölle. Koordinoituun haavoittuvuuksien ilmaisemiseen olisi kuuluttava myös raportoivan tahon ja organisaation välinen koordinointi korjaamisen ajoituksen ja haavoittuvuuksien julkistamisen osalta.

**Tarkistus 16**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 28 a kappale (uusi)**

*Komission teksti*

*Tarkistus*

***(28 a) Komission, ENISAn ja jäsenvaltioiden olisi edelleen edistettävä kansainvälistä yhdenmukaistamista standardien ja alan olemassa olevien parhaiden käytäntöjen kanssa riskinhallinnan alalla, esimerkiksi toimitusketjun turvallisuusarviointien, tietojenvaihdon ja haavoittuvuuksien julkistamisen aloilla.***

**Tarkistus 17**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 30 kappale**

*Komission teksti*

*Tarkistus*

(30) Virheetön ja nopea tiedonsaanti tieto- ja viestintätekniikan tuotteisiin ja palveluihin vaikuttavista haavoittuvuuksista parantaa kyberturvallisuusriskien hallintaa. Tässä mielessä julkisesti saatavilla olevat haavoittuvuuksia koskevat tietolähteet ovat tärkeä apuväline organisaatioille ja niiden käyttäjille mutta myös kansallisille toimivaltaisille viranomaisille ja

(30) Virheetön ja nopea tiedonsaanti tieto- ja viestintätekniikan tuotteisiin ja palveluihin vaikuttavista haavoittuvuuksista parantaa kyberturvallisuusriskien hallintaa. Tässä mielessä julkisesti saatavilla olevat haavoittuvuuksia koskevat tietolähteet ovat tärkeä apuväline organisaatioille ja niiden käyttäjille mutta myös kansallisille toimivaltaisille viranomaisille ja

CSIRT-yksiköille. Tästä syystä ENISAn olisi perustettava **haavoittuvuusrekisteri**, jossa **keskeisen** ja tärkeät toimijat ja niiden alihankkijat sekä tahot, jotka eivät kuulu tämän direktiivin soveltamisalaan, voivat vapaaehtoisesti ilmoittaa haavoittuvuuksista ja antaa haavoittuvuustietoja, joiden avulla käyttäjät voivat toteuttaa asianmukaisia lieventäviä toimenpiteitä.

## **Tarkistus 18**

### **Ehdotus direktiiviksi**

### **Johdanto-osan 31 kappale**

#### *Komission teksti*

(31) Vaikka vastaavia haavoittuvuusrekistereitä tai tietokantoja on olemassa, niitä isännöivät ja ylläpitävät tahot, jotka eivät ole sijoittautuneet unioniin. ENISAn ylläpitämä Euroopan **haavoittuvuusrekisteri** lisäksi julkistamisprosessin läpinäkyvyyttä ennen kuin haavoittuvuus virallisesti paljastetaan ja selviytymiskykyä tilanteissa, joissa samankaltaisten palvelujen tarjonta heikentyy tai keskeytyy. Pällekkäisyyksien välttämiseksi ja täydentävyyden saavuttamiseksi mahdollisimman pitkälle ENISAn olisi tutkittava mahdollisuutta tehdä järjestelmällisiä yhteistyösopimuksia kolmansien maiden lainkäyttöalueilla sijaitsevien **vastaavien rekisterien** kanssa.

## **Tarkistus 19**

### **Ehdotus direktiiviksi**

### **Johdanto-osan 32 kappale**

CSIRT-yksiköille. Tästä syystä ENISAn olisi perustettava **haavoittuvuustietokanta**, jossa **keskeiset** ja tärkeät toimijat ja niiden alihankkijat sekä tahot, jotka eivät kuulu tämän direktiivin soveltamisalaan, voivat vapaaehtoisesti ilmoittaa haavoittuvuuksista ja antaa haavoittuvuustietoja, joiden avulla käyttäjät voivat toteuttaa asianmukaisia lieventäviä toimenpiteitä.

#### *Tarkistus*

(31) Vaikka vastaavia haavoittuvuusrekistereitä tai tietokantoja on olemassa, niitä isännöivät ja ylläpitävät tahot, jotka eivät ole sijoittautuneet unioniin. ENISAn ylläpitämä Euroopan **haavoittuvuustietokanta** lisäksi julkistamisprosessin läpinäkyvyyttä ennen kuin haavoittuvuus virallisesti paljastetaan ja selviytymiskykyä tilanteissa, joissa samankaltaisten palvelujen tarjonta heikentyy tai keskeytyy. Pällekkäisyyksien välttämiseksi ja täydentävyyden saavuttamiseksi mahdollisimman pitkälle ENISAn olisi tutkittava mahdollisuutta tehdä järjestelmällisiä yhteistyösopimuksia kolmansien maiden lainkäyttöalueilla sijaitsevien **haavoittuvuustietokantojen tai -rekisterien** kanssa **ja lähettää raportteja asianomaisille rekistereille edellyttäen, että näillä toimilla ei heikennetä luottamuksellisuuden ja liikesalaisuuksien suojaa.**

*Komission teksti*

(32) Yhteistyöryhmän olisi laadittava joka toinen vuosi työohjelma, joka sisältää toimet, jotka ryhmän on määrä saada aikaan tavoitteidensa ja tehtäviensä toteuttamiseksi. Tämän direktiivin mukaisesti hyväksytyin ensimmäisen ohjelman aikataulu olisi mukautettava direktiivin (EU) 2016/1148 mukaisesti hyväksytyin viimeisen ohjelman aikatauluun, jotta vältetään mahdolliset häiriöt ryhmän työskentelyssä.

*Tarkistus*

(32) Yhteistyöryhmän olisi **keskusteltava kyberturvallisuuteen liittyvistä poliittisista painopisteistä ja keskeisistä haasteista ja** laadittava joka toinen vuosi työohjelma, joka sisältää toimet, jotka ryhmän on määrä saada aikaan tavoitteidensa ja tehtäviensä toteuttamiseksi. Tämän direktiivin mukaisesti hyväksytyin ensimmäisen ohjelman aikataulu olisi mukautettava direktiivin (EU) 2016/1148 mukaisesti hyväksytyin viimeisen ohjelman aikatauluun, jotta vältetään mahdolliset häiriöt ryhmän työskentelyssä.

**Tarkistus 20**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 32 a kappale (uusi)**

*Komission teksti*

*Tarkistus*

**(32 a) Yhteistyöryhmän olisi koostuttava jäsenvaltioiden, komission ja ENISAn edustajista.**

**Tarkistus 21**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 34 kappale**

*Komission teksti*

*Tarkistus*

(34) Yhteistyöryhmän olisi pysyttävä joustavana foorumina, ja sen olisi voitava reagoida muuttuviin ja uusiin poliittisiin painopisteisiin ja haasteisiin ottaen samalla huomioon käytettävissä olevat resurssit. Sen olisi järjestettävä säännöllisiä yhteisiä kokouksia asiaankuuluvien yksityisten sidosryhmien kanssa eri puolilta unionia keskustellakseen ryhmän toteuttamista toimista ja kerätäkseen näkemyksiä esiin nousevista politiikkaan vaikuttavista haasteista. Unionin tason yhteistyön

(34) Yhteistyöryhmän olisi pysyttävä joustavana foorumina, ja sen olisi voitava reagoida muuttuviin ja uusiin poliittisiin painopisteisiin ja haasteisiin ottaen samalla huomioon käytettävissä olevat resurssit. Sen olisi järjestettävä säännöllisiä yhteisiä kokouksia asiaankuuluvien yksityisten sidosryhmien kanssa eri puolilta unionia keskustellakseen ryhmän toteuttamista toimista ja kerätäkseen näkemyksiä esiin nousevista politiikkaan vaikuttavista haasteista. Unionin tason yhteistyön



tehostamiseksi ryhmän olisi harkittava kyberturvallisuuspolitiikkaan osallistuvien unionin elinten ja virastojen, kuten Euroopan verkkorikostorjuntakeskuksen (EC3), Euroopan unionin lentoturvallisuusviraston (EASA) ja Euroopan unionin avaruusohjelman (EUSPA), kutsumista osallistumaan sen työhön.

tehostamiseksi ryhmän olisi harkittava kyberturvallisuuspolitiikkaan osallistuvien unionin elinten ja virastojen, kuten Euroopan verkkorikostorjuntakeskuksen (EC3), Euroopan unionin lentoturvallisuusviraston (EASA) ja Euroopan unionin avaruusohjelman (EUSPA) **sekä muiden asiaankuuluvien unionin elinten ja virastojen**, kutsumista osallistumaan sen työhön.

**Tarkistus 22**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 35 kappale**

*Komission teksti*

(35) Toimivaltaisille viranomaisille ja CSIRT-yksiköille olisi annettava valtuudet osallistua muiden jäsenvaltioiden virkamiesten vaihtojärjestelmiin yhteistyön parantamiseksi. Toimivaltaisten viranomaisten olisi toteutettava tarvittavat toimenpiteet, jotta muiden jäsenvaltioiden virkamiehet voivat tuloksellisesti osallistua vastaanottavan toimivaltaisen viranomaisen toimintaan.

*Tarkistus*

(35) Toimivaltaisille viranomaisille ja CSIRT-yksiköille olisi annettava valtuudet osallistua muiden jäsenvaltioiden virkamiesten vaihtojärjestelmiin **ja yhteisiin koulutusohjelmiin** yhteistyön parantamiseksi **ja jäsenvaltioiden välisen luottamuksen vahvistamiseksi**. Toimivaltaisten viranomaisten olisi toteutettava tarvittavat toimenpiteet, jotta muiden jäsenvaltioiden virkamiehet voivat tuloksellisesti osallistua vastaanottavan toimivaltaisen viranomaisen **tai CSIRT-yksikön** toimintaan.

**Tarkistus 23**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 39 kappale**

*Komission teksti*

(39) **Tässä direktiivissä termillä 'läheltä piti -tilanne' olisi viitattava tapahtumaan, joka olisi voinut aiheuttaa vahinkoa, mutta jonka täysi toteutuminen kyettiin estämään.**

*Tarkistus*

**Poistetaan.**

**Tarkistus 24**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 45 a kappale (uusi)**

*Komission teksti*

*Tarkistus*

**(45 a) Lisäksi toimijoiden olisi myös varmistettava henkilöstön riittävä kyberturvallisuuskoulutus organisaation kaikilla tasoilla.**

**Tarkistus 25**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 46 kappale**

*Komission teksti*

*Tarkistus*

(46) Jotta voidaan edelleen paremmin puuttua keskeisiin toimitusketjun riskeihin ja auttaa tämän direktiivin soveltamisalaan kuuluvien alojen toimijoita hallitsemaan asianmukaisesti toimitusketjuun ja alihankkijoihin liittyviä kyberturvallisuusriskejä, yhteistyöryhmän, johon osallistuvat asiaankuuluvat kansalliset viranomaiset, olisi yhteistyössä komission ja ENISAn kanssa toteutettava koordinoituja alakohtaisia toimitusketjun riskinarviointeja, kuten tehtiin jo 5G-verkkojen osalta 5G-verkkojen kyberturvallisuudesta annetun suosituksen (EU) 2019/534<sup>21</sup> mukaisesti, jotta voidaan määrittää **alakohtaiset** kriittiset tieto- ja viestintäteknikan palvelut, järjestelmät tai tuotteet sekä kyseeseen tulevat uhat ja haavoittuvuudet.

(46) Jotta voidaan edelleen paremmin puuttua keskeisiin toimitusketjun riskeihin ja auttaa tämän direktiivin soveltamisalaan kuuluvien alojen toimijoita hallitsemaan asianmukaisesti toimitusketjuun ja alihankkijoihin liittyviä kyberturvallisuusriskejä, yhteistyöryhmän, johon osallistuvat asiaankuuluvat kansalliset viranomaiset, olisi yhteistyössä komission ja ENISAn kanssa toteutettava koordinoituja alakohtaisia toimitusketjun riskinarviointeja, kuten tehtiin jo 5G-verkkojen osalta 5G-verkkojen kyberturvallisuudesta annetun suosituksen (EU) 2019/534<sup>21</sup> mukaisesti, jotta voidaan määrittää **kunkin alan** kriittiset tieto- ja viestintäteknikan palvelut, järjestelmät tai tuotteet sekä kyseeseen tulevat uhat ja haavoittuvuudet.

---

<sup>21</sup> Komission suositus (EU) 2019/534, annettu 26 päivänä maaliskuuta 2019, 5G-verkkojen kyberturvallisuudesta (EUVL L 88, 29.3.2019, s. 42).

---

<sup>21</sup> Komission suositus (EU) 2019/534, annettu 26 päivänä maaliskuuta 2019, 5G-verkkojen kyberturvallisuudesta (EUVL L 88, 29.3.2019, s. 42).

**Tarkistus 26**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 47 kappale**

(47) Toimitusketjun riskinarvioinneissa olisi kyseisen alan erityispiirteiden mukaisesti otettava huomioon sekä tekniset että tarvittaessa muut tekijät, mukaan lukien suosituksessa (EU) 2019/534, 5G-verkkojen turvallisuutta koskevassa EU:n laajuisessa koordinoitussa riskinarvioinnissa ja yhteistyöryhmän hyväksymässä 5G-kyberturvallisuutta koskevassa EU:n välineistössä määritellyt yhteistyöryhmän hyväksymät tekijät. Koordinoitua riskinarviointia edellyttävien toimitusketjujen määrittämisessä olisi otettava huomioon seuraavat kriteerit: i) se, missä määrin keskeiset ja tärkeät toimijat käyttävät tiettyjä kriittisiä tieto- ja viestintätekniikan palveluja, järjestelmiä tai tuotteita ja tukeutuvat niihin; ii) tiettyjen kriittisten tieto- ja viestintätekniikan palvelujen, järjestelmien tai tuotteiden merkitys kriittisten tai arkaluonteisten toimintojen suorittamisessa, mukaan lukien henkilötietojen käsittely; iii) vaihtoehtoisten tieto- ja viestintätekniikan palvelujen, järjestelmien tai tuotteiden saatavuus; iv) tieto- ja viestintätekniikan palvelujen, järjestelmien tai tuotteiden koko toimitusketjun kyky sietää häiriötilanteita ja v) käyttöön tulevien uusien tieto- ja viestintätekniikan palvelujen, järjestelmien tai tuotteiden osalta niiden mahdollinen tuleva merkitys toimijoille.

**Tarkistus 27****Ehdotus direktiiviksi****Johdanto-osan 51 kappale**

(51) Sisämarkkinat ovat entistä riippuvaisempia internetin toiminnasta. Käytännöllisesti katsoen kaikkien keskeisten ja tärkeiden toimijoiden palvelut

(47) Toimitusketjun riskinarvioinneissa olisi kyseisen alan erityispiirteiden **ja kriittisyyden** mukaisesti otettava huomioon sekä tekniset että tarvittaessa muut tekijät, mukaan lukien suosituksessa (EU) 2019/534, 5G-verkkojen turvallisuutta koskevassa EU:n laajuisessa koordinoitussa riskinarvioinnissa ja yhteistyöryhmän hyväksymässä 5G-kyberturvallisuutta koskevassa EU:n välineistössä määritellyt yhteistyöryhmän hyväksymät tekijät. Koordinoitua riskinarviointia edellyttävien toimitusketjujen määrittämisessä olisi otettava huomioon seuraavat kriteerit: i) se, missä määrin keskeiset ja tärkeät toimijat käyttävät tiettyjä kriittisiä tieto- ja viestintätekniikan palveluja, järjestelmiä tai tuotteita ja tukeutuvat niihin; ii) tiettyjen kriittisten tieto- ja viestintätekniikan palvelujen, järjestelmien tai tuotteiden merkitys kriittisten tai arkaluonteisten toimintojen suorittamisessa, mukaan lukien henkilötietojen käsittely; iii) vaihtoehtoisten tieto- ja viestintätekniikan palvelujen, järjestelmien tai tuotteiden saatavuus; iv) tieto- ja viestintätekniikan palvelujen, järjestelmien tai tuotteiden koko toimitusketjun kyky sietää häiriötilanteita ja v) käyttöön tulevien uusien tieto- ja viestintätekniikan palvelujen, järjestelmien tai tuotteiden osalta niiden mahdollinen tuleva merkitys toimijoille.

(51) Sisämarkkinat ovat entistä riippuvaisempia internetin toiminnasta. Käytännöllisesti katsoen kaikkien keskeisten ja tärkeiden toimijoiden palvelut

ovat riippuvaisia internetin kautta tarjottavista palveluista. Keskeisten ja tärkeiden palvelujen sujuvan tarjonnan varmistamiseksi on tärkeää, että yleisten sähköisten viestintäverkkojen osien, kuten internetin runkoverkon tai merenalaisten tietoliikennekaapelien, suhteen on käytössä asianmukaiset kyberturvatoimet ja että niihin liittyvistä turvapoikkeamista raportoidaan.

**Tarkistus 28**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 52 kappale**

*Komission teksti*

(52) Toimijoiden olisi **tarvittaessa tiedotettava** palvelujensa käyttäjille yksittäisistä ja merkittävistä uhkista sekä toimenpiteistä, joita käyttäjät voivat toteuttaa pienentääkseen niistä itselleen aiheutuvaa riskiä. **Vaatus ilmoittaa palvelun käyttäjille uhkista** ei saisi vapauttaa toimijoita velvollisuudesta toteuttaa omalla kustannuksellaan asianmukaisia ja välittömiä toimenpiteitä uhkien ehkäisemiseksi tai korjaamiseksi ja palvelun normaalin turvallisuustason palauttamiseksi. Turvallisuusuhkia koskevien tietojen toimittamisen käyttäjille olisi oltava käyttäjille maksutonta.

**Tarkistus 29**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 53 kappale**

*Komission teksti*

(53) Yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla

ovat riippuvaisia internetin kautta tarjottavista palveluista, **ja kuluttajat luottavat siihen arkielämänsä keskeisillä osa-alueilla**. Keskeisten ja tärkeiden palvelujen sujuvan tarjonnan varmistamiseksi on tärkeää, että yleisten sähköisten viestintäverkkojen osien, kuten internetin runkoverkon tai merenalaisten tietoliikennekaapelien, suhteen on käytössä asianmukaiset kyberturvatoimet ja että niihin liittyvistä turvapoikkeamista raportoidaan.

*Tarkistus*

(52) Toimijoiden olisi **pyrittävä tiedottamaan** palvelujensa käyttäjille yksittäisistä ja merkittävistä uhkista sekä toimenpiteistä, joita käyttäjät voivat toteuttaa pienentääkseen niistä itselleen aiheutuvaa riskiä, **erityisesti silloin, kun tällaiset toimenpiteet voivat lisätä kuluttajansuojaa**. **Tämä** ei saisi vapauttaa toimijoita velvollisuudesta toteuttaa omalla kustannuksellaan asianmukaisia ja välittömiä toimenpiteitä uhkien ehkäisemiseksi tai korjaamiseksi ja palvelun normaalin turvallisuustason palauttamiseksi. Turvallisuusuhkia koskevien tietojen toimittamisen käyttäjille olisi oltava käyttäjille maksutonta, **ja tiedot olisi esitettävä kielellä, jota on helppo ymmärtää**.

*Tarkistus*

(53) Yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla

olevien sähköisten viestintäpalvelujen tarjoajien olisi tiedotettava palvelujensa käyttäjille yksittäisistä merkittävistä kyberuhkista sekä *toimenpiteistä*, joita käyttäjät voivat toteuttaa viestintänsä turvallisuuden suojelemiseksi esimerkiksi käyttämällä tietyn tyyppisiä ohjelmistoja tai salaustekniikoita.

### **Tarkistus 30** **Ehdotus direktiiviksi** **Johdanto-osan 54 kappale**

#### *Komission teksti*

(54) Sähköisten viestintäverkkojen ja -palvelujen turvallisuuden takaamiseksi olisi edistettävä salauksen ja erityisesti yhteyden päästä päähän ulottuvan läpialauksen käyttöä, ja sen olisi tarvittaessa oltava pakollista tällaisten palvelujen ja verkkojen tarjoajille oletusarvoisen ja sisäänrakennetun turvallisuuden ja yksityisyydensuojan periaatteiden mukaisesti **18 artiklaa sovellettaessa**. Läpialauksen **käytön olisi kuvastettava** jäsenvaltioiden **toimivaltaa varmistaa niiden keskeisten turvallisuusintressien** ja yleisen turvallisuuden **suojelu** ja **mahdollistaa rikosten tutkinta, selvittäminen ja syyteeseenpano** unionin oikeuden mukaisesti. Ratkaisujen, joilla mahdollistetaan laillinen pääsy tietoihin läpialatusta viestinnässä, olisi säilytettävä salauksen kyky suojata viestinnän yksityisyyttä ja tietoturva samalla kun rikollisuuteen voidaan puuttua tuloksellisesti.

olevien sähköisten viestintäpalvelujen tarjoajien olisi tiedotettava palvelujensa käyttäjille yksittäisistä merkittävistä kyberuhkista sekä *lisätoimenpiteistä*, joita käyttäjät voivat toteuttaa *laitteidensa ja* viestintänsä turvallisuuden suojelemiseksi esimerkiksi käyttämällä tietyn tyyppisiä ohjelmistoja tai salaustekniikoita.

#### *Tarkistus*

(54) Sähköisten viestintäverkkojen ja -palvelujen turvallisuuden takaamiseksi olisi edistettävä salauksen ja erityisesti yhteyden päästä päähän ulottuvan läpialauksen käyttöä, ja sen olisi tarvittaessa oltava pakollista tällaisten palvelujen ja verkkojen tarjoajille oletusarvoisen ja sisäänrakennetun turvallisuuden ja yksityisyydensuojan periaatteiden mukaisesti **kyberturvariskien hallintatoimenpiteitä toteutettaessa**. Läpialauksen **käyttö ei vaikuta jäsenvaltioiden toimivaltaan, toimintapolitiikkoihin ja menettelyihin, joilla ne varmistavat keskeisten turvallisuusintressiensä** ja yleisen turvallisuuden **suojelun** ja **mahdollistavat rikosten tutkinnan, selvittämisen ja syyteeseenpanon** unionin oikeuden mukaisesti. Ratkaisujen, joilla mahdollistetaan laillinen pääsy tietoihin läpialatusta viestinnässä, olisi säilytettävä salauksen kyky suojata viestinnän yksityisyyttä ja tietoturva samalla kun rikollisuuteen voidaan puuttua tuloksellisesti. **Kaikissa toteutettavissa toimissa on noudatettava tiukasti oikeasuhteisuuden ja toissijaisuuden periaatteita.**

**Tarkistus 31**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 55 kappale**

*Komission teksti*

(55) Tässä direktiivissä säädetään poikkeamien ilmoittamista koskevasta **kaksivaiheisesta** lähestymistavasta, jotta löydetään oikea tasapaino toisaalta nopean raportoinnin, joka auttaa lieventämään poikkeamien mahdollista leviämistä ja antaa toimijoille mahdollisuuden hakea tukea, ja toisaalta sellaisen syvällisemmän raportoinnin välillä, jossa otetaan tärkeää oppia yksittäisistä poikkeamista ja parannetaan ajan mittaan yksittäisten yritysten ja kokonaisten toimialojen kykyä sietää kyberuhkia. Kun toimija saa tietoonsa poikkeaman, sitä olisi vaadittava toimittamaan ensimmäinen ilmoitus **24 tunnin** kuluessa ja sen jälkeen loppuraportti viimeistään kuukauden kuluttua. Ensimmäisen ilmoituksen olisi sisällettävä ainoastaan ne tiedot, jotka ovat ehdottoman välttämättömiä, jotta toimivaltaiset viranomaiset tulevat tietoisiksi poikkeamasta ja kyseinen toimija voi tarvittaessa pyytää apua. Ensimmäisessä ilmoituksessa olisi soveltuvien osin ilmoitettava, johtuuko tapahtuma oletettavasti laittomasta tai vihamielisestä toiminnasta. Jäsenvaltioiden olisi varmistettava, että vaatimus tämän ensimmäisen ilmoituksen toimittamisesta ei vie raportoivan toimijan resursseja pois poikkeamien käsittelyyn liittyvistä toimista, jotka olisi asetettava etusijalle. Jotta voidaan edelleen estää se, että poikkeamista ilmoittamista koskevat velvoitteet joko ohjaavat resursseja pois poikkeamiin reagoimisesta tai voivat muulla tavoin vaarantaa toimijan tähän liittyvät toimet, jäsenvaltioiden olisi myös säädettävä, että asianmukaisesti perustelluissa tapauksissa ja yhteisymmärryksessä toimivaltaisten viranomaisten tai CSIRT-yksikön kanssa kyseinen toimija voi poiketa **24 tunnin**

*Tarkistus*

(55) Tässä direktiivissä säädetään poikkeamien ilmoittamista koskevasta **peräkkäisestä** lähestymistavasta, jotta löydetään oikea tasapaino toisaalta nopean raportoinnin, joka auttaa lieventämään poikkeamien mahdollista leviämistä ja antaa toimijoille mahdollisuuden hakea tukea, ja toisaalta sellaisen syvällisemmän raportoinnin välillä, jossa otetaan tärkeää oppia yksittäisistä poikkeamista ja parannetaan ajan mittaan yksittäisten yritysten ja kokonaisten toimialojen kykyä sietää kyberuhkia. Kun toimija saa tietoonsa poikkeaman **tai läheltä piti -tilanteen**, sitä olisi vaadittava toimittamaan ensimmäinen ilmoitus **72 tunnin** kuluessa ja sen jälkeen **kattava raportti viimeistään kolmen kuukauden kuluessa ensimmäisen ilmoituksen toimittamisesta sekä sen jälkeen loppuraportti viimeistään kuukauden kuluttua poikkeaman lieventämisestä**. Ensimmäisen ilmoituksen olisi sisällettävä ainoastaan ne tiedot, jotka ovat ehdottoman välttämättömiä, jotta toimivaltaiset viranomaiset tulevat tietoisiksi poikkeamasta ja kyseinen toimija voi tarvittaessa pyytää apua. Ensimmäisessä ilmoituksessa olisi soveltuvien osin ilmoitettava, johtuuko tapahtuma oletettavasti laittomasta tai vihamielisestä toiminnasta. Jäsenvaltioiden olisi varmistettava, että vaatimus tämän ensimmäisen ilmoituksen toimittamisesta ei vie raportoivan toimijan resursseja pois poikkeamien käsittelyyn liittyvistä toimista, jotka olisi asetettava etusijalle. **Ennen ensimmäistä ilmoitusta olisi ensimmäisten 24 tunnin kuluessa annettava ennakkovaroitus ilman velvoitetta antaa lisätietoja. Tämä ennakkovaroitus olisi toimitettava mahdollisimman pian, jotta toimijat voivat**

*määräajasta ensimmäisen ilmoituksen osalta ja yhden kuukauden määräajasta loppuraportin osalta.*

*nopeasti hakea tukea toimivaltaisilta viranomaisilta tai CSIRT-yksiköiltä ja jotta toimivaltaiset viranomaiset tai CSIRT-yksiköt voivat lieventää raportoidun poikkeaman mahdollista leviämistä sekä toimia CSIRT-yksiköiden tilannetietoisuutta edistävänä välineenä.* Jotta voidaan edelleen estää se, että poikkeamista ilmoittamista koskevat velvoitteet joko ohjaavat resursseja pois poikkeamiin reagoimisesta tai voivat muulla tavoin vaarantaa toimijan tähän liittyvät toimet, jäsenvaltioiden olisi myös säädettävä, että asianmukaisesti perustelluissa tapauksissa ja yhteisymmärryksessä toimivaltaisten viranomaisten tai CSIRT-yksikön kanssa kyseinen toimija voi poiketa *asetetuista määräajoista.*

**Tarkistus 32**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 56 kappale**

*Komission teksti*

(56) Keskeiset ja tärkeät toimijat ovat usein tilanteessa, jossa tietyistä poikkeamasta on sen ominaisuuksien vuoksi ilmoitettava eri viranomaisille eri säädöksiin sisältyvien ilmoitusvelvoitteiden vuoksi. Tällaiset tapaukset aiheuttavat lisärasitteita ja voivat myös johtaa epävarmuuteen tällaisten ilmoitusten muodon ja menettelyjen suhteen. Tätä varten ja turvapoikkeamien raportoinnin yksinkertaistamiseksi jäsenvaltioiden olisi perustettava keskitetty asiointipiste kaikille tässä direktiivissä ja myös muussa unionin lainsäädännössä, kuten asetuksessa (EU) 2016/679 ja direktiivissä 2002/58/EY, edellytetyille ilmoituksille. ENISAn olisi yhteistyössä yhteistyöryhmän kanssa kehitettävä yhteiset ilmoitusmallit ohjeilla, joilla yksinkertaistettaisiin ja virtaviivaistettaisiin unionin lainsäädännössä edellytetyjä raportointitietoja ja vähennettäisiin

*Tarkistus*

(56) Keskeiset ja tärkeät toimijat ovat usein tilanteessa, jossa tietyistä poikkeamasta on sen ominaisuuksien vuoksi ilmoitettava eri viranomaisille eri säädöksiin sisältyvien ilmoitusvelvoitteiden vuoksi. Tällaiset tapaukset aiheuttavat lisärasitteita ja voivat myös johtaa epävarmuuteen tällaisten ilmoitusten muodon ja menettelyjen suhteen. Tätä varten ja turvapoikkeamien raportoinnin yksinkertaistamiseksi *sekä yhden kerran periaatteen ylläpitämiseksi* jäsenvaltioiden olisi perustettava keskitetty asiointipiste kaikille tässä direktiivissä ja myös muussa unionin lainsäädännössä, kuten asetuksessa (EU) 2016/679 ja direktiivissä 2002/58/EY, edellytetyille ilmoituksille. ENISAn olisi yhteistyössä yhteistyöryhmän kanssa kehitettävä yhteiset ilmoitusmallit ohjeilla, joilla yksinkertaistettaisiin ja virtaviivaistettaisiin unionin lainsäädännössä edellytetyjä

yrityksille aiheutuvaa rasitetta.

raportointitietoja ja vähennettäisiin  
yrityksille aiheutuvaa rasitetta.

**Tarkistus 33**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 59 kappale**

*Komission teksti*

(59) Verkkotunnusten ja rekisteröintitietojen (ns. WHOIS-tiedot) tarkkojen ja kattavien tietokantojen ylläpitäminen ja laillisen pääsyn tarjoaminen tällaisiin tietoihin on olennaisen tärkeää, jotta voidaan varmistaa internetin DNS-nimipalvelinjärjestelmän turvallisuus, vakaus ja häiriönsietokyky, mikä puolestaan edistää yhteistä korkeatasoista kyberturvallisuutta unionissa. Jos käsittelyyn sisältyy henkilötietoja, käsittelyssä on noudatettava unionin tietosuojalainsäädäntöä.

*Tarkistus*

(59) Verkkotunnusten ja rekisteröintitietojen (ns. WHOIS-tiedot) tarkkojen, **varmennettujen** ja kattavien tietokantojen ylläpitäminen ja laillisen pääsyn tarjoaminen tällaisiin tietoihin on olennaisen tärkeää, jotta voidaan varmistaa internetin DNS-nimipalvelinjärjestelmän turvallisuus, vakaus ja häiriönsietokyky, mikä puolestaan edistää yhteistä korkeatasoista kyberturvallisuutta unionissa. Jos käsittelyyn sisältyy henkilötietoja, käsittelyssä on noudatettava unionin tietosuojalainsäädäntöä.

**Tarkistus 34**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 61 kappale**

*Komission teksti*

(61) Tarkkojen ja täydellisten verkkotunnusten rekisteröintitietojen saatavuuden varmistamiseksi aluetunnusrekisterien (TLD-rekisterien) ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden (**niin kutsuttujen** rekisterinpitäjien) olisi kerättävä verkkotunnusten rekisteröintitiedot ja taattava niiden eheys ja saatavuus. TLD-rekisterien ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavien tahojen olisi erityisesti vahvistettava toimintatavat ja menettelyt, joilla kerätään ja ylläpidetään tarkkoja ja täydellisiä rekisteröintitietoja sekä ehkäistään ja korjataan virheellisiä

*Tarkistus*

(61) Tarkkojen ja täydellisten verkkotunnusten rekisteröintitietojen saatavuuden varmistamiseksi aluetunnusrekisterien (TLD-rekisterien) ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden (**mukaan lukien verkkotunnusrekisterien ja rekisterinpitäjien, yksityisyys- tai välityspalvelujen rekisteröintipalvelujen tarjoajien, verkkotunnusten välittäjien tai jälleenmyyjien tarjoamat palvelut sekä kaikki muut verkkotunnusten rekisteröintiin liittyvät palvelut**) olisi kerättävä verkkotunnusten rekisteröintitiedot ja taattava niiden eheys ja saatavuus. TLD-rekisterien ja niiden



rekisteröintitietoja unionin tietosuojasääntöjen mukaisesti.

alaisten verkkotunnusten rekisteröintipalveluja tarjoavien tahojen olisi erityisesti vahvistettava toimintatavat ja menettelyt, joilla kerätään ja ylläpidetään tarkkoja ja täydellisiä rekisteröintitietoja sekä ehkäistään ja korjataan virheellisiä rekisteröintitietoja unionin tietosuojasääntöjen mukaisesti.

**Tarkistus 35**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 68 kappale**

*Komission teksti*

(68) Toimijoita olisi kannustettava hyödyntämään kollektiivisesti omaa tietämystään ja käytännön kokemustaan strategisella, taktisella ja operatiivisella tasolla, jotta voidaan parantaa niiden valmiuksia arvioida ja seurata kyberuhkia, puolustautua niitä vastaan ja reagoida niihin. Sen vuoksi on tarpeen mahdollistaa vapaaehtoisten tietojenvaihtojärjestelyjen synty unionin tasolla. Tätä varten jäsenvaltioiden olisi aktiivisesti tuettava ja kannustettava myös sellaisia asiaankuuluvia toimijoita, jotka eivät kuulu tämän direktiivin soveltamisalaan, osallistumaan tällaisiin tietojenvaihtojärjestelyihin. Järjestelyt olisi toteutettava noudattaen kaikilta osin unionin kilpailusääntöjä ja unionin tietosuojalainsäädännön sääntöjä.

**Tarkistus 36**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 69 kappale**

*Komission teksti*

(69) ***Siinä määrin kuin on ehdottoman välttämätöntä ja oikeasuhteista verkko- ja tietoturvan varmistamiseksi***, toimijoiden, viranomaisten, CERT-ryhmien,

*Tarkistus*

(68) Toimijoita olisi kannustettava ***ja tuettava jäsenvaltioiden toimin*** hyödyntämään kollektiivisesti omaa tietämystään ja käytännön kokemustaan strategisella, taktisella ja operatiivisella tasolla, jotta voidaan parantaa niiden valmiuksia arvioida ja seurata kyberuhkia, puolustautua niitä vastaan ja reagoida niihin. Sen vuoksi on tarpeen mahdollistaa vapaaehtoisten tietojenvaihtojärjestelyjen synty unionin tasolla. Tätä varten jäsenvaltioiden olisi aktiivisesti tuettava ja kannustettava myös sellaisia asiaankuuluvia toimijoita, jotka eivät kuulu tämän direktiivin soveltamisalaan, osallistumaan tällaisiin tietojenvaihtojärjestelyihin. Järjestelyt olisi toteutettava noudattaen kaikilta osin unionin kilpailusääntöjä ja unionin tietosuojalainsäädännön sääntöjä.

*Tarkistus*

(69) Toimijoiden, viranomaisten, CERT-ryhmien, CSIRT-yksiköiden sekä turvallisuusteknologioiden ja -palvelujen tarjoajien suorittaman henkilötietojen

CSIRT-yksiköiden sekä turvallisuusteknologioiden ja -palvelujen tarjoajien suorittaman henkilötietojen käsittelyn olisi katsottava muodostavan asianomaisen rekisterinpitäjän osalta asetuksessa (EU) 2016/679 tarkoitetun oikeutetun intressin. Tämän olisi katettava toimenpiteet, jotka liittyvät poikkeamien ehkäisemiseen, havaitsemiseen, analysointiin ja niihin reagoimiseen, toimenpiteet yksittäisistä kyberuhkista tiedottamiseksi, tietojenvaihto haavoittuvuuden korjaamisen ja koordinoitun paljastamisen yhteydessä sekä näitä poikkeamia koskeva vapaaehtoinen tietojenvaihto sekä toimenpiteet, jotka liittyvät kyberuhkiin ja haavoittuvuuksiin, riskien ilmenemisen indikaattoreihin, taktiikkaan, tekniikoihin ja menettelyihin, kyberturvallisuushälytyksiin ja konfigurointivälineisiin. Tällaiset toimenpiteet voivat edellyttää seuraavan tyyppisten henkilötietojen käsittelyä: IP-osoitteet, URL-osoitteet, verkkotunnukset ja sähköpostiosoitteet.

käsittelyn olisi katsottava muodostavan asianomaisen rekisterinpitäjän osalta asetuksessa (EU) 2016/679 tarkoitetun oikeutetun intressin, **ja se olisi rajoitettava siihen, mikä on ehdottoman välttämätöntä ja oikeasuhteista verkko- ja tietoturvan ja kuluttajansuojan varmistamiseksi**. Tämän olisi katettava toimenpiteet, jotka liittyvät poikkeamien ehkäisemiseen, havaitsemiseen, analysointiin ja niihin reagoimiseen, toimenpiteet yksittäisistä kyberuhkista tiedottamiseksi, tietojenvaihto haavoittuvuuden korjaamisen ja koordinoitun paljastamisen yhteydessä sekä näitä poikkeamia koskeva vapaaehtoinen tietojenvaihto sekä toimenpiteet, jotka liittyvät kyberuhkiin ja haavoittuvuuksiin, riskien ilmenemisen indikaattoreihin, taktiikkaan, tekniikoihin ja menettelyihin, kyberturvallisuushälytyksiin ja konfigurointivälineisiin. Tällaiset toimenpiteet voivat edellyttää seuraavan tyyppisten henkilötietojen käsittelyä: IP-osoitteet, URL-osoitteet, verkkotunnukset ja sähköpostiosoitteet.

### **Tarkistus 37** **Ehdotus direktiiviksi** **Johdanto-osan 70 kappale**

#### *Komission teksti*

(70) Jotta voidaan vahvistaa valvontavaltuuksia ja -toimia, jotka auttavat varmistamaan sääntöjen tosiasiallisen noudattamisen, tässä direktiivissä olisi vahvistettava vähimmäisluettelo valvontatoimista ja -keinoista, joiden avulla toimivaltaiset viranomaiset voivat valvoa keskeisiä ja tärkeitä toimijoita. Lisäksi tässä direktiivissä olisi säädettävä valvontajärjestelmän eriyttämisestä keskeisten ja tärkeiden toimijoiden välillä, jotta voidaan varmistaa sekä toimijoiden että toimivaltaisten viranomaisten velvoitteiden oikeudenmukainen tasapaino.

#### *Tarkistus*

(70) Jotta voidaan vahvistaa valvontavaltuuksia ja -toimia, jotka auttavat varmistamaan sääntöjen tosiasiallisen noudattamisen, **ja saavuttaa yhteinen korkea turvallisuuden taso digitaalisella kaikkialla unionissa myös estämällä käyttäjille tai muille verkoille, tietojärjestelmille ja palveluille aiheutuvat riskit**, tässä direktiivissä olisi vahvistettava vähimmäisluettelo valvontatoimista ja -keinoista, joiden avulla toimivaltaiset viranomaiset voivat valvoa keskeisiä ja tärkeitä toimijoita. Lisäksi tässä direktiivissä olisi säädettävä valvontajärjestelmän eriyttämisestä

Näin ollen keskeisiin toimijoihin olisi sovellettava täysimittaista valvontajärjestelmää (etukäteisvalvonta ja jälkikäteisvalvonta), kun taas tärkeisiin toimijoihin olisi sovellettava kevyttä valvontajärjestelmää eli vain jälkikäteisvalvontaa. Viimeksi mainittujen osalta tämä tarkoittaa sitä, että tärkeiden toimijoiden ei pitäisi dokumentoida järjestelmällisesti kyberturvallisuusriskien hallintaa koskevien vaatimusten noudattamista, ja toimivaltaisten viranomaisten olisi harjoitettava reaktiivista jälkikäteisvalvontaa eikä niillä näin ollen olisi yleistä velvoitetta valvoa kyseisiä toimijoita.

keskeisten ja tärkeiden toimijoiden välillä, jotta voidaan varmistaa sekä toimijoiden että toimivaltaisten viranomaisten velvoitteiden oikeudenmukainen tasapaino. Näin ollen keskeisiin toimijoihin olisi sovellettava täysimittaista valvontajärjestelmää (etukäteisvalvonta ja jälkikäteisvalvonta), kun taas tärkeisiin toimijoihin olisi sovellettava kevyttä valvontajärjestelmää eli vain jälkikäteisvalvontaa **siten, että otetaan huomioon riskiperusteinen lähestymistapa**. Viimeksi mainittujen osalta tämä tarkoittaa sitä, että tärkeiden toimijoiden ei pitäisi dokumentoida järjestelmällisesti kyberturvallisuusriskien hallintaa koskevien vaatimusten noudattamista, ja toimivaltaisten viranomaisten olisi harjoitettava reaktiivista jälkikäteisvalvontaa eikä niillä näin ollen olisi yleistä velvoitetta valvoa kyseisiä toimijoita, **paitsi jos velvoitteiden rikkominen on todistettavissa**.

### **Tarkistus 38** **Ehdotus direktiiviksi** **Johdanto-osan 76 kappale**

#### *Komission teksti*

(76) Jotta voidaan edelleen vahvistaa tämän direktiivin nojalla säädettyjen velvoitteiden rikkomiseen sovellettavien seuraamusten vaikuttavuutta ja varoittavuutta, toimivaltaisilla viranomaisilla olisi oltava valtuudet asettaa seuraamuksia, jotka koostuvat keskeisen toimijan tarjoamiin palveluihin ***tai osaan niistä*** liittyvän todistuksen tai luvan voimassaolon keskeyttämisestä ***ja luonnollisen henkilön määräämisestä väliaikaiseen kieltoon harjoittaa johtotehtäviä***. Kun otetaan huomioon tällaisten seuraamusten vakavuus ja vaikutus toimijoiden palveluihin ja viime kädessä niiden kuluttajiin, niitä olisi sovellettava ainoastaan suhteessa rikkomisen vakavuuteen ja ottaen

#### *Tarkistus*

(76) Jotta voidaan edelleen vahvistaa tämän direktiivin nojalla säädettyjen velvoitteiden rikkomiseen sovellettavien seuraamusten vaikuttavuutta ja varoittavuutta, toimivaltaisilla viranomaisilla olisi oltava valtuudet asettaa seuraamuksia, jotka koostuvat keskeisen toimijan tarjoamiin ***asiaankuuluviin*** palveluihin liittyvän todistuksen tai luvan voimassaolon keskeyttämisestä. Kun otetaan huomioon tällaisten seuraamusten vakavuus ja vaikutus toimijoiden palveluihin ja viime kädessä niiden kuluttajiin, niitä olisi sovellettava ainoastaan suhteessa rikkomisen vakavuuteen ja ottaen huomioon kunkin tapauksen erityisolosuhteet, mukaan lukien rikkomisen tahallisuus tai

huomioon kunkin tapauksen erityisolosuhteet, mukaan lukien rikkomisen tahallisuus tai tuottamuksellisuus sekä toimet, joita on toteutettu aiheutuneen vahingon ja/tai menetyksen estämiseksi tai lieventämiseksi. Tällaisia seuraamuksia olisi sovellettava ainoastaan ultima ratio -periaatteen mukaisesti eli vasta viimeisenä keinona sen jälkeen, kun muut tässä direktiivissä säädetyt asiaankuuluvat täytäntöönpanotoimet on käytetty, ja ainoastaan siihen asti, kunnes toimijat, joihin niitä sovelletaan, toteuttavat tarvittavat toimet puutteiden korjaamiseksi tai niiden toimivaltaisen viranomaisen vaatimusten noudattamiseksi, joiden johdosta seuraamuksia on sovellettu. Tällaisten seuraamusten määräämiseen olisi sovellettava asianmukaisia menettelyllisiä suojatoimia unionin oikeuden ja Euroopan unionin perusoikeuskirjan yleisten periaatteiden mukaisesti, mukaan lukien tehokas oikeussuoja, asianmukainen käsittelyprosessi, syyttömyysolettama ja oikeus puolustukseen.

**Tarkistus 39**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 79 kappale**

*Komission teksti*

(79) Olisi otettava käyttöön vertaisarviointimekanismi, jonka avulla jäsenvaltioiden nimeämät asiantuntijat voivat arvioida kyberturvallisuuspolitiikkojen täytäntöönpanoa, myös jäsenvaltioiden valmiuksien ja käytettävissä olevien resurssien tasoa.

tuottamuksellisuus sekä toimet, joita on toteutettu aiheutuneen vahingon ja/tai menetyksen estämiseksi tai lieventämiseksi. Tällaisia seuraamuksia olisi sovellettava ainoastaan ultima ratio -periaatteen mukaisesti eli vasta viimeisenä keinona sen jälkeen, kun muut tässä direktiivissä säädetyt asiaankuuluvat täytäntöönpanotoimet on käytetty, ja ainoastaan siihen asti, kunnes toimijat, joihin niitä sovelletaan, toteuttavat tarvittavat toimet puutteiden korjaamiseksi tai niiden toimivaltaisen viranomaisen vaatimusten noudattamiseksi, joiden johdosta seuraamuksia on sovellettu. Tällaisten seuraamusten määräämiseen olisi sovellettava asianmukaisia menettelyllisiä suojatoimia unionin oikeuden ja Euroopan unionin perusoikeuskirjan yleisten periaatteiden mukaisesti, mukaan lukien tehokas oikeussuoja, asianmukainen käsittelyprosessi, syyttömyysolettama ja oikeus puolustukseen.

*Tarkistus*

(79) Olisi otettava käyttöön vertaisarviointimekanismi, jonka avulla jäsenvaltioiden **ja ENISAn** nimeämät asiantuntijat voivat arvioida kyberturvallisuuspolitiikkojen täytäntöönpanoa, myös jäsenvaltioiden valmiuksien ja käytettävissä olevien resurssien tasoa, **sekä vaihtaa parhaita käytäntöjä.**

**Tarkistus 40**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 80 kappale**

*Komission teksti*

(80) Uusien kyberuhkien, teknologian kehityksen tai alakohtaisten erityispiirteiden huomioon ottamiseksi komissiolle olisi siirrettävä valta hyväksyä Euroopan unionin toiminnasta tehdyn sopimuksen 290 artiklan mukaisesti säädösvallan siirron nojalla annettavia delegoituja säädöksiä, jotka koskevat tässä direktiivissä edellytettyihin riskinhallintatoimenpiteisiin liittyviä seikkoja. Komissiolle olisi myös siirrettävä valta antaa delegoituja säädöksiä, joissa **vahvistetaan, miltä** keskeisten toimijoiden **luokilta edellytetään sertifiointia ja minkä eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti**. On erityisen tärkeää, että komissio asiaa valmistellessaan toteuttaa asianmukaiset kuulemiset, myös asiantuntijatasolla, ja että nämä kuulemiset toteutetaan paremmasta lainsäädännöstä 13 päivänä huhtikuuta 2016 tehdyssä toimielinten välisessä sopimuksessa<sup>26</sup> vahvistettujen periaatteiden mukaisesti. Jotta voitaisiin erityisesti varmistaa tasavertainen osallistuminen delegoitujen säädösten valmisteluun, Euroopan parlamentille ja neuvostolle toimitetaan kaikki asiakirjat samaan aikaan kuin jäsenvaltioiden asiantuntijoille, ja Euroopan parlamentin ja neuvoston asiantuntijoilla on järjestelmällisesti oikeus osallistua komission asiantuntijaryhmien kokouksiin, joissa valmistellaan delegoituja säädöksiä.

*Tarkistus*

(80) Uusien kyberuhkien, teknologian kehityksen tai alakohtaisten erityispiirteiden huomioon ottamiseksi komissiolle olisi siirrettävä valta hyväksyä Euroopan unionin toiminnasta tehdyn sopimuksen 290 artiklan mukaisesti säädösvallan siirron nojalla annettavia delegoituja säädöksiä, jotka koskevat tässä direktiivissä edellytettyihin riskinhallintatoimenpiteisiin liittyviä seikkoja. Komissiolle olisi **siirrettävä valta antaa delegoituja säädöksiä, joissa vahvistetaan riskinhallintatoimenpiteisiin liittyvät tekniset seikat**. Komissiolle olisi myös siirrettävä valta antaa delegoituja säädöksiä, joissa **määritetään, minkä tyyppisiä tietoja keskeisten ja tärkeiden toimijoiden on toimitettava kaikista poikkeamista, joilla on merkittävä vaikutus niiden palvelujen tarjoamiseen, tai läheltä piti -tilanteista, ja täsmennetään tapaukset, joissa poikkeamaa olisi pidettävä merkittävänä**. On erityisen tärkeää, että komissio asiaa valmistellessaan toteuttaa asianmukaiset kuulemiset, myös asiantuntijatasolla, ja että nämä kuulemiset toteutetaan paremmasta lainsäädännöstä 13 päivänä huhtikuuta 2016 tehdyssä toimielinten välisessä sopimuksessa<sup>26</sup> vahvistettujen periaatteiden mukaisesti. Jotta voitaisiin erityisesti varmistaa tasavertainen osallistuminen delegoitujen säädösten valmisteluun, Euroopan parlamentille ja neuvostolle toimitetaan kaikki asiakirjat samaan aikaan kuin jäsenvaltioiden asiantuntijoille, ja Euroopan parlamentin ja neuvoston asiantuntijoilla on järjestelmällisesti oikeus osallistua komission asiantuntijaryhmien kokouksiin, joissa valmistellaan delegoituja säädöksiä.

**Tarkistus 41**  
**Ehdotus direktiiviksi**  
**Johdanto-osan 81 kappale**

*Komission teksti*

(81) Jotta voidaan varmistaa tämän direktiivin asiaankuuluvien säännösten yhdenmukainen täytäntöönpano yhteistyöryhmän toiminnan edellyttämien menettelyllisten järjestelyjen, **riskinhallintatoimenpiteisiin liittyvien teknisten seikkojen** tai poikkeamailmoitusten **tietotyyppien**, muodon ja menettelyn osalta, komissiolle olisi siirrettävä täytäntöönpanovaltaa. Tätä valtaa olisi käytettävä Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 182/2011<sup>27</sup> mukaisesti.

---

<sup>27</sup> Euroopan parlamentin ja neuvoston asetus (EU) N:o 182/2011, annettu 16 päivänä helmikuuta 2011, yleisistä säännöistä ja periaatteista, joiden mukaisesti jäsenvaltiot valvovat komission täytäntöönpanovallan käyttöä (EUVL L 55, 28.2.2011, s. 13).

**Tarkistus 42**  
**Ehdotus direktiiviksi**  
**1 artikla – 1 kohta**

*Komission teksti*

1. Tässä direktiivissä säädetään toimenpiteistä, joilla varmistetaan yhteinen korkea kyberturvallisuuden taso unionissa.

*Tarkistus*

(81) Jotta voidaan varmistaa tämän direktiivin asiaankuuluvien säännösten yhdenmukainen täytäntöönpano yhteistyöryhmän toiminnan edellyttämien menettelyllisten järjestelyjen tai poikkeamailmoitusten muodon ja menettelyn osalta, komissiolle olisi siirrettävä täytäntöönpanovaltaa. Tätä valtaa olisi käytettävä Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 182/2011<sup>27</sup> mukaisesti.

---

<sup>27</sup> Euroopan parlamentin ja neuvoston asetus (EU) N:o 182/2011, annettu 16 päivänä helmikuuta 2011, yleisistä säännöistä ja periaatteista, joiden mukaisesti jäsenvaltiot valvovat komission täytäntöönpanovallan käyttöä (EUVL L 55, 28.2.2011, s. 13).

*Tarkistus*

1. Tässä direktiivissä säädetään toimenpiteistä, joilla varmistetaan yhteinen korkea kyberturvallisuuden taso unionissa, **jotta voidaan saavuttaa kuluttajien ja talouden toimijoiden kannalta luotettava digitaalinen ympäristö sekä parantaa sisämarkkinoiden toimintaa ja poistaa siitä koskevat esteet.**

**Tarkistus 43**  
**Ehdotus direktiiviksi**  
**2 artikla – 2 kohta – 1 alakohta – johdantokappale**

*Komission teksti*

2. Tätä direktiiviä sovelletaan kuitenkin myös toimijan koosta riippumatta liitteissä I ja II tarkoitettuihin toimijoihin, kun

*Tarkistus*

2. Tätä direktiiviä sovelletaan kuitenkin myös toimijan koosta riippumatta liitteissä I ja II tarkoitettuihin **tietyntyyppisiin** toimijoihin, kun

**Tarkistus 44**  
**Ehdotus direktiiviksi**  
**2 artikla – 2 kohta – 2 a alakohta (uusi)**

*Komission teksti*

*Tarkistus*

***Komissio laatii suuntavivoja jäsenvaltioiden tukemiseksi soveltamisalaa koskevien säännösten asianmukaisessa täytäntöönpanossa ja mahdollisten direktiivin soveltamisalaa tai direktiivin tiettyjä säännöksiä koskevien poikkeusten myöntämiseksi tietyille tärkeille toimijoille, jotta voidaan ottaa huomioon niiden vähäinen kriittisyys alalla, jolla ne toimivat, ja/tai niiden vähäinen riippuvuus muista aloista tai palvelutyypeistä. Jäsenvaltioiden on komission suuntaviivat täysimääräisesti huomioon ottaen ilmoitettava tähän liittyvät päätöksensä perusteluineen komissiolle.***

**Tarkistus 45**  
**Ehdotus direktiiviksi**  
**4 artikla – 1 kohta – 4 alakohta**

*Komission teksti*

4) kansallisella kyberturvallisuusstrategialla jäsenvaltion yhtenäistä kehystä, jossa esitetään verkko- ja tietojärjestelmien turvallisuutta koskevat strategiset tavoitteet ja painopisteet kyseisessä jäsenvaltiossa;

*Tarkistus*

4) kansallisella kyberturvallisuusstrategialla jäsenvaltion yhtenäistä kehystä, jossa esitetään verkko- ja tietojärjestelmien turvallisuutta koskevat strategiset tavoitteet ja painopisteet kyseisessä jäsenvaltiossa **sekä niiden**

*saavuttamiseksi tarvittavat  
toimintapolitiikat;*

**Tarkistus 46**  
**Ehdotus direktiiviksi**  
**4 artikla – 1 kohta – 5 a alakohta (uusi)**

*Komission teksti*

*Tarkistus*

**5 a) 'rajatylittävällä poikkeamalla'**  
**poikkeamaa, joka vaikuttaa vähintään**  
**kahden eri jäsenvaltion kansallisten**  
**toimivaltaisten viranomaisten**  
**valvonnassa toimiviin**  
**toiminnanharjoittajiin;**

**Tarkistus 47**  
**Ehdotus direktiiviksi**  
**4 artikla – 1 kohta – 6 a alakohta (uusi)**

*Komission teksti*

*Tarkistus*

**6 a) 'läheltä piti -tilanteella'**  
**tapahtumaa, joka olisi voinut aiheuttaa**  
**vahinkoa mutta jonka täysi toteutuminen**  
**kyettiin estämään;**

**Tarkistus 48**  
**Ehdotus direktiiviksi**  
**4 artikla – 1 kohta – 15 a alakohta (uusi)**

*Komission teksti*

*Tarkistus*

**15 a) 'verkkotunnusten**  
**rekisteröintipalveluilla'**  
**verkkotunnusrekisterien ja**  
**-rekisterinpitäjien, yksityis- tai**  
**välityspalvelujen rekisteröintipalvelujen**  
**tarjoajien ja verkkotunnusten välittäjien**  
**tai jälleenmyyjien tarjoamia palveluja**  
**sekä muita verkkotunnusten**  
**rekisteröintiin liittyviä palveluja;**



**Tarkistus 49**  
**Ehdotus direktiiviksi**  
**5 artikla – 1 kohta – johdantokappale**

*Komission teksti*

1. Kunkin jäsenvaltion on hyväksyttävä kansallinen kyberturvallisuusstrategia, jossa määritellään strategiset tavoitteet sekä asianmukaiset politiikka- ja sääntelytoimenpiteet kyberturvallisuuden korkean tason saavuttamiseksi ja ylläpitämiseksi. Kansalliseen kyberturvallisuusstrategiaan on sisällyttävä erityisesti seuraavat:

*Tarkistus*

1. Kunkin jäsenvaltion on hyväksyttävä kansallinen kyberturvallisuusstrategia, jossa määritellään strategiset tavoitteet sekä asianmukaiset politiikka- ja sääntelytoimenpiteet, **mukaan lukien asianmukaiset taloudelliset ja henkilöresurssit**, kyberturvallisuuden korkean tason saavuttamiseksi ja ylläpitämiseksi. Kansalliseen kyberturvallisuusstrategiaan on sisällyttävä erityisesti seuraavat:

**Tarkistus 50**  
**Ehdotus direktiiviksi**  
**5 artikla – 1 kohta – b alakohta**

*Komission teksti*

b) hallintokehys näiden tavoitteiden ja painopisteiden saavuttamiseksi, mukaan lukien 2 kohdassa tarkoitetut toimintaperiaatteet sekä julkisten elinten ja toimijoiden sekä muiden asiaankuuluvien tahojen roolit ja vastuut;

*Tarkistus*

b) hallintokehys näiden tavoitteiden ja painopisteiden saavuttamiseksi, mukaan lukien 2 kohdassa tarkoitetut toimintaperiaatteet sekä julkisten elinten ja toimijoiden sekä muiden asiaankuuluvien tahojen roolit ja vastuut, **myös niiden, jotka vastaavat kybertiedustelusta ja kyberpuolustuksesta**;

**Tarkistus 51**  
**Ehdotus direktiiviksi**  
**5 artikla – 1 kohta – c alakohta**

*Komission teksti*

c) arvio asiaankuuluvista toiminnoista ja kyberturvallisuusriskeistä kyseisessä jäsenvaltiossa;

*Tarkistus*

c) arvio asiaankuuluvista toiminnoista ja kyberturvallisuusriskeistä kyseisessä jäsenvaltiossa, **mukaan lukien mahdolliset vajeet, jotka voivat vaikuttaa haitallisesti sisämarkkinoihin**;

**Tarkistus 52**  
**Ehdotus direktiiviksi**  
**5 artikla – 1 kohta – e alakohta**

*Komission teksti*

e) luettelo kansallisen kyberturvallisuusstrategian täytäntöönpanoon osallistuvista eri viranomaisista ja tahoista;

*Tarkistus*

e) luettelo kansallisen kyberturvallisuusstrategian täytäntöönpanoon osallistuvista eri viranomaisista ja tahoista, ***mukaan lukien pk-yrityksille tarkoitettu keskitetty asiointipiste***;

**Tarkistus 53**  
**Ehdotus direktiiviksi**  
**5 artikla – 2 kohta – b alakohta**

*Komission teksti*

b) toimintaperiaatteet tieto- ja viestintätekniisten tuotteiden ja palvelujen kyberturvallisuusvaatimusten huomioimiseksi ja määrittelyä julkisissa hankinnoissa;

*Tarkistus*

b) toimintaperiaatteet tieto- ja viestintätekniisten tuotteiden ja palvelujen kyberturvallisuusvaatimusten huomioimiseksi ja määrittelyä julkisissa hankinnoissa, ***mukaan lukien avoimeen lähdekoodiin perustuvien kyberturvallisuustuotteiden käyttö***;

**Tarkistus 54**  
**Ehdotus direktiiviksi**  
**5 artikla – 2 kohta – c alakohta**

*Komission teksti*

c) toimintaperiaatteet 6 artiklassa tarkoitetun koordinoitun haavoittuvuuksien ilmaisemisen edistämiseksi ja sujuvoittamiseksi;

*Tarkistus*

c) toimintaperiaatteet 6 artiklassa tarkoitetun koordinoitun haavoittuvuuksien ilmaisemisen edistämiseksi ja sujuvoittamiseksi ***myös vahvistamalla suuntaviivoja ja parhaita käytäntöjä, jotka perustuvat jo vakiintuneisiin, kansainvälisesti tunnustettuihin haavoittuvuuksien käsittelyä ja ilmaisemista koskeviin standardeihin***;

**Tarkistus 55**  
**Ehdotus direktiiviksi**  
**5 artikla – 2 kohta – e alakohta**

*Komission teksti*

e) toimintaperiaatteet **kyberturvaosaamisen edistämiseksi ja kehittämiseksi, kyberturvatietoisuuden lisäämiseksi** sekä alan tutkimuksen ja kehityksen **edistämiseksi**;

*Tarkistus*

e) toimintaperiaatteet,  **jotka koskevat kuluttajien kyberturvallisuuden edistämistä, kuluttajien kyberuhkatietoisuuden lisäämistä, kyberlukutaidon parantamista, käyttäjien luottamuksen lisäämistä, teknologianeutraalia kyberturvaosaamista ja -koulutusta** sekä alan tutkimuksen ja kehityksen **edistämistä ja verkkoon liitettyjen tuotteiden kyberturvallisuutta**;

**Tarkistus 56**  
**Ehdotus direktiiviksi**  
**5 artikla – 2 kohta – e a alakohta (uusi)**

*Komission teksti*

**e a) toimintaperiaatteet salaustekniikoiden ja salauksen käytön edistämiseksi erityisesti pk-yrityksissä;**

*Tarkistus*

**Tarkistus 57**  
**Ehdotus direktiiviksi**  
**5 artikla – 2 kohta – h alakohta**

*Komission teksti*

h) toimintaperiaatteet, joilla vastataan pk-yritysten, **erityisesti** tämän direktiivin soveltamisalan ulkopuolelle jäävien **pk-yritysten**, erityistarpeisiin, jotka liittyvät ohjeistukseen ja tukeen niiden kyberturvauhkien sietokyvyn parantamiseksi.

*Tarkistus*

h) toimintaperiaatteet, joilla **edistetään kyberturvallisuutta ja** vastataan pk-yritysten **erityistarpeisiin, jotka liittyvät tässä direktiivissä asetettujen velvoitteiden noudattamiseen, sekä** tämän direktiivin soveltamisalan ulkopuolelle jäävien **yritysten** erityistarpeisiin, jotka liittyvät ohjeistukseen ja tukeen niiden kyberturvauhkien sietokyvyn parantamiseksi, **kuten kyberturvatoimien käyttöönoton rahoittamiseen ja niitä koskevaan koulutukseen;**

**Tarkistus 58**  
**Ehdotus direktiiviksi**  
**5 artikla – 2 kohta – h a alakohta (uusi)**

*Komission teksti*

*Tarkistus*

***h a) tähän toimintaperiaatteeseen on sisällyttävä pk-yrityksille tarkoitetun kansallisen keskitetyn yhteyspisteen perustaminen sekä digitaali-innovaatiokeskittymien ja käytettävissä olevien varojen mahdollisimman tehokkaan käytön takaavat puitteet, jotta saavutetaan toimintapolitiikan tavoitteet;***

**Tarkistus 59**  
**Ehdotus direktiiviksi**  
**5 artikla – 2 kohta – h b alakohta (uusi)**

*Komission teksti*

*Tarkistus*

***h b) toimintaperiaate käytettävissä olevien varojen johdonmukaisen ja synergisen käytön edistämiseksi;***

**Tarkistus 60**  
**Ehdotus direktiiviksi**  
**5 artikla – 4 kohta**

*Komission teksti*

*Tarkistus*

4. Jäsenvaltioiden on arvioitava kansalliset kyberturvallisuusstrategiansa vähintään neljän vuoden välein keskeisten suorituskykyindikaattoreiden perusteella ja tarvittaessa muutettava strategioita. Euroopan unionin kyberturvallisuusvirasto (ENISA) avustaa pyynnöstä jäsenvaltioita kansallisen strategian ja keskeisten suorituskykyindikaattoreiden laatimisessa strategian arviointia varten.

4. Jäsenvaltioiden on arvioitava kansalliset kyberturvallisuusstrategiansa vähintään neljän vuoden välein keskeisten suorituskykyindikaattoreiden perusteella ja tarvittaessa muutettava strategioita. Euroopan unionin kyberturvallisuusvirasto (ENISA) avustaa pyynnöstä jäsenvaltioita kansallisen strategian ja keskeisten suorituskykyindikaattoreiden laatimisessa strategian arviointia varten. ***ENISA esittää myös jäsenvaltioille suosituksia kansallisen strategian arvioimiseen tarkoitettujen, unionin tasolla vertailukelpoisten keskeisten suorituskykyindikaattoreiden***

*kehittämiseksi.*

**Tarkistus 61**  
**Ehdotus direktiiviksi**  
**6 artikla – otsikko**

*Komission teksti*

Koordinoitu haavoittuvuuden ilmaiseminen ja Euroopan *haavoittuvuusrekisteri*

*Tarkistus*

Koordinoitu haavoittuvuuden ilmaiseminen ja Euroopan *haavoittuvuustietokanta*

**Tarkistus 62**  
**Ehdotus direktiiviksi**  
**6 artikla – 2 kohta**

*Komission teksti*

2. ENISA perustaa Euroopan *haavoittuvuusrekisterin* ja ylläpitää sitä. Tätä varten ENISA luo asianmukaiset tietojärjestelmät, toimintatavat ja menettelyt ja pitää niitä yllä, jotta tärkeät ja keskeiset toimijat ja niiden verkko- ja tietojärjestelmien toimittajat voivat ilmaista ja rekisteröidä tieto- ja viestintäteknisissä tuotteissa tai palveluissa esiintyviä haavoittuvuuksia ja jotta rekisterin sisältämät haavoittuvuustiedot ovat kaikkien asianomaisten osapuolten saatavilla. *Rekisterin* on sisällettävä erityisesti tiedot haavoittuvuudesta, siitä, mihin tieto- ja viestintäteknikan tuotteeseen tai palveluun se vaikuttaa, sekä haavoittuvuuden vakavuudesta niiden olosuhteiden perusteella, joissa sitä voidaan hyödyntää, asiaan liittyvien ohjelmistokorjausten saatavuudesta ja tällaisten puuttuessa haavoittuvien tuotteiden ja palvelujen käyttäjille suunnatusta ohjeistuksesta siitä, miten haavoittuvuudesta johtuvia riskejä voidaan vähentää.

*Tarkistus*

2. ENISA perustaa Euroopan *haavoittuvuustietokannan* ja ylläpitää sitä. Tätä varten ENISA luo asianmukaiset tietojärjestelmät, toimintatavat ja menettelyt *sekä asianmukaiset julkistamista koskevat toimintaperiaatteet* ja pitää niitä yllä, jotta tärkeät ja keskeiset toimijat ja niiden verkko- ja tietojärjestelmien toimittajat voivat ilmaista ja *helposti* rekisteröidä tieto- ja viestintäteknisissä tuotteissa tai palveluissa esiintyviä haavoittuvuuksia ja jotta rekisterin sisältämät *asiaankuuluvat* haavoittuvuustiedot ovat kaikkien asianomaisten osapuolten saatavilla *edellyttäen, että tällaiset toimet eivät vaaranna luottamuksellisuuden ja liikesalaisuuksien suojaa.* *Haavoittuvuustietokannan* on sisällettävä erityisesti tiedot haavoittuvuudesta, siitä, mihin tieto- ja viestintäteknikan tuotteeseen tai palveluun se vaikuttaa, sekä haavoittuvuuden vakavuudesta niiden olosuhteiden perusteella, joissa sitä voidaan hyödyntää, asiaan liittyvien ohjelmistokorjausten saatavuudesta ja tällaisten puuttuessa haavoittuvien tuotteiden ja palvelujen käyttäjille suunnatusta ohjeistuksesta siitä, miten

haavoittuvuudesta johtuvia riskejä voidaan vähentää. ***Päällekkäisten toimien välttämiseksi ENISA tekee tietojen jakamista ja jäsennelyä yhteistyötä koskevan sopimuksen CVE-rekisterin (Common Vulnerabilities and Exposures) kanssa ja tarvittaessa muiden luotettavien kumppanien kehittämien ja ylläpitämien maailmanlaajuisten tietokantojen kanssa.***

**Tarkistus 63**  
**Ehdotus direktiiviksi**  
**7 artikla – 1 a kohta (uusi)**

*Komission teksti*

*Tarkistus*

***1 a. Jos jäsenvaltio nimeää useamman kuin yhden 1 kohdassa tarkoitetun toimivaltaisen viranomaisen, sen on selkeästi ilmoitettava, mitkä näistä toimivaltaisista viranomaisista toimivat pääasiallisena yhteyspisteenä laajamittaisen poikkeaman tai kriisin aikana.***

**Tarkistus 64**  
**Ehdotus direktiiviksi**  
**7 artikla – 3 kohta – f alakohta**

*Komission teksti*

*Tarkistus*

f) asiaankuuluvien kansallisten viranomaisten ja elinten väliset kansalliset menettelyt ja ***järjestelyt*** sen varmistamiseksi, että jäsenvaltio osallistuu tuloksellisesti laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien koordinoituun hallintointiin unionin tasolla ja tukee sitä.

f) asiaankuuluvien kansallisten viranomaisten ja elinten, ***myös niiden, jotka vastaavat kybertiedustelusta ja kyberpuolustuksesta***, väliset kansalliset menettelyt ja ***niiden välinen koordinointi*** sen varmistamiseksi, että jäsenvaltio osallistuu tuloksellisesti laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien koordinoituun hallintointiin unionin tasolla ja tukee sitä.

**Tarkistus 65**  
**Ehdotus direktiiviksi**  
**10 artikla – 2 kohta – d alakohta**

*Komission teksti*

d) laatia dynaamisesti tilanteen mukaan kyberturvallisuuteen liittyviä riski- ja poikkeama-analyysejä ja ylläpitää kyberturvallisuuden tilannekuvaa;

*Tarkistus*

d) laatia dynaamisesti tilanteen mukaan kyberturvallisuuteen liittyviä riski- ja poikkeama-analyysejä ja ylläpitää kyberturvallisuuden tilannekuvaa, **myös analysoimalla 20 artiklassa tarkoitettuja ennakkovaroituksia ja -ilmoituksia**;

**Tarkistus 66**

**Ehdotus direktiiviksi**

**10 artikla – 2 kohta – e alakohta**

*Komission teksti*

e) toteuttaa toimijoiden pyynnöstä niiden palveluntarjonnassa käyttämien verkko- ja tietojärjestelmien ennakoivia kartoituksia;

*Tarkistus*

e) toteuttaa toimijoiden pyynnöstä niiden palveluntarjonnassa käyttämien verkko- ja tietojärjestelmien ennakoivia kartoituksia **erityisten uhkien tunnistamiseksi, lieventämiseksi tai ehkäisemiseksi**;

**Tarkistus 67**

**Ehdotus direktiiviksi**

**10 artikla – 2 kohta – f alakohta**

*Komission teksti*

f) osallistua CSIRT-verkoston ja antaa pyynnöstä apua verkoston muille jäsenille.

*Tarkistus*

f) osallistua **aktiivisesti** CSIRT-verkoston ja antaa pyynnöstä apua verkoston muille jäsenille;

**Tarkistus 68**

**Ehdotus direktiiviksi**

**10 artikla – 2 kohta – f a alakohta (uusi)**

*Komission teksti*

*Tarkistus*

**f a) antaa operatiivista apua ja ohjausta liitteissä I ja II tarkoitetuille toimijoille ja erityisesti pk-yrityksille**;

**Tarkistus 69**  
**Ehdotus direktiiviksi**  
**2 artikla – 2 kohta – f b alakohta (uusi)**

*Komission teksti*

*Tarkistus*

***f b) osallistua yhteisiin  
kyberturvallisuusharjoituksiin unionin  
tasolla.***

**Tarkistus 70**  
**Ehdotus direktiiviksi**  
**11 artikla – 2 kohta**

*Komission teksti*

*Tarkistus*

2. Jäsenvaltioiden on varmistettava, että joko niiden toimivaltaiset viranomaiset tai CSIRT-yksiköt saavat tämän direktiivin nojalla toimitetut ilmoitukset poikkeamista ja merkittävistä kyberuhista ja läheltä piti -tilanteista. Jos jäsenvaltio päättää, että sen CSIRT-yksiköt eivät saa kyseisiä ilmoituksia, CSIRT-yksiköille on annettava pääsy keskeisten tai tärkeiden toimijoiden 20 artiklan nojalla ilmoittamien poikkeamien tietoihin siinä määrin kuin se on tarpeen niiden tehtävien hoitamiseksi.

2. Jäsenvaltioiden on varmistettava, että joko niiden toimivaltaiset viranomaiset tai CSIRT-yksiköt saavat tämän direktiivin nojalla toimitetut ilmoitukset poikkeamista ja merkittävistä kyberuhista ja läheltä piti -tilanteista. Jos jäsenvaltio päättää, että sen CSIRT-yksiköt eivät saa kyseisiä ilmoituksia, CSIRT-yksiköille on annettava ***asianmukainen*** pääsy keskeisten tai tärkeiden toimijoiden 20 artiklan nojalla ilmoittamien poikkeamien tietoihin siinä määrin kuin se on tarpeen niiden tehtävien ***tehokkaaksi*** hoitamiseksi.

**Tarkistus 71**  
**Ehdotus direktiiviksi**  
**11 artikla – 4 kohta**

*Komission teksti*

*Tarkistus*

4. Siinä määrin kuin se on tarpeen tässä direktiivissä säädettyjen tehtävien ja velvollisuuksien tehokkaan suorittamisen kannalta, jäsenvaltioiden on varmistettava asianmukainen yhteistyö toimivaltaisten viranomaisten ja keskitettyjen asiointipisteiden ja lainvalvontaviranomaisten, tietosuojaviranomaisten sekä kriittisestä infrastruktuurista direktiivin (EU)

4. Siinä määrin kuin se on tarpeen tässä direktiivissä säädettyjen tehtävien ja velvollisuuksien tehokkaan suorittamisen kannalta, jäsenvaltioiden on varmistettava asianmukainen yhteistyö toimivaltaisten viranomaisten ja keskitettyjen asiointipisteiden ja lainvalvontaviranomaisten, tietosuojaviranomaisten sekä kriittisestä infrastruktuurista



XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] nojalla vastaavien viranomaisten ja Euroopan parlamentin ja neuvoston asetuksen (EU) XXXX/XXXX<sup>39</sup> [DORA-asetus] mukaisesti nimettyjen kansallisten finanssialan viranomaisten välillä kyseisessä jäsenvaltiossa.

---

<sup>39</sup> [lisätään koko nimi ja EUVL:n julkaisuviite, kun ne ovat tiedossa]

**Tarkistus 72**  
**Ehdotus direktiiviksi**  
**12 artikla – 2 kohta**

*Komission teksti*

2. Yhteistyöryhmä suorittaa tehtävänsä 6 kohdassa tarkoitettujen kaksivuotisten työohjelmien pohjalta.

**Tarkistus 73**  
**Ehdotus direktiiviksi**  
**12 artikla – 3 kohta – 2 alakohta**

*Komission teksti*

Yhteistyöryhmä voi tarvittaessa kutsua asiaankuuluvien sidosryhmien edustajia osallistumaan työskentelynsä.

**Tarkistus 74**  
**Ehdotus direktiiviksi**  
**12 artikla – 4 kohta – a alakohta**

*Komission teksti*

a) ohjeistaa toimivaltaisia

direktiivin (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] nojalla vastaavien viranomaisten ja Euroopan parlamentin ja neuvoston asetuksen (EU) XXXX/XXXX<sup>39</sup> [DORA-asetus] mukaisesti nimettyjen kansallisten finanssialan viranomaisten välillä kyseisessä jäsenvaltiossa **samoin kuin kyberpuolustuksesta ja kybertiedustelusta vastaavien viranomaisten kanssa.**

---

<sup>39</sup> [lisätään koko nimi ja EUVL:n julkaisuviite, kun ne ovat tiedossa]

*Tarkistus*

2. Yhteistyöryhmä **kokoontuu säännöllisesti ja** suorittaa tehtävänsä 6 kohdassa tarkoitettujen kaksivuotisten työohjelmien pohjalta.

Yhteistyöryhmä voi tarvittaessa kutsua asiaankuuluvien **unionin elinten ja virastojen sekä** sidosryhmien edustajia osallistumaan työskentelynsä.

*Tarkistus*

*Tarkistus*

a) ohjeistaa toimivaltaisia

viranomaisia tämän direktiivin saattamisessa osaksi kansallista lainsäädäntöä ja sen täytäntöönpanossa;

viranomaisia tämän direktiivin saattamisessa osaksi kansallista lainsäädäntöä ja sen täytäntöönpanossa **ja edistää sen yhdenmukaista täytäntöönpanoa jäsenvaltioissa;**

**Tarkistus 75**  
**Ehdotus direktiiviksi**  
**12 artikla – 4 kohta – a a alakohta (uusi)**

*Komission teksti*

*Tarkistus*

**a a) vaihtaa tietoja kyberturvallisuuteen liittyvistä poliittisista painopisteistä ja keskeisistä haasteista sekä määrittää kyberturvallisuuden päätavoitteet;**

**Tarkistus 76**  
**Ehdotus direktiiviksi**  
**12 artikla – 4 kohta – a b alakohta (uusi)**

*Komission teksti*

*Tarkistus*

**a b) keskustella jäsenvaltioiden kansallisista strategioista ja niiden varautumisesta;**

**Tarkistus 77**  
**Ehdotus direktiiviksi**  
**12 artikla – 4 kohta – c alakohta**

*Komission teksti*

*Tarkistus*

c) antaa neuvoja ja tehdä yhteistyötä komission kanssa tulevissa kyberturvallisuuspoliittisissa aloitteissa;

c) antaa neuvoja ja tehdä yhteistyötä komission kanssa tulevissa kyberturvallisuuspoliittisissa aloitteissa **ja Euroopan ulkosuhdehallinnon kanssa tarkasteltaessa kyberturvallisuuden geopoliittisia näkökohtia unionissa;**

**Tarkistus 78**  
**Ehdotus direktiiviksi**  
**12 artikla – 4 kohta – f alakohta**

*Komission teksti*

f) keskustella 16 artiklan 7 kohdassa tarkoitetuista vertaisarviointiraporteista;

*Tarkistus*

f) keskustella 16 artiklan 7 kohdassa tarkoitetuista vertaisarviointiraporteista, **arvioida niiden toimivuutta sekä esittää päätelmiä ja suosituksia;**

**Tarkistus 79**

**Ehdotus direktiiviksi**

**12 artikla – 4 kohta – k a alakohta (uusi)**

*Komission teksti*

*Tarkistus*

**k a) tukea ENISAA kansallisten toimivaltaisten viranomaisten yhteisen koulutuksen järjestämisessä unionin tasolla.**

**Tarkistus 80**

**Ehdotus direktiiviksi**

**12 artikla – 6 kohta**

*Komission teksti*

*Tarkistus*

6. Viimeistään [24 kuukautta tämän direktiivin voimaantulosta] ja sen jälkeen joka toinen vuosi yhteistyöryhmä laatii työohjelman tavoitteidensa saavuttamiseksi ja tehtäviensä hoitamiseksi. Tämän direktiivin mukaisesti hyväksytyt ensimmäisen ohjelman aikataulu on mukautettava direktiivin (EU) 2016/1148 mukaisesti hyväksytyt viimeisen ohjelman aikatauluun.

6. Viimeistään [12 kuukautta tämän direktiivin voimaantulosta] ja sen jälkeen joka toinen vuosi yhteistyöryhmä laatii työohjelman tavoitteidensa saavuttamiseksi ja tehtäviensä hoitamiseksi. Tämän direktiivin mukaisesti hyväksytyt ensimmäisen ohjelman aikataulu on mukautettava direktiivin (EU) 2016/1148 mukaisesti hyväksytyt viimeisen ohjelman aikatauluun.

**Tarkistus 81**

**Ehdotus direktiiviksi**

**12 artikla – 8 a kohta (uusi)**

*Komission teksti*

*Tarkistus*

**8 a. Yhteistyöryhmä julkaisee säännöllisesti toiminnastaan tiivistelmän, jossa ei kuitenkaan rikota sen**

***kokouksissa vaihdettujen tietojen luottamuksellisuutta.***

**Tarkistus 82**

**Ehdotus direktiiviksi**

**13 artikla – 3 kohta – a alakohta**

*Komission teksti*

a) vaihtaa tietoa CSIRT-yksiköiden valmiuksista;

*Tarkistus*

a) vaihtaa tietoa CSIRT-yksiköiden valmiuksista ***ja varautumisesta;***

**Tarkistus 83**

**Ehdotus direktiiviksi**

**13 artikla – 3 kohta – b alakohta**

*Komission teksti*

b) vaihtaa asiaankuuluvaa tietoa poikkeamista, läheltä piti -tilanteista, kyberuhista, riskeistä ja haavoittuvuuksista;

*Tarkistus*

b) vaihtaa asiaankuuluvaa tietoa poikkeamista, läheltä piti -tilanteista, kyberuhista, riskeistä ja haavoittuvuuksista ***sekä tukea jäsenvaltioiden operatiivisia valmiuksia;***

**Tarkistus 84**

**Ehdotus direktiiviksi**

**13 artikla – 3 kohta – d a alakohta (uusi)**

*Komission teksti*

*Tarkistus*

***d a) vaihtaa tietoja rajatylittävistä poikkeamista ja keskustella näistä tiedoista;***

**Tarkistus 85**

**Ehdotus direktiiviksi**

**13 artikla – 3 kohta – g alakohta – i a alakohta (uusi)**

*Komission teksti*

*Tarkistus*

***i a) jakaa tietoja;***

**Tarkistus 86**  
**Ehdotus direktiiviksi**  
**13 artikla – 3 kohta – j alakohta**

*Komission teksti*

j) *yksittäisen CSIRT-yksikön pyynnöstä keskustella kyseisen CSIRT-yksikön* valmiuksista ja varautumisesta;

*Tarkistus*

j) *keskustella CSIRT-yksiköiden* valmiuksista ja varautumisesta;

**Tarkistus 87**  
**Ehdotus direktiiviksi**  
**13 artikla – 4 kohta**

*Komission teksti*

4. CSIRT-verkoston on 35 artiklassa tarkoitettua uudelleentarkastelua varten ja viimeistään [24 kuukauden kuluttua tämän direktiivin voimaantulosta] ja sen jälkeen joka *toinen* vuosi arvioitava operatiivisen yhteistyön edistymistä ja laadittava siitä raportti. Raportissa on erityisesti esitettävä päätelmät 16 artiklassa tarkoitettujen, kansallisia CSIRT-yksiköitä koskevien vertaisarviointien tuloksista, mukaan lukien johtopäätökset ja suositukset, joihin on päädytty tämän artiklan nojalla. Kyseinen raportti toimitetaan myös yhteistyöryhmälle.

*Tarkistus*

4. CSIRT-verkoston on 35 artiklassa tarkoitettua uudelleentarkastelua varten ja viimeistään [24 kuukauden kuluttua tämän direktiivin voimaantulosta] ja sen jälkeen joka vuosi arvioitava operatiivisen yhteistyön edistymistä ja laadittava siitä raportti. Raportissa on erityisesti esitettävä päätelmät 16 artiklassa tarkoitettujen, kansallisia CSIRT-yksiköitä koskevien vertaisarviointien tuloksista, mukaan lukien johtopäätökset ja suositukset, joihin on päädytty tämän artiklan nojalla. Kyseinen raportti toimitetaan myös yhteistyöryhmälle.

**Tarkistus 88**  
**Ehdotus direktiiviksi**  
**14 artikla – 3 kohta – a alakohta**

*Komission teksti*

a) parantaa valmistautumista laajamittaisten poikkeamien ja kriisien hallintaan;

*Tarkistus*

a) parantaa valmistautumista laajamittaisten poikkeamien ja kriisien hallintaan, *mukaan lukien rajat ylittävät kyberuhat*;

**Tarkistus 89**  
**Ehdotus direktiiviksi**  
**14 artikla – 5 kohta**

*Komission teksti*

5. EU-CyCLONe raportoi säännöllisesti yhteistyöryhmälle kyberuhkista, poikkeamista ja alan suuntauksista keskittyen erityisesti niiden vaikutuksiin keskeisiin ja tärkeisiin toimijoihin.

*Tarkistus*

5. EU-CyCLONe raportoi säännöllisesti yhteistyöryhmälle kyberuhkista, poikkeamista ja alan suuntauksista keskittyen erityisesti niiden vaikutuksiin keskeisiin ja tärkeisiin toimijoihin **ja näiden häiriönsietokykyyn.**

**Tarkistus 90**  
**Ehdotus direktiiviksi**  
**14 artikla – 6 kohta**

*Komission teksti*

6. EU-CyCLONe tekee yhteistyötä CSIRT-verkoston kanssa sovittujen menettelyjen pohjalta.

*Tarkistus*

6. EU-CyCLONe tekee **tiivistä** yhteistyötä CSIRT-verkoston kanssa sovittujen menettelyjen pohjalta.

**Tarkistus 91**  
**Ehdotus direktiiviksi**  
**15 artikla – 1 kohta – johdantokappale**

*Komission teksti*

1. ENISA laatii yhteistyössä komission kanssa joka toinen vuosi raportin kyberturvallisuuden tilasta unionissa. Raportissa on esitettävä arvio erityisesti seuraavista:

*Tarkistus*

1. ENISA laatii yhteistyössä komission kanssa joka toinen vuosi raportin kyberturvallisuuden tilasta unionissa **ja esittää sen Euroopan parlamentille.** Raportissa on esitettävä arvio erityisesti seuraavista:

**Tarkistus 92**  
**Ehdotus direktiiviksi**  
**15 artikla – 1 kohta – a alakohta**

*Komission teksti*

a) kyberturvallisuusvalmiuksien kehittyminen unionissa;

*Tarkistus*

a) kyberturvallisuusvalmiuksien kehittyminen unionissa, **myös kyberturvallisuutta koskevien taitojen ja**

*pätevyyksien yleinen taso,  
sisämarkkinoiden yleinen kyky sietää  
kyberuhkia ja direktiivin täytäntöönpanon  
aste eri jäsenvaltioissa;*

**Tarkistus 93**  
**Ehdotus direktiiviksi**  
**15 artikla – 1 kohta – c alakohta**

*Komission teksti*

c) kyberturvallisuusindeksi, joka muodostaa kokonaisarvion kyberturvallisuusvalmiuksien kehitystasosta.

*Tarkistus*

c) kyberturvallisuusindeksi, joka muodostaa kokonaisarvion kyberturvallisuusvalmiuksien kehitystasosta, ***kuluttajien kyberturvallisuutta koskeva yleisarvio mukaan luettuna;***

**Tarkistus 94**  
**Ehdotus direktiiviksi**  
**15 artikla – 1 kohta – c a alakohta (uusi)**

*Komission teksti*

*Tarkistus*

***c a) geopolitiittiset näkökohdat, joilla on suora tai välillinen vaikutus unionin kyberturvallisuuden tilaan.***

**Tarkistus 95**  
**Ehdotus direktiiviksi**  
**16 artikla – 1 kohta – johdantokappale**

*Komission teksti*

*Tarkistus*

1. Komissio vahvistaa yhteistyöryhmää ja ENISAA kuultuaan ja viimeistään **18** kuukauden kuluttua tämän direktiivin voimaantulosta toimintatavat ja -mallin vertaisarviointijärjestelmälle, jolla arvioidaan kunkin jäsenvaltion kyberturvallisuuspolitiikan toimivuutta. Vertaisarvioinnit suorittavat ***muista*** kuin arvioitavasta jäsenvaltiosta tulevat kyberturvallisuuden tekniset asiantuntijat ja arviointien on katettava vähintään

1. Komissio vahvistaa yhteistyöryhmää ja ENISAA kuultuaan ja viimeistään **12** kuukauden kuluttua tämän direktiivin voimaantulosta toimintatavat ja -mallin vertaisarviointijärjestelmälle, jolla arvioidaan kunkin jäsenvaltion kyberturvallisuuspolitiikan toimivuutta. Vertaisarvioinnit suorittavat ***vähintään kahdesta muusta*** kuin arvioitavasta jäsenvaltiosta ***ja ENISASTA*** tulevat kyberturvallisuuden tekniset asiantuntijat ja

seuraavat seikat:

arviointien on katettava vähintään seuraavat seikat:

**Tarkistus 96**  
**Ehdotus direktiiviksi**  
**16 artikla – 2 kohta**

*Komission teksti*

2. Vertailumenetelmässä käytetään objektiivisia, syrjimättömiä, oikeudenmukaisia ja läpinäkyviä kriteerejä, joiden perusteella jäsenvaltioiden on nimettävä vertaisarviointien suorittamiseen kykenevät asiantuntijat. ENISA ja komissio nimeävät omat asiantuntijansa osallistumaan vertaisarviointeihin tarkkailijoina. Komissio luo ENISAn tuella 1 kohdassa tarkoitettujen toimintatapojen osaksi objektiivisen, syrjimättömän, oikeudenmukaisen ja läpinäkyvän järjestelmän asiantuntijoiden valitsemiseksi ja osoittamiseksi satunnaisesti kuhunkin vertaisarviointiin.

**Tarkistus 97**  
**Ehdotus direktiiviksi**  
**18 artikla – 1 kohta**

*Komission teksti*

1. Jäsenvaltioiden on varmistettava, että keskeiset ja tärkeät toimijat toteuttavat **asianmukaiset ja oikeasuhteiset** tekniset ja organisatoriset toimenpiteet hallitakseen riskejä, joita kohdistuu niiden palveluntarjonnassaan käyttämien verkko- ja tietojärjestelmien turvallisuuteen. Näillä toimenpiteillä on varmistettava riskiin suhteutettu verkko- ja tietojärjestelmien turvallisuuden taso uusien tekniikka huomioon ottaen.

*Tarkistus*

2. Vertailumenetelmässä käytetään objektiivisia, syrjimättömiä, **teknologianeutraaleja**, oikeudenmukaisia ja läpinäkyviä kriteerejä, joiden perusteella jäsenvaltioiden on nimettävä vertaisarviointien suorittamiseen kykenevät asiantuntijat. ENISA ja komissio nimeävät omat asiantuntijansa osallistumaan vertaisarviointeihin tarkkailijoina. Komissio luo ENISAn tuella 1 kohdassa tarkoitettujen toimintatapojen osaksi objektiivisen, syrjimättömän, oikeudenmukaisen ja läpinäkyvän järjestelmän asiantuntijoiden valitsemiseksi ja osoittamiseksi satunnaisesti kuhunkin vertaisarviointiin.

*Tarkistus*

1. Jäsenvaltioiden on varmistettava, että keskeiset ja tärkeät toimijat toteuttavat tekniset ja organisatoriset toimenpiteet hallitakseen riskejä, joita kohdistuu niiden palveluntarjonnassaan käyttämien verkko- ja tietojärjestelmien turvallisuuteen. **Näiden toimenpiteiden on oltava asianmukaisia ja oikeassa suhteessa alan tai palvelutyyppin kriittisyyteen sekä toimijan riippuvuuteen muista aloista tai palvelutyypeistä, ja ne on hyväksyttävä riskiperusteisen arvioinnin jälkeen.** Näillä toimenpiteillä on varmistettava riskiin suhteutettu verkko- ja tietojärjestelmien



turvallisuuden taso uusin tekniikka huomioon ottaen. ***On erityisesti toteutettava toimenpiteitä turvallisuuspoikkeamista toimijoiden palveluiden vastaanottajille aiheutuvien vaikutusten ehkäisemiseksi ja minimoimiseksi.***

**Tarkistus 98**  
**Ehdotus direktiiviksi**  
**18 artikla – 2 kohta – d alakohta**

*Komission teksti*

d) ***toimitusketjun turvallisuus***, mukaan lukien turvallisuuteen ***liittyvät näkökohdat***, jotka koskevat kunkin toimijan ja sen alihankkijoiden tai palveluntarjoajien, kuten datatallennus- ja -käsittelypalvelujen tai tietoturvapalveluntarjoajien (MSSP), välisiä suhteita;

*Tarkistus*

d) ***toimien toteuttaminen toimitusketjun turvallisuuden riskinarviointia varten***, mukaan lukien turvallisuuteen ***liittyvien näkökohtien osalta***, jotka koskevat kunkin toimijan ja sen alihankkijoiden tai palveluntarjoajien, kuten datatallennus- ja -käsittelypalvelujen tai tietoturvapalveluntarjoajien (MSSP), välisiä suhteita;

**Tarkistus 99**  
**Ehdotus direktiiviksi**  
**18 artikla – 2 kohta – f alakohta**

*Komission teksti*

f) toimintatavat ja menettelyt (testaus ja auditointi), joilla arvioidaan kyberturvallisuuteen liittyvien riskinhallintatoimenpiteiden toimivuutta;

*Tarkistus*

f) toimintatavat ja menettelyt (testaus ja auditointi) ***ja säännölliset kyberturvallisuusharjoitukset***, joilla arvioidaan kyberturvallisuuteen liittyvien riskinhallintatoimenpiteiden toimivuutta;

**Tarkistus 100**  
**Ehdotus direktiiviksi**  
**18 artikla – 2 kohta – g alakohta**

*Komission teksti*

g) salaustekniikoiden käyttö.

*Tarkistus*

g) salaustekniikoiden, ***erityisesti yhteyden päästä päähän ulottuvan läpisalauksen***, käyttö.

**Tarkistus 101**  
**Ehdotus direktiiviksi**  
**18 artikla – 2 kohta – g a alakohta (uusi)**

*Komission teksti*

*Tarkistus*

***g a) toimintaperiaatteet, joilla varmistetaan asianmukainen kyberturvallisuuskoulutus ja kybertietoisuus.***

**Tarkistus 102**  
**Ehdotus direktiiviksi**  
**18 artikla – 3 kohta**

*Komission teksti*

*Tarkistus*

3. Jäsenvaltioiden on varmistettava, että harkitessaan 2 kohdan d alakohdassa tarkoitettuja asianmukaisia toimenpiteitä toimijoiden on otettava huomioon kullekin alihankkijalle ja palveluntarjoajalle ominaiset haavoittuvuudet, tuotteiden yleinen laatu sekä alihankkijoidensa ja palveluntarjoajiensa kyberturvallisuuskäytännöt, mukaan lukien niiden tuotekehityksen suojausmenettelyt.

3. Jäsenvaltioiden on varmistettava, että harkitessaan 2 kohdan d alakohdassa tarkoitettuja asianmukaisia toimenpiteitä toimijoiden on otettava huomioon kullekin alihankkijalle ja palveluntarjoajalle ominaiset haavoittuvuudet, tuotteiden yleinen laatu sekä alihankkijoidensa ja palveluntarjoajiensa kyberturvallisuuskäytännöt, mukaan lukien niiden tuotekehityksen suojausmenettelyt, ***mikäli asiaankuuluvat tiedot ovat toimijoiden saatavilla.***

**Tarkistus 103**  
**Ehdotus direktiiviksi**  
**18 artikla – 5 kohta**

*Komission teksti*

*Tarkistus*

5. ***Komissio voi hyväksyä täytäntöönpanosäädöksiä***, joissa vahvistetaan 2 kohdassa tarkoitettujen osatekijöiden ***teknisiä ja metodologisia eritelmiä. Valmistellessaan näitä säädöksiä komissio noudattaa 37 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä ja noudattaa*** mahdollisimman pitkälle kansainvälisiä ja

5. ***Siirretään komissiolle valta antaa delegoituja säädöksiä***, joissa vahvistetaan 2 kohdassa tarkoitettujen osatekijöiden ***tekniset ja metodologiset eritelmät ja noudatetaan*** mahdollisimman pitkälle kansainvälisiä ja eurooppalaisia standardeja sekä asiaankuuluvia teknisiä eritelmiä. ***Komission on myös kuultava kaikkia asiaankuuluvia sidosryhmiä***

eurooppalaisia standardeja sekä asiaankuuluvia teknisiä eritelmiä.

*laatiessaan delegoituja säädöksiä.*

**Tarkistus 104**  
**Ehdotus direktiiviksi**  
**18 artikla – 6 kohta**

*Komission teksti*

6. *Siirretään komissiolle valta antaa 36 artiklan mukaisesti delegoituja säädöksiä, joilla täydennetään 2 kohdassa säädettyjä osatekijöitä uusien kyberuhkien, teknologian kehityksen tai alakohtaisten erityispiirteiden huomioon ottamiseksi.*

*Tarkistus*

6. *Komission on tarjottava yhteistyössä yhteistyöryhmän ja ENISAn kanssa ohjeistusta sekä tietoa parhaista käytännöistä, jotka koskevat sitä, miten toimijoiden on noudatettava oikeasuhteisella tavalla 2 kohdassa säädettyjä vaatimuksia ja erityisesti mainitun kohdan d alakohdassa säädettyä vaatimusta.*

**Tarkistus 105**  
**Ehdotus direktiiviksi**  
**19 artikla – 1 kohta**

*Komission teksti*

1. *Yhteistyöryhmä* voi yhteistyössä komission ja ENISAn kanssa tehdä koordinoituja turvallisuusriskinarviointeja yksittäisistä kriittisistä tieto- ja viestintätekniikan palvelujen, järjestelmien tai tuotteiden toimitusketjuista ottaen huomioon tekniset ja tarvittaessa muut kuin tekniset riskitekijät.

*Tarkistus*

1. *Yleisen kyberturvataso* *parantamiseksi yhteistyöryhmä* voi yhteistyössä komission ja ENISAn kanssa tehdä koordinoituja turvallisuusriskinarviointeja yksittäisistä kriittisistä tieto- ja viestintätekniikan palvelujen, järjestelmien tai tuotteiden toimitusketjuista ottaen huomioon tekniset ja tarvittaessa muut kuin tekniset riskitekijät, *kuten geopoliittiset riskit.*

**Tarkistus 106**  
**Ehdotus direktiiviksi**  
**20 artikla – 1 kohta**

*Komission teksti*

1. Jäsenvaltioiden on varmistettava, että keskeiset ja tärkeät toimijat ilmoittavat ilman aiheetonta viivytystä toimivaltaisille

*Tarkistus*

1. Jäsenvaltioiden on varmistettava, että keskeiset ja tärkeät toimijat ilmoittavat ilman aiheetonta viivytystä toimivaltaisille

viranomaisille tai CSIRT-yksikölle 3 ja 4 kohdan mukaisesti kaikista poikkeamista, joilla on merkittävä vaikutus niiden palvelujen tarjoamiseen. Näiden toimijoiden on tarvittaessa ilmoitettava ilman aiheetonta viivytystä palvelujensa käyttäjille poikkeamista, jotka todennäköisesti vaikuttavat haitallisesti kyseisen palvelun tarjoamiseen. Jäsenvaltioiden on varmistettava, että kyseiset toimijat ilmoittavat muun muassa kaikki tiedot, joiden avulla toimivaltaiset viranomaiset tai CSIRT-yksikkö voivat määrittää poikkeaman mahdolliset maiden rajat ylittävät vaikutukset.

viranomaisille tai CSIRT-yksikölle 3 ja 4 kohdan mukaisesti kaikista poikkeamista **ja läheltä piti -tilanteista**, joilla on merkittävä vaikutus niiden palvelujen tarjoamiseen. Näiden toimijoiden on tarvittaessa ilmoitettava ilman aiheetonta viivytystä palvelujensa käyttäjille poikkeamista, jotka todennäköisesti vaikuttavat haitallisesti kyseisen palvelun tarjoamiseen. Jäsenvaltioiden on varmistettava, että kyseiset toimijat ilmoittavat muun muassa kaikki tiedot, joiden avulla toimivaltaiset viranomaiset tai CSIRT-yksikkö voivat määrittää poikkeaman **tai läheltä piti -tilanteen** mahdolliset maiden rajat ylittävät vaikutukset.

**Tarkistus 107**  
**Ehdotus direktiiviksi**  
**20 artikla – 1 a kohta (uusi)**

*Komission teksti*

*Tarkistus*

**1 a. Raportointivaltteiden yksinkertaistamiseksi jäsenvaltioiden on perustettava keskitetty asiointipiste kaikille tässä direktiivissä ja myös muussa unionin lainsäädännössä, kuten asetuksessa (EU) 2016/679 ja direktiivissä 2002/58/EY, edellytetyille ilmoituksille.**

**Tarkistus 108**  
**Ehdotus direktiiviksi**  
**20 artikla – 1 b kohta (uusi)**

*Komission teksti*

*Tarkistus*

**1 b. ENISAn on yhteistyössä yhteistyöryhmän kanssa kehitettävä yhteiset ilmoitusmallit sellaisten ohjeiden avulla, joilla yksinkertaistettaisiin ja virtaviivaistettaisiin unionin lainsäädännössä edellytetyt raportointitietoja ja vähennettäisiin**

*yrityksille aiheutuvaa  
lainsäädäntörasitetta.*

**Tarkistus 109**  
**Ehdotus direktiiviksi**  
**20 artikla – 2 kohta – 1 alakohta**

*Komission teksti*

*Tarkistus*

**2. Jäsenvaltioiden on varmistettava, että keskeiset ja tärkeät toimijat ilmoittavat ilman aiheutonta viivytystä toimivaltaisille viranomaisille tai CSIRT-yksikölle kaikista havaitsemistaan merkittävistä kyberuhkista, jotka olisivat voineet johtaa merkittävään poikkeamaan.**

**Poistetaan.**

**Tarkistus 110**  
**Ehdotus direktiiviksi**  
**20 artikla – 2 kohta – 2 alakohta**

*Komission teksti*

*Tarkistus*

**Näiden toimijoiden on tarvittaessa ilmoitettava ilman aiheutonta viivytystä palvelujensa käyttäjille, joihin merkittävä kyberuhka saattaa vaikuttaa, kaikista toimenpiteistä tai suojakeinoista, joita käyttäjät voivat toteuttaa uhan torjumiseksi. Asianmukaisissa tapauksissa toimijoiden on ilmoitettava käyttäjille myös itse uhasta. Ilmoittaminen ei lisää ilmoituksen tekevän toimijan vastuuta.**

**Poistetaan.**

**Tarkistus 111**  
**Ehdotus direktiiviksi**  
**20 artikla – 3 kohta – a alakohta**

*Komission teksti*

*Tarkistus*

**a) poikkeama on aiheuttanut *tai voi aiheuttaa* kyseiselle toimijalle merkittävän toimintahäiriön tai merkittäviä taloudellisia**

**a) poikkeama on aiheuttanut kyseiselle toimijalle merkittävän toimintahäiriön tai merkittäviä taloudellisia**

tappioita;

tappioita;

**Tarkistus 112**  
**Ehdotus direktiiviksi**  
**20 artikla – 3 kohta – b alakohta**

*Komission teksti*

b) poikkeama on vaikuttanut ***tai voi vaikuttaa*** muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavia aineellisia tai aineettomia tappioita.

*Tarkistus*

b) poikkeama on vaikuttanut muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavia aineellisia tai aineettomia tappioita.

**Tarkistus 113**  
**Ehdotus direktiiviksi**  
**20 artikla – 3 a kohta (uusi)**

*Komission teksti*

*Tarkistus*

**3 a. Siirretään komissiolle valta antaa 36 artiklan mukaisesti delegoituja säädöksiä, joilla täydennetään tätä direktiiviä täsmentämällä tämän artiklan 1 kohdan mukaisesti toimitettujen tietojen tyyppi ja täsmentämällä tarkemmin tapaukset, joissa poikkeama katsotaan merkittäväksi tämän artiklan 3 kohdassa tarkoitetulla tavalla.**

**Tarkistus 114**  
**Ehdotus direktiiviksi**  
**20 artikla – 4 kohta – -a alakohta (uusi)**

*Komission teksti*

*Tarkistus*

**-a) ennakkovaroitus 24 tunnin kuluessa siitä, kun poikkeama on tullut tietoon, asettamatta asianomaiselle toimijalle velvoitetta antaa lisätietoja poikkeamasta;**

**Tarkistus 115**  
**Ehdotus direktiiviksi**  
**20 artikla – 4 kohta – a alakohta**

*Komission teksti*

a) ilman aiheetonta viivytystä ja joka tapauksessa **24** tunnin kuluessa siitä, kun poikkeama on tullut tietoon, alustavan ilmoituksen, jossa on tarvittaessa ilmoitettava, johtuuko poikkeama oletettavasti laittomasta tai vihamielisestä toiminnasta;

*Tarkistus*

a) ilman aiheetonta viivytystä ja joka tapauksessa **72** tunnin kuluessa siitä, kun poikkeama on tullut tietoon, alustavan ilmoituksen, jossa on tarvittaessa ilmoitettava, johtuuko poikkeama oletettavasti laittomasta tai vihamielisestä toiminnasta;

**Tarkistus 116**  
**Ehdotus direktiiviksi**  
**20 artikla – 4 kohta – c alakohta – johdantokappale**

*Komission teksti*

c) viimeistään kuukauden kuluttua a alakohdan mukaisesta ilmoituksesta **loppuraportin**, joka sisältää vähintään seuraavat tiedot:

*Tarkistus*

c) viimeistään **kolmen** kuukauden kuluttua a alakohdan mukaisesta ilmoituksesta **kattavan raportin**, joka sisältää vähintään seuraavat tiedot:

**Tarkistus 117**  
**Ehdotus direktiiviksi**  
**20 artikla – 4 kohta – c alakohta – i alakohta**

*Komission teksti*

i) **yksityiskohtainen** kuvaus poikkeamasta, sen vakavuudesta ja vaikutuksista;

*Tarkistus*

i) **yksityiskohtaisempi** kuvaus poikkeamasta, sen vakavuudesta ja vaikutuksista;

**Tarkistus 118**  
**Ehdotus direktiiviksi**  
**20 artikla – 4 kohta – c a alakohta (uusi)**

*Komission teksti*

*Tarkistus*

**c a) jos poikkeama on edelleen meneillään c alakohdassa tarkoitettun kattavan raportin toimittamishetkellä, loppuraportti on toimitettava kuukauden**

*kuluttua poikkeaman lieventämisestä;*

**Tarkistus 119**  
**Ehdotus direktiiviksi**  
**20 artikla – 7 kohta**

*Komission teksti*

7. Jos yleinen tiedotus on tarpeen poikkeaman estämiseksi tai meneillään olevan poikkeaman käsittelemiseksi tai jos poikkeaman ilmaiseminen on muutoin yleisen edun mukaista, **toimivaltainen viranomainen** tai **CSIRT-yksikkö** ja tarvittaessa muiden asianomaisten jäsenvaltioiden **viranomaiset** tai **CSIRT-yksiköt voivat** asianomaista toimijaa kuultuaan **tiedottaa** poikkeamasta yleisölle tai **vaatia** toimijaa tekemään niin.

*Tarkistus*

7. Jos yleinen tiedotus on tarpeen poikkeaman estämiseksi tai meneillään olevan poikkeaman käsittelemiseksi tai jos poikkeaman ilmaiseminen on muutoin yleisen edun mukaista, **toimivaltaisen viranomaisen** tai **CSIRT-yksikön** ja tarvittaessa muiden asianomaisten jäsenvaltioiden **viranomaisten** tai **CSIRT-yksiköiden on** asianomaista toimijaa kuultuaan **tiedotettava** poikkeamasta yleisölle tai **vaadittava** toimijaa tekemään niin.

**Tarkistus 120**  
**Ehdotus direktiiviksi**  
**20 artikla – 8 kohta**

*Komission teksti*

8. Keskitetyn yhteyspisteen on toimivaltaisen viranomaisen tai CSIRT-yksikön pyynnöstä toimitettava 1 ja 2 kohdan mukaisesti vastaanotetut ilmoitukset muiden asianomaisten jäsenvaltioiden keskitetyille yhteyspisteille.

*Tarkistus*

8. Keskitetyn yhteyspisteen on toimivaltaisen viranomaisen tai CSIRT-yksikön pyynnöstä toimitettava 1 kohdan mukaisesti vastaanotetut ilmoitukset muiden asianomaisten jäsenvaltioiden keskitetyille yhteyspisteille.

**Tarkistus 121**  
**Ehdotus direktiiviksi**  
**20 artikla – 9 kohta**

*Komission teksti*

9. Keskitetyn yhteyspisteen on toimitettava ENISAlle kuukausittain tiivistelmä, joka sisältää anonymisoidut koontitiedot poikkeamista, merkittävistä kyberuhista ja läheltä piti -tilanteista, joista

*Tarkistus*

9. Keskitetyn yhteyspisteen on toimitettava ENISAlle kuukausittain tiivistelmä, joka sisältää anonymisoidut koontitiedot poikkeamista, merkittävistä kyberuhista ja läheltä piti -tilanteista, joista



on ilmoitettu 1 *ja* 2 kohdan ja 27 artiklan mukaisesti. Parantaakseen tietojen vertailukelpoisuutta ENISA voi antaa teknisiä ohjeita tiivistelmään sisältyvien tietojen rakenteesta.

**Tarkistus 122**  
**Ehdotus direktiiviksi**  
**20 artikla – 10 kohta**

*Komission teksti*

10. Toimivaltaisten viranomaisten on toimitettava direktiivin (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] mukaisesti nimetyille toimivaltaisille viranomaisille tiedot poikkeamista ja kyberuhista, jotka direktiivin (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] mukaisesti kriittisiksi toimijoiksi tai niitä vastaaviksi toimijoiksi määritellyt keskeiset toimijat ovat ilmoittaneet 1 *ja* 2 kohdan mukaisesti.

**Tarkistus 123**  
**Ehdotus direktiiviksi**  
**20 artikla – 11 kohta**

*Komission teksti*

11. Komissio voi hyväksyä täytäntöönpanosäädöksiä, joissa määritellään tarkemmin 1 *ja* 2 kohdan nojalla toimitettavan ilmoituksen tietorakenne, muoto ja toimitustapa. Komissio voi myös hyväksyä täytäntöönpanosäädöksiä, joissa määritellään tarkemmin tapaukset, joissa poikkeama katsotaan 3 kohdassa tarkoitetuksi merkittäväksi tapahtumaksi. Nämä täytäntöönpanosäädökset hyväksytään 37 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

on ilmoitettu 1 kohdan ja 27 artiklan mukaisesti. Parantaakseen tietojen vertailukelpoisuutta ENISA voi antaa teknisiä ohjeita tiivistelmään sisältyvien tietojen rakenteesta.

*Tarkistus*

10. Toimivaltaisten viranomaisten on toimitettava direktiivin (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] mukaisesti nimetyille toimivaltaisille viranomaisille tiedot poikkeamista ja kyberuhista, jotka direktiivin (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] mukaisesti kriittisiksi toimijoiksi tai niitä vastaaviksi toimijoiksi määritellyt keskeiset toimijat ovat ilmoittaneet 1 kohdan mukaisesti.

*Tarkistus*

11. Komissio voi hyväksyä täytäntöönpanosäädöksiä, joissa määritellään tarkemmin 1 kohdan nojalla toimitettavan ilmoituksen tietorakenne, muoto ja toimitustapa. Komissio voi myös hyväksyä täytäntöönpanosäädöksiä, joissa määritellään tarkemmin tapaukset, joissa poikkeama katsotaan 3 kohdassa tarkoitetuksi merkittäväksi tapahtumaksi. Nämä täytäntöönpanosäädökset hyväksytään 37 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

**Tarkistus 124**  
**Ehdotus direktiiviksi**  
**21 artikla – 1 kohta**

*Komission teksti*

1. Tiettyjen 18 artiklan vaatimusten noudattamisen osoittamiseksi **jäsenvaltiot voivat edellyttää, että keskeiset ja tärkeät toimijat sertifioivat** tietyt tieto- ja viestintätekniset tuotteet, palvelut ja prosessit asetuksen (EU) 2019/881 49 artiklan nojalla hyväksytyjen **erityisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukaisesti. Sertifioitavat tuotteet, palvelut ja prosessit voivat olla keskeisen tai tärkeän toimijan itse kehittämiä tai ulkopuoliselta taholta hankittuja.**

**Tarkistus 125**  
**Ehdotus direktiiviksi**  
**21 artikla – 2 kohta**

*Komission teksti*

2. **Siirretään komissiolle valta antaa delegoituja säädöksiä, joissa vahvistetaan, miltä keskeisten toimijoiden luokilta edellytetään 1 kohdan nojalla sertifiointia** ja minkä eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti. **Delegoidut säädökset hyväksytään 36 artiklan mukaisesti.**

*Tarkistus*

1. Tiettyjen 18 artiklan vaatimusten noudattamisen osoittamiseksi **ja kyberturvallisuuden tason nostamiseksi jäsenvaltioiden on yhteistyöryhmää ja ENISAA kuultuaan kannustettava keskeisiä ja tärkeitä toimijoita sertifioimaan** tietyt tieto- ja viestintätekniset tuotteet, palvelut ja prosessit,  **jotka ovat joko keskeisen tai tärkeän toimijan itse kehittämiä tai ulkopuoliselta taholta hankittuja,** asetuksen (EU) 2019/881 49 artiklan nojalla hyväksytyjen eurooppalaisten **kyberturvallisuusjärjestelmien tai vastaavien kansainvälisesti tunnustettujen sertifiointijärjestelmien mukaisesti. Jäsenvaltioiden on mahdollisuuksien mukaan kannustettava käyttämään hyväksytyjä sertifiointijärjestelmiä yhdenmukaisella tavalla.**

*Tarkistus*

2. **Komission on arvioitava säännöllisesti asetuksen (EU) 2019/881 49 artiklan mukaisten hyväksytyjen eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien tehokkuutta ja käyttöä ja määritettävä, mitä keskeisten toimijoiden luokkia on kannustettava 1 kohdan nojalla sertifiointiin** ja minkä eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti.

**Tarkistus 126**  
**Ehdotus direktiiviksi**  
**22 artikla – -1 kohta (uusi)**

*Komission teksti*

*Tarkistus*

**-1. Komissio tukee ja edistää yhteistyössä ENISAn kanssa asiaankuuluvien unionin ja kansainvälisten standardointielinten 18 artiklan 1 ja 2 kohdan johdonmukaista täytäntöönpanoa varten laatimien standardien kehittämistä ja täytäntöönpanoa. Komissio tukee standardien päivittämistä teknologian kehityksen perusteella.**

**Tarkistus 127**  
**Ehdotus direktiiviksi**  
**22 artikla – 1 kohta**

*Komission teksti*

*Tarkistus*

1. Jäsenvaltioiden on 18 artiklan 1 ja 2 kohdan johdonmukaisen täytäntöönpanon edistämiseksi kannustettava käyttämään verkko- ja tietojärjestelmien turvallisuuden kannalta merkityksellisiä eurooppalaisia tai kansainvälisesti hyväksytyjä standardeja ja eritelmiä ilman, että ne määräävät käyttämään jotain tiettyä teknologiaa tai harjoittavat syrjintää jonkin tietyn teknologian käytön suosimiseksi.

1. Jäsenvaltioiden on 18 artiklan 1 ja 2 kohdan johdonmukaisen täytäntöönpanon edistämiseksi kannustettava **ENISAn ja yhteistyöryhmän ohjeiden mukaisesti** käyttämään verkko- ja tietojärjestelmien turvallisuuden kannalta merkityksellisiä eurooppalaisia tai kansainvälisesti hyväksytyjä standardeja ja eritelmiä ilman, että ne määräävät käyttämään jotain tiettyä teknologiaa tai harjoittavat syrjintää jonkin tietyn teknologian käytön suosimiseksi.

**Tarkistus 128**  
**Ehdotus direktiiviksi**  
**23 artikla – otsikko**

*Komission teksti*

*Tarkistus*

Verkkotunnusten ja rekisteröintitietojen **tietokannat**

Verkkotunnusten ja rekisteröintitietojen **tietokantainfrastruktuuri**

**Tarkistus 129**  
**Ehdotus direktiiviksi**  
**23 artikla – 1 kohta**

*Komission teksti*

1. DNS-nimipalvelinjärjestelmän turvallisuuden, vakauden ja häiriönsietokyvyn edistämiseksi jäsenvaltioiden on varmistettava, että TLD-rekisterit ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavat toimijat keräävät ja ylläpitävät tarkkoja ja täydellisiä verkkotunnusten rekisteröintitietoja erityisessä tietokantajärjestelmässä noudattaen asianmukaista huolellisuutta, johon sovelletaan henkilötietoja koskevaa unionin tietosuojalainsäädäntöä.

**Tarkistus 130**  
**Ehdotus direktiiviksi**  
**23 artikla – 2 kohta**

*Komission teksti*

2. Jäsenvaltioiden on varmistettava, että 1 kohdassa **tarkoitettut** verkkotunnusten rekisteröintitietojen **tietokannat sisältävät** asiaankuuluvat tiedot verkkotunnusten haltijoiden ja TLD-alue-tunnusten alaisia verkkotunnuksia hallinnoivien yhteyspisteiden tunnistamiseksi ja niihin yhteyden saamiseksi.

**Tarkistus 131**  
**Ehdotus direktiiviksi**  
**23 artikla – 3 kohta**

*Tarkistus*

1. DNS-nimipalvelinjärjestelmän turvallisuuden, vakauden ja häiriönsietokyvyn edistämiseksi jäsenvaltioiden on varmistettava, että TLD-rekisterit ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavat toimijat keräävät, **varmentavat** ja ylläpitävät **palvelujensa tarjoamiseen tarvittavia** tarkkoja ja täydellisiä verkkotunnusten rekisteröintitietoja erityisessä tietokantajärjestelmässä noudattaen asianmukaista huolellisuutta, johon sovelletaan henkilötietoja koskevaa unionin tietosuojalainsäädäntöä.

*Tarkistus*

2. Jäsenvaltioiden on varmistettava, että 1 kohdassa **tarkoitettu** verkkotunnusten rekisteröintitietojen **tietokantainfrastruktura sisältää** asiaankuuluvat **ja tarvittavat** tiedot, **joihin on sisällyttävä vähintään rekisteröijien nimi, fyysinen osoite ja sähköpostiosoite sekä puhelinnumero**, verkkotunnusten haltijoiden ja TLD-alue-tunnusten alaisia verkkotunnuksia hallinnoivien yhteyspisteiden tunnistamiseksi ja niihin yhteyden saamiseksi. rekisteröijien nimi, fyysinen osoite ja sähköpostiosoite sekä puhelinnumero mukaan luettuina;

*Komission teksti*

3. Jäsenvaltioiden on varmistettava, että TLD-rekistereillä ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavilla toimijoilla on käytössä toimintaperiaatteet ja menettelyt, joilla varmistetaan, että **tietokannat sisältävät** tarkat ja täydelliset tiedot. Jäsenvaltioiden on varmistettava, että tiedot näistä toimintaperiaatteista ja menettelyistä asetetaan julkisesti saataville.

**Tarkistus 132**  
**Ehdotus direktiiviksi**  
**23 artikla – 4 kohta**

*Komission teksti*

4. Jäsenvaltioiden on varmistettava, että TLD-rekisterit ja **niiden alaisten** verkkotunnusten rekisteröintipalveluja tarjoavat toimijat **julkaisevat** ilman aiheutonta viivytystä verkkotunnuksen rekisteröinnin jälkeen **verkkotunnuksen rekisteröintitiedot henkilötietoja lukuun ottamatta**.

**Tarkistus 133**  
**Ehdotus direktiiviksi**  
**23 artikla – 5 kohta**

*Komission teksti*

5. Jäsenvaltioiden on varmistettava, että TLD-rekisterit ja **niiden alaisten** verkkotunnusten rekisteröintipalveluja tarjoavat toimijat **antavat pääsyn** tiettyihin verkkotunnusten rekisteröintitietoihin laillisten ja asianmukaisesti perusteltujen

*Tarkistus*

3. Jäsenvaltioiden on varmistettava, että TLD-rekistereillä ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavilla toimijoilla on käytössä toimintaperiaatteet ja menettelyt, joilla varmistetaan, että **tietokantainfrastruktuuri sisältää** tarkat, **varmennetut** ja täydelliset **tiedot, ja että rekisteröijä korjaa tai poistaa viipymättä virheelliset tai puutteelliset** tiedot. Jäsenvaltioiden on varmistettava, että tiedot näistä toimintaperiaatteista ja menettelyistä asetetaan julkisesti saataville.

*Tarkistus*

4. Jäsenvaltioiden on varmistettava, että TLD-rekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat **asettavat julkisesti saataville** ilman aiheutonta viivytystä **ja joka tapauksessa 24 tunnin kuluessa** verkkotunnuksen rekisteröinnin jälkeen **rekisteröityjen asemassa olevien oikeushenkilöiden kaikki verkkotunnuksen rekisteröintitiedot**.

*Tarkistus*

5. Jäsenvaltioiden on varmistettava, että TLD-rekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat **velvoitetaan antamaan pääsy** tiettyihin verkkotunnusten rekisteröintitietoihin laillisten ja asianmukaisesti perusteltujen

pyyntöjen perusteella unionin tietosuojalainsäädännön mukaisesti. Jäsenvaltioiden on varmistettava, että TLD-rekisterit ja **niiden alaisten** verkkotunnusten rekisteröintipalveluja tarjoavat toimijat vastaavat ilman aiheetonta viivytystä kaikkiin pyyntöihin, jotka koskevat tietoihin pääsyä. Jäsenvaltioiden on varmistettava, että tiedot tällaisten tietojen antamista koskevista toimintaperiaatteista ja menettelyistä asetetaan julkisesti saataville.

pyyntöjen perusteella unionin tietosuojalainsäädännön mukaisesti. Jäsenvaltioiden on varmistettava, että TLD-rekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat vastaavat ilman aiheetonta viivytystä **ja joka tapauksessa 72 tunnin kuluessa** kaikkiin **lainmukaisiin ja perusteltuihin** pyyntöihin, jotka koskevat tietoihin pääsyä. Jäsenvaltioiden on varmistettava, että tiedot tällaisten tietojen antamista koskevista toimintaperiaatteista ja menettelyistä asetetaan julkisesti saataville.

**Tarkistus 134**  
**Ehdotus direktiiviksi**  
**24 artikla – 2 kohta**

*Komission teksti*

2. Tätä direktiiviä sovellettaessa 1 kohdassa tarkoitettujen toimijoiden päätoimipaikan katsotaan olevan unionissa siinä jäsenvaltiossa, jossa kyberturvallisuusriskien hallintatoimenpiteisiin liittyvät päätökset tehdään. Jos tällaisia päätöksiä ei tehdä missään unionissa sijaitsevassa toimipaikassa, päätoimipaikan katsotaan olevan siinä jäsenvaltiossa, jossa toimijalla on eniten työntekijöitä unionissa.

*Tarkistus*

2. Tätä direktiiviä sovellettaessa 1 kohdassa tarkoitettujen toimijoiden päätoimipaikan katsotaan olevan unionissa siinä jäsenvaltiossa, jossa kyberturvallisuusriskien hallintatoimenpiteisiin liittyvät päätökset tehdään. Jos tällaisia päätöksiä ei tehdä missään unionissa sijaitsevassa toimipaikassa, päätoimipaikan katsotaan olevan siinä jäsenvaltiossa, jossa toimijalla on eniten työntekijöitä unionissa. **Tämä on toteutettava siten, ettei kansallisille sääntelyelimille aiheudu kohtuutonta taakkaa.**

**Tarkistus 135**  
**Ehdotus direktiiviksi**  
**25 artikla – 1 kohta – johdantokappale**

*Komission teksti*

1. ENISA perustaa 24 artiklan 1 kohdassa tarkoitettujen keskeisten ja tärkeiden toimijoiden rekisterin ja ylläpitää sitä. Toimijoiden on toimitettava ENISAlle seuraavat tiedot viimeistään [12 kuukauden

*Tarkistus*

1. ENISA perustaa 24 artiklan 1 kohdassa tarkoitettujen keskeisten ja tärkeiden toimijoiden rekisterin ja ylläpitää sitä. Toimijoiden on **tätä varten** toimitettava ENISAlle seuraavat tiedot

kuluttua direktiivin voimaantulosta]:

viimeistään [12 kuukauden kuluttua  
direktiivin voimaantulosta]:

### Tarkistus 136

#### Ehdotus direktiiviksi

#### 26 artikla – 1 kohta – b alakohta

##### *Komission teksti*

b) parantaa kyberturvallisuuden tasoa erityisesti lisäämällä tietoisuutta kyberuhkista, rajoittamalla tai estämällä tällaisten uhkien leviämiskykyä tai tukemalla erilaisia puolustusvalmiuksia, haavoittuvuuden korjaamista ja ilmaisemista, uhkien **havaitsemistekniikoita**, lieventämisstrategioita tai reagointi- ja palautumisvaiheita.

##### *Tarkistus*

b) parantaa kyberturvallisuuden tasoa erityisesti lisäämällä tietoisuutta kyberuhkista, rajoittamalla tai estämällä tällaisten uhkien leviämiskykyä tai tukemalla erilaisia puolustusvalmiuksia, haavoittuvuuden korjaamista ja ilmaisemista, uhkien **havaitsemis- ja ehkäisemistekniikoita**, lieventämisstrategioita tai reagointi- ja palautumisvaiheita.

### Tarkistus 137

#### Ehdotus direktiiviksi

#### 26 artikla – 3 kohta

##### *Komission teksti*

3. Jäsenvaltioiden on vahvistettava **säännöt**, joissa täsmennetään 2 kohdassa tarkoitettujen tietojenvaihtojärjestelyjen menettelytavat, operatiiviset osat (mukaan lukien tiettyjen tieto- ja viestintätekniisten alustojen käyttö), sisältö ja edellytykset. **Säännöissä** on myös **vahvistettava** yksityiskohtaiset tiedot viranomaisten osallistumisesta tällaisiin järjestelyihin sekä operatiiviset osat, mukaan lukien erityisten tietotekniisten alustojen käyttö. Jäsenvaltioiden on tarjottava tukea tällaisten järjestelyjen käyttöön 5 artiklan 2 kohdan g alakohdassa tarkoitettujen toimintaperiaatteidensa mukaisesti.

##### *Tarkistus*

3. Jäsenvaltioiden on vahvistettava **ohjeet**, joissa täsmennetään 2 kohdassa tarkoitettujen tietojenvaihtojärjestelyjen menettelytavat, operatiiviset osat (mukaan lukien tiettyjen tieto- ja viestintätekniisten alustojen käyttö), sisältö ja edellytykset. **Ohjeisiin** on myös **tarvittaessa sisällyttävä** yksityiskohtaiset tiedot viranomaisten **ja riippumattomien asiantuntijoiden** osallistumisesta tällaisiin järjestelyihin sekä operatiiviset osat, mukaan lukien erityisten tietotekniisten alustojen käyttö. Jäsenvaltioiden on tarjottava tukea tällaisten järjestelyjen käyttöön 5 artiklan 2 kohdan g alakohdassa tarkoitettujen toimintaperiaatteidensa mukaisesti.

**Tarkistus 138**  
**Ehdotus direktiiviksi**  
**26 artikla – 5 kohta**

*Komission teksti*

5. ENISA tukee unionin oikeuden mukaisesti kyberturvallisuustietojen jakamista koskevien 2 kohdassa tarkoitettujen järjestelyjen toteuttamista tarjoamalla tietoa parhaista käytännöistä *sekä* ohjeistusta.

*Tarkistus*

5. ENISA tukee unionin oikeuden mukaisesti kyberturvallisuustietojen jakamista koskevien 2 kohdassa tarkoitettujen järjestelyjen toteuttamista tarjoamalla tietoa parhaista käytännöistä *ja* ohjeistusta *sekä helpottamalla tietojenvaihtoa unionin tasolla suojaten samalla liiketoiminnan kannalta arkaluonteisia tietoja. Yhteistyöryhmää kehoitetaan antamaan keskeisten ja tärkeiden toimijoiden pyynnöstä tietoa parhaista käytännöistä sekä ohjeistusta.*

**Tarkistus 139**  
**Ehdotus direktiiviksi**  
**27 artikla – -1 kohta (uusi)**

*Komission teksti*

*-1. Jäsenvaltioiden on varmistettava, että keskeiset ja tärkeät toimijat voivat toimittaa vapaaehtoisesti ilmoituksia havaitsemistaan kyberuhkista, jotka olisivat voineet johtaa merkittävään poikkeamaan. Jäsenvaltioiden on varmistettava, että toimijat noudattavat 20 artiklassa säädettyä menettelyä näitä ilmoituksia tehdessään. Vapaaehtoiset ilmoitukset eivät saa johtaa lisävelvoitteiden asettamiseen raportoivalle toimijalle.*

*Tarkistus*

**Tarkistus 140**  
**Ehdotus direktiiviksi**  
**27 artikla – 1 kohta**

*Komission teksti*

*Jäsenvaltioiden on varmistettava, että tämän direktiivin soveltamisalan ulkopuolelle jäävät toimijat voivat*

*Tarkistus*

*1. Jäsenvaltioiden on varmistettava, että tämän direktiivin soveltamisalan ulkopuolelle jäävät toimijat voivat*



vapaaehtoisesti ilmoittaa merkittävistä poikkeamista, kyberuhista tai läheltä piti - tilanteista, sanotun kuitenkin rajoittamatta 3 artiklan soveltamista. Kun jäsenvaltiot käsittelevät ilmoituksia, niiden on noudatettava 20 artiklassa säädettyä menettelyä. **Jäsenvaltiot voivat antaa etusijan** pakollisten ilmoitusten käsittelylle vapaaehtoisten ilmoitusten käsittelyyn nähden. Vapaaehtoinen raportointi ei saa johtaa sellaisten velvollisuuksien asettamiseen raportoivalle toimijalle, joita siihen ei olisi sovellettu, jos se ei olisi antanut kyseistä ilmoitusta.

vapaaehtoisesti ilmoittaa merkittävistä poikkeamista, kyberuhista tai läheltä piti - tilanteista, sanotun kuitenkin rajoittamatta 3 artiklan soveltamista. Kun jäsenvaltiot käsittelevät ilmoituksia, niiden on noudatettava 20 artiklassa säädettyä menettelyä. **Jäsenvaltioiden on annettava etusija** pakollisten ilmoitusten käsittelylle vapaaehtoisten ilmoitusten käsittelyyn nähden. Vapaaehtoinen raportointi ei saa johtaa sellaisten velvollisuuksien asettamiseen raportoivalle toimijalle, joita siihen ei olisi sovellettu, jos se ei olisi antanut kyseistä ilmoitusta, **mutta jäsenvaltiolle voidaan tarjota CSIRT-yksiköiden apua.**

**Tarkistus 141**  
**Ehdotus direktiiviksi**  
**28 artikla – 1 kohta**

*Komission teksti*

1. Jäsenvaltioiden on varmistettava, että toimivaltaiset viranomaiset valvovat tosiasiallisesti tämän direktiivin ja erityisesti sen 18 ja 20 artiklassa säädettyjen velvoitteiden noudattamista ja toteuttavat tarvittavat toimenpiteet sen varmistamiseksi.

*Tarkistus*

1. Jäsenvaltioiden on varmistettava, että toimivaltaiset viranomaiset valvovat tosiasiallisesti tämän direktiivin ja erityisesti sen 18 ja 20 artiklassa säädettyjen velvoitteiden noudattamista ja toteuttavat tarvittavat toimenpiteet sen varmistamiseksi, **ja että niille annetaan asianmukaiset keinot tehtäviensä hoitamiseksi.**

**Tarkistus 142**  
**Ehdotus direktiiviksi**  
**28 artikla – 2 kohta**

*Komission teksti*

2. Toimivaltaisten viranomaisten on toimittava tiiviisti yhteistyössä tietosuojaviranomaisten kanssa käsitellessään henkilötietojen tietoturvaloukkauksiin johtaneita poikkeamia.

*Tarkistus*

2. Toimivaltaisten viranomaisten on toimittava tiiviisti yhteistyössä tietosuojaviranomaisten kanssa käsitellessään henkilötietojen tietoturvaloukkauksiin johtaneita poikkeamia, **mukaan lukien tarvittaessa muiden jäsenvaltioiden**

**Tarkistus 143**  
**Ehdotus direktiiviksi**  
**29 artikla – 2 kohta – c alakohta**

*Komission teksti*

c) riskinarviointeihin tai käytettävissä oleviin riskitietoihin perustuvat kohdennetut turvallisuusauditoinnit;

*Tarkistus*

c) riskinarviointeihin tai käytettävissä oleviin riskitietoihin perustuvat ***pätevän riippumattoman elimen tai toimivaltaisen viranomaisen suorittamat*** kohdennetut turvallisuusauditoinnit;

**Tarkistus 144**  
**Ehdotus direktiiviksi**  
**29 artikla – 2 kohta – f alakohta**

*Komission teksti*

f) pyynnöt saada tutustua kaikkeen dataan ja kaikkiin asiakirjoihin tai muihin tietoihin, joita ne tarvitsevat valvontatehtäviensä suorittamiseksi;

*Tarkistus*

f) pyynnöt saada tutustua kaikkeen ***asiaankuuluvaan*** dataan ja kaikkiin ***asiaankuuluviin*** asiakirjoihin tai muihin tietoihin, joita ne tarvitsevat valvontatehtäviensä suorittamiseksi;

**Tarkistus 145**  
**Ehdotus direktiiviksi**  
**29 artikla – 3 kohta**

*Komission teksti*

3. Käyttäessään 2 kohdan e–g alakohdan mukaisia valtuuksiaan toimivaltaisten viranomaisten on ilmoitettava pyynnön tarkoitus ***ja*** täsmennettävä pyydetyt tiedot.

*Tarkistus*

3. Käyttäessään 2 kohdan e–g alakohdan mukaisia valtuuksiaan toimivaltaisten viranomaisten on ilmoitettava pyynnön tarkoitus, täsmennettävä pyydetyt tiedot ***ja rajattava pyyntönsä koskemaan ainoastaan poikkeaman tai huolenaiheen vaikutusalaa.***

**Tarkistus 146**  
**Ehdotus direktiiviksi**  
**29 artikla – 5 kohta – 1 alakohta – a alakohta**

*Komission teksti*

a) keskeyttää tai pyytää sertifiointi- tai lupaelintä keskeyttämään ***kokonaan tai osittain*** keskeisen toimijan tarjoamia palveluja tai toimintoja koskevan sertifiointin tai luvan;

*Tarkistus*

a) keskeyttää tai pyytää sertifiointi- tai lupaelintä keskeyttämään keskeisen toimijan tarjoamia ***asiaankuuluvia*** palveluja tai toimintoja koskevan sertifiointin tai luvan;

**Tarkistus 147**

**Ehdotus direktiiviksi**

**29 artikla – 5 kohta – 1 alakohta – b alakohta**

*Komission teksti*

***b) määrätty tai pyytää asiaankuuluvia elimiä tai tuomioistuimia määräämään kansallisen lainsäädännön mukaisesti väliaikainen kielto, jolla kielletään ketä tahansa toimitusjohtajan tai laillisen edustajan tasolla kyseisen keskeisen toimijan johtotehtävissä toimivaa henkilöä ja ketä tahansa muuta rikkomisesta vastuussa olevana pidettyä luonnollista henkilöä hoitamasta kyseisen toimijan johtotehtäviä.***

*Tarkistus*

***Poistetaan.***

**Tarkistus 148**

**Ehdotus direktiiviksi**

**30 artikla – 1 kohta**

*Komission teksti*

1. Jos jäsenvaltiot saavat näyttöä tai viitteitä siitä, että tärkeä toimija ei noudata tässä direktiivissä ja erityisesti sen 18 ja 20 artiklassa säädettyjä velvoitteita, niiden on varmistettava, että toimivaltaiset viranomaiset puuttuvat tilanteeseen tarpeen mukaan jälkikäteisvalvonnallisin toimin.

*Tarkistus*

1. Jos jäsenvaltiot saavat näyttöä tai viitteitä siitä, että tärkeä toimija ei noudata tässä direktiivissä ja erityisesti sen 18 ja 20 artiklassa säädettyjä velvoitteita, niiden on varmistettava, että toimivaltaiset viranomaiset puuttuvat tilanteeseen tarpeen mukaan ***ja riskiperusteisen lähestymistavan huomioon ottaen*** jälkikäteisvalvonnallisin toimin.

**Tarkistus 149**  
**Ehdotus direktiiviksi**  
**30 artikla – 2 kohta – b alakohta**

*Komission teksti*

b) riskinarviointeihin tai käytettävissä oleviin riskitietoihin perustuvat kohdennetut turvallisuusauditoinnit;

*Tarkistus*

b) riskinarviointeihin tai käytettävissä oleviin riskitietoihin perustuvat **pätevän riippumattoman elimen tai toimivaltaisen viranomaisen suorittamat** kohdennetut turvallisuusauditoinnit;

**Tarkistus 150**  
**Ehdotus direktiiviksi**  
**30 artikla – 3 kohta**

*Komission teksti*

3. Käyttäessään 2 kohdan d tai e alakohdan mukaisia valtuuksiaan toimivaltaisten viranomaisten on ilmoitettava pyynnön tarkoitus **ja** täsmennettävä pyydetyt tiedot.

*Tarkistus*

3. Käyttäessään 2 kohdan d tai e alakohdan mukaisia valtuuksiaan toimivaltaisten viranomaisten on ilmoitettava pyynnön tarkoitus, täsmennettävä pyydetyt tiedot **ja rajattava pyyntönsä koskemaan ainoastaan poikkeaman tai huolenaiheen vaikutusala.**

**Tarkistus 151**  
**Ehdotus direktiiviksi**  
**31 artikla – 4 kohta**

*Komission teksti*

4. Jäsenvaltioiden on varmistettava, että 18 artiklassa tai 20 artiklassa säädettyjen velvoitteiden rikkomisesta määrätään tämän artiklan 2 ja 3 kohdan mukaisesti hallinnollinen sakko, joka voi olla enimmillään **vähintään** 10 000 000 euroa tai enimmillään 2 % yrityksen, johon keskeinen tai tärkeä toimija kuuluu, edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

*Tarkistus*

4. Jäsenvaltioiden on varmistettava, että 18 artiklassa tai 20 artiklassa säädettyjen velvoitteiden rikkomisesta määrätään tämän artiklan 2 ja 3 kohdan mukaisesti hallinnollinen sakko, joka voi olla enimmillään 10 000 000 euroa tai enimmillään 2 % yrityksen, johon keskeinen tai tärkeä toimija kuuluu, edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

**Tarkistus 152**  
**Ehdotus direktiiviksi**  
**32 artikla – 1 kohta**

*Komission teksti*

1. Jos toimivaltaisilla viranomaisilla on viitteitä siitä, että keskeisen tai tärkeän toimijan 18 ja 20 artiklassa säädettyjen velvollisuuksien laiminlyönti aiheuttaa asetuksen (EU) 2016/679 4 artiklan 12 kohdassa määritellyn henkilötietojen tietoturvaloukkauksen, josta on ilmoitettava mainitun asetuksen 33 artiklan mukaisesti, niiden on ilmoitettava asiasta kyseisen asetuksen 55 ja 56 artiklan nojalla toimivaltaisille valvontaviranomaisille **kohtuullisen ajan** kuluessa.

*Tarkistus*

1. Jos toimivaltaisilla viranomaisilla on viitteitä siitä, että keskeisen tai tärkeän toimijan 18 ja 20 artiklassa säädettyjen velvollisuuksien laiminlyönti aiheuttaa asetuksen (EU) 2016/679 4 artiklan 12 kohdassa määritellyn henkilötietojen tietoturvaloukkauksen, josta on ilmoitettava mainitun asetuksen 33 artiklan mukaisesti, niiden on ilmoitettava asiasta kyseisen asetuksen 55 ja 56 artiklan nojalla toimivaltaisille valvontaviranomaisille **ilman aiheetonta viivytystä ja joka tapauksessa 72 tunnin** kuluessa.

**Tarkistus 153**  
**Ehdotus direktiiviksi**  
**32 artikla – 3 kohta**

*Komission teksti*

3. Jos asetuksen (EU) 2016/679 nojalla toimivaltainen valvontaviranomainen on sijoittautunut toiseen jäsenvaltioon kuin toimivaltainen viranomainen, **toimivaltainen viranomaisen voi ilmoittaa** asiasta samaan jäsenvaltioon sijoittautuneelle valvontaviranomaiselle.

*Tarkistus*

3. Jos asetuksen (EU) 2016/679 nojalla toimivaltainen valvontaviranomainen on sijoittautunut toiseen jäsenvaltioon kuin toimivaltainen viranomainen, **toimivaltaisen viranomaisen on myös ilmoitettava** asiasta samaan jäsenvaltioon sijoittautuneelle valvontaviranomaiselle.

**Tarkistus 154**  
**Ehdotus direktiiviksi**  
**36 artikla – 2 kohta**

*Komission teksti*

2. Siirretään komissiolle [...] lähtien viideksi vuodeksi valta antaa 18 artiklan **6** kohdassa ja **21** artiklan **2** kohdassa tarkoitettuja delegoituja säädöksiä.

*Tarkistus*

2. Siirretään komissiolle [...] lähtien viideksi vuodeksi valta antaa 18 artiklan **5** kohdassa ja **20** artiklan **3** kohdassa tarkoitettuja delegoituja säädöksiä.

**Tarkistus 155**  
**Ehdotus direktiiviksi**  
**36 artikla – 3 kohta**

*Komission teksti*

3. *Euroopan parlamentti tai neuvosto voi milloin tahansa peruuttaa 18 artiklan 6 kohdassa ja 21 artiklan 2 kohdassa tarkoitetun säädösvallan siirron. Peruuttamispäätöksellä lopetetaan tuossa päätöksessä mainittu säädösvallan siirto. Peruuttaminen tulee voimaan sitä päivää seuraavana päivänä, jona sitä koskeva päätös julkaistaan Euroopan unionin virallisessa lehdessä, tai jonakin myöhempänä, kyseisessä päätöksessä mainittuna päivänä. Peruuttamispäätös ei vaikuta jo voimassa olevien delegoitujen säädösten pätevyyteen.*

**Tarkistus 156**  
**Ehdotus direktiiviksi**  
**36 artikla – 6 kohta**

*Komission teksti*

6. Edellä olevien 18 artiklan 6 kohdan tai 21 artiklan 2 kohdan nojalla annettu delegoitu säädös tulee voimaan ainoastaan, jos Euroopan parlamentti tai neuvosto ei ole kahden kuukauden kuluessa siitä, kun asianomainen säädös on annettu tiedoksi Euroopan parlamentille ja neuvostolle, ilmaissut vastustavansa sitä tai jos sekä Euroopan parlamentti että neuvosto ovat ennen mainitun määräajan päättymistä ilmoittaneet komissiolle, että ne eivät vastusta säädöstä. Euroopan parlamentin tai neuvoston aloitteesta tätä määräaika jatketaan kahdella kuukaudella.

*Tarkistus*

3. *Edellä olevien 18 artiklan 5 kohdan tai 20 artiklan 3 kohdan nojalla annettu delegoitu säädös tulee voimaan ainoastaan, jos Euroopan parlamentti tai neuvosto ei ole kolmen kuukauden kuluessa siitä, kun asianomainen säädös on annettu tiedoksi Euroopan parlamentille ja neuvostolle, ilmaissut vastustavansa sitä tai jos sekä Euroopan parlamentti että neuvosto ovat ennen mainitun määräajan päättymistä ilmoittaneet komissiolle, että ne eivät vastusta säädöstä. Euroopan parlamentin tai neuvoston aloitteesta tätä määräaika jatketaan kolmella kuukaudella.*

*Tarkistus*

6. Edellä olevien 18 artiklan 5 kohdan tai 20 artiklan 3 kohdan nojalla annettu delegoitu säädös tulee voimaan ainoastaan, jos Euroopan parlamentti tai neuvosto ei ole kahden kuukauden kuluessa siitä, kun asianomainen säädös on annettu tiedoksi Euroopan parlamentille ja neuvostolle, ilmaissut vastustavansa sitä tai jos sekä Euroopan parlamentti että neuvosto ovat ennen mainitun määräajan päättymistä ilmoittaneet komissiolle, että ne eivät vastusta säädöstä. Euroopan parlamentin tai neuvoston aloitteesta tätä määräaika jatketaan kahdella kuukaudella.

## LIITE: LUETTELO YHTEISÖISTÄ TAI HENKILÖISTÄ, JOILTA VALMISTELIJA ON SAANUT TIETOJA

Seuraavan luettelon laatiminen on täysin vapaaehtoista, ja valmistelija on siitä yksin vastuussa. Valmistelija on saanut tietoja seuraavilta yhteisöiltä tai henkilöiltä valmistellessaan lausuntoa ennen sen hyväksymistä valiokunnassa:

Henkilö	Yhteisö
	BSA (The Software Alliance)
	BusinessEurope
	Confederation of Danish Industries
	Danish Permanent Representation
	Deutsche Telekom
	Digital Europe
	DOT Europe
	ETNO (European Telecommunications Network Operators)
	French Permanent Representation
	German Permanent Representation
	HUAWEI
	IFPI
	INTEL
	ITI (The Information Technology Industry Council)
	Kaspersky
	MÆRSK
	Microsoft
	ICANN
	MOTION PICTURE ASSOCIATION
	Orgalim
	Palo Alto Networks

	Rettighedsalliancen
--	---------------------



**ASIAN KÄSITTELY**  
**LAUSUNNON ANTAVASSA VALIOKUNNASSA**

<b>Otsikko</b>	Toimenpiteet yhteisen korkeatasoisen kyberturvallisuuden varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoaminen
<b>Viiteasiakirjat</b>	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
<b>Asiasta vastaava valiokunta</b> Ilmoitettu istunnossa (pvä)	ITRE 21.1.2021
<b>Lausunnon antanut valiokunta</b> Ilmoitettu istunnossa (pvä)	IMCO 21.1.2021
<b>Valmistelija</b> Nimitetty (pvä)	Morten Løkkegaard 9.2.2021
<b>Valiokuntakäsittely</b>	26.5.2021                      21.6.2021
<b>Hyväksytty (pvä)</b>	12.7.2021
<b>Lopullisen äänestyksen tulos</b>	+:                      42 -:                      1 0:                      2
<b>Lopullisessa äänestyksessä läsnä olleet jäsenet</b>	Alex Agius Saliba, Andrus Ansip, Pablo Arias Echeverría, Alessandra Basso, Brando Benifei, Adam Bielan, Hynek Blaško, Biljana Borzan, Vlad-Marius Botoș, Markus Buchheit, Andrea Caroppo, Anna Cavazzini, Dita Charanzová, Deirdre Clune, David Cormand, Carlo Fidanza, Evelyne Gebhardt, Alexandra Geese, Sandro Gozi, Maria Grapini, Svenja Hahn, Virginie Joron, Eugen Jurzyca, Marcel Kolaja, Kateřina Konečná, Andrey Kovatchev, Jean-Lin Lacapelle, Maria-Manuel Leitão-Marques, Morten Løkkegaard, Antonius Manders, Leszek Miller, Anne-Sophie Pelletier, Miroslav Radačovský, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róza Thun und Hohenstein, Marco Zullo
<b>Lopullisessa äänestyksessä läsnä olleet varajäsenet</b>	Clara Aguilera, Maria da Graça Carvalho, Christian Doleschal, Claude Gruffat, Jiří Pospíšil, Kosma Złotowski

**LOPULLINEN ÄÄNESTYS NIMENHUUTOÄÄNESTYKSENÄ  
LAUSUNNON ANTAVASSA VALIOKUNNASSA**

42	+
ECR	Adam Bielan, Carlo Fidanza, Kosma Zlotowski
ID	Alessandra Basso, Hynek Blaško, Markus Buchheit, Virginie Joron, Jean-Lin Lacapelle
PPE	Pablo Arias Echeverría, Andrea Caroppo, Maria da Graça Carvalho, Deirdre Clune, Christian Doleschal, Andrey Kovatchev, Antonius Manders, Jiří Pospíšil, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róza Thun und Hohenstein
Renew	Andrus Ansip, Vlad-Marius Botoș, Dita Charanzová, Sandro Gozi, Morten Løkkegaard, Marco Zullo
S&D	Alex Agius Saliba, Clara Aguilera, Brando Benifei, Biljana Borzan, Evelyne Gebhardt, Maria Grapini, Maria-Manuel Leitão-Marques, Leszek Miller, Christel Schaldemose
The Left	Kateřina Konečná, Anne-Sophie Pelletier
Verts/ALE	Anna Cavazzini, David Cormand, Alexandra Geese, Claude Gruffat, Marcel Kolaja

1	-
NI	Miroslav Radačovský

2	0
ECR	Eugen Jurzyca
Renew	Svenja Hahn

Symbolien selitys:

+ : puolesta

- : vastaan

0 : tyhjää