Euroopan unionin
neuvosto

Bryssel, 26. marraskuuta 2021
(OR. en)

14337/21

Toimielinten välinen asia:
2020/0359(COD)

CODEC 1541
CSC 416
CSCI 147
CYBER 312
DATAPROTECT 269
JAI 1295
MI 891
TELECOM 435

ILMOITUS

Lähettäjä:	Neuvoston pääsihteeristö
Vastaanottaja:	Neuvosto
Ed. asiak. nro:	9583/2/21, 11724/21
Kom:n asiak. nro:	14150/20
Asia:	Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta – *Yleisnäkemys*

I JOHDANTO

1. Komissio antoi 16. joulukuuta 2020 ehdotuksen direktiiviksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa (tarkistettu verkko- ja tietoturvadirektiivi tai NIS 2- direktiivi)[1]. Sen tarkoituksena on korvata nykyinen verkko- ja tietoturvadirektiivi[2].

---

[1] Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta.

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

Direktiiviehdotus oli yksi niistä toimenpiteistä, joita esitettiin EU:n kyberturvallisuusstrategiassa digitaaliselle vuosikymmenelle[3] tarkoituksena varmistaa, että kansalaiset ja yritykset voivat hyötyä luotettavista digitaaliteknologioista.

2. Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 114 artiklaan perustuvan ehdotuksen tarkoituksena on parantaa julkisten ja yksityisten toimijoiden, toimivaltaisten viranomaisten ja yleensäkin koko unionin häiriönsietokykyä ja kykyä vastata uhkiin.

3. Euroopan parlamentissa ehdotuksen käsittelystä vastaa teollisuus-, tutkimus- ja energiavaliokunta (ITRE). Valiokunta hyväksyi esittelijän raportin 28. lokakuuta 2021.

4. Euroopan talous- ja sosiaalikomitea antoi lausuntonsa 28. huhtikuuta 2021.

5. Pysyvien edustajien komitea päätti 3. helmikuuta 2021 kuulla ehdotuksesta Euroopan alueiden komiteaa[4]. Euroopan alueiden komitea ei ole toistaiseksi antanut lausuntoaan.

6. Euroopan tietosuojavaltuutettu antoi lausuntonsa 11. maaliskuuta 2021[5].

7. EU:n kyberturvallisuusstrategiasta digitaaliselle vuosikymmenelle 22. maaliskuuta 2021 antamissaan päätelmissä[6] neuvosto pani merkille verkko- ja tietoturvadirektiiviin perustuvan uuden ehdotuksen ja muistutti tukevansa kansallisten kyberturvallisuuskehysten vahvistamista ja yhdenmukaistamista sekä jäsenvaltioiden välistä jatkuvaa yhteistyötä.

8. Eurooppa-neuvosto kehotti 21.–22. lokakuuta 2021 antamissaan päätelmissä jatkamaan työtä tarkistettua verkko- ja tietoturvadirektiiviä koskevan ehdotuksen parissa.

---

[3] 14133/20.

[4] 5573/21.

[5] Lausunto 5/2021 kyberturvallisuusstrategiasta ja tarkistetusta verkko- ja tietoturvadirektiivistä.

[6] 6722/21.

II KÄSITTELY NEUVOSTON VALMISTELUELIMISSÄ

9. Neuvostossa ehdotusta on tarkasteltu kyberkysymysten horisontaalisessa työryhmässä. Ehdotuksen tarkastelu alkoi Portugalin puheenjohtajakaudella 19. tammikuuta, jolloin ehdotus luettiin läpi tarkkaan ja jäsenvaltiot saattoivat esittää kysymyksiä ja tärkeimpiä huolenaiheitaan komissiolle, joka selitti yksityiskohtaisesti tarkistettuun direktiiviin tehtyjä muutoksia.

10. Portugalin puheenjohtajakaudella ehdotusta esiteltiin ja käytiin läpi 17:ssä kyberkysymysten horisontaalisen työryhmän kokouksessa. Tämän jälkeen laadittu tilanneselvitys toimitettiin liikenne-, televiestintä- ja energianeuvostolle, joka kokoontui 4. kesäkuuta 2021.

11. Työskentelyä on jatkettu ja tehostettu Slovenian puheenjohtajakaudella tavoitteena yleisnäkemyksen muodostaminen liikenne-, televiestintä- ja energianeuvoston istunnossa 3. joulukuuta 2021. Slovenian puheenjohtajakaudella tarkistettua NIS 2 -direktiiviehdotusta käsiteltiin 15 kokouksessa ja siitä käytiin useita kahdenvälisiä keskusteluja kaikilla tasoilla.

12. Kyberkysymysten horisontaalisessa työryhmässä keskityttiin ensiksi ehdotuksen uudelleenlaadintaan, NIS 2 -direktiivin vuorovaikutukseen alakohtaisen lainsäädännön kanssa ja sen soveltamisalaan erityisesti julkishallinnon, DNS-juuripalvelinten ja poissulkemislausekkeen osalta. Tämän jälkeen käsiteltiin muun muassa vertaisarviointeja, lainkäyttövaltaa ja keskinäistä avunantoa, koordinoitua haavoittuvuuksien ilmaisemista, verkkotunnusten tietokantoja sekä rekisteröintitietoja ja kansainvälistä yhteistyötä.

13. Direktiiviehdotuksen tekstistä esitettiin ensimmäinen kompromissiehdotus 21. syyskuuta 2021[7] jäsenvaltioilta saatujen kirjallisten huomautusten ja epävirallisten asiakirjojen perusteella. Siinä otettiin huomioon myös aiempi kompromissiehdotus NIS 2 -direktiivin soveltamisalasta ja sen vuorovaikutuksesta alakohtaisen lainsäädännön kanssa.

---

[7] 12019/21.

14. Puheenjohtajavaltion kompromissiehdotuksen viimeisimmästä versiosta[8] keskusteltiin työryhmätasolla 22. marraskuuta 2021. Valtuuskunnat suhtautuivat yleisesti ottaen myönteisesti kompromissiehdotukseen, mutta jotkin niistä pitivät voimassa tarkasteluvaraumansa tai kommentoivat joitakin ehdotuksen osia. Joihinkin tekstin osiin ehdotettiin vielä teknistä uudelleenmuotoilua.

III ASIASISÄLTÖ

15. Työryhmätason keskustelujen perusteella seuraavat seikat on määritelty tärkeimmiksi poliittisiksi kysymyksiksi:

a) Soveltamisala (2 artikla)

Jäsenvaltioiden esittämä tärkein huolenaihe NIS 2 -ehdotuksesta käytyjen keskustelujen alusta lähtien on ollut direktiivin soveltamisalaan kuuluvien toimijoiden määrän merkittävä lisääntyminen ja erityisesti kokokattosäännön käyttöönotto. Tämän säännön mukaan NIS 2 -direktiivin soveltamisalaan kuuluvat kaikki direktiivin kattamilla aloilla toimivat tai sen kattamia palveluja tarjoavat keskisuuret ja suuret toimijat. Kompromissiehdotuksessa säilytetään tämä yleissääntö, mutta siinä esitetään lisäsäännöksiä, joilla varmistetaan tarvittava oikeasuhteisuus, korkeatasoisempi riskinhallinta ja selkeät kriittisyyttä koskevat kriteerit, joilla määritetään direktiivin soveltamisalaan kuuluvat toimijat. Kompromissiehdotus sisältää lisäksi säännöksiä valvontatoimenpiteiden käytön ensisijaisuudesta riskiperusteisessa arviointitavassa.

---

[8] 12019/5/21 REV 5.

b) Julkishallinto (2 artiklan 2 a kohta)

Julkishallinnon sisällyttäminen NIS 2 -direktiivin soveltamisalaan oli kiistanalainen aihe, sillä julkishallinto eroaa muista NIS 2 -direktiivin kattamista aloista. Puheenjohtajavaltio on pyrkinyt tekstiin, jossa otetaan tasapainoisesti huomioon kansallisten julkishallintojen erityispiirteet ja varmistetaan jäsenvaltioille tietty joustavuus niiden määritellessä NIS 2 -direktiivin soveltamisalaan kuuluvia julkishallinnon toimijoita. Kompromissitekstin mukaan NIS 2 -direktiiviä sovelletaan näin ollen keskushallintojen julkisiin toimijoihin, mutta jäsenvaltiot voivat säätää, että sitä sovelletaan myös alue- ja paikallishallintojen julkisiin toimijoihin.

c) Poissulkemislauseke (2 artiklan 3 a ja 3 aa kohdat)

Jäsenvaltiot halusivat selventää poissulkemislauseketta entisestään siltä osin, että direktiiviä ei sovelleta toimijoihin, jotka toimivat pääasiassa puolustuksen, kansallisen turvallisuuden, yleisen turvallisuuden tai lainvalvonnan alalla tai joiden toiminta liittyy kansalliseen turvallisuuteen tai puolustukseen. Soveltamisalan ulkopuolelle jäävät myös oikeuslaitos, kansanedustuslaitokset ja keskuspankit.

d) Vuorovaikutus alakohtaisen lainsäädännön kanssa

Jäsenvaltiot korostivat, että NIS 2 -direktiivi on linjattava alakohtaiseen lainsäädäntöön, erityisesti finanssialan digitaalisesta häiriönsietokyvystä annettuun asetukseen ja kriittisten toimijoiden häiriönsietokykyä koskevaan direktiiviin. NIS 2 -direktiivin on tarkoitus muodostaa perustaso kyberturvallisuuden vähimmäistason yhdenmukaistamiselle, ja se sisältää alakohtaisia unionin säädöksiä koskevan artiklan (2 b artikla). Mitä tulee vuorovaikutukseen kriittisten toimijoiden häiriönsietokyvystä annetun direktiivin kanssa, kompromissiehdotuksessa selkeytetään kaikki vaaratekijät huomioon ottavaa toimintatapaa. Muut tärkeät lisäykset liittyvät toimivaltaisten viranomaisten yhteistyöjärjestelyihin asianomaisten säädösten mukaisesti.

e) Vertaisoppiminen (16 artikla)

Lähes kaikki jäsenvaltiot vastustivat komission aikomusta ottaa käyttöön pakolliset vertaisarvioinnit. Ehdotetulla kompromissilla varmistetaan, että uusi vertaisoppimismenetelmä perustuu keskinäiseen luottamukseen ja että se on vapaaehtoinen, jäsenvaltiojohtoinen prosessi.

f) Lainkäyttövalta ja alueperiaate (24 artikla) ja keskinäinen avunanto (34 artikla)

Jäsenvaltiot ovat ilmaisseet huolensa komission ehdottamien tieto- ja viestintätekniikan alan toimijoiden eriytettyjen lainkäyttöalueiden seurauksista. Kompromississa on selkeytetty toimijoiden tyyppiin perustuvan lainkäyttövallan käsitettä ja lujitettu keskinäisen avunannon säännöksiä.

g) Raportointivelvoitteet (20 artikla)

Jäsenvaltioiden mielestä raportointivelvoitteet aiheuttaisivat kohtuutonta rasitetta NIS 2 -direktiiviin kuuluville toimijoille ja johtaisivat liialliseen raportointiin, joten kompromissitekstistä on poistettu merkittäviä kyberuhkia koskeva pakollinen raportointi.

IV LOPUKSI

16. Pysyvien edustajien komitea pääsi 24. marraskuuta 2021 yhteisymmärrykseen liitteessä olevasta kompromissitekstistä ja päätti toimittaa sen liikenne-, televiestintä- ja energianeuvostolle yleisnäkemyksen muodostamista varten.

17. Neuvostoa pyydetään näin ollen hyväksymään liitteessä oleva puheenjohtajavaltion esittämä kompromissiteksti ja muodostamaan yleisnäkemys istunnossaan 3. joulukuuta 2021.

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI

toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa, asetuksen (EU) 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta

(ETA:n kannalta merkityksellinen teksti)

EUROOPAN PARLAMENTTI JA EUROOPAN UNIONIN NEUVOSTO, jotka

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

ottavat huomioon Euroopan komission ehdotuksen,

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

ottavat huomioon Euroopan talous- ja sosiaalikomitean lausunnon[9],

ottavat huomioon alueiden komitean lausunnon[10],

noudattavat tavallista lainsäätämisjärjestystä,

---

[9] EUVL C , , s. .

[10] EUVL C , , s. .

sekä katsovat seuraavaa:

(1) Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/1148[11] tavoitteena oli kehittää kyberturvallisuusvalmiuksia kaikkialla unionissa, lieventää keskeisten palvelujen tarjoamiseen keskeisillä aloilla käytettäviin verkko- ja tietojärjestelmiin kohdistuvia uhkia ja varmistaa tällaisten palvelujen jatkuvuus kyberturvapoikkeamatilanteissa, ja tukea näin unionin talouden ja yhteiskunnan tehokasta toimintaa.

(2) Direktiivin (EU) 2016/1148 voimaantulon jälkeen on edistytty merkittävästi kyberturvavalmiuksien parantamisessa unionissa. Kyseisen direktiivin uudelleentarkastelu on osoittanut, että se on vauhdittanut institutionaalista ja sääntelyyn perustuvaa lähestymistapaa kyberturvallisuuteen unionissa ja tasoittanut tietä merkittävälle ajattelutavan muutokselle. Direktiivillä on varmistettu kansallisten kehysten luominen määrittelemällä kansalliset [...] **verkko- ja tietojärjestelmien** turvallisuusstrategiat, luomalla kansallisia valmiuksia ja toteuttamalla sääntelytoimenpiteitä, jotka kattavat kunkin jäsenvaltion yksilöimät keskeiset infrastruktuurit ja toimijat. Se on myös edistänyt yhteistyötä unionin tasolla, kun on perustettu erityinen yhteistyöryhmä[12] ja tietoturvaloukkauksiin reagoivien kansallisten yksiköiden verkosto, jäljempänä 'CSIRT-verkosto'[13]. Näistä saavutuksista huolimatta direktiivin (EU) 2016/1148 uudelleentarkastelussa on tullut esiin sisälähtöisiä puutteita, joiden vuoksi direktiivillä ei kyetä tuloksellisesti puuttumaan nykyisiin ja esiin nousemassa oleviin kyberturvallisuushaasteisiin.

---

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

[12] Direktiivin (EU) 2016/1148 11 artikla.

[13] Direktiivin (EU) 2016/1148 12 artikla.

(3) Verkko- ja tietojärjestelmät ovat kehittyneet arjen keskeiseksi osaksi yhteiskuntien nopean digitalisaation ja verkottumisen myötä, myös rajat ylittävässä yhteydenpidossa. Tämä kehitys on laajentanut kyberturvauhkia ja tuonut mukanaan uusia haasteita, jotka edellyttävät mukautettuja, koordinoituja ja innovatiivisia vastatoimia kaikissa jäsenvaltioissa. Kyberturvapoikkeamien määrä, laajuus, kehittyneisyys, esiintymistiheys ja vaikutukset lisääntyvät, ja ne muodostavat merkittävän uhan verkko- ja tietojärjestelmien toiminnalle. Tämän seurauksena kyberturvapoikkeamat voivat haitata taloudellisen toiminnan harjoittamista sisämarkkinoilla, aiheuttaa taloudellisia tappioita, heikentää käyttäjien luottamusta ja aiheuttaa huomattavaa vahinkoa unionin taloudelle ja yhteiskunnalle. Kyberturvavalmiudet ja kyberturvan toimivuus ovat siksi nyt tärkeämpiä kuin koskaan sisämarkkinoiden moitteettoman toiminnan kannalta.

(4) Direktiivin 1148/2016/EU oikeusperusta oli Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 114 artikla, jonka tavoitteena on sisämarkkinoiden toteuttaminen ja toiminta tehostamalla toimenpiteitä kansallisten sääntöjen lähentämiseksi. Palveluja tai taloudellisesti merkityksellisiä toimintoja tarjoaville toimijoille asetetut kyberturvallisuusvaatimukset vaihtelevat huomattavasti jäsenvaltioittain vaatimusten tyypin, yksityiskohtaisuuden ja valvontamenetelmän osalta. Nämä erot aiheuttavat lisäkustannuksia ja vaikeuksia yrityksille, jotka tarjoavat tavaroita tai palveluja rajojen yli. Yhden jäsenvaltion asettamat vaatimukset, jotka ovat erilaisia tai jopa ristiriidassa toisen jäsenvaltion asettamien vaatimusten suhteen, voivat vaikuttaa merkittävästi rajat ylittävään toimintaan.

Lisäksi kyberturva**toimenpiteiden** [...] puutteellisella toteutuksella yhdessä jäsenvaltiossa on todennäköisesti vaikutuksia muiden jäsenvaltioiden kyberturvatasoon, erityisesti kun otetaan huomioon rajojen yli tapahtuvan toiminnan määrä. Direktiivin (EU) 2016/1148 uudelleentarkastelu on osoittanut, että jäsenvaltiot ovat panneet sen täytäntöön hyvin eri tavoin, myös sen soveltamisalan osalta, jonka rajaaminen on suurelta osin jätetty jäsenvaltioiden harkintavaltaan. Direktiivissä (EU) 2016/1148 säädetään myös, että jäsenvaltioilla on hyvin laaja harkintavalta siinä säädettyjen turvallisuutta ja vaaratilanteista ilmoittamista koskevien velvoitteiden täytäntöönpanossa. Nämä velvoitteet on näin ollen pantu täytäntöön huomattavasti eri tavoin kansallisella tasolla. Samankaltaisia eroja esiintyi valvontaa ja täytäntöönpanoa koskevien direktiivin säännösten osalta.

(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 [...] **toimenpiteitä**. Tällä direktiivillä pyritään poistamaan näitä suuria eroja jäsenvaltioiden välillä erityisesti vahvistamalla vähimmäissäännöt koordinoidun 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.

(6) [...] Jäsenvaltioiden **olisi voitava** toteuttaa tarvittavat toimenpiteet keskeisten turvallisuusetujensa suojaamiseksi, yleisen järjestyksen ja turvallisuuden takaamiseksi sekä rikosten tutkinnan, selvittämisen ja syytteeseenpanon mahdollistamiseksi unionin oikeuden mukaisesti. [...] **Direktiiviä ei olisi sovellettava tiettyihin julkisiin tai yksityisiin toimijoihin, jotka harjoittavat toimintaansa näillä aloilla. Sitä ei myöskään olisi sovellettava toimijoiden näillä aloilla toteuttamaan toimintaan.** Mikään jäsenvaltio ei **myöskään** ole velvollinen antamaan tietoja, joiden ilmaiseminen olisi vastoin sen keskeisiä yleiseen turvallisuuteen liittyviä etuja. [...] Merkityksellisiä ovat turvallisuusluokiteltujen tietojen suojaamista koskevat kansalliset [...] **tai** unionin säännöt, salassapitosopimukset ja epäviralliset salassapitosopimukset, kuten Traffic Light Protocol -käsittelyluokitus[14].

(6 a) Kaikkeen tämän direktiivin mukaiseen henkilötietojen käsittelyyn sovelletaan henkilötietojen ja yksityisyyden suojaa koskevaa unionin oikeutta. Tämä direktiivi ei etenkään rajoita Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 ja direktiivin 2002/21/EY soveltamista, eikä sen siten pitäisi etenkään vaikuttaa edellä mainitun unionin tietosuojalainsäädännön noudattamisen valvonnassa toimivaltaisten riippumattomien valvontaviranomaisten tehtäviin ja valtuuksiin.

---

[14] Liikennevalomalli (Traffic Light Protocol, TLP) on tapa, jolla tietoa antava taho voi tiedottaa tiedon vastaanottajille mahdollisista rajoituksista tietojen levittämisessä edelleen. Sitä käytetään lähes kaikissa CSIRT-yhteisöissä ja joissakin ISAC-keskuksissa (Information Analysis and Sharing Centres).

(7) Kun direktiivi (EU) 2016/1148 kumotaan, toimialoittainen soveltamisala olisi laajennettava koskemaan suurempaa osaa taloudesta johdanto-osan kappaleissa 4–6 esitettyjen huomioiden perusteella. Direktiivin (EU) 2016/1148 soveltamisalaa olisi sen vuoksi laajennettava kattavasti niihin aloihin ja palveluihin, jotka ovat olennaisen tärkeitä yhteiskunnan ja talouden avaintoimintojen kannalta sisämarkkinoilla. Säännöt eivät saisi poiketa toisistaan sen mukaan, ovatko toimijat keskeisten palvelujen tarjoajia vai digitaalisten palvelujen tarjoajia. Tämä erottelu on osoittautunut vanhentuneeksi, koska se ei kuvasta toimialojen tai palvelujen todellista merkitystä yhteiskunnalliselle ja taloudelliselle toiminnalle sisämarkkinoilla.

(8) Direktiivin (EU) 2016/1148 mukaisesti jäsenvaltiot olivat vastuussa sen määrittämisestä, mitkä toimijat täyttävät kriteerit, joiden perusteella niitä voidaan pitää keskeisten palvelujen tarjoajina, jäljempänä 'tunnistamisprosessi'. Jotta voidaan poistaa jäsenvaltioiden väliset suuret erot tältä osin ja varmistaa kaikkien asianomaisten toimijoiden riskinhallintavaatimusten ja raportointivelvoitteiden oikeusvarmuus, olisi vahvistettava yhdenmukainen kriteeri, jolla määritetään tämän direktiivin soveltamisalaan kuuluvat toimijat. Tämän kriteerin olisi koostuttava kokokattosäännön soveltamisesta, jolloin kaikki komission suosituksessa 2003/361/EY[15] määritellyt keskisuuret ja suuret yritykset, jotka toimivat tämän direktiivin kattamilla aloilla tai tarjoavat tämän direktiivin kattamia palveluja, kuuluvat sen soveltamisalaan. [...]

---

[15] Komission suositus 2003/361/EY, annettu 6 päivänä toukokuuta 2003, mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä (EUVL L 124, 20.5.2003, s. 36).

(8 a) Jotta saadaan selkeä yleiskuva siitä, mitkä toimijat kuuluvat tämän direktiivin soveltamisalaan, jäsenvaltioiden olisi voitava ottaa käyttöön kansalliset ilmoitusmenetelmät, joiden mukaan tämän direktiivin soveltamisalaan kuuluvien toimijoiden on toimitettava tämän direktiivin mukaisesti toimivaltaisille viranomaisille tai jäsenvaltioiden tätä tarkoitusta varten nimeämille elimille ainakin nimensä, osoitteensa ja yhteystietonsa, ilmoitettava toimialansa tai tarjoamansa palvelun tyyppi ja tarvittaessa toimitettava luettelo niistä jäsenvaltioista, joissa toimija tarjoaa palvelujaan. Jäsenvaltiot voivat päättää tarkoituksenmukaisista menetelmistä, jos olemassa on kansallisen tason rekisterejä, joiden avulla tämän direktiivin soveltamisalaan kuuluvat toimijat voidaan määritellä.

(9) Tämän direktiivin olisi [...] katettava myös sellaiset pienet tai mikrotoimijat, jotka täyttävät tietyt kriteerit, jotka osoittavat niiden olevan avainasemassa jäsenvaltion taloudessa tai yhteiskunnassa tai tietyllä alalla tai tietyntyyppisissä palveluissa. Jäsenvaltioiden [...] vastuulla olisi oltava toimittaa komissiolle **ainakin merkitykselliset tiedot määriteltyjen toimijoiden lukumäärästä, niiden toimialasta tai niiden tarjoaman palvelun tyypistä sekä kriteereistä, joiden perusteella toimijat on määritelty. Jäsenvaltiot voivat myös päättää toimittaa komissiolle näiden toimijoiden nimet, jos se on kansallisten turvallisuussääntöjen mukaista.**

(9 a) Tämän direktiivin soveltamisalan ulkopuolelle on suljettu ne julkishallinnon toimijat, jotka harjoittavat toimintaansa kansallisen turvallisuuden, puolustuksen, yleisen turvallisuuden tai lainvalvonnan alalla, sekä oikeuslaitokset, kansanedustuslaitokset ja keskuspankit. Tämän direktiivin soveltamiseksi sääntelyvaltaa käyttävien toimijoiden ei katsota harjoittavan toimintaansa lainvalvonnan alalla, joten niitä ei ole suljettu tällä perusteella tämän direktiivin soveltamisalan ulkopuolelle. Tämän direktiivin soveltamisalaan eivät kuulu myöskään ne keskushallintojen julkiset toimijat, jotka on perustettu yhteisesti kolmannen maan kanssa kansainvälisen sopimuksen mukaisesti.

(9 aa) **Jäsenvaltioiden olisi voitava säätää, että ne toimijat, jotka on määritelty ennen tämän direktiivin voimaantuloa direktiivin (EU) 2016/1148 mukaisiksi keskeisten palvelujen tarjoajiksi, on katsottava keskeisiksi toimijoiksi.**

(9 aaa) **Tätä direktiiviä ei sovelleta jäsenvaltioiden ulkomailla sijaitseviin diplomaattisiin edustustoihin ja konsuliedustustoihin ja niiden käyttämään omaan tieto- ja viestintätekniikan infrastruktuuriin siltä osin kuin kyseinen infrastruktuuri sijaitsee ulkomailla tai sitä ylläpidetään ulkomailla sijaitsevia käyttäjiä varten.**

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

(11) **[...] Tämän direktiivin soveltamisalaan kuuluvat toimijat olisi luokiteltava kahteen ryhmään eli keskeisiin ja tärkeisiin toimijoihin toimialan tai tarjottujen palvelujen tyypin kriittisyyden sekä toimijan koon perusteella. Tältä osin olisi tapauksen mukaan otettava asianmukaisesti huomioon myös mahdolliset merkitykselliset alakohtaiset riskinarvioinnit tai toimivaltaisten viranomaisten antama ohjeistus.** Sekä keskeisiin että tärkeisiin toimijoihin olisi sovellettava [...] riskinhallintavaatimuksia ja raportointivelvoitteita. Näiden kahden toimijaluokan valvonta- ja seuraamusjärjestelmät olisi eriytettävä, jotta voidaan varmistaa oikeudenmukainen tasapaino toisaalta **riskiperusteisten** vaatimusten ja velvoitteiden ja toisaalta sääntöjen noudattamisen valvonnasta aiheutuvan hallinnollisen rasituksen välillä.

(12) **Tässä direktiivissä vahvistetaan kyberturvallisuusriskien hallintatoimenpiteiden ja raportointivelvoitteiden perustaso kaikilla direktiivin soveltamisalaan kuuluvilla aloilla. Jos** kyberturvallisuusriskien hallintatoimenpiteisiin **ja raportointivelvoitteisiin liittyvien alakohtaisten täydentävien säännösten katsotaan olevan tarpeen korkeatasoisen kyberturvallisuuden varmistamiseksi, komission olisi arvioitava, voitaisiinko tällaisia säännöksiä antaa täytäntöönpanosäädöksessä, sille tässä direktiivissä annetun vallan nojalla, jotta vältetään unionin säädösten kyberturvallisuutta koskevien säännösten hajanaisuus. Jos täytäntöönpanosäädökset eivät sovi tähän tarkoitukseen,** alakohtaisella lainsäädännöllä **voitaisiin** osaltaan varmistaa korkea kyberturvallisuustaso samalla kun otetaan kaikilta osin huomioon [...] **kyseisten** alojen erityispiirteet ja monitahoisuus. **Kyseisessä alakohtaisessa lainsäädännössä on esitettävä perustelut sille, miksi tässä direktiivissä annetun valtuutuksen mukainen täytäntöönpanosäädös ei ollut asianmukainen tähän tarkoitukseen. Tällaisissa unionin säädösten alakohtaisissa säännöksissä olisi samalla otettava asianmukaisesti huomioon kattavan ja yhdenmukaistetun kyberturvallisuuskehyksen tarve.** Tämä [...] ei vaikuta nykyiseen täytäntöönpanovaltaan, joka on siirretty komissiolle useilla aloilla, mukaan lukien liikenne ja energia.

(12 a) Jos alakohtainen unionin säädös **sisältää säännöksiä, joissa** edellytetään, että keskeiset tai tärkeät toimijat ottavat käyttöön kyberturvariskien hallintaan **ja velvoitteisiin liittyviä toimenpiteitä**, joilla ilmoitetaan **merkittävistä** poikkeamista tai [...] kyberuhista **ja joilla on vähintään vastaava vaikutus kuin tässä direktiivissä säädetyillä velvoitteilla**, olisi sovellettava kyseisiä alakohtaisia säännöksiä**, mukaan lukien valvontaa ja täytäntöönpanoa koskevat säännökset**. **Unionin säädöksen alakohtaisissa säännöksissä säädettyjen velvoitteiden vastaavaa vaikutusta määritettäessä olisi otettava huomioon seuraavat seikat: i) kyberturvallisuusriskien hallintatoimenpiteiden olisi koostuttava asianmukaisista ja oikeasuhteisista teknisistä ja organisatorisista toimenpiteistä niiden riskien hallitsemiseksi, joita kohdistuu toimijoiden palveluntarjonnassaan käyttämien verkko- ja tietojärjestelmien turvallisuuteen, ja niiden olisi sisällettävä vähintään kaikki tässä direktiivissä säädetyt osatekijät; ii) merkittävistä poikkeamista ja kyberuhista ilmoittamista koskevan velvoitteen olisi vastattava vähintään tässä direktiivissä säädettyjä velvoitteita ilmoitusten sisällön, muodon ja määräaikojen osalta; iii) alakohtaisten unionin säädösten mukaisten toimijoiden ja asiaankuuluvien viranomaisten raportointimenettelyjen olisi vastattava vähintään tässä direktiivissä säädettyjä velvoitteita raportoinnin sisällön, muodon ja määräaikojen osalta, ja niissä olisi otettava huomioon CSIRT-yksiköiden rooli; iv) asiaankuuluvien viranomaisten rajatylittävää yhteistyötä koskevien vaatimusten olisi vastattava vähintään tässä direktiivissä säädettyjä vaatimuksia. Jos unionin säädöksen alakohtaiset säännökset eivät kata tämän direktiivin soveltamisalaan kuuluvan toimialan kaikkia toimijoita, tämän direktiivin asiaankuuluvia säännöksiä olisi edelleen sovellettava niihin toimijoihin, joita nämä alakohtaiset säännökset eivät kata.**

(12 aa) Komission **olisi tarkasteltava säännöllisesti vastaavaa vaikutusta suhteessa unionin säädösten alakohtaisiin säännöksiin koskevan vaatimuksen soveltamista**. **Komissio kuulee yhteistyöryhmää valmistellessaan tätä määräaikaista tarkastelua.**

(12 aaa) Tulevissa alakohtaisissa unionin säädöksissä olisi otettava asianmukaisesti huomioon tämän direktiivin 4 artiklassa esitetyt määritelmät ja tämän direktiivin VI luvussa säädetty täytäntöönpanokehys.

(12 ab) **Kun unionin säädösten alakohtaisissa säännöksissä edellytetään, että keskeiset tai tärkeät toimijat ottavat käyttöön toimenpiteitä, joilla on vähintään vastaava vaikutus kuin tässä direktiivissä säädetyillä velvoitteilla, olisi vältettävä päällekkäisiä raportointivelvoitteita ja varmistettava kyberuhista tai poikkeamista tehtyjen ilmoitusten tehokas käsittely. Tätä tarkoitusta varten näissä alakohtaisissa säännöksissä jäsenvaltioiden voidaan sallia ottaa käyttöön yhteinen, automaattinen ja suora raportointimenetelmä kyberuhista ja poikkeamista ilmoittamiseksi sekä viranomaisille, joiden tehtävät on vahvistettu asiaankuuluvissa alakohtaisissa säännöksissä, että tässä direktiivissä säädetyistä kyberturvallisuustehtävistä vastaaville toimivaltaisille viranomaisille, mukaan luettuina tapauksen mukaan yhteyspisteet ja CSIRT-yksiköt, tai menetelmä, jolla varmistetaan järjestelmällinen ja välitön tiedonjako ja yhteistyö asiaankuuluvien viranomaisten ja CSIRT-yksiköiden välillä näiden ilmoitusten käsittelemiseksi. Raportoinnin yksinkertaistamiseksi ja yhteisen, automaattisen ja suoran raportointimenetelmän täytäntöön panemiseksi jäsenvaltiot voivat alakohtaisten lainsäädäntöjen mukaisesti käyttää yhteyspistettä, jonka ne perustavat tämän direktiivin 11 artiklan 5 a kohdan mukaisesti. Yhdenmukaistamisen varmistamiseksi alakohtaisten unionin säädösten raportointivelvoitteet olisi mukautettava tässä direktiivissä määriteltyihin velvoitteisiin. Jäsenvaltiot voivat päättää, että raportit toimitetaan tämän direktiivin mukaisesti toimivaltaisille viranomaisille tai CSIRT-yksiköille alakohtaisten lainsäädäntöjen mukaisesti.**

(13) Euroopan parlamentin ja neuvoston asetusta XXXX/XXXX olisi pidettävä tähän direktiiviin liittyvänä alakohtaisena unionin säädöksenä finanssialan toimijoiden osalta. Tämän direktiivin säännösten asemasta olisi sovellettava asetuksen XXXX/XXXX säännöksiä, jotka liittyvät tieto- ja viestintätekniikan riskinhallintatoimenpiteisiin, tieto- ja viestintätekniikkaan liittyvien poikkeamien hallintaan ja erityisesti poikkeamista raportointiin sekä digitaalisen toiminnallisen häiriönsietokyvyn testaukseen, tiedonjakojärjestelyihin ja kolmannen osapuolen tieto- ja viestintätekniikan riskeihin. Sen vuoksi jäsenvaltioiden ei pitäisi soveltaa tämän direktiivin säännöksiä, jotka koskevat kyberturvariskien hallintaa ja raportointivelvoitteita [...] sekä valvontaa ja täytäntöönpanoa, asetuksen XXXX/XXXX soveltamisalaan kuuluviin finanssialan toimijoihin. Samalla on tärkeää säilyttää tämän direktiivin mukainen vahva yhteys ja tiedonvaihto finanssialan kanssa. Tätä varten asetuksessa XXXX/XXXX annetaan [...] finanssialan osalta Euroopan valvontaviranomaisille ja asetuksen XXXX/XXXX mukaisille kansallisille toimivaltaisille viranomaisille mahdollisuus osallistua yhteistyöryhmän [...] **työhön** sekä vaihtaa tietoja ja tehdä yhteistyötä tämän direktiivin nojalla nimettyjen keskitettyjen asiointipisteiden ja kansallisten CSIRT-yksiköiden kanssa. Asetuksen XXXX/XXXX mukaisten toimivaltaisten viranomaisten olisi toimitettava tiedot merkittävistä tieto- ja viestintätekniikkaan liittyvistä poikkeamista **ja merkittävistä kyberuhista** myös tämän direktiivin mukaisesti nimetyille yhteyspisteille**, toimivaltaisille kansallisille viranomaisille tai kansallisille CSIRT-yksiköille**. **Tämä voidaan toteuttaa välittämällä poikkeamailmoitukset automaattisesti suoraan asianomaiselle vastaanottajalle tai ottamalla käyttöön yhteinen raportointialusta.** Lisäksi jäsenvaltioiden olisi edelleen sisällytettävä rahoitusala kyberturvallisuusstrategioihinsa, ja kansalliset CSIRT-yksiköt voivat kattaa finanssisektorin toiminnassaan.

(13 a) Jotta vältetään liitteessä I olevan 2 kohdan a alakohdassa tarkoitetuille ilmailualan toimijoille asetettujen kyberturvallisuusvaatimusten väliset puutteet ja päällekkäisyydet, Euroopan parlamentin ja neuvoston asetusten (EY) 300/2008[16] ja (EU) 2018/1139[17] mukaisesti nimettyjen kansallisten viranomaisten ja tämän direktiivin mukaisten toimivaltaisten viranomaisten olisi tehtävä yhteistyötä kyberturvallisuusriskien hallintatoimenpiteiden täytäntöönpanon ja näiden toimenpiteiden kansallisella tasolla tapahtuvan valvonnan osalta. Asetusten (EY) 300/2008 ja (EU) 2018/1139 mukaisesti nimetyt kansalliset viranomaiset voisivat katsoa, että toimija on noudattanut tämän direktiivin mukaisia kyberturvallisuusriskien hallintatoimenpiteitä näissä asetuksissa ja näiden asetusten nojalla annetuissa asiaankuuluvissa delegoiduissa säädöksissä ja täytäntöönpanosäädöksissä säädettyjen vaatimusten mukaisesti.

---

[16] **Euroopan parlamentin ja neuvoston asetus (EY) N:o 300/2008, annettu 11 päivänä maaliskuuta 2008, yhteisistä siviili-ilmailun turvaamista koskevista säännöistä ja asetuksen (EY) N:o 2320/2002 kumoamisesta (EUVL L 97, 9.4.2008, s. 72).**

[17] **Euroopan parlamentin ja neuvoston asetus (EU) 2018/1139, annettu 4 päivänä heinäkuuta 2018, yhteisistä siviili-ilmailua koskevista säännöistä ja Euroopan unionin lentoturvallisuusviraston perustamisesta, Euroopan parlamentin ja neuvoston asetusten (EY) N:o 2111/2005, (EY) N:o 1008/2008, (EU) N:o 996/2010, (EU) N:o 376/2014 ja direktiivien 2014/30/EU ja 2014/53/EU muuttamisesta sekä Euroopan parlamentin ja neuvoston asetusten (EY) N:o 552/2004, (EY) N:o 216/2008 ja neuvoston asetuksen (ETY) N:o 3922/91 kumoamisesta (EUVL L 212, 22.8.2018, s. 1).**

(14) Kyberturvallisuuden ja toimijoiden fyysisen turvallisuuden välisten yhteyksien vuoksi olisi varmistettava johdonmukainen lähestymistapa Euroopan parlamentin ja neuvoston direktiivin (EU) XXX/XXX 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 [...] mukaisesti **toimivaltaisten** viranomaisten olisi tehtävä yhteistyötä ja vaihdettava tietoja erityisesti kriittisten toimijoiden, kyberuhkien, kyberturvallisuusriskien ja poikkeamien **sekä** kriittisiin toimijoihin **ja niitä vastaaviin muihin toimijoihin** vaikuttavien **muiden kuin kyberturvallisuuteen liittyvien riskien, uhkien ja poikkeamien** tunnistamisen suhteen; yhteistyön ja tietojenvaihdon olisi koskettava **myös** kriittisten toimijoiden toteuttamia kyberturvallisuustoimenpiteitä **ja fyysisiä toimenpiteitä sekä näitä toimijoita koskevien valvontatoimien tuloksia**. **Lisäksi jotta valvontatoimia voitaisiin virtaviivaistaa molempien direktiivien mukaisesti nimettyjen toimivaltaisten viranomaisten välillä ja jotta kyseisten toimijoiden hallinnollinen rasite voitaisiin minimoida, toimivaltaisten viranomaisten olisi pyrittävä yhdenmukaistamaan poikkeamailmoitusmallit ja valvontamenettelyt.** Direktiivin (EU) XXX/XXX mukaisesti toimivaltaiset viranomaiset [...] **voivat tarvittaessa pyytää** tämän direktiivin mukaisesti toimivaltaisia viranomaisia [...] käyttämään valvonta- ja täytäntöönpanovaltuuksiaan **suhteessa** kriittiseksi määriteltyyn keskeiseen toimijaan [...]. [...]

(14 a) **Digitaalisen infrastruktuurin toimialaan kuuluvien toimijoiden toiminta perustuu lähtökohtaisesti verkko- ja tietojärjestelmiin, ja näin ollen tästä direktiivistä johtuvien näitä toimijoita koskevien velvoitteiden, jotka ovat osa niiden kyberturvallisuusriskien hallinta- ja raportointivelvoitteita, olisi liityttävä kattavasti kyseisten järjestelmien fyysiseen turvallisuuteen. Koska näistä seikoista säädetään tässä direktiivissä, direktiivin (EU) XXX/XXX [kriittisten yksiköiden häiriönsietokykyä koskeva direktiivi] III–VI lukua ei sovelleta näihin toimijoihin.**

(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 [...] **sisämarkkinoiden kannalta tärkeisiin** DNS-palvelujen tarjoajiin DNS-**palveluntarjonta- ja** selvitysketjussa, mukaan lukien [...] aluetunnusrekisterit (TLD-rekisterit) [...], **verkkotunnusten rekisteröintipalveluja tarjoavat toimijat,** verkkotunnuksia vastaavia IP-osoitteita selvittävien auktoritatiivisten nimipalvelinten **ylläpitäjät** ja osoitteita ensin sisäisesti selvittävien rekursiivisten nimipalvelinten **ylläpitäjät**. **Käsitteen 'DNS-palveluntarjoaja' ei pitäisi tarkoittaa kyseisen toimijan ja siihen sidoksissa olevien toimijoiden omiin tarkoituksiin ylläpidettyjä DNS-palveluja. Tästä direktiivistä johtuvat tätä toimijaluokkaa koskevat kyberturvallisuusvelvoitteet on rajattu tiukasti koskemaan ainoastaan kyberturvallisuusriskien hallintatoimenpiteitä ja raportointia, ja näin ollen ne eivät vaikuta monisidosryhmäisen yhteisön harjoittamaan maailmanlaajuisen DNS-järjestelmän hallinnointiin.**

(16) Pilvipalvelujen olisi katettava palvelut, jotka mahdollistavat skaalattavien ja joustavien tietoteknisten resurssien jaettavan ja hajautetun reservin laajan tarveperusteisen etäkäytön. Näihin tietoteknisiin resursseihin kuuluu esimerkiksi verkkoja, palvelimia ja muuta infrastruktuuria, käyttöjärjestelmiä, ohjelmistoja, tallennustilaa, sovelluksia ja palveluja. **Pilvipalvelujen palvelumalleihin kuuluvat muun muassa infrastruktuuripalvelu (IaaS), alustapalvelu (PaaS), sovelluspalvelu (SaaS) ja tietoverkkopalvelu (NaaS).** Pilvipalvelujen toimintamalleina olisi otettava huomioon yksityiset, yhteisövetoiset, julkiset ja hybridipilvipalvelut. Edellä mainituilla palvelu- ja toimintamalleilla tarkoitetaan samaa kuin standardissa ISO/IEC 17788:2014 määritellyillä palvelu- ja toimintamalleilla. Pilvipalvelun käyttäjän kykyä käyttää yksipuolisesti ja oma-aloitteisesti tietojenkäsittelyvalmiuksia, kuten palvelinaikaa tai verkkotallennustilaa ilman pilvipalveluntarjoajan inhimillistä panosta voitaisiin kuvata 'tarvepohjaiseksi ohjaukseksi'. 'Laajalla etäkäytöllä' tarkoitetaan sitä, että pilvipalveluresursseja tarjotaan verkossa ja niitä voidaan käyttää menetelmillä, jotka sallivat erilaisten prosessointivalmiuksiltaan kevyiden tai raskaiden päätelaitteiden käytön (esim. älypuhelimet, tablettitietokoneet, kannettavat tietokoneet, työasemat).

Termi 'skaalautuva' viittaa tietoteknisiin resursseihin, joita pilvipalvelujen tarjoaja jakaa muuntuvasti resurssien maantieteellisestä sijainnista riippumatta kysynnän vaihtelun mukaan. 'Joustavuudella' viitataan tietoteknisiin resursseihin joita vapautetaan käyttöön ja tarjotaan kysynnän mukaan niin, että resursseja voidaan nopeasti kasvattaa ja vähentää kuormituksen mukaisesti. 'Jaettavalla' viitataan tietoteknisiin resursseihin, joita tarjotaan yhteisen pääsyn resursseihin jakavalle käyttäjäkunnalle niin, että prosessointi tapahtuu käyttäjäkohtaisesti vaikka palvelua tarjotaan saman laitteiston kautta. Termiä 'hajautettu' käytetään kuvaamaan tietoteknisiä resursseja, jotka sijaitsevat erillisissä verkotetuissa tietokoneissa tai laitteissa ja jotka viestivät ja koordinoivat toimintaansa keskenään rakenteisella viestinvaihdolla.

(17) Innovatiivisten teknologioiden ja uusien liiketoimintamallien myötä markkinoille odotetaan tulevan uusia pilvipalvelujen käyttö- ja palvelumalleja vastauksena asiakkaiden muuttuviin tarpeisiin. Pilvipalveluja voidaan tarjota hyvin hajautetussa muodossa ja entistä lähempänä paikkaa, jossa dataa tuotetaan tai kerätään, jolloin siirrytään perinteisestä mallista pitkälle hajautettuun malliin (ns. reunalaskentamalli).

(18) Datakeskuspalveluja ei välttämättä aina tarjota pilvipalveluna. Näin ollen datakeskukset eivät välttämättä aina ole osa pilvipalveluinfrastruktuuria. Kaikkien verkko- ja tietojärjestelmien turvallisuuteen kohdistuvien riskien hallitsemiseksi tämän direktiivin olisi katettava myös sellaisten datakeskuspalvelujen tarjoajat, jotka eivät ole pilvipalveluja. Tässä direktiivissä 'datakeskuspalvelulla' olisi tarkoitettava sellaisen palvelun tarjoamista, joka käsittää rakenteita tai rakenteiden ryhmiä, jotka on tarkoitettu datan tallennus-, käsittely- ja siirtopalveluja tarjoavien tietoteknisten ja verkkolaitteiden keskitettyyn ylläpitoon, yhteenliittämiseen ja ohjaukseen yhdessä kaikkien tarvittavien sähkönjakeluun ja toimintaolosuhteiden säätelyyn tarkoitettujen laitteiden ja infrastruktuurien kanssa. Termi 'datakeskuspalvelu' ei kata tietyn toimijan itse omistamia ja omiin käyttötarkoituksiinsa käyttämiä sisäisiä datakeskuksia.

(19) Euroopan parlamentin ja neuvoston direktiivissä 97/67/EY[18] tarkoitettujen postipalvelujen tarjoajien, [...] **mukaan luettuina** [...] kuriiripalvelujen tarjoajat, olisi kuuluttava tämän direktiivin soveltamisalaan, jos ne tarjoavat vähintään yhden postiketjun vaiheista ja erityisesti osoitteenselvityksen, lajittelun tai jakelun, mukaan lukien noutopalvelut. Kuljetuspalvelut, jotka eivät koske jotain näistä vaiheista, olisi jätettävä postipalvelujen määritelmän ulkopuolelle.

---

[18] Euroopan parlamentin ja neuvoston direktiivi 97/67/EY, annettu 15 päivänä joulukuuta 1997, yhteisön postipalvelujen sisämarkkinoiden kehittämistä ja palvelun laadun parantamista koskevista yhteisistä säännöistä (EYVL L 15, 21.1.1998, s. 14).

(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.

(2**0 a)** **Korkeatasoisen kyberturvallisuuden saavuttamiseksi ja ylläpitämiseksi tässä direktiivissä vaadittujen kansallisten kyberturvallisuusstrategioiden olisi käsitettävä yhtenäiset kehykset, joilla varmistetaan kyberturvallisuusalan hallinnointi. Nämä strategiat voivat koostua yhdestä tai useammasta lainsäädäntöasiakirjasta tai muusta kuin lainsäädäntöasiakirjasta.**

(21) Kansallisten hallintorakenteiden erojen vuoksi ja jo olemassa olevien alakohtaisten järjestelyjen tai unionin valvonta- ja sääntelyelinten turvaamiseksi jäsenvaltioiden olisi voitava nimetä useampi kuin yksi kansallinen toimivaltainen viranomainen, joka vastaa keskeisten ja tärkeiden toimijoiden verkko- ja tietojärjestelmien turvallisuuteen liittyvien tämän direktiivin mukaisten tehtävien suorittamisesta. Jäsenvaltioiden olisi voitava antaa tämä tehtävä jo olemassa olevalle viranomaiselle.

(22) Viranomaisten välisen rajat ylittävän yhteistyön ja viestinnän helpottamiseksi ja tämän direktiivin tehokkaan täytäntöönpanon mahdollistamiseksi on tarpeen, että kukin jäsenvaltio nimeää kansallisen keskitetyn yhteyspisteen, joka vastaa verkko- ja tietojärjestelmien turvallisuuteen ja rajat ylittävään yhteistyöhön liittyvien kysymysten koordinoinnista unionin tasolla.

(23) Toimivaltaisten viranomaisten tai CSIRT-yksiköiden olisi saatava ilmoitukset poikkeamista toimijoilta toimivalla ja tehokkaalla tavalla**, jotta voidaan tarvittaessa myös helpottaa oikea-aikaista reagointia poikkeamatapauksissa ja vastata ilmoituksen tehneelle toimijalle.** Keskitetyille yhteyspisteille olisi annettava tehtäväksi toimittaa poikkeamailmoitukset edelleen muiden asianomaisten jäsenvaltioiden keskitettyihin yhteyspisteisiin. [...]

(23 a) Alakohtaisissa unionin säädöksissä, joissa edellytetään kyberturvallisuusriskien hallintatoimenpiteitä tai raportointivelvoitteita, joilla on vähintään vastaava vaikutus kuin tässä direktiivissä säädetyillä velvoitteilla, voitaisiin säätää, että nimetyt toimivaltaiset viranomaiset käyttävät valvonta- ja täytäntöönpanovaltuuksiaan suhteessa näihin toimenpiteisin tai velvoitteisiin tämän direktiivin mukaisesti nimettyjen toimivaltaisten viranomaisten avustuksella. Kyseiset toimivaltaiset viranomaiset voisivat ottaa käyttöön yhteistyöjärjestelyjä tätä varten. Tällaisissa yhteistyöjärjestelyissä voitaisiin täsmentää muun muassa valvontatoimien koordinointia koskevat menettelyt, mukaan luettuina kansallisen lainsäädännön mukaiset tutkintamenettelyt ja paikalla suoritettavia tarkastuksia koskevat menettelyt sekä menettelyt toimivaltaisten viranomaisten välistä valvontaa ja täytäntöönpanoa koskevaa tietojenvaihtoa varten, myös pääsy tämän direktiivin mukaisesti nimettyjen toimivaltaisten viranomaisten pyytämiin kyberturvallisuutta koskeviin tietoihin.

(24) Jäsenvaltioilla olisi oltava käytössään riittävät sekä tekniset että organisatoriset valmiudet, jotta voidaan ehkäistä ja havaita verkko- ja tietojärjestelmien poikkeamia ja riskejä, reagoida niihin ja lieventää niiden vaikutuksia. Jäsenvaltioiden olisi sen vuoksi varmistettava, että niillä on hyvin toimivat CSIRT-yksiköt, joita kutsutaan myös tietotekniikan CERT-kriisiryhmiksi ja jotka täyttävät keskeiset vaatimukset, jotta voidaan taata tehokkaat ja yhteensopivat valmiudet käsitellä poikkeamia ja riskejä ja varmistaa tehokas yhteistyö unionin tasolla. Toimijoiden ja CSIRT-yksiköiden välisen luottamussuhteen parantamiseksi tapauksissa, joissa CSIRT on osa toimivaltaista viranomaista, jäsenvaltiot [...] **voivat** harkita CSIRT-yksiköiden operatiivisten tehtävien erottamista toiminnallisesti erityisesti tietojen jakamisen ja yhteisöille annettavan tuen osalta ja toimivaltaisten viranomaisten valvontatoimista.

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

(26) Kun otetaan huomioon kyberturvallisuutta koskevan kansainvälisen yhteistyön tärkeys, CSIRT-yksiköiden olisi voitava osallistua kansainvälisiin yhteistyöverkostoihin tällä direktiivillä perustetun CSIRT-verkoston lisäksi. **Näin ollen CSIRT-yksiköt ja toimivaltaiset viranomaiset voisivat vaihtaa kolmansien maiden CSIRT-yksiköiden tai viranomaisten kanssa tietoja, myös henkilötietoja, asetuksen (EU) 2016/679 mukaisten tehtäviensä suorittamista varten. Jos olemassa ei ole asetuksen (EU) 2016/679 45 artiklan mukaisesti tehtyä päätöstä tietosuojan riittävyydestä tai saman asetuksen 46 artiklassa säädettyjä asianmukaisia suojatoimia, henkilötietojen vaihdon voitaisiin katsoa olevan asetuksen (EU) 2016/679 49 artiklan 1 kohdan d alakohdassa tarkoitettu yleistä etua koskeva tärkeä syy, jos se on tarpeen merkittävien kyberuhkien vähentämiseen ja meneillään oleviin kyberturvallisuuspoikkeamiin vastaamiseen liittyviä tarkoituksia varten.**

---

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

(27) Koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin annetun komission suosituksen (EU) 2017/1548[20] 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, elinten ja virastojen olisi tehtävä yhteistyötä teknisellä, operatiivisella ja poliittisella tasolla, jotta reagointia voidaan koordinoida asianmukaisesti kaikkialla unionissa.

(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 **tai hallinnoivien** 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 viestintätekniikan 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 [...] **29147** annetaan ohjeita haavoittuvuuksien käsittelystä ja haavoittuvuuksien havaitsemisesta. Haavoittuvuuksien julkistamisen osalta on erityisen tärkeää koordinoida toimia raportoivien tahojen ja tieto- ja viestintätekniikan tuotteiden tai palvelujen valmistajien tai tarjoajien välillä. Koordinoidussa haavoittuvuuksien ilmaisemisessa määritellään jäsennelty 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.

---

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

(29) Jäsenvaltioiden olisi sen vuoksi toteutettava toimenpiteitä haavoittuvuuksien koordinoidun ilmaisemisen helpottamiseksi laatimalla asiaa koskevat kansalliset toimintaperiaatteet. **Jäsenvaltioiden olisi kansallisissa toimintaperiaatteissaan pyrittävä mahdollisuuksien mukaan vastaamaan haavoittuvuuksien tutkijoiden kohtaamiin haasteisiin, myös mahdolliseen rikosoikeudelliseen vastuuseen, kansallisen oikeusjärjestelmänsä mukaisesti.** [...] Jäsenvaltioiden olisi nimettävä CSIRT-yksikkö toimimaan koordinaattorina, joka toimii tarvittaessa välittäjänä raportoivien tahojen ja tieto- ja viestintätekniikan tuotevalmistajien tai palveluntarjoajien välillä. CSIRT-koordinaattorin tehtäviin olisi kuuluttava erityisesti asianomaisten tahojen tunnistaminen ja kontaktointi, ilmoittavien tahojen tukeminen, tietojen ilmaisemisen aikataulusta neuvotteleminen ja useisiin organisaatioihin vaikuttavien haavoittuvuuksien hallinta (monenvälinen **koordinoitu** haavoittuvuuden ilmaiseminen). Jos **raportoidulla** haavoittuvuudella **voi mahdollisesti olla merkittävä vaikutus** [...] useamman kuin yhden jäsenvaltion **toimijoihin**, [...] nimettyjen CSIRT-yksiköiden olisi **tarvittaessa** tehtävä yhteistyötä CSIRT-verkostossa.

(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, **tai nimetyt CSIRT-yksiköt** voivat vapaaehtoisesti ilmoittaa haavoittuvuuksista ja antaa haavoittuvuustietoja, joiden avulla käyttäjät voivat toteuttaa asianmukaisia lieventäviä toimenpiteitä.

(31) Vaikka vastaavia haavoittuvuusrekistereitä tai tietokantoja on olemassa, niitä isännöivät ja ylläpitävät tahot, jotka eivät ole sijoittautuneet unioniin. ENISAn ylläpitämä Euroopan haavoittuvuusrekisteri lisäisi julkistamisprosessin läpinäkyvyyttä ennen kuin haavoittuvuus virallisesti paljastetaan ja selviytymiskykyä tilanteissa, joissa samankaltaisten palvelujen tarjonta heikentyy tai keskeytyy. Päällekkäisyyksien välttämiseksi ja täydentävyyden saavuttamiseksi mahdollisimman pitkälle ENISAn olisi tutkittava mahdollisuutta tehdä järjestelmällisiä yhteistyösopimuksia kolmansien maiden lainkäyttöalueilla sijaitsevien vastaavien rekisterien kanssa. **Erityisesti ENISAn olisi tutkittava mahdollisuutta tehdä tiivistä yhteistyötä haavoittuvuuksien ja paljastuneiden tietoturvapuutteiden CVE-järjestelmän (Common Vulnerabilities and Exposures) kanssa, myös mahdollisuutta toimia CVE-numeroinnista vastaavana Root CVE Numbering Authority -viranomaisena.**

(32) **Yhteistyöryhmän olisi jatkossakin tuettava ja helpotettava strategista yhteistyötä ja tietojenvaihtoa sekä vahvistettava jäsenvaltioiden keskinäistä luottamusta.** Yhteistyöryhmän olisi laadittava joka toinen vuosi työohjelma, joka sisältää toimet, jotka ryhmän on määrä saada aikaan tavoitteidensa ja tehtäviensä toteuttamiseksi. Tämän direktiivin mukaisesti hyväksytyn ensimmäisen ohjelman aikataulu olisi mukautettava direktiivin (EU) 2016/1148 mukaisesti hyväksytyn viimeisen ohjelman aikatauluun, jotta vältetään mahdolliset häiriöt ryhmän työskentelyssä.

(33) Laatiessaan ohjeasiakirjoja yhteistyöryhmän olisi säännönmukaisesti kartoitettava kansallisia ratkaisuja ja kokemuksia, arvioitava yhteistyöryhmän tulosten vaikutusta kansallisiin lähestymistapoihin, keskusteltava täytäntöönpanon haasteista ja laadittava erityisiä suosituksia olemassa olevien sääntöjen täytäntöönpanon parantamiseksi.

(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.

(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.

(35 a) CSIRT-yksiköiden verkoston olisi jatkossakin edistettävä luottamuksen vahvistumista sekä ripeää ja tuloksellista operatiivista yhteistyötä jäsenvaltioiden välillä. Unionin tason operatiivisen yhteistyön lisäämiseksi CSIRT-verkoston olisi harkittava kyberturvallisuuspolitiikkaan osallistuvien unionin elinten ja virastojen kutsumista osallistumaan sen työhön.

(36) [...]

(36 a) Tämän direktiivin säännösten, kuten haavoittuvuuksien hallinnan, kyberturvallisuusriskien hallinnan, raportointitoimenpiteiden ja tietojen jakamista koskevien järjestelyjen, tehokkaan täytäntöönpanon helpottamiseksi jäsenvaltiot voivat tehdä yhteistyötä kolmansien maiden kanssa ja toteuttaa tähän tarkoitukseen sopivaksi katsomiaan toimia, kuten uhkiin, poikkeamiin, haavoittuvuuksiin, välineisiin ja menetelmiin, taktiikkaan, tekniikoihin ja menetelmiin liittyvää tietojenvaihtoa, kyberturvallisuuskriisien hallintaan valmistautumista ja harjoituksia, koulutusta, luottamuksen vahvistamista ja jäsenneltyjä tiedonjakojärjestelyjä. Näiden yhteistyöjärjestelyjen olisi oltava unionin tietosuojalainsäädännön mukaisia.

(37) Jäsenvaltioiden olisi osallistuttava suosituksessa (EU) 2017/1584 esitetyn EU:n kyberturvallisuuden kriisinhallintakehyksen perustamiseen olemassa olevien yhteistyöverkostojen, erityisesti **Euroopan** kyberkriisien yhteysorganisaatioiden verkoston (EU-CyCLONe), CSIRT-verkoston ja yhteistyöryhmän kautta. EU-CyCLONen ja CSIRT-verkoston olisi tehtävä yhteistyötä sellaisten menettelyllisten järjestelyjen pohjalta, joissa määritellään kyseisen yhteistyön yksityiskohtaiset säännöt**, ja vältettävä tehtävien päällekkäisyyttä**. EU-CyCLONen työjärjestyksessä olisi täsmennettävä tarkemmin verkoston toimintatavat, mukaan lukien muun muassa roolit, yhteistyömuodot, vuorovaikutus muiden asiaankuuluvien toimijoiden kanssa ja tiedonvaihdon mallit sekä tiedonvaihdon tekninen toteutustapa. Unionin **poliittisen** tason kriisinhallinnassa asianomaisten osapuolten olisi tukeuduttava poliittisen kriisitoiminnan integroituihin järjestelyihin (IPCR). Komission olisi käytettävä tähän tarkoitukseen ARGUS-ohjelman korkean tason monialaista kriisinkoordinointiprosessia. Jos kriisiin liittyy merkittävä ulkoinen tai yhteisen turvallisuus- ja puolustuspolitiikan (YTPP) ulottuvuus, olisi aktivoitava Euroopan ulkosuhdehallinnon (EUH) kriisinhallintamekanismi (CRM).

(37 a) **EU-CyCLONen olisi toimittava teknisen ja poliittisen tason välisenä verkostona laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien aikana. Sen olisi tehostettava operatiivisen tason yhteistyötä CSIRT-verkoston havaintojen perusteella ja hyödyntämällä omia valmiuksiaan laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien vaikutusten analysoimiseksi ja poliittisen tason päätöksenteon tukemiseksi. EU:n toimielinten, elinten ja virastojen olisi nimettävä EU-CyCLONen jäseneksi laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallinnasta vastaava toimivaltainen viranomainen.**

(38) [...]

(39) [...]

(39 a) **Vastuu verkko- ja tietojärjestelmän turvallisuuden varmistamisesta lankeaa suurelta osin keskeisille ja tärkeille toimijoille. Olisi edistettävä ja kehitettävä riskinhallintakulttuuria, johon sisältyy riskinarviointi ja riskeihin suhteutettujen turvallisuustoimenpiteiden toteuttaminen.**

(40) Riskinhallintatoimenpiteissä **olisi otettava huomioon se, miten riippuvainen toimija on verkko- ja tietojärjestelmistä ja niihin** olisi sisällyttävä toimenpiteitä, joilla tunnistetaan poikkeamariskit, ehkäistään, havaitaan ja käsitellään niitä ja lievennetään niiden vaikutuksia. Verkko- ja tietojärjestelmien turvallisuuden olisi katettava tallennettavan, siirrettävän ja käsiteltävän datan turvallisuus.

(40 a) Koska verkko- ja tietojärjestelmien turvallisuuteen kohdistuvia uhkia on monenlaisia, tässä direktiivissä sovelletaan kaikki vaaratekijät huomioon ottavaa toimintatapaa, joka käsittää verkko- ja tietojärjestelmien ja niiden fyysisen ympäristön suojelemisen kaikilta tapahtumilta, kuten varkaudelta, tulipalolta, tulvalta, televiestintä- ja sähkökatkoilta tai luvattomalta fyysiseltä pääsyltä toimijan tietoihin tai tiedonkäsittely-ympäristöön, sille aiheutuvalta vahingolta tai siihen puuttumiselta, jotka saattaisivat vaarantaa verkko- ja tietojärjestelmissä tarjottujen tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen saatavuuden, aitouden, eheyden tai luottamuksellisuuden. Riskinhallintatoimenpiteet olisi näin ollen kohdistettava myös fyysiseen turvallisuuteen ja ympäristön turvallisuuteen, mukaan lukien toimenpiteet, joilla suojataan toimijan verkko- ja tietojärjestelmät järjestelmän toimintahäiriöiltä, inhimillisiltä virheiltä, vihamielisiltä toimilta tai luonnonilmiöiltä eurooppalaisten tai kansainvälisesti hyväksyttyjen standardien, kuten ISO 27000 -sarjaan sisältyvien standardien, mukaisesti. Toimijoiden olisi riskinhallintatoimenpiteissään käsiteltävä tältä osin myös henkilöresurssien turvallisuutta ja otettava käyttöön asianmukainen pääsynvalvontapolitiikka. Toimenpiteiden olisi oltava direktiivin XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] mukaisia.

(40 b) Jos käytettävissä ei ole asetuksen (EU) 2019/881 mukaisesti hyväksyttyä asianmukaista eurooppalaista kyberturvallisuuden sertifiointijärjestelmää, jäsenvaltiot voisivat vaatia toimijoita käyttämään sertifioituja tieto- ja viestintätekniikan tuotteita, palveluja ja prosesseja tai hankkimaan käytettävissä olevan kansallisen kyberturvallisuusjärjestelmän mukaisen todistuksen, jotta ne voisivat osoittaa noudattavansa tämän direktiivin mukaisia kyberturvallisuusriskien hallintaa koskevia vaatimuksia.

(41) Jotta keskeisille ja tärkeille toimijoille ei aiheutuisi kohtuutonta taloudellista ja hallinnollista rasitetta, kyberturvallisuusriskien hallintaa koskevien vaatimusten olisi oltava oikeassa suhteessa asianomaiseen verkko- ja tietojärjestelmään [...] **kohdistuvaan** riskiin, ottaen huomioon suojatoimenpiteiden viimeisin kehitys **ja niiden toteuttamisen kustannukset**. **Toimijan koko sekä poikkeamien todennäköisyys ja niiden vakavuus olisi myös otettava asianmukaisesti huomioon.**

(41 a) Sääntelytaakan keventämiseksi pienille, keskisuurille ja mikrotoimijoille olisi lähtökohtaisesti asetettava löyhemmät kyberturvallisuusriskien hallintatoimenpiteiden toteuttamista koskevat vaatimukset, jollei tiukempien vaatimusten soveltaminen ole perusteltua kriittisyyttä koskevien kriteerien tai kansallisten riskinarviointien perusteella erityisesti tässä direktiivissä säädetyt kriittisyyteen liittyvät kriteerit täyttävien toimijoiden osalta.

(42) Keskeisten ja tärkeiden toimijoiden olisi varmistettava toiminnassaan käyttämiensä verkko- ja tietojärjestelmien turvallisuus. Nämä ovat pääasiassa yksityisiä verkko- ja tietojärjestelmiä, joita hallinnoi organisaation sisäinen tietotekniikkahenkilöstö tai joiden turvallisuudesta vastaa alihankkija. Tämän direktiivin mukaisia kyberturvallisuusriskien hallintaa ja raportointia koskevia vaatimuksia olisi sovellettava asiaankuuluviin keskeisiin ja tärkeisiin toimijoihin riippumatta siitä, hoitavatko ne verkko- ja tietojärjestelmiensä ylläpidon sisäisesti vai on se ulkoistettu.

(42 aa) Kun otetaan huomioon DNS-palveluntarjoajien, TLD-rekisterien ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden, pilvipalvelujen tarjoajien, datakeskuspalvelujen tarjoajien, sisällönjakeluverkkojen tarjoajien, hallintapalvelujen tarjoajien ja tietoturvapalveluntarjoajien rajatylittävä luonne, niihin olisi sovellettava pidemmälle menevää yhdenmukaistamista unionin tasolla. Kyberturvallisuustoimenpiteiden toteuttamista olisi siksi helpotettava täytäntöönpanosäädöksellä.

(43) Toimijan toimitusketjusta ja toimijan suhteesta alihankkijoihin johtuviin kyberturvallisuusriskeihin puuttuminen on erityisen tärkeää, kun otetaan huomioon sellaisten poikkeamien yleisyys, joissa toimijat ovat joutuneet kyberhyökkäysten uhreiksi ja joissa vihamieliset toimijat ovat voineet vaarantaa toimijan verkko- ja tietojärjestelmien turvallisuuden hyödyntämällä kolmansien osapuolten tuotteisiin ja palveluihin vaikuttavia haavoittuvuuksia. Toimijoiden olisi sen vuoksi arvioitava ja otettava huomioon käyttämiensä alihankkijoiden ja palveluntarjoajien tuotteiden ja kyberturvallisuuskäytäntöjen kokonaislaatu, mukaan lukien tuotekehityksen suojausmenettelyt.

(44) Palveluntarjoajista erityisen tärkeällä sijalla ovat turvapoikkeamavalvontaa, tunkeutumisenestotestausta, turva-auditointeja ja konsultointia tarjoavat tietoturvapalveluntarjoajat (MSSP), joiden tehtävänä on avustaa toimijoita niiden pyrkiessä havaitsemaan turvapoikkeamat ja reagoimaan niihin. Nämä MSSP-yritykset ovat kuitenkin itsekin olleet kyberhyökkäysten kohteina, ja niiden tiivis integroituminen toimijoiden toimintarakenteisiin aiheuttaa erityisen kyberturvallisuusriskin. Toimijoiden olisi sen vuoksi noudatettava entistä suurempaa huolellisuutta MSSP-palveluntarjoajaa valitessaan.

(44 a) Kansalliset toimivaltaiset viranomaiset voivat valvontatehtäviään toteuttaessaan hyödyntää myös kyberturvallisuuspalveluja, kuten turva-auditointeja, tunkeutumisenestotestausta ja turvapoikkeamavalvontaa. Auttaakseen toimijoita ja kansallisia toimivaltaisia viranomaisia valitsemaan ammattitaitoiset ja luotettavat kyberturvallisuuspalvelujen tarjoajat komission olisi yhteistyöryhmän ja ENISAn avustuksella harkittava mahdollisuutta pyytää eurooppalaista kyberturvallisuuden sertifiointijärjestelmää asetuksen (EU) 2019/881 48 artiklan mukaisesti.

(45) Toimijoiden olisi puututtava myös sellaisiin kyberturvallisuusriskeihin, jotka johtuvat niiden vuorovaikutussuhteista ja muista kytköksistä sidosryhmiin laajemmassa ekosysteemissä. Toimijoiden olisi erityisesti varmistettava, että niiden yhteistyö akateemisten laitosten ja tutkimuslaitosten kanssa tapahtuu niiden kyberturvallisuusperiaatteiden mukaisesti ja että yhteistyössä noudatetaan hyviä käytäntöjä yleisesti tiedon suojatun saatavuuden ja levittämisen ja erityisesti teollis- ja tekijänoikeuksien suojan suhteen. Kun otetaan huomioon datan merkitys ja arvo toimijoille, niiden olisi vastaavasti toteutettava kaikki asianmukaiset kyberturvallisuustoimenpiteet tukeutuessaan kolmansilta osapuolilta hankittaviin tietojen muuntamis- ja analysointipalveluihin.

(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[21] mukaisesti, jotta voidaan määrittää alakohtaiset kriittiset tieto- ja viestintätekniikan palvelut, järjestelmät tai tuotteet sekä kyseeseen tulevat uhat ja haavoittuvuudet.

---

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

(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 koordinoidussa 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 viestintäteknisten 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.

(48) Jotta voidaan virtaviivaistaa yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajille ja luottamuspalvelujen tarjoajille asetettuja oikeudellisia velvoitteita, jotka liittyvät niiden verkko- ja tietojärjestelmien turvallisuuteen, sekä antaa näille toimijoille ja niitä säänteleville toimivaltaisille viranomaisille mahdollisuus hyötyä tällä direktiivillä perustetusta oikeudellisesta kehyksestä (mukaan lukien riskien ja poikkeamien käsittelystä vastaavan CSIRT-yksikön nimeäminen sekä toimivaltaisten viranomaisten ja elinten osallistuminen yhteistyöryhmän ja CSIRT-verkoston työhön), ne olisi sisällytettävä tämän direktiivin soveltamisalaan. Euroopan parlamentin ja neuvoston asetuksessa (EU) N:o 910/2014[22] ja Euroopan parlamentin ja neuvoston direktiivissä (EU) 2018/1972[23] vahvistetut vastaavat säännökset, jotka koskevat tällaisten toimijoiden turvallisuus- ja ilmoitusvaatimuksia, olisi sen vuoksi kumottava.

---

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

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

(48 a) Tässä direktiivissä säädettyjen turvallisuusvaatimusten olisi katsottava täydentävän asetuksessa (EU) N:o 910/2014 (eIDAS-asetus) luottamuspalvelujen tarjoajille asetettuja vaatimuksia. Luottamuspalvelujen tarjoajia olisi vaadittava toteuttamaan asianmukaiset ja oikeasuhteiset toimenpiteet niiden palveluihin kohdistuvien riskien hallitsemiseksi, myös suhteessa asiakkaisiin ja luottaviin kolmansiin osapuoliin, ja raportoimaan tämän direktiivin mukaisista turvallisuuspoikkeamista. Näiden turvallisuus- ja raportointivelvoitteiden olisi koskettava myös tarjotun palvelun fyysistä suojaamista. Sovelletaan edelleen asetuksen (EU) N:o 910/2014 24 artiklaa.

(48 aa) Jäsenvaltiot voivat antaa luottamuspalvelujen toimivaltaisen viranomaisen tehtävän eIDAS-valvontaelimille varmistaakseen nykyisten käytäntöjen jatkumisen ja hyödyntääkseen eIDAS-asetuksen soveltamisesta saadun tietämyksen ja kokemuksen. Jos tämä tehtävä annetaan jollekin muulle elimelle, tämän direktiivin mukaisten kansallisten toimivaltaisten viranomaisten olisi tehtävä tiivistä ja oikea-aikaista yhteistyötä vaihtamalla asiaankuuluvia tietoja sen varmistamiseksi, että valvonta on tehokasta ja että luottamuspalvelujen tarjoajat noudattavat tässä direktiivissä ja asetuksessa [XXXX/XXXX] säädettyjä vaatimuksia.

Tämän direktiivin mukaisten kansallisten toimivaltaisten viranomaisten olisi tarvittaessa ilmoitettava eIDAS-valvontaelimelle välittömästi kaikista sille ilmoitetuista merkittävistä kyberuhkista ja -poikkeamista, jotka vaikuttavat luottamuspalveluihin, sekä luottamuspalvelujen tarjoajien mahdollisesta tässä direktiivissä säädettyjen vaatimusten noudattamatta jättämisestä. Raportointia varten jäsenvaltiot voivat tarvittaessa käyttää yhteyspistettä, joka on perustettu yhteisen ja automaattisen poikkeamaraportoinnin varmistamiseksi sekä eIDAS-valvontaelimelle että tämän direktiivin mukaiselle toimivaltaiselle viranomaiselle. Raportointivelvoitteita koskevat säännöt eivät saisi rajoittaa asetuksen (EU) 2016/679 ja Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY[24] soveltamista.

---

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

(49) Tarkoituksenmukaisissa tapauksissa ja tarpeettomien katkosten välttämiseksi **jäsenvaltioiden tähän direktiiviin liittyen toteuttamissa täytäntöönpanojärjestelyissä** olisi **otettava huomioon** olemassa oleva kansallinen ohjeistus [...], joka koskee direktiivin (EU) 2018/1972 40 [...] ja 41 artiklassa säädettyjen turvatoimiin liittyvien sääntöjen [...] täytäntöönpanoa**, jotta voidaan hyödyntää direktiivin (EU) 2018/1972 soveltamisesta kyberturvariskien hallintatoimenpiteiden ja poikkeamailmoitusten osalta saatua tietämystä ja ammattitaitoa**. **ENISA voi myös laatia yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajille ohjeistusta turvallisuus- ja raportointivaatimuksista yhdenmukaistamisen ja siirtymisen helpottamiseksi ja häiriöiden minimoimiseksi. Jäsenvaltiot voivat antaa sähköisen viestinnän toimivaltaisen viranomaisen tehtävän kansallisille sääntelyviranomaisille varmistaakseen nykyisten käytäntöjen jatkumisen ja hyödyntääkseen direktiivin (EU) 2018/1972 soveltamisesta saadun tietämyksen ja kokemuksen.**

(50) Kun otetaan huomioon numeroista riippumattomien henkilöviestintäpalvelujen kasvava merkitys, on tarpeen varmistaa, että myös tällaisiin palveluihin sovelletaan asianmukaisia turvallisuusvaatimuksia niiden erityisluonteen ja taloudellisen merkityksen mukaisesti. Myös tällaisten palvelujen tarjoajien olisi näin ollen varmistettava, että verkko- ja tietojärjestelmien turvallisuustaso on oikeassa suhteessa aiheutuvaan riskiin. Koska numeroista riippumattomien henkilöiden välisten viestintäpalvelujen tarjoajat eivät yleensä tosiasiallisesti valvo signaalien siirtoa verkoissa, tällaisten palvelujen osalta riskiä voidaan joiltakin osin pitää perinteisiä sähköisiä viestintäpalveluja alhaisempana. Sama koskee sellaisia henkilöviestintäpalveluja, joissa käytetään yhteysnumeroita, mutta joissa palveluntarjoaja ei tosiasiallisesti valvo signaalinsiirtoa.

(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.

(52) Toimijoiden olisi tarvittaessa tiedotettava palvelujensa käyttäjille yksittäisistä [...] toimenpiteistä, joita käyttäjät voivat toteuttaa pienentääkseen **merkittävästä kyberuhkasta** itselleen aiheutuvaa riskiä. **Toimijoiden olisi tarvittaessa ja erityisesti silloin, kun merkittävä kyberuhka voi toteutua, ilmoitettava uhkasta myös palvelujensa käyttäjille samalla kun ne ilmoittavat siitä toimivaltaisille viranomaisille tai CSIRT-yksiköille.** Vaatimus 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. [...] **Kyber**uhkia koskevien tietojen toimittamisen käyttäjille olisi oltava käyttäjille maksutonta.

(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 tietyntyyppisiä ohjelmistoja tai salaustekniikoita.

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

(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 soveltuvin 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 määräajasta ensimmäisen ilmoituksen osalta ja yhden kuukauden määräajasta loppuraportin osalta.

(55 a) Kyberuhkia koskeva ennakoiva lähestymistapa on ratkaiseva osa kyberturvallisuuden riskinhallintaa, ja toimivaltaisten viranomaisten pitäisi pystyä estämään sen avulla tehokkaasti kyberuhkien toteutuminen poikkeamina, jotka voivat aiheuttaa huomattavia aineellisia ja aineettomia tappioita. Tätä varten merkittävistä kyberuhkista ilmoittaminen on olennaisen tärkeää.

(56) Keskeiset ja tärkeät toimijat ovat usein tilanteessa, jossa tietystä 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 jäsenvaltiot [...] **voisivat** perustaa keskitetyn asiointipisteen 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 edellytettyjä raportointitietoja ja vähennettäisiin yrityksille aiheutuvaa rasitetta.

(57) Jos epäillään, että poikkeama liittyy unionin tai kansallisen lainsäädännön nojalla vakavaan rikolliseen toimintaan, jäsenvaltioiden olisi kannustettava keskeisiä ja tärkeitä toimijoita raportoimaan epäillyistä vakavista rikosoikeudellisista poikkeamista asiaankuuluville lainvalvontaviranomaisille sovellettavien rikosoikeudellisia menettelyjä koskevien sääntöjen perusteella ja unionin lainsäädännön mukaisesti. Tarvittaessa ja rajoittamatta Europoliin sovellettavien henkilötietojen suojaa koskevien sääntöjen soveltamista on suotavaa, että eri jäsenvaltioiden toimivaltaisten viranomaisten ja lainvalvontaviranomaisten välinen koordinointi tapahtuu Euroopan verkkorikostorjuntakeskuksen (EC3) ja ENISAn myötävaikutuksella.

(58) Turvapoikkeamat vaarantavat monissa tapauksissa henkilötietojen suojan. Tässä yhteydessä toimivaltaisten viranomaisten olisi tehtävä yhteistyötä ja vaihdettava tietoja kaikista asiaankuuluvista asioista tietosuojaviranomaisten ja valvontaviranomaisten kanssa direktiivin 2002/58/EY mukaisesti.

(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.

(60) Näiden tietojen saatavuus ja nopea pääsy niihin viranomaisille, kuten unionin tai kansallisen lainsäädännön mukaisesti toimivaltaisille viranomaisille rikosten ehkäisemistä, tutkimista tai syytteeseenpanoa varten, CERT-yksiköille, CSIRT-yksiköille ja asiakkaitaan koskevien tietojen osalta kyseisten asiakkaiden puolesta toimiville sähköisten viestintäverkkojen ja -palvelujen tarjoajille ja kyberturvallisuusteknologioiden ja -palvelujen tarjoajille on olennaisen tärkeää DNS-verkkotunnusjärjestelmän väärinkäytön ehkäisemiseksi ja torjumiseksi, erityisesti kyberturvallisuuspoikkeamien ehkäisemiseksi, havaitsemiseksi ja niihin reagoimiseksi. Tällaisen pääsyn olisi oltava unionin tietosuojalainsäädännön mukaista siltä osin kuin se liittyy henkilötietoihin.

(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. **Rekisteröintitietojen osalta toimijoiden olisi erityisesti todennettava rekisteröijän nimi ja sähköpostiosoite.** TLD-rekisterien ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavien tahojen olisi [...] vahvistettava toimintatavat ja menettelyt, joilla kerätään ja ylläpidetään tarkkoja ja täydellisiä rekisteröintitietoja sekä ehkäistään ja korjataan virheellisiä rekisteröintitietoja unionin tietosuojasääntöjen mukaisesti.

(62) TLD-rekisterien ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavien tahojen olisi asetettava julkisesti saataville verkkotunnusten rekisteröintitiedot, jotka eivät kuulu unionin tietosuojasääntöjen soveltamisalaan, kuten oikeushenkilöitä koskevat tiedot[25]. TLD-rekisterien ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavien tahojen olisi myös unionin tietosuojalainsäädännön mukaisesti annettava perustelluissa tapauksissa tietoja pyytäville laillinen pääsy yksittäisiin luonnollisia henkilöitä koskeviin verkkotunnusten rekisteröintitietoihin. Jäsenvaltioiden olisi varmistettava, että TLD-rekisterit ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavat toimijat vastaavat ilman aiheetonta viivytystä [...] verkkotunnusten rekisteröintitietojen luovuttamista koskeviin pyyntöihin**, joita ovat esittäneet sitä perustellusti pyytävät tahot, kuten unionin tai kansallisen lainsäädännön mukaisesti kansallisen turvallisuuden ja rikosoikeuden alalla toimivaltaiset viranomaiset tai CSIRT-yksiköt**. TLD-rekisterien ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavien tahojen olisi vahvistettava periaatteet ja menettelyt rekisteröintitietojen julkaisemista ja luovuttamista varten, mukaan lukien palvelutasosopimukset laillisten tietopyyntöjen käsittelemiseksi. Tietojenluovutusmenettelyyn voi kuulua myös rajapinnan, portaalin tai muun teknisen menetelmän käyttö tehokkaan järjestelyn tarjoamiseksi rekisteröintitietojen pyytämistä ja niihin pääsyä varten. **Jäsenvaltioiden olisi varmistettava, että kaikenlainen pääsy verkkotunnusten rekisteröintitietoihin (henkilötietoihin ja muihin kuin henkilötietoihin) on ilmaista.** Yhdenmukaisten käytäntöjen edistämiseksi sisämarkkinoilla komissio voi antaa tällaisia menettelyjä koskevia ohjeita**, jotka ovat monisidosryhmäisen yhteisön kehittämien kansainvälisten standardien mukaisia ja täydentävät niitä,** sanotun kuitenkaan rajoittamatta Euroopan tietosuojaneuvoston toimivaltaa.

---

[25] Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 johdanto-osan 14 kappale, jonka mukaan "tämä asetus ei koske oikeushenkilöiden ja erityisesti oikeushenkilön muodossa perustettujen yritysten henkilötietojen käsittelyä, kuten oikeushenkilön nimeä, oikeudellista muotoa ja yhteystietoja".

(63) [...]Tämän direktiivin soveltamisalaan kuuluvien keskeisten ja tärkeiden toimijoiden olisi kuuluttava sen jäsenvaltion lainkäyttövaltaan, jossa ne tarjoavat palvelujaan. **Liitteessä I olevissa 1–7 ja 10 kohdassa tarkoitettujen toimijoiden sekä liitteessä I olevassa 8 kohdassa ja liitteessä II olevissa 1–5 kohdassa tarkoitettujen luottamuspalvelun tarjoajien ja Internetin yhdysliikennepisteiden ylläpitäjien olisi kuuluttava sen jäsenvaltion lainkäyttövaltaan, johon ne ovat sijoittautuneet.** Jos toimija tarjoaa palveluja useammassa kuin yhdessä jäsenvaltiossa **tai se on sijoittautunut useampaan kuin yhteen jäsenvaltioon**, sen olisi kuuluttava kunkin jäsenvaltion erillisen ja rinnakkaisen lainkäyttövallan piiriin. Näiden jäsenvaltioiden toimivaltaisten viranomaisten olisi tehtävä yhteistyötä, annettava toisilleen keskinäistä apua ja tarvittaessa toteutettava yhteisiä valvontatoimia. **Jos jäsenvaltiot päättävät käyttää lainkäyttövaltaansa, niiden olisi vältettävä määräämästä seuraamuksia tämän direktiivin mukaisia velvoitteita rikkovasta toiminnasta useammin kuin kerran.**

(64) Jotta voidaan ottaa huomioon internetin nimipalvelinjärjestelmän DNS-palveluntarjoajien, aluetunnusrekisterien (TLD-rekisterien), **aluetunnusten alaisten verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden,** sisällönjakeluverkon tarjoajien, pilvipalvelujen tarjoajien, datakeskuspalvelujen tarjoajien ja digitaalisten palvelujen tarjoajien palvelujen ja toimintojen rajat ylittävä luonne, vain yhdellä jäsenvaltiolla olisi oltava lainkäyttövalta näihin toimijoihin nähden. Lainkäyttövalta olisi oltava sillä jäsenvaltiolla, jossa kyseisen toimijan päätoimipaikka sijaitsee unionissa. Tätä direktiiviä sovellettaessa sijoittautumiskriteerillä tarkoitetaan toiminnan tosiasiallista harjoittamista kiinteiden toimipaikkojen kautta. Sijoittautumisen oikeudellisella muodolla eli sillä, onko kyseessä sivuliike vai tytäryhtiö, jolla on oikeushenkilöys, ei ole tässä suhteessa ratkaisevaa merkitystä.

Tämän kriteerin täyttyminen ei saisi riippua siitä, sijaitsevatko verkko- ja tietojärjestelmät fyysisesti kyseisessä paikassa; tällaisten järjestelmien sijainti ja käyttöpaikka eivät itsessään muodosta tällaista päätoimipaikkaa, eivätkä ne näin ollen ole ratkaisevia perusteita päätoimipaikan määrittämisessä. Päätoimipaikan olisi oltava paikka, jossa kyberturvallisuusriskien hallintatoimenpiteisiin liittyvät päätökset tehdään **pääasiassa** unionissa. Tämä vastaa tyypillisesti yritysten keskushallinnon paikkaa unionissa. Jos **paikkaa, jossa tällaiset päätökset pääasiassa tehdään, ei voida määrittää tai** tällaisia päätöksiä ei tehdä unionissa, päätoimipaikan olisi katsottava sijaitsevan niissä jäsenvaltioissa, joissa toimijalla on eniten työntekijöitä unionissa. Jos palvelut suorittaa yritysryhmä, sen päätoimipaikaksi olisi katsottava määräysvaltaa käyttävän yrityksen päätoimipaikka.

(64 a) Jos yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoaja tarjoaa rekursiivista DNS-palvelua vain osana internetyhteyspalvelua, kyseisen toimijan olisi katsottava kuuluvan kaikkien sellaisten jäsenvaltioiden lainkäyttövaltaan, joissa se tarjoaa palvelujaan.

(64 a a) Jotta saadaan selkeä yleiskuva DNS-palveluntarjoajista, TLD-rekistereistä, aluetunnusten alaisten verkkotunnusten rekisteröintipalveluja tarjoavista toimijoista, sisällönjakeluverkon tarjoajista, pilvipalvelujen tarjoajista, datakeskuspalvelujen tarjoajista sekä tämän direktiivin soveltamisalaan kuuluvia palveluja unionissa tarjoavista digitaalisten palvelujen tarjoajista, ENISAn olisi luotava rekisteri tällaisista toimijoista jäsenvaltioilta tarvittaessa niiden kansallisten ilmoitusmenetelmien kautta saatujen ilmoitusten perusteella ja ylläpidettävä kyseistä rekisteriä. Jäsenvaltioiden olisi toimitettava ENISAlle niiden kansallisissa rekistereissä saatavilla olevat tiedot kyseisistä toimijoista, jotta voitaisiin varmistaa, että rekisterin tiedot ovat täsmälliset ja täydelliset. ENISAn ja jäsenvaltioiden olisi toteutettava toimenpiteitä, joilla edistetään tällaisten rekisterien yhteentoimivuutta, ja varmistettava samalla luottamuksellisten tai turvallisuusluokiteltujen tietojen suoja.

(65) Kun internetin nimipalvelinjärjestelmän DNS-palveluntarjoaja, aluetunnusrekisteri (TLD-rekisterien), sisällönjakeluverkon tarjoaja, pilvipalvelujen tarjoaja, datakeskuspalvelujen tarjoaja tai digitaalisten palvelujen tarjoaja, joka ei ole sijoittautunut unioniin, tarjoaa palveluja unionissa, sen olisi nimettävä edustaja. Jotta voidaan määrittää, tarjoaako tällainen toimija palveluja unionissa, olisi varmistettava, onko ilmeistä, että toimija aikoo tarjota palveluja henkilöille yhdessä tai useammassa jäsenvaltiossa. Pelkkä toimijan tai välittäjän verkkosivuston tai sähköpostiosoitteen ja muiden yhteystietojen saatavuus unionissa taikka se, että käytetään siinä kolmannessa maassa, johon toimija on sijoittautunut, yleisesti käytettävää kieltä, ei sellaisenaan riitä tällaisen aikomuksen varmistamiseksi. Sellaiset seikat, kuten yhdessä tai useammassa jäsenvaltiossa yleisesti käytettävän kielen tai rahayksikön käyttö ja mahdollisuus tilata palveluja kyseisellä muulla kielellä tai maininta unionissa olevista asiakkaista tai käyttäjistä, voivat kuitenkin osoittaa olevan ilmeistä, että toimija aikoo tarjota palveluja unionissa. Edustajan olisi toimittava toimijan puolesta, ja toimivaltaisten viranomaisten tai CSIRT-yksiköiden olisi voitava ottaa yhteyttä edustajaan. Edustaja olisi nimenomaisesti nimettävä toimijan antamalla kirjallisella valtuutuksella hoitamaan tämän puolesta tämän direktiivin mukaiset velvollisuudet, mukaan lukien poikkeamista raportointi.

(66) Jos kansallisen tai unionin lainsäädännön mukaisesti turvallisuusluokiteltuina pidettyjä tietoja vaihdetaan, ilmoitetaan tai muutoin jaetaan tämän direktiivin säännösten mukaisesti, olisi sovellettava turvallisuusluokiteltujen tietojen käsittelyä koskevia vastaavia erityissääntöjä.

(67) Koska kyberuhat muuttuvat monimutkaisemmiksi ja kehittyneemmiksi, hyvät havaitsemis- ja ennaltaehkäisytoimenpiteet edellyttävät suurelta osin uhkiin ja haavoittuvuuteen liittyvän tiedon säännöllistä jakamista toimijoiden välillä. Tietojenvaihto lisää tietoisuutta kyberuhkista, mikä puolestaan parantaa toimijoiden valmiuksia estää uhkia kehittymästä todellisiksi poikkeamiksi ja auttaa niitä hallitsemaan paremmin poikkeamien vaikutuksia ja palautumaan niistä tehokkaammin. Koska unionin tasolla ei ole annettu ohjeita, vaikuttaa siltä, että useat tekijät, erityisesti epävarmuus yhteensopivuudesta kilpailu- ja vastuusääntöjen kanssa, ovat estäneet tällaisen tietojen jakamisen.

(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.

(69) Siinä määrin kuin on ehdottoman välttämätöntä ja oikeasuhteista verkko- ja tietoturvan varmistamiseksi, **keskeisten ja tärkeiden** toimijoiden [...] sekä turvallisuusteknologioiden ja -palvelujen tarjoajien suorittama **henkilötietojen käsittely voitaisiin katsoa olevan tarpeen** asianomaisen rekisterinpitäjän **lakisääteisen velvoitteen noudattamiseksi tai [...]** muodostavan asianomaisen rekisterinpitäjän osalta [...] asetuksessa (EU) 2016/679 tarkoitetun oikeutetun intressin. Tämä [...] **voisi kattaa toimenpiteet**, jotka liittyvät poikkeamien ehkäisemiseen, havaitsemiseen, analysointiin ja niihin reagoimiseen, toimenpiteet yksittäisistä kyberuhkista tiedottamiseksi, tietojenvaihdon haavoittuvuuden korjaamisen ja koordinoidun paljastamisen yhteydessä, näitä poikkeamia koskevan vapaaehtoisen tietojenvaihdon [...] sekä toimenpiteet, jotka liittyvät kyberuhkiin ja haavoittuvuuksiin, riskien ilmenemisen indikaattoreihin, taktiikkaan, tekniikoihin ja menettelyihin, kyberturvallisuushälytyksiin ja konfigurointivälineisiin. Tällaiset toimenpiteet voivat edellyttää [...] **monentyyppisten** henkilötietojen käsittelyä. **Näitä voivat olla esimerkiksi** IP-osoitteet, URL-osoitteet, verkkotunnukset ja sähköpostiosoitteet. **Toimivaltaisten viranomaisten, kyberturvallisuuden kansallisten keskitettyjen yhteyspisteiden ja CSIRT-yksiköiden suorittamasta henkilötietojen käsittelystä olisi säädettävä kansallisessa lainsäädännössä, ja se olisi katsottava välttämättömäksi lakisääteisen velvoitteen noudattamiseksi taikka yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi asetuksen (EU) 2016/679 6 artiklan 1 kohdan c tai e alakohdassa tarkoitetulla tavalla.**

(69 a) Jäsenvaltioiden lainsäädännössä voidaan vahvistaa sääntöjä, joiden nojalla, siinä määrin kuin on ehdottoman välttämättömiä ja oikeasuhteista keskeisten ja tärkeiden toimijoiden verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi, toimivaltaiset viranomaiset, kyberturvallisuuden kansalliset keskitetyt yhteyspisteet ja CSIRT-yksiköt voivat käsitellä erityisiä henkilötietoryhmiä asetuksen (EU) 2016/679 9 artiklan [...] mukaisesti, erityisesti säätämällä asianmukaisista ja erityisistä toimenpiteistä luonnollisten henkilöiden perusoikeuksien ja etujen suojaamiseksi, mukaan lukien tällaisten tietojen uudelleenkäyttöä koskevien teknisten rajoitusten sekä uusinta tekniikkaa hyödyntävien tietoturvaa ja yksityisyyden suojaa parantavien toimenpiteiden, kuten pseudonymisoinnin, taikka salauksen käyttö, jos anonymisointi voi vaikuttaa merkittävästi aiottuun käyttötarkoitukseen.

(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. 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 **tärkeitä toimijoita ei pitäisi vaatia dokumentoimaan** [...] järjestelmällisesti kyberturvallisuusriskien hallintaa koskevien vaatimusten noudattamista, ja toimivaltaisten viranomaisten olisi harjoitettava reaktiivista jälkikäteisvalvontaa eikä niillä näin ollen olisi yleistä velvoitetta valvoa kyseisiä toimijoita. **Tärkeiden toimijoiden jälkikäteisvalvonta voidaan käynnistää, jos toimivaltaisen viranomaisen tietoon tulee näyttöä, viitteitä tai tietoja, joiden perusteella kyseinen viranomainen katsoo, että tässä direktiivissä säädettyjä velvoitteita on saatettu jättää noudattamatta. Tällainen näyttö, viitteet tai tiedot voivat esimerkiksi olla muiden viranomaisten, toimijoiden, kansalaisten, tiedotusvälineiden tai muiden lähteiden toimivaltaiselle viranomaiselle toimittamia tietoja, julkisesti saatavilla olevia tietoja tai ne voivat käydä ilmi, kun toimivaltainen viranomainen hoitaa muita tehtäviään.**

(70 a) Kun toimivaltaiset viranomaiset harjoittavat etukäteisvalvontaa, niiden olisi voitava päättää käytettävissään olevien valvontatoimien ja -keinojen käytön ensisijaisuudesta oikeasuhteisella tavalla. Tämä merkitsee sitä, että toimivaltaiset viranomaiset voivat päättää ensisijaisuudesta sellaisten valvontamenetelmien perusteella, joissa olisi noudatettava riskiperusteista toimintatapaa. Tällaiset menetelmät voisivat erityisesti sisältää kriteerejä tai perusteita, joiden mukaan luokitellaan keskeiset toimijat riskiluokkiin ja määritellään kutakin riskiluokkaa vastaavat suositellut valvontatoimet ja -keinot, kuten esimerkiksi paikalla suoritettavien tarkastusten, kohdennettujen turvallisuusauditointien tai turvallisuuskartoitusten käyttö, aikavälit ja tyyppi sekä pyydettävien tietojen tyyppi ja yksityiskohtaisuustaso. Tällaisten valvontamenetelmien lisäksi voidaan käyttää työohjelmia, ja niitä voidaan arvioida ja tarkastella uudelleen säännöllisesti, myös esimerkiksi resurssien jaon ja niitä koskevien tarpeiden osalta.

(70 b) Julkishallinnon toimijoiden osalta valvontavaltuuksia olisi käytettävä kansallisten kehysten ja oikeusjärjestyksen mukaisesti. Jäsenvaltioiden olisi voitava päättää määrätä kyseisiä toimijoita koskevia asianmukaisia, oikeasuhteisia ja tehokkaita valvonta- ja täytäntöönpanotoimenpiteitä.

(70 c) Tiettyjen kyberturvallisuusriskien hallintatoimenpiteiden noudattamisen osoittamiseksi jäsenvaltiot voisivat vaatia keskeisiä ja tärkeitä toimijoita käyttämään asetuksen (EU) 910/2014 mukaisia hyväksyttyjä luottamuspalveluja tai ilmoitettuja sähköisen tunnistamisen järjestelmiä.

(71) Jotta valvonta olisi tuloksellista, olisi vahvistettava vähimmäisluettelo hallinnollisista seuraamuksista, joita määrätään tässä direktiivissä säädettyjen kyberturvallisuusriskien hallintaa ja raportointia koskevien velvoitteiden laiminlyömisestä, ja vahvistettava selkeä ja johdonmukainen kehys tällaisille seuraamuksille koko unionissa. Olisi otettava asianmukaisesti huomioon rikkomisen luonne, vakavuus ja kesto, aiheutetut todelliset vahingot tai menetykset tai mahdolliset vahingot tai menetykset, jotka olisi voitu aiheuttaa, rikkomisen tahallisuus tai tuottamuksellisuus, vahingon ja/tai menetysten ehkäisemiseksi tai lieventämiseksi toteutetut toimet, vastuun aste tai asiaan liittyvät aiemmat laiminlyönnit, toimivaltaisen viranomaisen kanssa tehdyn yhteistyön aste ja mahdolliset muut raskauttavat tai lieventävät tekijät. Seuraamusten, myös hallinnollisten sakkojen, määräämiseen olisi sovellettava asianmukaisia menettelyllisiä suojatoimenpiteitä unionin oikeuden ja Euroopan unionin perusoikeuskirjan yleisten periaatteiden mukaisesti, mukaan lukien tosiasiallinen oikeussuoja ja asianmukainen käsittelyprosessi.

(71 a) Säännöksissä, jotka koskevat sellaisten luonnollisten henkilöiden vastuuta tässä direktiivissä säädettyjen velvoitteiden noudattamista koskevan velvollisuuden laiminlyönnistä, joilla on tiettyjä vastuita toimijan sisällä, ei velvoiteta jäsenvaltioita varmistamaan syytteen nostamista tai ajamista taikka yksityisoikeudellista vastuuta vahingoista, joita tällainen laiminlyönti aiheuttaa kolmansille osapuolille.

(72) Tässä direktiivissä säädettyjen velvoitteiden tuloksellisen täytäntöönpanon varmistamiseksi kullakin toimivaltaisella viranomaisella olisi oltava valtuudet määrätä hallinnollisia sakkoja tai pyytää niiden määräämistä.

(73) Silloin kun sakkoja määrätään yritykselle, yritys olisi ymmärrettävä Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 101 ja 102 artiklan mukaiseksi yritykseksi. Jos hallinnollisia sakkoja määrätään henkilöille, jotka eivät ole yrityksiä, valvontaviranomaisen olisi sakon sopivan määrän harkinnassa otettava huomioon jäsenvaltion yleinen tulotaso ja henkilön taloudellinen tilanne. Jäsenvaltioilla olisi oltava vastuu määritellä onko viranomaisille määrättävä hallinnollisia sakkoja ja missä määrin. Hallinnollisen sakon määrääminen ei vaikuta toimivaltaisten viranomaisten muihin valtuuksiin tai muihin seuraamuksiin, joista säädetään tämän direktiivin kansalliseen lainsäädäntöön sisällyttävissä kansallisissa säännöissä.

(74) **Jäsenvaltiot voivat** [...] vahvistaa rikosoikeudellisia seuraamuksia koskevia sääntöjä, joita sovelletaan tämän direktiivin kansalliseen lainsäädäntöön sisällyttävien kansallisten sääntöjen rikkomiseen. Tällaisten kansallisten sääntöjen rikkomisesta määrättävien rikosoikeudellisten seuraamusten ja niihin liittyvien hallinnollisten seuraamusten ei kuitenkaan pitäisi johtaa ne bis in idem -periaatteen rikkomiseen, sellaisena kuin unionin tuomioistuin on sitä tulkinnut.

(75) Sikäli kuin tässä direktiivissä ei yhdenmukaisteta hallinnollisia seuraamuksia tai tarvittaessa muissa tapauksissa, esimerkiksi silloin, kun kyseessä on tämän direktiivin velvoitteiden vakava laiminlyönti, jäsenvaltioiden olisi pantava täytäntöön järjestelmä, jossa määrätään tehokkaista, oikeasuhteisista ja varoittavista seuraamuksista. Tällaisten rikosoikeudellisten tai hallinnollisten seuraamusten luonne olisi määriteltävä jäsenvaltion lainsäädännössä.

(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 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.

(76 a) Jotta voidaan varmistaa tehokas valvonta ja täytäntöönpano, erityisesti rajatylittävissä tapauksissa, keskinäistä avunantoa koskevan pyynnön saaneiden jäsenvaltioiden olisi kyseisen pyynnön rajoissa toteutettava asianmukaisia valvonta- ja täytäntöönpanotoimenpiteitä sellaisen toimijan osalta, joka tarjoaa niiden alueella palveluja tai jolla on siellä verkko- ja tietojärjestelmä.

(77) Tässä direktiivissä olisi vahvistettava toimivaltaisten viranomaisten ja valvontaviranomaisten välistä yhteistyötä koskevat säännöt asetuksen (EU) 2016/679 mukaisesti henkilötietoihin liittyvien rikkomusten käsittelemiseksi.

(78) Tällä direktiivillä olisi pyrittävä varmistamaan organisaatiotasolla korkeatasoinen vastuu kyberturvallisuusriskien hallintatoimenpiteistä ja raportointivelvoitteista. Näistä syistä tämän direktiivin soveltamisalaan kuuluvien toimijoiden hallintoelinten olisi hyväksyttävä kyberturvallisuusriskitoimenpiteet ja valvottava niiden täytäntöönpanoa.

(79) Olisi otettava käyttöön [...] **vertaisoppimisjärjestelmä, joka auttaisi vahvistamaan keskinäistä luottamusta ja oppimaan hyvistä käytännöistä ja kokemuksista ja** jonka avulla jäsenvaltioiden nimeämät asiantuntijat voivat [...] **vaihtaa keskenään tietoja** kyberturvallisuuspolitiikkojen täytäntöönpanosta. **Vertaisoppimisjärjestelmää toteutettaessa olisi kiinnitettävä huomiota erityisesti sen varmistamiseen, että järjestelmä ei aiheuta asianomaisten jäsenvaltioiden viranomaisille tarpeetonta tai kohtuutonta rasitetta. Komission olisi selvitettävä kaikki mahdolliset keinot taata vertaisoppimiskomennuksien järjestämisestä aiheutuvien kustannusten kattaminen. Vertaisoppimisjärjestelmässä olisi myös otettava huomioon tulokset, joita on saatu vastaavista mekanismeista, kuten CSIRT-verkoston vertaisarviointijärjestelmästä, ja sen olisi lisäksi tuotava lisäarvoa ja siinä olisi vältettävä päällekkäisyydet. Vertaisoppimisjärjestelmän toteuttamisen ei olisi rajoitettava luottamuksellisten tai turvallisuusluokiteltujen tietojen suojaamista koskevan kansallisen tai unionin lainsäädännön soveltamista. Jäsenvaltiot voivat suorittaa itsearvioinnin vertaisoppimiskierroksiin liittyvistä olennaisista näkökohdista, ennen kuin kierrokset aloitetaan. ENISA voi yhteistyöryhmän pyynnöstä antaa tarvittaessa itsearviointia ja siihen liittyviä malleja koskevia ohjeita. Jäsenvaltiot voisivat päättää asettaa omat raporttinsa julkisesti saataville.**

(80) [...]

(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 **sekä tiettyjä sertifioituja tieto- ja viestintätekniikan tuotteita, palveluja ja prosesseja käyttämään velvoitettavien toimijoiden luokkien** osalta, komissiolle olisi siirrettävä täytäntöönpanovaltaa. Tätä valtaa olisi käytettävä Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 182/2011[26] mukaisesti.

(82) Komission olisi tarkasteltava tätä direktiiviä säännöllisin väliajoin uudelleen asianomaisia osapuolia kuullen, erityisesti yhteiskunnan, politiikan, tekniikan ja markkinaolojen kehitykseen perustuvien muutostarpeiden selvittämiseksi.

---

[26] 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).

(83) Jäsenvaltiot eivät voi riittävällä tavalla saavuttaa tämän direktiivin tavoitetta, joka on yhteinen korkea kyberturvallisuuden taso unionissa, vaan se voidaan toiminnan vaikutusten vuoksi saavuttaa paremmin unionin tasolla. Sen vuoksi unioni voi toteuttaa toimenpiteitä Euroopan unionista tehdyn sopimuksen 5 artiklassa vahvistetun toissijaisuusperiaatteen mukaisesti. Mainitussa artiklassa vahvistetun suhteellisuusperiaatteen mukaisesti tässä direktiivissä ei ylitetä sitä, mikä on tarpeen tämän tavoitteen saavuttamiseksi.

(84) Tässä direktiivissä kunnioitetaan Euroopan unionin perusoikeuskirjassa tunnustettuja perusoikeuksia ja noudatetaan siinä tunnustettuja periaatteita, erityisesti oikeutta yksityiselämän ja viestien kunnioittamiseen, henkilötietojen suojaa, elinkeinovapautta, omistusoikeutta, oikeutta tehokkaisiin oikeussuojakeinoihin tuomioistuimessa ja oikeutta tulla kuulluksi. Tämä direktiivi olisi pantava täytäntöön näiden oikeuksien ja periaatteiden mukaisesti,

OVAT HYVÄKSYNEET TÄMÄN DIREKTIIVIN:

I LUKU

Yleiset säännökset

1 artikla

Kohde

1. Tässä direktiivissä säädetään toimenpiteistä yhteisen korkeatasoisen kyberturvallisuuden varmistamiseksi unionissa **sisämarkkinoiden toiminnan parantamiseksi**.

2. Tätä varten tässä direktiivissä

   a) vahvistetaan jäsenvaltioiden velvoitteet hyväksyä kansalliset kyberturvallisuusstrategiat sekä nimetä toimivaltaiset kansalliset viranomaiset, keskitetyt yhteyspisteet ja tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (CSIRT-yksiköt);

   b) vahvistetaan kyberturvallisuusriskien hallintaa ja raportointia koskevat velvoitteet **liitteissä I ja II** [...] tarkoitetuille [...] toimijoille;

   c) vahvistetaan kyberturvallisuustietojen jakamista koskevat **säännöt ja** velvoitteet.

2 artikla

Soveltamisala

1. Tätä direktiiviä sovelletaan [...] **liitteissä I ja II** tarkoitettuihin julkisiin ja yksityisiin toimijoihin**, jotka täyttävät tai ylittävät** [...] komission suosituksessa 2003/361/EY[27] tarkoitetut **keskisuurten yritysten määrittelyssä käytettävät kynnysarvot**. **Kyseisen suosituksen liitteessä olevaa 3 artiklan 4 kohtaa sekä 6 artiklan 2 kohdan toista ja kolmatta alakohtaa ei sovelleta tätä direktiiviä sovellettaessa.**

2. [...] **Edellä 1 kohdassa tarkoitetusta toimijoiden** [...] koosta riippumatta tätä direktiiviä sovelletaan myös**, jos** [...]

   a) palveluntarjoaja on jokin seuraavista toimijoista:

      i) liitteessä I olevassa 8 kohdassa tarkoitetun yleisen sähköisen viestintäverkon tai yleisesti saatavilla olevan sähköisen viestintäpalvelun **tarjoaja**;

      ii) liitteessä I olevassa XX kohdassa tarkoitettu hyväksytty luottamuspalvelun tarjoaja;

      iii) liitteessä I olevassa XX kohdassa tarkoitettu ei-hyväksytty luottamuspalvelun tarjoaja;

      iv) liitteessä I olevassa 8 kohdassa tarkoitettu aluetunnusrekisteri (TLD-rekisteri);

   b) [...]

---

[27] Komission suositus 2003/361/EY, annettu 6 päivänä toukokuuta 2003, mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä (EUVL L 124, 20.5.2003, s. 36).

c) toimija tarjoaa **jossakin jäsenvaltiossa ainoana palveluntarjoajana** palvelua [...]**, joka on keskeinen yhteiskunnan tai talouden kriittisten toimintojen ylläpitämiseksi**;

d) häiriö toimijan tarjoamassa palvelussa voisi vaikuttaa **merkittävästi** yleiseen järjestykseen, yleiseen turvallisuuteen tai kansanterveyteen;

e) häiriö toimijan tarjoamassa palvelussa voisi aiheuttaa **merkittäviä** järjestelmäriskejä erityisesti aloilla, joilla häiriöllä voisi olla valtioiden rajat ylittäviä vaikutuksia;

f) [...];

g) toimija on määritelty kriittiseksi toimijaksi Euroopan parlamentin ja neuvoston direktiivin (EU) XXXX/XXXX[28] [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] mukaisesti tai **[**kriittistä toimijaa vastaavaksi toimijaksi kyseisen direktiivin 7 artiklan mukaisesti**]**.

2 a. **Tätä direktiiviä sovelletaan myös toimijoihin, jotka jokin jäsenvaltio katsoo kansallisen lainsäädännön mukaisesti liitteessä I olevassa 9 kohdassa tarkoitetuksi keskushallintonsa julkiseksi toimijaksi, riippumatta kyseisen toimijan koosta. Jäsenvaltiot voivat säätää, että tätä direktiiviä sovelletaan myös alue- ja paikallishallintojen julkisiin toimijoihin.**

---

[28] [lisätään koko nimi ja EUVL:n julkaisuviite, kun ne ovat tiedossa]

3. [...]

Tällä direktiivillä ei rajoiteta jäsenvaltioiden velvollisuutta turvata kansallinen turvallisuus eikä niiden valtuuksia suojata muita keskeisiä valtiolla kuuluvia tehtäviä, mukaan lukien valtion alueellisen koskemattomuuden turvaaminen ja yleisen järjestyksen ylläpitäminen.

3 a. 1) Tätä direktiiviä ei sovelleta

a) toimijoihin, jotka eivät kuulu unionin lainsäädännön soveltamisalaan, ja joka tapauksessa mihinkään toimijoihin, jotka toimivat pääasiassa puolustuksen, kansallisen turvallisuuden, yleisen turvallisuuden tai lainvalvonnan alalla, riippumatta siitä, mikä toimija kyseistä toimintaa harjoittaa ja onko kyseessä julkinen vai yksityinen toimija, sanotun kuitenkaan rajoittamatta 2 kohdan soveltamista;

b) **toimijoihin, jotka harjoittavat oikeuslaitoksille, kansanedustuslaitoksille tai keskuspankeille kuuluvaa toimintaa.**[...]

2) Jos julkishallinnon toimijat harjoittavat näihin aloihin kuuluvaa toimintaa vain osana kaikkea toimintaansa, ne on jätettävä kokonaan tämän direktiivin soveltamisalan ulkopuolelle.

3 a a. Tätä direktiiviä ei sovelleta

i) sellaisten toimijoiden toimintaan, jotka eivät kuulu unionin lainsäädännön soveltamisalaan, ja joka tapauksessa mihinkään toimintaan, joka liittyy kansalliseen turvallisuuteen tai puolustukseen, riippumatta siitä, mikä toimija kyseistä toimintaa harjoittaa ja onko kyseessä julkinen vai yksityinen toimija;

ii) oikeuslaitoksille, kansanedustuslaitoksille ja keskuspankeille kuuluvaa toimintaa harjoittavien toimijoiden toimintaan sekä toimintaan yleisen turvallisuuden alalla, mukaan lukien julkishallinnon toimijat, jotka toimivat lainvalvonnan alalla rikosten ennalta estämiseksi, tutkimiseksi, paljastamiseksi taikka rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten.

3 a a a. Tässä direktiivissä säädettyihin velvoitteisiin ei kuulu sellaisten tietojen toimittaminen, joiden ilmaiseminen olisi vastoin jäsenvaltion keskeisiä kansalliseen turvallisuuteen, yleiseen turvallisuuteen tai puolustukseen liittyviä etuja.

3 a a a a. Tämä direktiivi ei vaikuta henkilötietojen suojaa koskevan unionin lainsäädännön eikä etenkään asetuksen (EU) 2016/679 ja direktiivin 2002/58/EY soveltamiseen.

3 b. Tätä direktiiviä ei sovelleta toimijoihin, jotka on vapautettu Euroopan parlamentin ja neuvoston asetuksen (EU) XXXX/XXXX [DORA-asetus] soveltamisesta DORA-asetuksen 2 artiklan 4 kohdan mukaisesti.

4. Tämän direktiivin soveltaminen ei rajoita [...][29] [...] Euroopan parlamentin ja neuvoston direktiivien 2011/93/EU[30] ja 2013/40/EU[31] soveltamista.

5. Tietoja, jotka katsotaan luottamuksellisiksi unionin ja kansallisten sääntöjen, kuten liikesalaisuuksia koskevien sääntöjen mukaisesti, saa vaihtaa komission ja muiden asianomaisten viranomaisten kanssa **tämän direktiivin mukaisesti** vain silloin kun tällainen vaihtaminen on välttämätöntä tämän direktiivin soveltamiseksi, sanotun kuitenkaan rajoittamatta Euroopan unionin toiminnasta tehdyn sopimuksen 346 artiklan soveltamista. Tällöin on vaihdettava ainoastaan sellaisia tietoja, jotka ovat merkityksellisiä ja oikeasuhteisia tällaisen vaihdon tarkoituksen kannalta. Tällaisessa tiedonvaihdossa on säilytettävä kyseisten tietojen luottamuksellisuus sekä suojeltava keskeisten tai tärkeiden toimijoiden turvallisuusetuja ja kaupallisia etuja.

---

[29] [...]

[30] Euroopan parlamentin ja neuvoston direktiivi 2011/93/EU, annettu 13 päivänä joulukuuta 2011, lasten seksuaalisen hyväksikäytön ja seksuaalisen riiston sekä lapsipornografian torjumisesta ja neuvoston puitepäätöksen 2004/68/YOS korvaamisesta (EUVL L 335, 17.12.2011, s. 1).

[31] Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU, annettu 12 päivänä elokuuta 2013, tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta (EUVL L 218, 14.8.2013, s. 8).

2 a artikla

Keskeiset ja tärkeät toimijat

1. Toimijoista, joihin tätä direktiiviä sovelletaan, seuraavat on katsottava keskeisiksi:

i) tämän direktiivin liitteessä I olevissa 1–8 a kohdassa ja 10 kohdassa tarkoitetut toimijat, jotka ylittävät komission suosituksessa 2003/361/EY tarkoitetut keskisuurten yritysten määrittelyssä käytettävät kynnysarvot;

ii) edellä 2 artiklan 2 kohdan a alakohdan i alakohdassa tarkoitetut keskisuuret toimijat;

iii) tämän direktiivin 2 artiklan 2 kohdan a alakohdan ii ja iv alakohdassa tarkoitetut toimijat näiden koosta riippumatta;

iv) tämän direktiivin 2 artiklan 2 kohdan g alakohdassa ja 2 artiklan 2 a kohdassa tarkoitetut toimijat näiden koosta riippumatta;

v) toimijat, jotka jäsenvaltiot olivat direktiivin (EU) 2016/1148 tai kansallisen lainsäädännön mukaisesti yksilöineet keskeisten palvelujen tarjoajiksi ennen tämän direktiivin voimaantuloa, mikäli tällaisia toimijoita on yksilöity;

vi) liitteessä II tarkoitetut toimijat, jotka ylittävät komission suosituksessa 2003/361/EY tarkoitetut keskisuurten yritysten määrittelyssä käytettävät kynnysarvot ja jotka jäsenvaltiot ovat yksilöineet keskeisiksi 2 artiklan 2 kohdan c–e alakohdassa tarkoitettujen kriteerien perusteella;

vii) komission suosituksessa 2003/361/EY tarkoitetut keskisuuret toimijat, jotka jäsenvaltiot ovat yksilöineet keskeisiksi 2 artiklan 2 kohdan c–e alakohdassa tarkoitettujen kriteerien perusteella;

viii) komission suosituksessa 2003/361/EY ja tämän artiklan 2 kohdan a alakohdan i alakohdassa tarkoitetut tai tämän artiklan 2 kohdan c–e alakohdan nojalla yksilöidyt mikrotoimijat ja pienet toimijat, jotka jäsenvaltiot ovat yksilöineet keskeisiksi kansallisten riskinarviointien perusteella.

2. Toimijoista, joihin tätä direktiiviä sovelletaan, seuraavat on katsottava tärkeiksi:

i) tämän direktiivin liitteessä I tarkoitetut toimijat, jotka katsotaan komission suosituksen 2003/361/EY perusteella keskisuuriksi yrityksiksi, ja liitteessä II tarkoitetut toimijat, jotka täyttävät tai ylittävät komission suosituksessa 2003/361/EY tarkoitetut keskisuurten yritysten määrittelyssä käytettävät kynnysarvot[32];

ii) tämän direktiivin 2 artiklan 2 kohdan a alakohdan iii alakohdassa tarkoitetut toimijat näiden koosta riippumatta;

iii) edellä 2 artiklan 2 kohdan a alakohdan i alakohdassa tarkoitetut pienet ja mikrotoimijat;

iv) pienet ja mikrotoimijat, jotka jäsenvaltiot ovat yksilöineet tärkeiksi toimijoiksi 2 artiklan 2 kohdan c–e alakohdan perusteella.

---

[32] **Komission suositus 2003/361/EY, annettu 6 päivänä toukokuuta 2003, mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä (EUVL L 124, 20.5.2003, s. 36).**

2 a artikla

Ilmoitusmekanismit

1. **Jäsenvaltiot voivat ottaa käyttöön kansalliset ilmoitusmenetelmät, joiden mukaan kaikkien tämän direktiivin soveltamisalaan kuuluvien toimijoiden on toimitettava tämän direktiivin mukaisesti toimivaltaisille viranomaisille tai jäsenvaltioiden tätä tarkoitusta varten nimeämille elimille ainakin nimensä, osoitteensa, yhteystietonsa, toimialansa tai tarjoamansa palvelun tyyppi sekä tarvittaessa luettelo jäsenvaltioista, joissa ne tarjoavat palveluja, joihin tätä direktiiviä sovelletaan.**

2. Jäsenvaltioiden on [...] toimitettava komissiolle **2 artiklan 2 kohdan b–e alakohtien mukaisesti yksilöimiensä toimijoiden osalta ainakin asiaankuuluvat tiedot yksilöityjen toimijoiden määrästä, niiden toimialasta tai niiden tarjoaman palvelun tyypistä liitteiden mukaisesti sekä 2 artiklan 2 kohdan erityisistä säännöksistä, joiden perusteella toimijat on nimetty viimeistään [12 kuukautta siitä päivästä, johon mennessä tämä direktiivi on saatettava osaksi kansallista lainsäädäntöä].** Jäsenvaltioiden on tarkasteltava [...] **näitä tietoja** [...] uudelleen säännöllisesti ja vähintään joka toinen vuosi ja saatettava ne tarvittaessa ajan tasalle.

2 b artikla

Alakohtaiset unionin säädökset

1. Jos unionin **alakohtaisissa säädöksissä** [...] edellytetään, että keskeiset tai tärkeät toimijat [...] hyväksyvät kyberturvallisuusriskien hallintatoimenpiteitä tai ilmoittavat **merkittävistä** poikkeamista tai [...] kyberuhista, ja jos kyseiset vaatimukset vastaavat vaikutukseltaan vähintään tässä direktiivissä säädettyjä velvoitteita, tämän direktiivin asiaankuuluvia säännöksiä, **mukaan lukien VI luvussa säädetyt valvontaa ja täytäntöönpanoa koskevat säännökset,** ei sovelleta **tällaisiin toimijoihin**. **Jos unionin alakohtaiset säädökset eivät kata tämän direktiivin soveltamisalaan kuuluvan toimialan kaikkia toimijoita, tämän direktiivin asiaankuuluvia säännöksiä on edelleen sovellettava niihin toimijoihin, joita nämä alakohtaiset säännökset eivät kata.**

2. Tämän artiklan 1 kohdassa tarkoitetut vaatimukset on katsottava vaikutukseltaan vastaaviksi tässä direktiivissä vahvistettujen velvoitteiden kanssa, jos vastaavassa alakohtaisessa unionin säädöksessä säädetään välittömästä ja tarvittaessa automaattisesta ja suorasta pääsystä tämän direktiivin nojalla toimivaltaisten viranomaisten tai nimettyjen CSIRT-yksiköiden tekemiin poikkeamailmoituksiin ja jos

a) kyberturvallisuusriskien hallintatoimenpiteet ovat vaikutukseltaan vähintään vastaavat kuin tämän direktiivin 18 artiklan 1 ja 2 kohdassa vahvistetut toimenpiteet; tai

b) merkittävien poikkeamien ilmoittamista koskevat vaatimukset ovat vaikutukseltaan vähintään vastaavat kuin tämän direktiivin 20 artiklan 1 ja 6 kohdassa vahvistetut vaatimukset.

3. Komissio tarkastelee säännöllisesti uudelleen tämän artiklan 1 ja 2 kohdassa säädettyä vastaavaa vaikutusta koskevan vaatimuksen soveltamista suhteessa unionin säädösten alakohtaisiin säännöksiin. Komissio kuulee yhteistyöryhmää ja ENISAa valmistellessaan näitä määräaikaisia tarkasteluja.

3 artikla

Vähimmäistason yhdenmukaistaminen

Jäsenvaltiot voivat [...] antaa tai pitää voimassa säännöksiä, joilla varmistetaan kyberturvallisuuden korkeampi taso **tämän direktiivin soveltamisalaan kuuluvilla aloilla**, sanotun kuitenkaan rajoittamatta niiden muita unionin oikeuden mukaisia velvoitteita.

4 artikla

Määritelmät

Tässä direktiivissä tarkoitetaan:

1) 'verkko- ja tietojärjestelmällä'

   a) direktiivin (EU) 2018/1972 2 artiklan 1 kohdassa tarkoitettua sähköistä viestintäverkkoa;

   b) laitetta taikka yhteen kytkettyjen tai toisiinsa yhteydessä olevien laitteiden ryhmää, joista yksi tai useampi suorittaa ohjelman avulla digitaalisten tietojen automaattista käsittelyä;

   c) digitaalisia tietoja, joita a ja b alakohdassa tarkoitetuissa järjestelmissä säilytetään, käsitellään, haetaan tai siirretään niiden toimintaa, käyttöä, suojausta tai ylläpitoa varten;

2) 'verkko- ja tietojärjestelmien turvallisuudella' verkko- ja tietojärjestelmien kykyä suojautua tietyllä varmuudella **tapahtumilta**, jotka **saattavat vaarantaa** [...] kyseisissä verkko- ja tietojärjestelmissä tarjottujen tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen **taikka** [...] palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden;

2 a) 'sähköisillä viestintäpalveluilla' direktiivin (EU) 2018/1972 2 artiklan 4 kohdassa tarkoitettuja sähköisiä [...] viestintäpalveluja;

3) 'kyberturvallisuudella' ja 'kyberturvalla' Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881[33] 2 artiklan 1 kohdassa tarkoitettua kyberturvallisuutta;

4) 'kansallisella kyberturvallisuusstrategialla' jäsenvaltion yhtenäistä kehystä, jossa esitetään **kyberturvallisuusalan** [...] strategiset tavoitteet ja painopisteet kyseisessä jäsenvaltiossa;

5) 'poikkeamalla' tapahtumaa, joka vaarantaa verkko- ja tietojärjestelmissä tarjottujen tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen tai [...] palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden;

5 a) 'laajamittaisella kyberturvallisuuspoikkeamalla' poikkeamaa, jolla on merkittävä vaikutus vähintään kahteen jäsenvaltioon tai jonka aiheuttama häiriö ylittää yksittäisen jäsenvaltion valmiudet reagoida siihen;

---

[33] Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus) (EUVL L 151, 7.6.2019, s. 15).

6) 'poikkeaman käsittelyllä' kaikkia toimia ja menettelyjä, joilla pyritään havaitsemaan, analysoimaan ja estämään poikkeama ja reagoimaan siihen;

(6 a) 'riskillä' poikkeaman aiheuttaman menetyksen tai häiriön mahdollisuutta, joka ilmaistaan tällaisen menetyksen tai häiriön suuruuden ja kyseisen poikkeaman toteutumisen todennäköisyyden yhdistelmänä;

7) 'kyberuhalla' asetuksen (EU) 2019/881 2 artiklan 8 kohdassa tarkoitettua kyberuhkaa;

7 **a) 'merkittävällä kyberuhalla' kyberuhkaa, jonka voidaan sen teknisten ominaisuuksien perusteella olettaa vaikuttavan mahdollisesti vakavasti toimijan tai sen käyttäjien verkko- ja tietojärjestelmiin aiheuttamalla huomattavia aineellisia tai aineettomia tappioita;**

8) 'haavoittuvuudella' tieto- ja viestintäteknisen omaisuuden tai järjestelmän [...] heikkoutta, herkkyyttä tai vikaa, jota kyberuhka voi hyödyntää;

8 a) 'läheltä piti -tilanteilla' tapahtumaa, joka olisi voinut aiheuttaa vahinkoa toimijan tai sen käyttäjien verkko- ja tietojärjestelmille mutta jonka täysi toteutuminen onnistuttiin estämään;

9) 'edustajalla' unioniin sijoittautunutta luonnollista henkilöä tai oikeushenkilöä, joka on nimenomaisesti nimetty toimimaan i) liitteessä I olevassa 8 kohdassa tarkoitetun DNS-palveluntarjoajan, aluetunnusrekisterin (TLD-rekisteri), pilvipalveluntarjoajan, datakeskuspalvelun tarjoajan tai sisällönjakeluverkon tarjoajan tai ii) liitteessä II olevassa [...] **6** kohdassa tarkoitetun unioniin sijoittautumattoman toimijan puolesta ja johon kansallinen toimivaltainen viranomainen tai CSIRT-yksikkö voi olla yhteydessä toimijan sijaan kyseisen toimijan tämän direktiivin mukaisten velvoitteiden osalta;

10) 'standardilla' Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1025/2012[34] 2 artiklan 1 kohdassa tarkoitettua standardia;

11) 'teknisellä eritelmällä' asetuksen (EU) N:o 1025/2012 2 artiklan 4 kohdassa tarkoitettua teknistä eritelmää;

12) 'internetin yhdysliikennepisteellä (IXP)' verkkoinfrastruktuurin osaa, joka mahdollistaa useamman kuin kahden riippumattoman verkon (autonomisen järjestelmän) yhdistämisen pääasiassa internet-liikenteen välittämisen helpottamiseksi; IXP tarjoaa autonomisille järjestelmille ainoastaan yhteenliitäntää; IXP ei edellytä minkään yhteenliittämänsä kahden autonomisen järjestelmän väliseltä internet-liikenteeltä kulkemista minkään kolmannen autonomisen järjestelmän kautta, eikä se muokkaa tällaista liikennettä tai muutoin puutu siihen;

13) 'verkkotunnusjärjestelmällä (DNS)' hierarkkista hajautettua nimeämisjärjestelmää, jonka avulla loppukäyttäjät voivat tunnistaa palveluja ja resursseja internetissä;

14) 'DNS-palveluntarjoajalla' toimijaa, joka tarjoaa rekursiivisia tai autoritatiivisia verkkotunnusten selvityspalveluja [...] **kolmansien osapuolten käyttöön juuripalvelimia lukuun ottamatta** [...];

---

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

15) 'aluetunnusrekisterillä (TLD-rekisterillä)' toimijaa, jolle on myönnetty oikeus hallinnoida tiettyä aluetunnusta (TLD) ja joka vastaa muun muassa verkkotunnusten rekisteröinnistä kyseisen aluetunnuksen alle sekä kyseisen aluetunnuksen teknisestä toiminnasta, siihen liittyvien nimipalvelinten toiminnasta, sen tietokantojen ylläpidosta ja aluetunnuksen vyöhyketiedostojen jakelusta nimipalvelimille**, lukuun ottamatta tilanteita, joissa rekisteri hyödyntää aluetunnuksia vain omaan käyttöönsä**;

15 a) 'aluetunnusten alaisten verkkotunnusten rekisteröintipalveluja tarjoavilla toimijoilla' TLD-rekistereitä, aluetunnusten rekisterinpitäjiä sekä rekisterinpitäjien edustajia, kuten jälleenmyyjiä ja välityspalvelujen tarjoajia;

16) 'digitaalisella palvelulla' Euroopan parlamentin ja neuvoston direktiivin (EU) 2015/1535[35] 1 artiklan 1 kohdan b alakohdassa tarkoitettua palvelua;

16 a) 'luottamuspalveluilla' asetuksen (EU) N:o 910/2014 3 artiklan 16 kohdassa tarkoitettuja luottamuspalveluja;

---

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

16 b) 'hyväksytyllä luottamuspalvelun tarjoajalla' asetuksen (EU) N:o 910/2014 3 artiklan 20 kohdassa tarkoitettua hyväksyttyä luottamuspalvelun tarjoajaa;

17) 'verkon kauppapaikalla' Euroopan parlamentin ja neuvoston direktiivin 2005/29/EY[36] 2 artiklan n alakohdassa tarkoitettua digitaalista palvelua;

18) 'verkon hakukoneella' Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/1150[37] 2 artiklan 5 kohdassa tarkoitettua digitaalista palvelua;

19) 'pilvipalvelulla' digitaalista palvelua, joka mahdollistaa skaalattavien ja joustavien tietoteknisten resurssien jaettavan ja [...] laajan tarveperusteisen etäkäytön**, myös silloin, kun resurssit on hajautettu useisiin sijaintipaikkoihin**;

20) 'datakeskuspalvelulla' palvelua, joka käsittää rakenteita tai rakenteiden ryhmiä, jotka on tarkoitettu datan tallennus-, käsittely- ja siirtopalveluja tarjoavien tietoteknisten ja verkkolaitteiden keskitettyyn ylläpitoon, yhteenliittämiseen ja ohjaukseen yhdessä kaikkien tarvittavien sähkönjakeluun ja toimintaolosuhteiden säätelyyn tarkoitettujen laitteiden ja infrastruktuurien kanssa;

---

[36] Euroopan parlamentin ja neuvoston direktiivi 2005/29/EY, annettu 11 päivänä toukokuuta 2005, sopimattomista elinkeinonharjoittajien ja kuluttajien välisistä kaupallisista menettelyistä sisämarkkinoilla ja neuvoston direktiivin 84/450/ETY, Euroopan parlamentin ja neuvoston direktiivien 97/7/EY, 98/27/EY ja 2002/65/EY sekä Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 2006/2004 muuttamisesta (sopimattomia kaupallisia menettelyjä koskeva direktiivi) (EUVL L 149, 11.6.2005, s. 22).

[37] Euroopan parlamentin ja neuvoston asetus (EU) 2019/1150, annettu 20 päivänä kesäkuuta 2019, oikeudenmukaisuuden ja avoimuuden edistämisestä verkossa toimivien välityspalvelujen yrityskäyttäjiä varten (EUVL L 186, 11.7.2019, s. 57).

21) 'sisällönjakeluverkolla' maantieteellisesti hajautettujen palvelimien verkostoa, jonka tarkoituksena on varmistaa digitaalisen sisällön ja digitaalisten palvelujen korkea saatavuus, käytettävyys ja nopea jakelu internetin käyttäjille sisällön ja palvelujen tarjoajien puolesta;

22) 'verkkoyhteisöalustalla' alustaa, jonka avulla loppukäyttäjät voivat olla yhteydessä toisiinsa, jakaa sisältöä, hakea tietoa ja viestiä monenlaisilla päätelaitteilla erityisesti pikaviestikeskustelujen, julkaisujen, videoiden ja suositusten [...] muodossa;

23) 'julkishallinnon toimijalla' jäsenvaltiossa **kansallisen lainsäädännön mukaisesti sellaiseksi tunnustettua** [...] toimijaa, joka täyttää seuraavat kriteerit:

    a) se on perustettu tyydyttämään yleisen edun mukaisia tarpeita, eikä sillä ole teollista tai kaupallista luonnetta;

    b) se on oikeushenkilö **tai sillä on lain nojalla oikeus toimia toisen sellaisen toimijan puolesta, joka on oikeushenkilö**;

    c) sen rahoituksesta suurin osa on peräisin valtiolta, alueelliselta viranomaiselta tai muilta julkisoikeudellisilta laitoksilta; tai sen johto on näiden viranomaisten tai laitosten valvonnan alainen; tai valtio, alueviranomaiset tai muut julkisoikeudelliset laitokset nimittävät yli puolet sen hallinto-, johto- tai valvontaelimen jäsenistä;

    d) sillä on valtuudet osoittaa luonnollisille henkilöille tai oikeushenkilöille hallinnollisia tai sääntelyyn liittyviä päätöksiä, jotka vaikuttavat näiden oikeuksiin liittyen henkilöiden, tavaroiden, palvelujen tai pääoman liikkuvuuteen rajojen yli.

24) 'toimijalla' luonnollista henkilöä tai sijoittautumispaikkansa kansallisen oikeuden perusteella muodostettua ja tunnustettua oikeushenkilöä, joka voi omissa nimissään käyttää oikeuksia ja jolle voidaan asettaa velvoitteita;

25) 'keskeisellä toimijalla' liitteessä I tarkoitettua [...] **ja 2 a artiklan 1 kohdan mukaisesti keskeiseksi yksilöityä toimijaa**;

26) 'tärkeällä toimijalla' [...] **liitteissä I ja II tarkoitettua ja 2 a artiklan 2 kohdan mukaisesti tärkeäksi yksilöityä toimijaa**;

26 a) 'tieto- ja viestintätekniikan tuotteella' asetuksen (EU) N:o 2019/881 2 artiklan 12 kohdassa tarkoitettua tieto- ja viestintätekniikan tuotetta;

26 a a) 'tieto- ja viestintätekniikan palvelulla' asetuksen (EU) N:o 2019/881 2 artiklan 13 kohdassa tarkoitettua tieto- ja viestintätekniikan palvelua;

26 a b) 'tieto- ja viestintätekniikan prosessilla' asetuksen (EU) N:o 2019/881 2 artiklan 14 kohdassa tarkoitettua tieto- ja viestintätekniikan prosessia;

26 a c) 'hallintapalvelun tarjoajalla' toimijaa, joka tarjoaa palveluja, kuten verkko-, sovellus-, infrastruktuuri- ja turvallisuuspalveluja, joita se hallitsee, tukee ja hallinnoi jatkuvasti ja säännöllisesti asiakkaan tiloissa, niiden hallintapalvelujen tarjoajan datakeskuksessa (isännöinti) tai kolmannen osapuolen datakeskuksessa;

26 a d) 'tietoturvapalveluntarjoajalla' toimijaa, joka tarjoaa turvalaitteiden ja -järjestelmien ulkoistettuja seuranta- ja hallintapalveluja. Tällaisia palveluja ovat tavallisesti esimerkiksi palomuurin hallinta, tunkeutumisen havaitseminen, virtuaaliset yksityisverkot, haavoittuvuuksien kartoitus ja virustentorjuntapalvelut.

Niihin kuuluvat myös korkean saatavuuden turvaoperaatiokeskusten käyttö (joko omista tai muiden datakeskuspalvelujen tarjoajien tiloista käsin), sellaisten ympärivuorokautisten palvelujen tarjoamiseksi, joiden tarkoituksena on vähentää yritysten tarvetta palkata operatiivisesta turvallisuudesta vastaavaa henkilöstöä siten, että yrityksen kyberturvallisuuden taso säilyy kuitenkin hyväksyttävänä.

II LUKU

Koordinoidut kyberturvallisuuden sääntelykehykset

5 artikla

Kansallinen kyberturvallisuusstrategia

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 sisällytettävä erityisesti seuraavat:

   a) jäsenvaltion kyberturvallisuusstrategian tavoitteet ja painopisteet [...];

   b) hallintokehys näiden tavoitteiden ja painopisteiden saavuttamiseksi, mukaan lukien 2 kohdassa tarkoitetut toimintaperiaatteet sekä [...] strategian täytäntöönpanoon osallistuvien viranomaisten ja toimijoiden roolit ja vastuut;

   c) [...] **ohjeet** asiaankuuluvien toimintojen **yksilöintiin** ja kyberturvallisuusriskien **arviointiin** kyseisessä jäsenvaltiossa;

   d) toimenpiteet, joilla varmistetaan poikkeamiin varautuminen, reagointi ja niistä toipuminen, mukaan lukien julkisen ja yksityisen sektorin yhteistyö;

   e) [...]

f) toimintakehys toimivaltaisten viranomaisten välisen koordinoinnin tehostamiseksi tämän direktiivin ja Euroopan parlamentin ja neuvoston direktiivin (EU) XXXX/XXXX[38] [kriittisten yksiköiden häiriönsietokykyä koskeva direktiivi] mukaisesti **kyberturvallisuusriskejä,** [...] kyberuhkia **ja kyberturvallisuuspoikkeamia sekä muita kuin kyberturvallisuuteen liittyviä riskejä, uhkia ja poikkeamia** koskevien tietojen jakamiseksi ja **tarvittaessa** valvontatehtävien hoitamiseksi;

f a) toimintakehys tämän direktiivin mukaisesti sekä alakohtaisen lainsäädännön nojalla nimettyjen toimivaltaisten viranomaisten koordinointia ja yhteistyötä varten.

2. Osana kansallista kyberturvallisuusstrategiaa jäsenvaltioiden on erityisesti vahvistettava seuraavat toimintaperiaatteet:

a) toimintaperiaatteet, jotka koskevat kyberturvallisuutta sellaisten tieto- ja viestintätekniikan tuotteiden ja palvelujen toimitusketjussa, joita [...] toimijat käyttävät palvelujensa tarjoamiseen;

b) toimintaperiaatteet tieto- ja viestintäteknisten tuotteiden ja palvelujen kyberturvallisuusvaatimusten huomioimiseksi ja määrittelemiseksi julkisissa hankinnoissa, myös **kyberturvallisuussertifioinnin osalta**;

c) toimintaperiaatteet [...]**, jotka koskevat haavoittuvuuksien hallintaa ja joihin sisältyy** 6 artiklan **1 kohdassa** tarkoitetun **vapaaehtoisen** koordinoidun haavoittuvuuksien ilmaisemisen edistäminen ja sujuvoittaminen;

d) toimintaperiaatteet avoimen internetin yleisen ydinverkon yleisen saatavuuden**,** [...] eheyden **ja luottamuksellisuuden** ylläpitämiseksi;

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

---

[38] *[lisätään koko nimi ja EUVL:n julkaisuviite, kun ne ovat tiedossa]*

f) toimintaperiaatteet akateemisten ja tutkimuslaitosten tukemiseksi niiden kehittäessä kyberturvamenetelmiä ja turvallista verkkoinfrastruktuuria;

g) toimintaperiaatteet, asiaankuuluvat menettelyt ja asianmukaiset tiedonjakovälineet, joilla tuetaan vapaaehtoista kyberturvallisuustietojen jakamista yritysten välillä unionin oikeuden mukaisesti;

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

3. Jäsenvaltioiden on toimitettava kansalliset kyberturvallisuusstrategiansa komissiolle kolmen kuukauden kuluessa niiden hyväksymisestä. Jäsenvaltiot voivat [...] **tässä yhteydessä** jättää **strategiasta** pois kansallista turvallisuutta **koskevat osat**.

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

6 artikla

Koordinoitu haavoittuvuuden ilmaiseminen ja Euroopan haavoittuvuusrekisteri

1. Kunkin jäsenvaltion on nimettävä yksi 9 artiklassa tarkoitetuista CSIRT-yksiköistään koordinaattoriksi koordinoitua haavoittuvuuksien ilmaisemista varten. Nimetty CSIRT-yksikkö toimii luotettuna välittäjänä ja edesauttaa tarvittaessa raportoivan toimijan**, mahdollisen haavoittuvuuden omistajan** ja tieto- ja viestintätekniikan tuotteiden tai palvelujen valmistajan tai tarjoajan välistä vuorovaikutusta. **Kuka tahansa luonnollinen henkilö tai mikä tahansa oikeushenkilö voi ilmoittaa, mahdollisesti nimettömästi, nimetylle CSIRT-yksikölle 4 artiklan 8 kohdassa tarkoitetuista haavoittuvuuksista. Nimetyn CSIRT-yksikön on varmistettava, että ilmoituksen perusteella tehdään asianmukaiset jatkotoimet ja että haavoittuvuudesta ilmoittaneen henkilön henkilöllisyys pysyy salassa.** Jos raportoidulla haavoittuvuudella [...] **voi mahdollisesti olla merkittävä vaikutus useamman kuin yhden jäsenvaltion toimijoihin**, kunkin jäsenvaltion nimetyn CSIRT-yksikön on **tarvittaessa** toimittava yhteistyössä **muiden** CSIRT-verkoston **nimettyjen CSIRT-yksiköiden** kanssa.

2. ENISA perustaa Euroopan haavoittuvuusrekisterin ja ylläpitää sitä **yhteistyöryhmää kuullen**. 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 **vapaaehtoisesti** tieto- ja viestintäteknisissä tuotteissa tai palveluissa esiintyviä **julkisessa tiedossa olevia** haavoittuvuuksia ja jotta rekisterin sisältämät haavoittuvuustiedot ovat kaikkien asianomaisten osapuolten saatavilla. Rekisterin on sisällettävä erityisesti tiedot haavoittuvuudesta, siitä, mihin tieto- ja viestintätekniikan 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**, kansallisten toimivaltaisten viranomaisten tai CSIRT-yksiköiden toimittamasta** ohjeistuksesta siitä, miten haavoittuvuudesta johtuvia riskejä voidaan vähentää. **ENISA varmistaa, että Euroopan haavoittuvuusrekisteri käyttää suojattua ja häiriönsietokykyistä viestintä- ja tietoinfrastruktuuria.**

7 artikla

Kansalliset kyberturvallisuuden kriisinhallintapuitteet

1. Kunkin jäsenvaltion on nimettävä yksi tai useampi toimivaltainen viranomainen, joka vastaa laajamittaisten **kyberturvallisuus**poikkeamien ja kriisien hallinnasta. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on niille annettujen tehtävien tuloksellisen ja tehokkaan hoitamisen edellyttämät resurssit. **Jäsenvaltioiden on varmistettava johdonmukaisuus yleistä kriisien hallintaa varten käytössä olevien kehysten kanssa.**

2. Kunkin jäsenvaltion on yksilöitävä valmiudet, voimavarat ja menettelyt, joita voidaan käyttää kriisitilanteissa tämän direktiivin soveltamiseksi.

3. Kunkin jäsenvaltion on laadittava kansallinen kyberturvapoikkeama- ja -kriisinhallintasuunnitelma, jossa vahvistetaan laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallinnan tavoitteet ja menettelysäännöt. Suunnitelmassa on vahvistettava erityisesti seuraavat seikat:

    a) kansallisten varautumiskeinojen ja -toimien tavoitteet;

    b) kansallisten toimivaltaisten viranomaisten tehtävät ja vastuut;

    c) kyberturvallisuuskriisien hallintamenettelyt**, mukaan lukien niiden sisällyttäminen yleisiin kansallisiin kriisinhallintapuitteisiin,** ja tiedonvaihtokanavat;

    d) varautumiskeinot, mukaan lukien säännölliset harjoitukset ja koulutus;

    e) asianomaiset julkiset ja yksityiset sidosryhmät ja asiaan liittyvä infrastruktuuri;

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

4. Jäsenvaltioiden on ilmoitettava komissiolle 1 kohdassa tarkoitettujen toimivaltaisten viranomaistensa nimeämisestä ja toimitettava **asiaankuuluvat tämän artiklan 3 kohdan vaatimuksiin liittyvät tiedot, jotka koskevat** niiden kansallisia kyberturvapoikkeama- ja -kriisisuunnitelmia kolmen kuukauden kuluessa nimeämisestä ja kyseisten suunnitelmien hyväksymisestä. Jäsenvaltiot voivat tässä yhteydessä jättää [...] pois tiettyjä tietoja jos ja siinä määrin kuin se on kansallisen turvallisuuden**, yleisen turvallisuuden tai puolustuksen** kannalta ehdottoman välttämätöntä.

8 artikla

Kansalliset toimivaltaiset viranomaiset ja keskitetyt yhteyspisteet

1. Kunkin jäsenvaltion on nimettävä yksi tai useampi toimivaltainen viranomainen, joka vastaa kyberturvallisuudesta ja tämän direktiivin VI luvussa tarkoitetuista valvontatehtävistä. Jäsenvaltiot voivat nimetä tätä tarkoitusta varten yhden tai useamman jo olemassa olevan viranomaisen.

2. Edellä 1 kohdassa tarkoitettujen toimivaltaisten viranomaisten on valvottava tämän direktiivin soveltamista kansallisella tasolla.

3. Kunkin jäsenvaltion on nimettävä yksittäinen kansallinen kyberturvallisuusasioiden yhteyspiste, jäljempänä 'keskitetty yhteyspiste'. Jos jäsenvaltio nimeää vain yhden toimivaltaisen viranomaisen, kyseinen toimivaltainen viranomainen on myös kyseisen jäsenvaltion keskitetty yhteyspiste.

4. Kunkin keskitetyn yhteyspisteen on toimittava välittäjänä ja varmistettava oman jäsenvaltionsa viranomaisten yhteistyö muiden jäsenvaltioiden asiaankuuluvien viranomaisten kanssa sekä varmistettava hallinnonalojen rajat ylittävä yhteistyö maansa muiden kansallisten toimivaltaisten viranomaisten kanssa.

5. Jäsenvaltioiden on varmistettava, että 1 kohdassa tarkoitetuilla toimivaltaisilla viranomaisilla ja keskitetyillä yhteyspisteillä on riittävät resurssit suorittaa niille osoitetut tehtävät tuloksellisesti ja tehokkaasti ja siten saavuttaa tämän direktiivin tavoitteet. Jäsenvaltioiden on varmistettava, että nimetyt edustajat kykenevät tulokselliseen, toimivaan ja tietoturvattuun yhteistyöhön 12 artiklassa tarkoitetussa yhteistyöryhmässä.

6. Kunkin jäsenvaltion on ilmoitettava komissiolle ilman aiheetonta viivytystä 1 kohdassa tarkoitetun toimivaltaisen viranomaisen ja 3 kohdassa tarkoitetun keskitetyn yhteyspisteen nimeämisestä, niiden tehtävistä ja näihin myöhemmin mahdollisesti tehtävistä muutoksista. Kunkin jäsenvaltion on julkistettava nimitykset. Komissio julkaisee luettelon nimetyistä keskitetyistä yhteyspisteistä.

9 artikla

Tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (CSIRT)

1. Kunkin jäsenvaltion on nimettävä yksi tai useampi CSIRT-yksikkö, jonka on täytettävä 10 artiklan 1 kohdassa säädetyt vaatimukset ja joka kattaa ainakin liitteissä I ja II tarkoitetut toimialat, alasektorit tai toimijat ja joka on vastuussa poikkeamien käsittelystä tarkasti määritellyn prosessin mukaisesti. CSIRT voidaan perustaa 8 artiklassa tarkoitetun toimivaltaisen viranomaisen alaisuuteen.

2. Jäsenvaltioiden on varmistettava, että kullakin CSIRT-yksiköllä on 10 artiklan 2 kohdassa säädettyjen tehtäviensä tuloksellisen hoitamisen edellyttämät resurssit. **CSIRT-yksiköt voivat näitä tehtäviä hoitaessaan asettaa etusijalle tiettyjen palvelujen tarjoamisen toimijoille riskiperusteisen toimintatavan perusteella.**

3. Jäsenvaltioiden on varmistettava, että kullakin CSIRT-yksiköllä on käytössään asianmukainen, suojattu ja häiriönsietokykyinen viestintä- ja tietoinfrastruktuuri tietojen vaihtamiseksi keskeisten ja tärkeiden toimijoiden ja muiden asianomaisten osapuolten kanssa. Tätä varten jäsenvaltioiden on varmistettava, että CSIRT-yksiköt ovat mukana turvallisten tiedonjakovälineiden käyttöönotossa.

4. CSIRT-toimijoiden on tehtävä yhteistyötä ja tarvittaessa vaihdettava asiaankuuluvia tietoja 26 artiklan mukaisesti keskeisten ja tärkeiden toimijoiden luotettujen alakohtaisten tai monialaisten yhteisöjen kanssa.

5. CSIRT-yksiköiden on osallistuttava 16 artiklan mukaisesti järjestettävään [...] **vertaisoppimiseen**.

6. Jäsenvaltioiden on varmistettava, että niiden CSIRT-yksiköt tekevät tuloksellista, tehokasta ja tietoturvattua yhteistyötä 13 artiklassa tarkoitetussa CSIRT-verkostossa.

7. Jäsenvaltioiden on ilmoitettava komissiolle ilman aiheetonta viivytystä 1 kohdan mukaisesti nimetyt CSIRT-yksiköt, 6 artiklan 1 kohdan mukaisesti nimetty CSIRT-koordinaattori ja niiden liitteissä I ja II tarkoitettuihin toimijoihin liittyvät tehtävät.

8. Jäsenvaltiot voivat pyytää ENISAn apua kansallisten CSIRT-yksiköiden toiminnan kehittämiseen.

10 artikla

CSIRT-yksiköiden vaatimukset ja tehtävät

1. CSIRT-yksiköiden on täytettävä seuraavat vaatimukset:

   a) CSIRT-yksiköiden on varmistettava [...] **viestintäkanaviensa** kattava saatavuus välttämällä yksittäisiä pisteitä, joiden toimintahäiriö keskeyttäisi koko palvelun, ja niiden on pidettävä käytössä useita kanavia, joiden kautta niihin voidaan ottaa yhteyttä ja joiden kautta ne itse voivat ottaa yhteyttä muualle milloin tahansa. CSIRT-yksiköiden on määriteltävä selkeästi viestintäkanavat ja tiedotettava niistä kohderyhmilleen ja yhteistyökumppaneille;

   b) CSIRT-yksiköiden toimitilat ja tietojärjestelmät on sijoitettava suojattuihin paikkoihin;

c) CSIRT-yksiköillä on oltava tarkoituksenmukainen järjestelmä pyyntöjen hallintaa ja reititystä varten erityisesti tapausten tuloksellisen ja tehokkaan edelleenohjauksen helpottamiseksi;

d) CSIRT-yksiköillä on oltava riittävä henkilöstö, jotta ne voivat olla käytettävissä jatkuvasti;

e) CSIRT-yksiköillä on oltava varajärjestelmät ja -työtilat niiden palvelujen jatkuvuuden varmistamiseksi;

f) CSIRT-yksiköillä on oltava mahdollisuus osallistua kansainvälisiin yhteistyöverkostoihin.

2. CSIRT-yksiköiden tehtävänä on

a) seurata kyberuhkia, haavoittuvuuksia ja poikkeamia kansallisella tasolla;

b) antaa kyberuhkia, haavoittuvuuksia ja poikkeamia koskevia varhaisvaroituksia, hälytyksiä, ilmoituksia ja tietoja keskeisille ja tärkeille toimijoille sekä **toimivaltaisille viranomaisille ja** muille asianomaisille osapuolille;

c) reagoida poikkeamiin;

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

e) toteuttaa **[...]** verkko- ja tietojärjestelmien ennakoivia kartoituksia**, joiden tarkoituksena on havaita mahdollisesti merkittävästi vaikuttavia haavoittuvuuksia sillä edellytyksellä, että jos asianomaisen toimijan suostumusta ei ole, verkko- ja tietojärjestelmiin ei tunkeuduta eikä niiden toimintaan vaikuteta haitallisesti**;

f) osallistua CSIRT-verkostoon ja antaa pyynnöstä apua verkoston muille jäsenille **näiden valmiuksien ja osaamisen mukaisesti**;

f a) toimia tarvittaessa koordinaattorina 6 artiklan 1 kohdan mukaisessa koordinoidussa haavoittuvuuksien ilmaisemisprosessissa, johon kuuluu erityisesti raportoivien toimijoiden, mahdollisen haavoittuvuuden omistajan sekä tieto- ja viestintätekniikan tuotteiden tai palvelujen valmistajan tai tarjoajan välisen vuorovaikutuksen edesauttaminen tarvittaessa, asianosaisten toimijoiden yksilöinti ja yhteydenotto niihin, raportoivien toimijoiden tukeminen, tietojen ilmaisemisen aikataulusta neuvotteleminen sekä useisiin organisaatioihin vaikuttavien haavoittuvuuksien hallinta (monenvälinen koordinoitu haavoittuvuuksien ilmaiseminen).

3. CSIRT-yksiköiden on luotava yhteistyösuhteet asiaan liittyvien yksityisen sektorin tahojen kanssa, jotta direktiivin tavoitteet voidaan saavuttaa paremmin.

3 a. CSIRT-yksiköt voivat luoda yhteistyösuhteita kolmansien maiden kansallisten CSIRT-yksiköiden kanssa. Tämän yhteistyön yhteydessä ne voivat vaihtaa asiaankuuluvia tietoja, myös henkilötietoja unionin tietosuojalainsäädännön mukaisesti.

4. Yhteistyön helpottamiseksi CSIRT-yksiköiden on edistettävä yhteisten tai standardoitujen käytäntöjen, luokitusjärjestelmien ja taksonomioiden määrittämistä ja käyttöä seuraavien osalta:

a) poikkeamien käsittelymenettelyt;

b) kyberturvallisuuskriisien hallinta;

c) koordinoitu haavoittuvuuksien ilmaisu.

11 artikla

Kansallisen tason yhteistyö

1. Jos ne ovat erillisiä, saman jäsenvaltion 8 artiklassa tarkoitettujen toimivaltaisten viranomaisten, keskitetyn yhteyspisteen ja CSIRT-yksiköiden on tehtävä yhteistyötä tässä direktiivissä säädettyjen velvoitteiden täyttämiseksi.

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.

3. Kunkin jäsenvaltion on varmistettava, että sen toimivaltaiset viranomaiset tai CSIRT-yksiköt ilmoittavat keskitetylle yhteyspisteelleen tämän direktiivin nojalla saaduista poikkeamia, merkittäviä kyberuhkia ja läheltä piti -tilanteita koskevista ilmoituksista.

4. Siinä määrin kuin se on tarpeen tässä direktiivissä säädettyjen tehtävien ja velvollisuuksien tehokkaan suorittamisen kannalta, jäsenvaltioiden on varmistettava asianmukainen yhteistyö toimivaltaisten viranomaisten**, CSIRT-yksiköiden,** keskitettyjen asiointipisteiden, lainvalvontaviranomaisten, tietosuojaviranomaisten, direktiivin (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] nojalla **nimettyjen toimivaltaisten** viranomaisten, **komission täytäntöönpanoasetuksen 2019/1583 nojalla toimivaltaisten viranomaisten, direktiivin (EU) 2018/1972 mukaisesti nimettyjen kansallisten sääntelyviranomaisten, asetuksen (EU) N:o 910/2014 17 artiklan nojalla nimettyjen kansallisten viranomaisten,** [...] Euroopan parlamentin ja neuvoston asetuksen (EU) XXXX/XXXX [DORA-asetus] mukaisesti nimettyjen kansallisten finanssialan viranomaisten **sekä muiden alakohtaisten unionin säädösten nojalla nimettyjen toimivaltaisten viranomaisten** välillä kyseisessä jäsenvaltiossa.

5. Jäsenvaltioiden on varmistettava, että niiden **tämän direktiivin nojalla toimivaltaiset viranomaiset ja direktiivin (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] nojalla nimetyt** toimivaltaiset viranomaiset **vaihtavat** säännöllisesti [...] tietoja [...] **sellaisten kriittisten toimijoiden,** kyberturvallisuusriskien, **kyberuhkien ja kyberturvallisuuspoikkeamien sekä muiden kuin kyberturvallisuuteen liittyvien riskien, uhkien ja poikkeamien** tunnistamisesta, jotka vaikuttavat direktiivin (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] mukaisesti kriittisiksi tai **[**niitä vastaaviksi**]** yksilöityihin toimijoihin, sekä toimenpiteistä, joita [...] näiden riskien ja poikkeamien johdosta **on toteutettu**. **Jäsenvaltioiden on varmistettava myös, että tämän direktiivin nojalla toimivaltaiset viranomaiset ja asetuksen XXXX/XXXX [DORA-asetus], direktiivin 2018/1972 ja asetuksen (EU) 910/2014 nojalla nimetyt toimivaltaiset viranomaiset vaihtavat säännöllisesti asiaankuuluvia tietoja.**

Luottamuspalvelujen tarjoajien osalta ja[...] erityisesti [...] tapauksissa, joissa kyseinen tämän direktiivin mukainen valvontatehtävä annetaan jollekin muulle elimelle kuin asetuksen (EU) 910/2014 nojalla nimetylle valvontaelimelle, tämän direktiivin mukaisten kansallisten toimivaltaisten viranomaisten on tehtävä tiivistä ja oikea-aikaista yhteistyötä vaihtamalla asiaankuuluvia tietoja sen varmistamiseksi, että valvonta on tehokasta ja luottamuspalvelujen tarjoajat noudattavat tässä direktiivissä ja asetuksessa [XXXX/XXXX] säädettyjä vaatimuksia, **ja tämän direktiivin mukaisesti toimivaltaisen kansallisen viranomaisen on tarvittaessa ja ilman aiheetonta viivytystä ilmoitettava eIDAS-valvontaelimelle kaikista ilmoitetuista merkittävistä kyberuhista tai kyberturvallisuuspoikkeamista, jotka vaikuttavat luottamuspalveluihin**.

5 a. **[...] Poikkeamien raportoinnin yksinkertaistamiseksi jäsenvaltiot voivat tarvittaessa perustaa keskitetyn asiointipisteen kaikille tässä direktiivissä sekä asetuksessa (EU) 2016/679 ja direktiivissä 2002/58/EY edellytetyille ilmoituksille. Jäsenvaltiot voivat käyttää keskitettyä asiointipistettä muissa alakohtaisissa unionin säädöksissä vaadittuja ilmoituksia varten. Keskitetty asiointipiste ei saa vaikuttaa asetuksen (EU) 2016/679 ja direktiivin 2002/58/EY säännösten soveltamiseen, erityisesti riippumattomiin valvontaviranomaisiin liittyvien säännösten osalta.**

LUKU III

***EU:n** tason yhteistyö*

12 artikla

Yhteistyöryhmä

1. Perustetaan yhteistyöryhmä tukemaan ja helpottamaan jäsenvaltioiden välistä strategista yhteistyötä ja tietojenvaihtoa [...] **sekä vahvistamaan luottamusta**.

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

3. Yhteistyöryhmä koostuu jäsenvaltioiden, komission ja ENISAn edustajista. Euroopan ulkosuhdehallinto osallistuu yhteistyöryhmän toimintaan tarkkailijana. Euroopan valvontaviranomaiset **ja asetuksen (EU) XXXX/XXXX [DORA-asetus] nojalla nimetyt toimivaltaiset viranomaiset** voivat osallistua yhteistyöryhmän toimintaan [...] **asetuksen (EU) XXXX/XXXX [DORA-asetus] 42 artiklan 1 kohdan mukaisesti**.

   Yhteistyöryhmä voi tarvittaessa kutsua asiaankuuluvien sidosryhmien edustajia osallistumaan työskentelyynsä.

   Komissio huolehtii sihteeristötehtävistä.

4. Yhteistyöryhmän tehtävänä on

   a) ohjeistaa toimivaltaisia viranomaisia tämän direktiivin saattamisessa osaksi kansallista lainsäädäntöä ja sen täytäntöönpanossa;

   a a) antaa 5 artiklan 2 kohdan c alakohdassa ja 6 artiklan 1 alakohdassa tarkoitettua koordinoitua haavoittuvuuksien ilmaisemista koskevien politiikkojen laadintaan ja täytäntöönpanoon liittyviä ohjeita;

b) vaihtaa tietoa tämän direktiivin täytäntöönpanon parhaista käytännöistä ja käydä vuoropuhelua liittyen muun muassa kyberuhkiin, poikkeamiin, haavoittuvuuksiin, läheltä piti -tilanteisiin, tiedotushankkeisiin, koulutukseen, harjoituksiin ja osaamiseen, valmiuksien kehittämiseen sekä standardeihin ja teknisiin eritelmiin;

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

d) antaa neuvoja ja tehdä yhteistyötä komission kanssa liittyen ehdotuksiin tämän direktiivin nojalla annettaviksi komission täytäntöönpanosäädöksiksi [...];

e) vaihtaa tietoa parhaista käytännöistä ja käydä vuoropuhelua asiaankuuluvien unionin toimielinten, virastojen, elinten ja laitosten kanssa;

ea) vaihtaa näkemyksiä kyberturvallisuuteen liittyviä näkökohtia sisältävän alakohtaisen lainsäädännön täytäntöönpanosta;

f) keskustella 16 artiklan 7 kohdassa tarkoitetusta vertais[...]**oppimisesta**;

g) keskustella 34 artiklassa tarkoitetuista rajat ylittävistä yhteisvalvontatoimista saaduista **kokemuksista [...]**;

h) antaa CSIRT-verkostolle **ja EU-CyCLONelle** strategista ohjausta esiin nousevissa kysymyksissä;

ha) vaihtaa näkemyksiä laajamittaisten kyberturvallisuuspoikkeamien toimintapoliittisista jatkotoimista CSIRT-verkoston ja EU-CyCLONen kokemusten perusteella;

i) edesauttaa kyberturvallisuusvalmiuksien kehittymistä unionissa helpottamalla kansallisten virkamiesten vaihtoa kehitysohjelmalla, johon osallistuu jäsenvaltioiden toimivaltaisten viranomaisten tai CSIRT-yksiköiden henkilöstöä;

j) järjestää säännöllisesti eri puolilta unionia tulevien asiaankuuluvien yksityisten sidosryhmien kanssa yhteiskokouksia, joissa keskustellaan ryhmän toteuttamista toimista ja kerätään näkemyksiä esiin nousevista toimintapoliittisista haasteista;

k) keskustella kyberturvallisuusharjoituksiin liittyvästä työstä, mukaan lukien ENISAn tekemä työ;

ka) perustaa vertaisoppimismekanismi tämän direktiivin 16 artiklan mukaisesti.

5. Yhteistyöryhmä voi pyytää CSIRT-verkostolta teknisiä raportteja haluamistaan aiheista.

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

7. Komissio voi hyväksyä täytäntöönpanosäädöksiä, joissa vahvistetaan yhteistyöryhmän toimintaa varten tarvittavia menettelytapajärjestelyjä. Nämä täytäntöönpanosäädökset hyväksytään 37 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

8. Yhteistyöryhmä kokoontuu säännöllisesti ja vähintään kerran vuodessa direktiivillä (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] perustetun kriittisten toimijoiden häiriönsietokykyä käsittelevän ryhmän kanssa edistääkseen strategista yhteistyötä ja **helpottaakseen** tietojenvaihtoa.

13 artikla

CSIRT-verkosto

1. Jotta voidaan edistää luottamusta sekä ripeää ja tuloksellista operatiivista yhteistyötä jäsenvaltioiden välillä, perustetaan kansallisten CSIRT-yksiköiden verkosto.

2. CSIRT-verkosto koostuu jäsenvaltioiden **9 artiklan mukaisesti nimettyjen** CSIRT-yksiköiden ja tietotekniikan kriisiryhmän (CERT-EU) edustajista. Komissio osallistuu CSIRT-verkostoon tarkkailijana. ENISA huolehtii sihteeristötehtävistä ja tukee aktiivisesti CSIRT-yksiköiden välistä yhteistyötä.

3. CSIRT-verkoston tehtävänä on

   a) vaihtaa tietoa CSIRT-yksiköiden valmiuksista;

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

ba) vaihtaa tietoa kyberturvallisuutta koskevista julkaisuista ja suosituksista;

bb) jakaa teknisiä ratkaisuja, joilla helpotetaan poikkeamien teknistä käsittelyä;

bc) vaihtaa parhaita käytäntöjä, välineitä ja menettelyjä CSIRT-yksiköiden tehtävien osalta;

c) poikkeaman vaikutuspiiriin mahdollisesti kuuluvan CSIRT-verkoston **jäsenen** [...] pyynnöstä vaihtaa tietoa ja keskustella kyseisestä poikkeamasta ja siihen liittyvistä kyberuhista, riskeistä ja haavoittuvuuksista;

d) CSIRT-verkoston **jäsenen** [...] pyynnöstä keskustella kyseisen jäsenvaltion lainkäyttöalueella todettua poikkeamaa koskevasta koordinoidusta vasteesta ja mahdollisuuksien mukaan sen toteuttamisesta;

e) tukea jäsenvaltioita rajat ylittävien poikkeamien käsittelyssä tämän direktiivin mukaisesti;

f) tehdä yhteistyötä, **vaihtaa parhaita käytäntöjä** ja avustaa 6 artiklassa tarkoitettuja nimettyjä CSIRT-yksiköitä, kun ilmaistaan hallitusti ja [...] koordinoidusti haavoittuvuuksia, jotka vaikuttavat useisiin, eri jäsenvaltioihin sijoittautuneisiin tieto- ja viestintäteknisten tuotteiden, tieto- ja viestintäteknisten palvelujen ja tieto- ja viestintäteknisten prosessien valmistajiin tai tarjoajiin;

g) keskustella uusista operatiivisen yhteistyön muodoista liittyen esimerkiksi seuraaviin:

    i) kyberuhkien ja poikkeamien luokittelu;

    ii) ennakkovaroitukset;

    iii) keskinäinen avunanto;

iv) koordinoinnin periaatteet ja toimintatavat vastattaessa rajat ylittäviin riskeihin ja poikkeamiin;

v) osallistua **jäsenvaltion pyynnöstä** 7 artiklan 3 kohdassa tarkoitetun kansallisen kyberturvapoikkeama- ja -kriisinhallintasuunnitelman laadintaan;

h) tiedottaa yhteistyöryhmälle verkoston toiminnasta ja muista g alakohdan mukaisista käsitellyistä operatiivisen yhteistyön muodoista **ja** pyytää tarvittaessa ohjeistusta tältä osin;

i) koota yhteen oppeja kyberturvallisuusharjoituksista, myös ENISAn järjestämistä harjoituksista;

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

k) tehdä yhteistyötä ja vaihtaa tietoja alueellisten ja unionin tason turvaoperaatiokeskusten kanssa, jotta voidaan parantaa yhteistä tilannekuvaa poikkeamista ja uhista unionissa;

l) keskustella 16 artiklan 7 kohdassa tarkoitetuista vertais[...]**oppimis**raporteista;

m) antaa ohjeistusta operatiivisten käytäntöjen lähentämisen helpottamiseksi siltä osin kuin kyse on operatiivista yhteistyötä koskevien tämän artiklan säännösten soveltamisesta.

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 koskevan vertais**oppimisen** [...] tuloksista, mukaan lukien johtopäätökset ja suositukset, joihin on päädytty tämän artiklan nojalla. Kyseinen raportti toimitetaan myös yhteistyöryhmälle.

5. CSIRT-verkosto vahvistaa työjärjestyksensä.

6. CSIRT-verkosto tekee yhteistyötä EU-CyCLONen kanssa sovittujen menettelytapajärjestelyjen pohjalta.

14 artikla

Euroopan kyberkriisien yhteysorganisaatioiden verkosto (EU-CyCLONe)

1. Perustetaan Euroopan kyberkriisien yhteysorganisaatioiden verkosto (EU-CyCLONe) tukemaan laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien koordinoitua hallintaa operatiivisella tasolla ja varmistamaan säännöllinen tiedonvaihto jäsenvaltioiden ja unionin toimielinten, elinten ja virastojen välillä.

2. EU-CyCLONe koostuu 7 artiklan mukaisesti nimettyjen jäsenvaltioiden **kyber**kriisinhallintaviranomaisten [...] edustajista. **Komissio osallistuu verkoston toimintaan tarkkailijana.** ENISA huolehtii verkoston sihteeristön tehtävistä ja tukee tiedonvaihdon suojaamista **sekä antaa tarvittavat välineet jäsenvaltioiden yhteistyön tukemiseksi varmistaen suojatun tiedonvaihdon**.

   EU-CyCLONe voi tarvittaessa kutsua asiaankuuluvien sidosryhmien edustajia osallistumaan työskentelyynsä.

3. EU-CyCLONen tehtävänä on

   a) parantaa valmistautumista laajamittaisten kyberturvallisuus[...]poikkeamien ja -kriisien hallintaan;

   b) luoda yhteinen tilannekuva [...] laajamittaisista kyberturvallisuuspoikkeamista ja -kriiseistä;

   ba) arvioida asiaankuuluvien laajamittaisten kyberturvallisuuspoikkeamien seurauksia ja vaikutuksia ja ehdottaa mahdollisia toimenpiteitä niiden lieventämiseksi;

   c) koordinoida laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien **hallintaa** ja tukea tällaisiin poikkeamiin ja kriiseihin liittyvää poliittisen tason päätöksentekoa;

   d) keskustella **jäsenvaltion pyynnöstä tämän** 7 artiklan 3 [...] kohdassa tarkoitetuista kansallisista kyberturvapoikkeama- ja -kriisinhallintasuunnitelmista; [...]

4. EU-CyCLONe vahvistaa työjärjestyksensä.

5. EU-CyCLONe raportoi säännöllisesti yhteistyöryhmälle **laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallinnasta** [...] keskittyen erityisesti niiden vaikutuksiin keskeisiin ja tärkeisiin toimijoihin.

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

7. EU-CyCLONe toimittaa Euroopan parlamentille ja neuvostolle työnsä arviointia koskevan raportin viimeistään [24 kuukautta tämän direktiivin voimaantulosta].

14 a artikla

Kansainvälinen yhteistyö

Unioni voi tarvittaessa tehdä Euroopan unionin toiminnasta tehdyn sopimuksen 218 artiklan mukaisesti kolmansien maiden tai kansainvälisten järjestöjen kanssa kansainvälisiä sopimuksia, joissa sallitaan ja järjestetään niiden osallistuminen joihinkin yhteistyöryhmän, CSIRT-verkoston ja EU-CyCLONen toimiin unionin tietosuojalainsäädännön mukaisesti.

15 artikla

Raportti kyberturvallisuuden tilasta unionissa

1. ENISA laatii yhteistyössä komission **ja yhteistyöryhmän** kanssa joka toinen vuosi raportin kyberturvallisuuden tilasta unionissa. Raportissa on esitettävä **erityisesti** [...] seuraavaa:

aa) unionin tason kyberturvallisuusriskien arviointi ottaen huomioon uhkaympäristö;

a) [...] **arvio** kyberturvallisuusvalmiuksien kehittymisestä julkisella ja yksityisellä sektorilla unionissa;

b) [...]

c) kyberturvallisuutta [...] koskevien **määrällisten ja laadullisten indikaattoreiden perusteella kokonaisarvio**, jossa esitetään [...] **yleiskatsaus** kyberturvallisuusvalmiuksien kehitystasoon, **alakohtaiset valmiudet mukaan lukien**.

2. Raportin on sisällettävä toimintapoliittisia suosituksia kyberturvallisuuden tason nostamiseksi koko unionissa sekä yhteenveto kyseistä kautta koskevista havainnoista, jotka sisältyvät ENISAn asetuksen (EU) 2019/881 7 artiklan 6 kohdan mukaisesti antamiin unionin kyberturvallisuuden teknisiin tilanneraportteihin.

16 artikla

Vertaisoppiminen

1. **Jotta voidaan vahvistaa keskinäistä luottamusta, saavuttaa yhteinen korkea kyberturvallisuustaso ja vahvistaa tämän direktiivin tehokasta täytäntöönpanoa varten tarvittavia jäsenvaltioiden kyberturvallisuusvalmiuksia ja -politiikkoja, [...] yhteistyöryhmä** [...] vahvistaa **komission tuella** sekä ENISAa [...] **ja tarvittaessa CSIRT-verkostoa** kuultuaan ja viimeistään 24 [...] kuukauden kuluttua tämän direktiivin voimaantulosta menetelmät [...]**objektiiviselle, syrjimättömälle ja oikeudenmukaiselle** vertais**oppimis**järjestelmälle, [...] joka **koskee** tämän **direktiivin täytäntöönpanoa** [...] jäsenvaltioissa. **Vertaisoppimiseen osallistuminen on vapaaehtoista. Järjestelmä koostuu arviointikierroksista**, joita [...] suorittavat muista [...] jäsenvaltiosta tulevat kyberturvallisuus[...]asiantuntijat ja [...] joiden on katettava [....] **yksi tai useampi** seuraavista seikoista:

   i) jäljempänä 18 ja 20 artiklassa tarkoitettuja kyberturvallisuusriskien hallintaa koskevien vaatimusten ja raportointivelvoitteiden [...] täytäntöönpano;

   ii) **edellä 8 artiklassa tarkoitettujen** toimivaltaisten kansallisten viranomaisten **ja 9 artiklassa tarkoitettujen CSIRT-yksiköiden** [...] valmiudet, mukaan lukien käytettävissä olevat [...] resurssit, ja tehtävien hoitaminen [...];

[...]

iii[...]) jäljempänä 34 artiklassa tarkoitetun keskinäisen avunannon [...] **toteuttaminen;**

iv) [...] jäljempänä 26 artiklassa tarkoitetun tiedonvaihtojärjestelyn [...] **toteuttaminen**.

2. **Kriteerien, joiden perusteella jäsenvaltioiden on nimettävä vertaisoppimiskierrosten suorittamiseen kykenevät asiantuntijat, on oltava** [...] objektiivisia, syrjimättömiä, oikeudenmukaisia ja läpinäkyviä, **ja ne on sisällytettävä 1 kohdassa tarkoitettuihin menetelmiin.** ENISA ja komissio [...] **voivat** nimetä omat asiantuntijansa osallistumaan [...] **vertaisoppimiskierroksiin** tarkkailijoina. [...]

3. [...].

3 a. Jäsenvaltiot voivat ennen vertaisoppimiskierrosten alkamista suorittaa itsearvioinnin kyseisen vertaisoppimiskierroksen kattamista sekoista ja toimittaa kyseisen arvioinnin 2 kohdassa tarkoitetuille nimetyille asiantuntijoille.

4. Vertais**oppimiseen voi** sisältyä [...] **fyysisiä** tai virtuaalisia kohdeselvityksiä sekä yleistä tiedonvaihtoa. **Vertaisoppimiseen osallistuvien** [...] jäsenvaltioiden on hyvän yhteistyön hengessä annettava nimetyille asiantuntijoille [...] arviointiin tarvittavat tiedot [...], **sanotun kuitenkaan rajoittamatta luottamuksellisten tai turvallisuusluokiteltujen tietojen suojaamista koskevan kansallisen tai unionin lainsäädännön soveltamista tai keskeisten valtiolle kuuluvien tehtävien, kuten kansallisen turvallisuuden, suojaamista.** Vertais[...]**oppimis**prosessissa saatuja tietoja saa käyttää ainoastaan tähän tarkoitukseen. Vertais[...]**oppimiseen** osallistuvat asiantuntijat eivät saa paljastaa [...] **sen yhteydessä** saatuja arkaluonteisia tai luottamuksellisia tietoja ulkopuolisille. **Vertaisoppimiseen osallistuva jäsenvaltio voi vastustaa tiettyjen asiantuntijoiden nimeämistä yhteistyöryhmälle toimittaminsa asianmukaisin perustein.**

5. Jollakin **vertaisoppimiskierroksella [...]** jo arvioituja näkökohtia ei arvioida [...] vertais**oppimiskierroksiin** [...] **osallistuvien** jäsenvaltioiden **osalta** uudelleen [...] **neljään** vuoteen **kyseisen** [...] vertais[...]**oppimiskierroksen** päättymisestä, **ellei asianomainen jäsenvaltio sitä pyydä tai suostu siihen [...] yhteistyöryhmän ehdotuksesta [...].**

6. [...]

7. Vertais[...]**oppimiskierroksiin** osallistuvien asiantuntijoiden on laadittava raporttiluonnokset [...] **arviointien** tuloksista ja päätelmistä. **Jäsenvaltioiden on mahdollista esittää omista raporttiluonnoksistaan huomautuksia, jotka liitetään raporttiin.** Lopulliset raportit toimitetaan [...] yhteistyöryhmälle. **Jäsenvaltiot voivat päättää asettaa omat raporttinsa julkisesti saataville.**

IV LUKU

Kyberturvallisuusriskien hallinta- ja raportointivelvoitteet

I JAKSO

Kyberturvallisuusriskien hallinta ja raportointi

17 artikla

Hallinnointi

1. Jäsenvaltioiden on varmistettava, että keskeisten ja tärkeiden toimijoiden hallintoelimet hyväksyvät näiden toimijoiden 18 artiklan noudattamiseksi toteuttamat kyberturvallisuusriskien hallintatoimenpiteet, [...] **valvovat** sen täytäntöönpanoa ja **että ne voidaan asettaa** vastuuseen, jos toimijat eivät noudata tämän artiklan mukaisia velvoitteita.

   Tämän kohdan soveltaminen ei rajoita julkisten laitosten vastuuvelvollisuutta koskevista säännöistä tai viranhaltijoiden taikka vaalilla valittujen ja nimettyjen virkamiesten vastuuvelvollisuudesta annettujen jäsenvaltioiden kansallisen lakien soveltamista.

2. Jäsenvaltioiden on varmistettava, että nämä **hallintoelinten jäsenet [...] velvoitetaan** osallistumaan säännöllisesti [...] koulutukseen riittävien tietojen ja taitojen hankkimiseksi, jotta he voivat ymmärtää ja arvioida kyberturvallisuusriskejä ja -hallintakäytäntöjä sekä niiden vaikutusta toimijaan.

18 artikla

Kyberturvallisuusriskien hallintatoimenpiteet

1 **a. Tässä direktiivissä sovelletaan kaikki vaaratekijät huomioon ottavaa toimintatapaa, johon kuuluu verkko- ja tietojärjestelmien ja niiden fyysisen ympäristön suojaaminen tapahtumilta, jotka saattaisivat vaarantaa verkko- ja tietojärjestelmissä tarjottujen tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen saatavuuden, aitouden, eheyden tai luottamuksellisuuden.**

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 uusin tekniikka **ja toteutuksen kustannukset** huomioon ottaen. **Kyseisten toimenpiteiden oikeasuhteisuutta arvioitaessa on otettava asianmukaisesti huomioon se, missä määrin toimija altistuu riskeille, toimijan koko sekä poikkeamien todennäköisyys ja vakavuus. Kun otetaan huomioon, minkä tasoinen ja tyyppinen riski yhteiskunnalle aiheutuu keskeisiin ja tärkeisiin toimijoihin vaikuttavista poikkeamista, tärkeille toimijoille voidaan määrätä kevyempiä kyberturvallisuusriskien hallintatoimenpiteitä kuin keskeisille toimijoille.**

2. Edellä 1 kohdassa tarkoitettuihin toimenpiteisiin on sisällyttävä ainakin seuraavat:

a) riskianalyysejä ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet;

b) poikkeamien käsittely (poikkeamien ehkäisy, havaitseminen, niihin reagointi [...] **ja niistä palautuminen**);

c) toiminnan jatkuvuuden ja kriisitilanteiden hallinta;

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

e) verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja ilmaiseminen;

f) toimintatavat ja menettelyt [...], joilla arvioidaan kyberturvallisuuteen liittyvien riskinhallintatoimenpiteiden toimivuutta;

g) salaustekniikoiden käyttöä **koskeva toimintapolitiikka**;

ga) henkilöresurssien turvallisuus, pääsynvalvontapolitiikka ja omaisuudenhoito.

3. Jäsenvaltioiden on varmistettava, että harkitessaan 2 kohdan d alakohdassa tarkoitettuja asianmukaisia toimenpiteitä toimijat[...] **velvoitetaan** ottamaan huomioon kullekin **suoralle** alihankkijalle ja palveluntarjoajalle ominaiset haavoittuvuudet, tuotteiden yleinen laatu sekä alihankkijoidensa ja palveluntarjoajiensa kyberturvallisuuskäytännöt, mukaan lukien niiden tuotekehityksen suojausmenettelyt. **Jäsenvaltioiden on myös varmistettava, että harkitessaan 2 kohdan d alakohdassa tarkoitettuja asianmukaisia toimenpiteitä toimijat velvoitetaan ottamaan huomioon 19 artiklan 1 kohdan mukaisesti suoritettujen koordinoitujen riskinarviointien tulokset.**

4. Jäsenvaltioiden on varmistettava, että jos toimija toteaa, että sen palvelut tai tehtävät eivät ole 2 kohdassa säädettyjen vaatimusten mukaisia, sen on ilman aiheetonta viivytystä toteutettava kaikki tarvittavat korjaavat toimenpiteet kyseisen palvelun saattamiseksi vaatimusten mukaiseksi.

5. Komissio voi hyväksyä täytäntöönpanosäädöksiä, joissa vahvistetaan **tämän artiklan** 2 kohdassa tarkoitettujen osatekijöiden tekniset ja metodologiset eritelmät **sekä tarvittaessa alakohtaiset erityispiirteet. Komissio hyväksyy viimeistään [18 kuukauden kuluttua tämän direktiivin voimaantulosta] täytäntöönpanosäädöksiä, joissa vahvistetaan 24 artiklan 1 kohdassa tarkoitettuja toimijoita ja liitteessä I olevassa 8 kohdassa tarkoitettuja luottamuspalvelun tarjoajia koskevat tekniset ja metodologiset eritelmät**. **Nämä täytäntöönpanosäädökset hyväksytään 37 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.** Valmistellessaan [...] **tällaisia täytäntöönpano**säädöksiä komissio **noudattaa** [...] mahdollisimman pitkälle kansainvälisiä ja eurooppalaisia standardeja sekä asiaankuuluvia teknisiä eritelmiä **ja vaihtaa 12 artiklan 4 kohdan d alakohdan mukaisesti tietoja yhteistyöryhmän ja ENISAn kanssa ehdotuksesta täytäntöönpanosäädökseksi.**

6. [...]

19 artikla

Kriittisiä toimitusketjuja koskevat EU:n koordinoidut riskinarvioinnit

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.

2. Komissio määrittää yhteistyöryhmää ja ENISAa kuultuaan kriittiset tieto- ja viestintätekniset palvelut, järjestelmät tai tuotteet, joille voidaan tehdä 1 kohdassa tarkoitettu koordinoitu riskinarviointi.

20 artikla

Raportointivelvoitteet

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 **tällaisista** 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. **Ilmoittaminen ei itsessään lisää ilmoituksen tekevän toimijan vastuuta.**

2. [...]

[..] **Keskeisten ja tärkeiden** toimijoiden on tarvittaessa ilmoitettava ilman aiheetonta 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 **itsessään** lisää ilmoituksen tekevän toimijan vastuuta.

3. Poikkeama katsotaan merkittäväksi, jos

a) poikkeama on aiheuttanut tai voi aiheuttaa kyseiselle toimijalle **vakavan** [...] toimintahäiriön **palvelussa** tai merkittäviä taloudellisia tappioita;

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

4. Jäsenvaltioiden on varmistettava, että 1 kohdan mukaista ilmoitusta varten asianomaiset toimijat toimittavat toimivaltaisille viranomaisille tai CSIRT-yksikölle

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

b) toimivaltaisen viranomaisen tai CSIRT-yksikön pyynnöstä väliraportin asiaan liittyvistä tilapäivityksistä;

c) viimeistään kuukauden kuluttua a alakohdan mukaisesta [...] **alustavasta ilmoituksesta loppu**raportin, joka sisältää vähintään seuraavat tiedot:

i) yksityiskohtainen kuvaus poikkeamasta, sen vakavuudesta ja vaikutuksista;

ii) poikkeaman todennäköisesti aiheuttaneen uhan tai juurisyyn tyyppi;

iii) toteutetut ja meneillään olevat toimenpiteet vaikutusten lieventämiseksi.

Jäsenvaltioiden on säädettävä, että asianomainen toimija voi asianmukaisesti perustelluissa tapauksissa ja toimivaltaisten viranomaisten tai CSIRT-yksikön suostumuksella poiketa a ja c alakohdassa säädetyistä määräajoista. **Erityisesti poikkeaminen c alakohdassa tarkoitetusta määräajasta voi olla perusteltua tapauksissa, joissa poikkeama on vielä käynnissä.**

5. Toimivaltaisten kansallisten viranomaisten tai CSIRT-yksikön on annettava [...] **ilman aiheetonta viivytystä** 4 kohdan a alakohdassa tarkoitetun alustavan ilmoituksen vastaanottamisesta ilmoituksen tehneelle toimijalle vastaus, mukaan lukien alustava palaute poikkeamasta ja kyseisen toimijan pyynnöstä ohjeet mahdollisista toimenpiteistä vaikutusten lieventämiseksi. Jos CSIRT-yksikkö ei ole saanut 1 kohdassa tarkoitettua ilmoitusta, toimivaltaisen viranomaisen on annettava ohjeet yhteistyössä CSIRT-yksikön kanssa. CSIRT-yksikkö antaa teknistä lisätukea, jos asianomainen toimija sitä pyytää. Jos poikkeaman epäillään olevan luonteeltaan rikollinen, toimivaltaisten kansallisten viranomaisten tai CSIRT-yksikön on annettava ohjeita myös poikkeaman ilmoittamisesta lainvalvontaviranomaisille.

6. Toimivaltaisen viranomaisen, CSIRT-yksikön tai **keskitetyn yhteyspisteen** on tarvittaessa ja erityisesti silloin, kun 1 kohdassa tarkoitettu poikkeama koskee kahta tai useampaa jäsenvaltiota, tiedotettava asiasta muille asiaan liittyville jäsenvaltioille ja ENISAlle. **Tällöin on annettava vähintään tämän artiklan 4 kohdassa säädetyt tiedot.** Näin tehdessään toimivaltaisten viranomaisten, CSIRT-yksiköiden ja keskitettyjen yhteyspisteiden on unionin oikeuden tai unionin oikeuden mukaisen kansallisen lainsäädännön mukaisesti säilytettävä toimijan turvallisuusedut ja kaupalliset edut sekä annettujen tietojen luottamuksellisuus.

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.

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

9. Keskitetyn yhteyspisteen on toimitettava ENISAlle [...] **kuuden kuukauden välein** tiivistelmä, joka sisältää anonymisoidut koontitiedot poikkeamista, merkittävistä kyberuhista ja läheltä piti -tilanteista, joista on ilmoitettu 1 [...] kohdan ja 27 artiklan mukaisesti. Parantaakseen tietojen vertailukelpoisuutta ENISA voi antaa teknisiä ohjeita tiivistelmään sisältyvien tietojen rakenteesta. **ENISA tiedottaa kuuden kuukauden välein yhteistyöryhmälle ja CSIRT-verkostolle saatuja ilmoituksia koskevista havainnoistaan**.

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.

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.

21 artikla

Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien käyttö

1. Tiettyjen 18 artiklan vaatimusten noudattamisen osoittamiseksi **jäsenvaltiot voivat edellyttää, että toimijat käyttävät tiettyjä tieto- ja viestintätekniikan tuotteita, palveluja ja prosesseja, jotka on sertifioitu** asetuksen (EU) 2019/881 49 artiklan nojalla hyväksyttyjen erityisten eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukaisesti. Sertifioitavat **tieto- ja viestintätekniikan** tuotteet, palvelut ja prosessit voivat olla keskeisen tai tärkeän toimijan itse kehittämiä tai ulkopuoliselta taholta hankittuja.

2. Komissio voi [...] hyväksyä [...] **täytäntöönpano**säädöksiä, joissa vahvistetaan, mitkä keskeisten **tai tärkeiden** toimijoiden luokat velvoitetaan **käyttämään tiettyjä sertifioituja tieto- ja viestintätekniikan tuotteita, palveluja ja prosesseja tai** hankkimaan todistus [...] jonkin [...]**asetuksen (EU) 2019/881 49 artiklan nojalla hyväksytyn** eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti. **Nämä täytäntöönpanosäädökset hyväksytään 37 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen. Valmistellessaan tällaisia täytäntöönpanosäädöksiä komissio asetuksen (EU) 2019/881 56 artiklan mukaisesti**

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

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

(i) **ottaa huomioon täytäntöönpanon määräajat, siirtymätoimenpiteet ja -kaudet, erityisesti siltä osin kuin ne mahdollisesti vaikuttavat tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien valmistajiin tai tarjoajiin taikka niiden käyttäjiin, erityisesti pk-yrityksiin;**

(ii) **ottaa huomioon jäsenvaltioiden asiaankuuluvan lainsäädännön olemassaolon ja täytäntöönpanon.**

3. Komissio voi asetuksen (EU) 2019/881 48 artiklan 2 kohdan mukaisesti pyytää ENISAa valmistelemaan ehdolla olevan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän **tai tarkistamaan voimassa olevaa eurooppalaista kyberturvallisuuden sertifiointijärjestelmää** tapauksissa, joissa asianmukaista eurooppalaista kyberturvallisuuden sertifiointijärjestelmää **tämän artiklan** 2 kohdan soveltamiseksi ei ole käytettävissä.

22 artikla

Standardointi

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

2. ENISA antaa yhteistyössä jäsenvaltioiden kanssa neuvoja ja suuntaviivoja teknisistä aloista, joita on tarkasteltava 1 kohdan soveltamiseksi, sekä jo olemassa olevista standardeista, mukaan lukien jäsenvaltioiden kansalliset standardit, millä varmistetaan se, että nämä alat kuuluvat tarkastelun piiriin.

23 artikla

Verkkotunnusten ja rekisteröintitietojen tietokannat

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 [...] henkilötietoja koskevan unionin tietosuojalainsäädännön **mukaisesti.**

2. Jäsenvaltioiden on varmistettava, että 1 kohdassa tarkoitetut verkkotunnusten rekisteröintitietojen tietokannat sisältävät asiaankuuluvat tiedot verkkotunnusten haltijoiden ja TLD-aluetunnusten alaisia verkkotunnuksia hallinnoivien yhteyspisteiden tunnistamiseksi ja niihin yhteyden saamiseksi **ja että niissä on vähintään seuraavat tiedot:**

   a) verkkotunnus;

   b) rekisteröintipäivä;

   c) rekisteröijän tiedot, mukaan lukien:

      i) luonnollisten henkilöiden osalta nimi, sukunimi ja sähköpostiosoite;

      ii) oikeushenkilöiden osalta nimi ja sähköpostiosoite.

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.

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

5. Jäsenvaltioiden on varmistettava, että TLD-rekisterit ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavat toimijat antavat pääsyn 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 **ja joka tapauksessa 72 tunnin kuluessa** kaikkiin pyyntöihin, jotka koskevat tietoihin pääsyä. Jäsenvaltioiden on varmistettava, että tiedot tällaisten tietojen antamista koskevista toimintaperiaatteista ja menettelyistä asetetaan julkisesti saataville.

II jakso

Lainkäyttövalta ja rekisteröinti

24 artikla

Lainkäyttövalta ja alueperiaate

1 a. Tämän direktiivin soveltamisalaan kuuluvien toimijoiden katsotaan kuuluvan sen jäsenvaltion lainkäyttövaltaan, jossa ne tarjoavat palvelujaan. Liitteessä I olevissa 1–7 ja 10 kohdassa tarkoitettujen toimijoiden, liitteessä I olevassa 8 kohdassa tarkoitettujen luottamuspalvelun tarjoajien ja Internetin yhdysliikennepisteiden ylläpitäjien sekä liitteessä II olevassa 1–5 kohdassa tarkoitettujen toimijoiden katsotaan kuuluvan sen jäsenvaltion lainkäyttövaltaan, jonka alueelle ne ovat sijoittautuneet.

1. Liitteessä I olevassa 8 kohdassa tarkoitettujen DNS-palveluntarjoajien, TLD-rekisterien [...] **ja niiden alaisten verkkotunnusten rekisteröintipalveluja tarjoavat toimijat,** pilvipalvelujen tarjoajien, datakeskuspalvelujen tarjoajien, [...] sisällönjakeluverkkojen tarjoajien sekä liitteessä I olevassa 8 a kohdassa tarkoitettujen **hallintapalvelujen tarjoajien ja tietoturvapalveluntarjoajien** sekä liitteessä II olevassa 6 kohdassa tarkoitettujen digitaalisen palvelun tarjoajien katsotaan kuuluvan sen jäsenvaltion lainkäyttövaltaan, jossa niiden päätoimipaikka on unionissa.

2. Tätä direktiiviä sovellettaessa 1 kohdassa tarkoitettujen toimijoiden päätoimipaikan katsotaan olevan unionissa siinä jäsenvaltiossa, jossa kyberturvallisuusriskien hallintatoimenpiteisiin liittyvät päätökset **pääsääntöisesti** tehdään. Jos **ei voida määrittää paikkaa, jossa tällaiset päätökset pääsääntöisesti tehdään**, tai jos tällaisia päätöksiä ei tehdä missään unionissa sijaitsevassa toimipaikassa, päätoimipaikan katsotaan olevan siinä jäsenvaltiossa, jossa toimijalla on eniten työntekijöitä unionissa. **Jos palvelut tarjoaa yritysryhmä, päätoimipaikaksi olisi katsottava yritysryhmän päätoimipaikka.**

3. Jos 1 kohdassa tarkoitettu toimija ei ole sijoittautunut unioniin mutta tarjoaa palveluja unionissa, sen on nimettävä edustaja unioniin. Edustajan on oltava sijoittautunut johonkin niistä jäsenvaltioista, joissa palveluja tarjotaan. Tällaisen toimijan katsotaan kuuluvan sen jäsenvaltion lainkäyttövallan piiriin, johon edustaja on sijoittautunut. Jos toimijalla ei ole unionissa tämän artiklan mukaista nimettyä edustajaa, mikä tahansa jäsenvaltio, jossa toimija tarjoaa palveluja, voi ryhtyä oikeustoimiin toimijaa vastaan tämän direktiivin mukaisten velvoitteiden noudattamatta jättämisen vuoksi.

4. Se, että 1 kohdassa tarkoitettu toimija on nimennyt edustajan, ei rajoita oikeustoimia, joita voidaan panna vireille toimijaa itseään vastaan.

4 a. Jäsenvaltiot, jotka ovat saaneet 1 kohdassa tarkoitettuihin toimijoihin liittyvän keskinäistä avunantoa koskevan pyynnön, voivat pyynnön asettamissa rajoissa toteuttaa asianmukaisia valvonta- ja täytäntöönpanotoimenpiteitä sellaisen toimijan osalta, joka tarjoaa niiden alueella palveluja tai jolla on siellä verkko- ja tietojärjestelmä.

25 artikla

Tiettyjen digitaalisia infrastruktuureja tarjoavien toimijoiden ja digitaalisen palvelun tarjoajien rekisteri

1. [...] **Jäsenvaltioiden on varmistettava, että [...] 24 artiklan 1 kohdassa tarkoitetut toimijat, joiden päätoimipaikka on niiden alueella tai, jos ne eivät ole sijoittautuneet unioniin, joiden unioniin nimetty edustaja on sijoittautunut niiden alueelle, velvoitetaan** toimittamaan seuraavat tiedot **toimivaltaisille viranomaisille** [...] [viimeistään 12 kuukauden kuluttua direktiivin voimaantulosta];

a) toimijan nimi;

aa) toimijan tyyppi tämän direktiivin liitteiden I ja II mukaisesti;

b) päätoimipaikan ja muiden unionissa sijaitsevien laillisten toimipaikkojen osoite tai, jos toimija ei ole sijoittautunut unioniin, sen 24 artiklan 3 kohdan mukaisen nimetyn edustajan osoite;

c) ajantasaiset yhteystiedot, mukaan lukien toimijoiden **ja niiden edustajien** sähköpostiosoitteet ja puhelinnumerot;

d) jäsenvaltiot, joissa toimija tarjoaa palvelua.

Nämä tiedot on tarvittaessa toimitettava 2 a artiklassa tarkoitetun kansallisen [...] ilmoitusmekanismin kautta.

2. **Jäsenvaltioiden on varmistettava, että** [...] 1 kohdassa tarkoitetut toimijat [...] **myös ilmoittavat** ENISAlle kaikista muutoksista 1 kohdan mukaisesti toimittamiinsa tietoihin viipymättä ja joka tapauksessa kolmen kuukauden kuluessa päivästä, jona muutos tuli voimaan.

3. [...] **Jäsenvaltioiden yhteyspisteiden** on toimitettava **1 ja 2 kohdassa tarkoitetut tiedot [...] ENISAlle**. [...]

3 a. ENISA luo tämän artiklan 3 kohdan mukaisesti saamiensa tietojen perusteella rekisterin 1 kohdassa tarkoitetuista toimijoista ja pitää sitä yllä. Jäsenvaltioiden pyynnöstä ENISA antaa asiaankuuluville toimivaltaisille viranomaisille pääsyn rekisteriin ja varmistaa tarvittavat takeet tietojen luottamuksellisuuden suojaamiseksi tarpeen mukaan.

4. [...]

V LUKU

Tietojenvaihto

26 artikla

Kyberturvallisuustietojen jakamista koskevat järjestelyt

1. [...] Jäsenvaltioiden on varmistettava, että keskeiset ja tärkeät toimijat voivat **vapaaehtoisesti** vaihtaa keskenään asiaankuuluvia kyberturvallisuustietoja, mukaan lukien tietoja kyberuhkista, **läheltä piti -tilanteista**, haavoittuvuuksista, vaarantumista kuvaavista IoC-indikaattoreista, taktiikasta, tekniikoista ja menettelyistä, kyberturvallisuushälytyksistä ja konfigurointivälineistä, jos tällainen tiedonvaihto

   a) tähtää poikkeamien ehkäisyyn tai havaitsemiseen, niihin vastaamiseen tai niiden vaikutusten lieventämiseen;

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.

2. Jäsenvaltioiden on varmistettava, että tietojenvaihto tapahtuu keskeisten ja tärkeiden toimijoiden [...] yhteisöissä. Tällainen tietojenvaihto on toteutettava tietojenvaihtojärjestelyillä, joissa otetaan huomioon jaettujen tietojen mahdollinen arkaluonteisuus [...].

3. Jäsenvaltiot [...] **voivat** vahvistaa sääntöjä, joissa täsmennetään 2 kohdassa tarkoitettujen tietojenvaihtojärjestelyjen menettelytavat, operatiiviset osat (mukaan lukien tiettyjen tieto- ja viestintäteknisten alustojen käyttö), sisältö ja edellytykset. Säännöissä [...] **voidaan** myös vahvistaa yksityiskohtaiset tiedot viranomaisten osallistumisesta tällaisiin järjestelyihin sekä operatiiviset osat, mukaan lukien erityisten tietoteknisten alustojen käyttö. Jäsenvaltioiden on tarjottava tukea tällaisten järjestelyjen käyttöön 5 artiklan 2 kohdan g alakohdassa tarkoitettujen toimintaperiaatteidensa mukaisesti.

4. Keskeisten ja tärkeiden toimijoiden on ilmoitettava toimivaltaisille viranomaisille osallistumisestaan 2 kohdassa tarkoitettuihin tietojenvaihtojärjestelyihin, kun ne liittyvät tällaisiin järjestelyihin, tai tapauksen mukaan vetäytymisestään tällaisista järjestelyistä, kun vetäytyminen tulee voimaan.

5. ENISA tukee [...] kyberturvallisuustietojen jakamista koskevien 2 kohdassa tarkoitettujen järjestelyjen toteuttamista tarjoamalla tietoa parhaista käytännöistä sekä ohjeistusta.

27 artikla

Asiaankuuluvien tietojen vapaaehtoinen ilmoittaminen

1. Jäsenvaltioiden on varmistettava, että keskeiset ja tärkeät toimijat voivat vapaaehtoisesti ilmoittaa toimivaltaisille viranomaisille tai CSIRT-yksiköille asiaankuuluvista poikkeamista, kyberuhista tai läheltä piti -tilanteista, sanotun kuitenkaan rajoittamatta 20 artiklan soveltamista.

2. Jäsenvaltioiden on varmistettava, että tämän direktiivin soveltamisalan ulkopuolelle jäävät toimijat voivat vapaaehtoisesti ilmoittaa merkittävistä poikkeamista, kyberuhista tai läheltä piti -tilanteista, sanotun kuitenkaan 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, [...] **sanotun kuitenkaan rajoittamatta rikosten tutkintaa, selvittämistä ja syytteeseenpanoa**.

3. Vapaaehtoiset ilmoitukset käsitellään ainoastaan, jos tällainen käsittely ei muodosta kohtuutonta tai aiheetonta rasitusta kyseessä olevalle jäsenvaltiolle.

VI LUKU

Valvonta ja täytäntöönpano

28 artikla

Valvontaa ja täytäntöönpanoa koskevat yleiset näkökohdat

1. Jäsenvaltioiden on varmistettava, että toimivaltaiset viranomaiset valvovat tosiasiallisesti tämän direktiivin ja erityisesti sen 18, [...] 20 **ja 23** artiklassa säädettyjen velvoitteiden noudattamista ja toteuttavat tarvittavat toimenpiteet sen varmistamiseksi. **Jäsenvaltiot voivat sallia sen, että toimivaltaiset viranomaiset priorisoivat riskiperusteiseen toimintatapaan perustuvan valvonnan.**

2. Toimivaltaisten viranomaisten on toimittava tiiviissä yhteistyössä tietosuojaviranomaisten, **direktiivin (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] mukaisesti nimettyjen toimivaltaisten viranomaisten, asetuksen (EU) 910/2014 mukaisesti nimettyjen valvontaelinten sekä muiden alakohtaisten unionin säädösten nojalla nimettyjen toimivaltaisten viranomaisten** kanssa käsitellessään henkilötietojen tietoturvaloukkauksiin johtaneita poikkeamia. [...]

3. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla, jotka valvovat julkishallinnon toimijoita tämän direktiivin noudattamisessa ja panevat täytäntöön noudattamatta jättämisen johdosta mahdollisesti määrättäviä seuraamuksia, on asianmukaiset valtuudet tällaisten tehtävien suorittamiseksi ja että ne ovat toiminnallisesti riippumattomia valvottavista toimijoista, sanotun kuitenkaan rajoittamatta kansallisia institutionaalisia ja lainsäädäntökehyksiä. Jäsenvaltiot voivat kansallisten kehysten ja oikeusjärjestyksen mukaisesti päättää määrätä asianmukaisia, oikeasuhteisia ja tehokkaita valvonta- ja täytäntöönpanotoimenpiteitä kyseisten toimijoiden osalta.

29 artikla

Valvonta ja täytäntöönpano keskeisten toimijoiden osalta

1. Jäsenvaltioiden on varmistettava, että tässä direktiivissä säädettyjen velvoitteiden noudattamisen valvontaa tai täytäntöönpanoa koskevat toimenpiteet, jotka koskevat keskeisiä toimijoita, ovat vaikuttavia, oikeasuhteisia ja varoittavia ottaen huomioon kunkin yksittäisen tapauksen olosuhteet.

2. Jäsenvaltioiden on varmistettava, että hoitaessaan keskeisiä toimijoita koskevia valvontatehtäviään **toimivaltaiset viranomaiset noudattavat riskiperusteista toimintatapaa ja että niillä on kyseisten toimijoiden osalta** valtuudet **ainakin** seuraaviin:

   a) paikan päällä tehtävät tarkastukset ja toimipaikkojen ulkopuolinen valvonta, mukaan lukien satunnaistarkastukset;

   b) säännölliset **turvallisuus**auditoinnit;

   c) riskinarviointeihin tai käytettävissä oleviin riskitietoihin perustuvat kohdennetut turvallisuusauditoinnit;

   d) objektiivisiin, syrjimättömiin, oikeudenmukaisiin ja läpinäkyviin riskinarviointikriteereihin perustuvat turvallisuuskartoitukset, **jotka teknisistä syistä tehdään tarvittaessa yhteistyössä asianomaisen toimijan kanssa**;

   e) tietopyynnöt, jotka ovat tarpeen toimijan hyväksymien kyberturvallisuustoimenpiteiden arvioimiseksi, mukaan lukien dokumentoidut kyberturvaperiaatteet [...];

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

   g) pyynnöt saada näyttöä kyberturvallisuusperiaatteiden täytäntöönpanosta, kuten pätevän tarkastajan tekemien turvallisuusauditointien tulokset ja niiden perustana oleva näyttö.

2 a. Toimivaltaiset viranomaiset voivat tämän artiklan 2 kohdassa säädettyjä valvontatehtäviä suorittaessaan vahvistaa valvontamenetelmiä, joissa tällaiset tehtävät priorisoidaan riskiperusteista toimintatapaa noudattaen.

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

4. Jäsenvaltioiden on varmistettava, että käyttäessään täytäntöönpanovaltuuksiaan keskeisten toimijoiden osalta toimivaltaisilla viranomaisilla on **ainakin** valtuudet

   a) varoittaa toimijoita siitä, että ne eivät ole noudattaneet tässä direktiivissä säädettyjä velvoitteita;

   b) antaa sitovia määräyksiä, joissa kyseisiä toimijoita vaaditaan korjaamaan havaitut puutteet tai saattamaan toimintansa tässä direktiivissä säädettyjen velvoitteiden mukaiseksi;

   c) määrätä kyseiset toimijat lopettamaan toiminta, joka ei ole tässä direktiivissä säädettyjen velvoitteiden mukaista, ja pidättäytymään toistamasta tätä toimintaa;

   d) määrätä kyseiset toimijat saattamaan riskinhallintatoimenpiteensä ja/tai raportointivelvoitteensa 18 ja 20 artiklassa säädettyjen velvoitteiden mukaisiksi määrätyllä tavalla ja määrätyn ajan kuluessa;

   e) määrätä kyseiset toimijat ilmoittamaan niiden palveluja tai toimintoja hyödyntäville luonnollisille tai oikeushenkilöille, joihin merkittävä kyberuhka saattaa vaikuttaa, **uhan luonteesta ja** mahdollisista suoja- tai korjaavista toimenpiteistä, joita kyseiset luonnolliset tai oikeushenkilöt voivat toteuttaa uhan johdosta;

   f) määrätä kyseiset toimijat panemaan täytäntöön turvallisuusauditoinnin tuloksena annetut suositukset kohtuullisessa määräajassa;

   g) [...]

h) määrätä kyseiset toimijat julkistamaan tietyllä tavalla seikkoja, jotka liittyvät tässä direktiivissä säädettyjen velvoitteiden noudattamatta jättämiseen, **jos tällainen julkistaminen ei altista asianomaista toimijaa haitallisille vaikutuksille**;

i) [...]

j) määrätä tai pyytää asiaankuuluvia elimiä tai tuomioistuimia määräämään kansallisen lainsäädännön mukaisesti hallinnollisia sakkoja 31 artiklan nojalla tämän kohdan a–i alakohdassa tarkoitettujen toimenpiteiden lisäksi tai niiden sijasta kunkin yksittäisen tapauksen olosuhteista riippuen.

5. Jos 4 kohdan a–d ja f alakohdan mukaiset täytäntöönpanotoimet eivät tuota tulosta, jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on valtuudet asettaa määräaika, jonka kuluessa keskeistä toimijaa kehotetaan toteuttamaan tarvittavat toimet puutteiden korjaamiseksi tai kyseisten viranomaisten vaatimusten noudattamiseksi. Jos pyydettyjä toimia ei toteuteta asetetussa määräajassa, jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on valtuudet

a) keskeyttää tai pyytää sertifiointi- tai lupaelintä **taikka tuomioistuimia kansallisten lakien mukaisesti** keskeyttämään kokonaan tai osittain keskeisen toimijan tarjoamia palveluja tai toimintoja koskevan sertifioinnin tai luvan;

b) määrätä 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.

Näitä seuraamuksia on sovellettava ainoastaan siihen asti, kunnes toimija toteuttaa tarvittavat toimet seuraamusten syynä olleiden puutteiden korjaamiseksi tai toimivaltaisen viranomaisen vaatimusten noudattamiseksi.

Tässä kohdassa säädettyjä seuraamuksia ei sovelleta julkishallinnon toimijoihin, joihin sovelletaan tätä direktiiviä.

6. Jäsenvaltioiden on varmistettava, että jokaisella luonnollisella henkilöllä, joka on vastuussa keskeisestä toimijasta tai toimii sen edustajana sillä perusteella, että hänellä on valtuudet edustaa sitä, valtuudet tehdä päätöksiä sen puolesta tai valtuudet valvoa sitä, on valta varmistaa, että toimija noudattaa tässä direktiivissä säädettyjä velvoitteita. Jäsenvaltioiden on varmistettava, että nämä luonnolliset henkilöt voidaan saattaa vastuuseen, jos he ovat laiminlyöneet velvollisuutensa varmistaa, että toimija noudattaa tässä direktiivissä säädettyjä velvoitteita. **Tämä säännös ei julkishallinnon toimijoiden osalta rajoita viranhaltijoiden taikka vaalilla valittujen ja nimettyjen virkamiesten vastuuvelvollisuudesta annettujen jäsenvaltioiden kansallisen lakien soveltamista.**

7. Toteuttaessaan täytäntöönpanotoimia tai soveltaessaan seuraamuksia 4 ja 5 kohdan nojalla toimivaltaisten viranomaisten on kunnioitettava puolustautumisoikeuksia ja otettava huomioon kunkin yksittäisen tapauksen olosuhteet sekä vähintään seuraavat seikat:

   a) rikkomisen vakavuus ja rikottujen säännösten merkitys. Vakavina pidettäviä rikkomisia ovat muun muassa seuraavat: toistuvat väärinkäytökset, sellaisten poikkeamien ilmoittamatta tai korjaamatta jättäminen, joilla on merkittävä haitallinen vaikutus, toimivaltaisten viranomaisten sitovien ohjeiden mukaisten korjaavien toimenpiteiden laiminlyönti ja toimivaltaisen viranomaisen rikkomisen johdosta määräämien auditointien tai seurantatoimien estäminen sekä 18 ja 20 artiklassa säädettyihin riskinhallintavaatimuksiin tai raportointivelvoitteisiin liittyvien väärien tai erittäin virheellisten tietojen antaminen.

b) rikkomisen kesto, mukaan lukien toistuvuus;

c) tosiasiallisesti aiheutuneet vahingot tai menetykset tai mahdolliset vahingot tai menetykset, jotka olisi voitu aiheuttaa, jos ne ovat määritettävissä. Tätä näkökohtaa arvioitaessa on otettava huomioon muun muassa todelliset tai mahdolliset rahoitukseen liittyvät ja taloudelliset tappiot, vaikutukset muihin palveluihin sekä niiden käyttäjien määrä, joihin vaikutukset kohdistuvat tai voivat kohdistua;

d) rikkomisen tahallisuus tai tuottamuksellisuus;

e) toimenpiteet, jotka toimija on toteuttanut vahingon ja/tai menetysten ehkäisemiseksi tai lieventämiseksi;

f) hyväksyttyjen käytännesääntöjen tai hyväksyttyjen sertifiointimekanismien noudattaminen;

g) vastuussa olevana pidetyn yhden tai useamman luonnollisen henkilön tai oikeushenkilön yhteistyön taso toimivaltaisten viranomaisten kanssa.

8. Toimivaltaisten viranomaisten on esitettävä täytäntöönpanopäätöstensä yksityiskohtaiset perustelut. Ennen tällaisten päätösten tekemistä toimivaltaisten viranomaisten on ilmoitettava asianomaisille toimijoille alustavista havainnoistaan ja annettava toimijoille kohtuullinen aika huomautusten esittämiseen, **paitsi jos on kyse välittömästä vaarasta.**

9. Jäsenvaltioiden on varmistettava, että niiden **tämän direktiivin nojalla** toimivaltaiset viranomaiset ilmoittavat direktiivin (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] mukaisesti nimetyille tuon **saman** [...] jäsenvaltion toimivaltaisille viranomaisille, kun ne käyttävät valvonta- ja täytäntöönpanovaltuuksiaan, joiden tarkoituksena on varmistaa, että direktiivin (EU) XXXX/XXXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] nojalla kriittiseksi [tai kriittistä toimijaa vastaavaksi] todettu keskeinen toimija noudattaa tämän direktiivin mukaisia velvoitteita. Direktiivin (EU) XXX/XXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] nojalla toimivaltaiset viranomaiset [...] **voivat tarvittaessa** pyytää **tämän direktiivin** [...] nojalla toimivaltaisia viranomaisia käyttämään valvonta- ja täytäntöönpano**valtuuksiaan suhteessa** tämän direktiivin soveltamisalaan kuuluvaan keskeiseen toimijaan, joka on **direktiivin (EU) XXX/XXX [kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi] nojalla** määritelty myös kriittiseksi [tai kriittistä toimijaa vastaavaksi].

10. Jäsenvaltioiden on varmistettava, että niiden tämän direktiivin nojalla toimivaltaiset viranomaiset ilmoittavat asetuksen (EU) XXXX/XXXX [finanssialan digitaalista häiriönsietokykyä koskeva asetus] 29 artiklan 1 kohdan mukaiselle valvontafoorumille, kun ne käyttävät valvonta- ja täytäntöönpanovaltuuksiaan, joiden tarkoituksena on varmistaa, että mainitun asetuksen 28 artiklan mukaisesti nimetty kriittisten TVT-palveluntarjoajana toimiva kolmas osapuoli noudattaa tämän direktiivin mukaisia velvoitteita.

10 a. Jäsenvaltioiden on varmistettava, että niiden tämän direktiivin nojalla toimivaltaiset viranomaiset ilmoittavat asetuksen (EU) 910/2014 mukaisesti nimetyille asiaankuuluville toimivaltaisille viranomaisille, kun ne käyttävät valvonta- ja täytäntöönpanovaltuuksiaan varmistaakseen, että mainitun asetuksen mukaisesti luottamuspalvelun tarjoajaksi nimetty toimija noudattaa tämän direktiivin mukaisia velvoitteita.

30 artikla

Valvonta ja täytäntöönpano tärkeiden toimijoiden osalta

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

2. Jäsenvaltioiden on varmistettava, että hoitaessaan tärkeitä toimijoita koskevia valvontatehtäviään **toimivaltaiset viranomaiset noudattavat riskiperusteista toimintatapaa ja** että niillä on kyseisten toimijoiden osalta valtuudet **ainakin** seuraaviin:

   a) paikan päällä tehtävät tarkastukset ja toimipaikkojen ulkopuolinen jälkikäteisvalvonta;

   b) riskinarviointeihin tai käytettävissä oleviin riskitietoihin perustuvat kohdennetut turvallisuusauditoinnit;

   c) objektiivisiin, **syrjimättömiin**, oikeudenmukaisiin ja läpinäkyviin riskinarviointikriteereihin perustuvat turvallisuuskartoitukset, **jotka teknisistä syistä tehdään tarvittaessa yhteistyössä asianomaisen toimijan kanssa**;

   d) tietopyynnöt, jotka ovat tarpeen kyberturvallisuustoimenpiteiden arvioimiseksi jälkikäteen [...];

   e) pyynnöt saada tutustua kaikkeen dataan ja kaikkiin asiakirjoihin ja/tai muihin tietoihin, joita ne tarvitsevat valvontatehtävien suorittamiseksi.

   ea) pyynnöt saada näyttöä kyberturvallisuusperiaatteiden täytäntöönpanosta, kuten pätevän tarkastajan tekemien turvallisuusauditointien tulokset ja niiden perustana oleva näyttö.

2 a. **Toimivaltaiset viranomaiset voivat tämän artiklan 2 kohdassa säädettyjä valvontatehtäviä suorittaessaan vahvistaa valvontamenetelmiä, joissa tällaiset tehtävät priorisoidaan riskiperusteista toimintatapaa noudattaen.**

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

4. Jäsenvaltioiden on varmistettava, että käyttäessään täytäntöönpanovaltuuksiaan keskeisten toimijoiden osalta toimivaltaisilla viranomaisilla on **ainakin** valtuudet

   a) varoittaa toimijoita siitä, että ne eivät ole noudattaneet tässä direktiivissä säädettyjä velvoitteita;

   b) antaa sitovia määräyksiä, joissa kyseisiä toimijoita vaaditaan korjaamaan havaitut puutteet tai saattamaan toimintansa tässä direktiivissä säädettyjen velvoitteiden mukaiseksi;

   c) määrätä kyseiset toimijat lopettamaan toiminta, joka ei ole tässä direktiivissä säädettyjen velvoitteiden mukaista, ja pidättäytymään toistamasta tätä toimintaa;

   d) määrätä kyseiset toimijat saattamaan riskinhallintatoimenpiteensä ja/tai raportointivelvoitteensa 18 ja 20 artiklassa säädettyjen velvoitteiden mukaisiksi määrätyllä tavalla ja määrätyn ajan kuluessa;

   e) määrätä kyseiset toimijat ilmoittamaan niiden palveluja tai toimintoja hyödyntäville luonnollisille tai oikeushenkilöille, joihin merkittävä kyberuhka saattaa vaikuttaa, **uhan luonteesta ja** mahdollisista suoja- tai korjaavista toimenpiteistä, joita kyseiset luonnolliset tai oikeushenkilöt voivat toteuttaa uhan johdosta;

   f) määrätä kyseiset toimijat panemaan täytäntöön turvallisuusauditoinnin tuloksena annetut suositukset kohtuullisessa määräajassa;

g) määrätä kyseiset toimijat julkistamaan tietyllä tavalla seikkoja, jotka liittyvät tässä direktiivissä säädettyjen velvoitteiden noudattamatta jättämiseen, **jos tällainen julkistaminen ei altista asianomaista toimijaa haitallisille vaikutuksille**;

h) [...]

i) määrätä tai pyytää asiaankuuluvia elimiä tai tuomioistuimia määräämään kansallisen lainsäädännön mukaisesti hallinnollisia sakkoja 31 artiklan nojalla tämän kohdan a–h alakohdassa tarkoitettujen toimenpiteiden lisäksi tai niiden sijasta kunkin yksittäisen tapauksen olosuhteista riippuen.

5. Tämän asetuksen 29 artiklan 6–8 kohtaa sovelletaan myös tässä artiklassa [...] tärkeiden toimijoiden osalta säädettyihin valvonta- ja täytäntöönpanotoimenpiteisiin.

31 artikla

Yleiset edellytykset hallinnollisten sakkojen määräämiselle keskeisille ja tärkeille toimijoille

1. Jäsenvaltioiden on varmistettava, että tämän artiklan nojalla keskeisille ja tärkeille toimijoille tässä direktiivissä säädettyjen velvoitteiden rikkomisesta määrätyt hallinnolliset sakot ovat kussakin yksittäistapauksessa vaikuttavia, oikeasuhteisia ja varoittavia.

2. Hallinnolliset sakot määrätään kunkin yksittäisen tapauksen olosuhteiden mukaisesti 29 artiklan 4 kohdan a–i alakohdassa, 29 artiklan 5 kohdassa ja 30 artiklan 4 kohdan a–h alakohdassa tarkoitettujen toimenpiteiden lisäksi tai niiden sijasta.

3. Päätettäessä hallinnollisen sakon määräämisestä ja sen suuruudesta kussakin yksittäistapauksessa on otettava asianmukaisesti huomioon vähintään 29 artiklan 7 kohdassa säädetyt seikat.

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

4 a. Jäsenvaltioiden on varmistettava, että tärkeille toimijoille määrätään 18 tai 20 artiklassa säädettyjen velvoitteiden rikkomisesta tämän artiklan 2 ja 3 kohdan mukaisesti hallinnollinen sakko, joka voi olla enimmillään vähintään 2 000 000 euroa tai, kun on kyse oikeushenkilöstä, 1 prosentti yrityksen, johon tärkeä toimija kuuluu, edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

5. Jäsenvaltiot voivat säätää valtuudesta määrätä uhkasakkoja saadakseen keskeisen tai tärkeän toimijan lopettamaan rikkomisen toimivaltaisen viranomaisen etukäteen tekemän päätöksen mukaisesti.

6. Kukin jäsenvaltio voi vahvistaa säännöt siitä, voidaanko 4 artiklan 23 kohdassa tarkoitetuille julkishallinnon toimijoille, joihin sovelletaan tässä direktiivissä säädettyjä velvoitteita, määrätä hallinnollisia sakkoja ja missä määrin, sanotun kuitenkaan rajoittamatta toimivaltaisten viranomaisten 29 ja 30 artiklan mukaisia valtuuksia.

6 a. Jos jäsenvaltion oikeusjärjestelmässä ei säädetä hallinnollisista sakoista, sen on varmistettava, että tätä artiklaa voidaan soveltaa niin, että sakon panee vireille toimivaltainen viranomainen ja sen määräävät toimivaltaiset kansalliset tuomioistuimet siten, että samalla varmistetaan, että nämä oikeussuojakeinot ovat tehokkaita ja niillä on vastaava vaikutus kuin toimivaltaisten viranomaisten määräämillä hallinnollisilla sakoilla. Määrättävien sakkojen on joka tapauksessa oltava tehokkaita, oikeasuhteisia ja varoittavia. Näiden jäsenvaltioiden on toimitettava säännökset, jotka ne hyväksyvät tämän kohdan nojalla, tiedoksi komissiolle viimeistään[...] ja niiden mahdolliset myöhemmät muutokset mahdollisimman pian.

32 artikla

Henkilötietojen tietoturvaloukkaukseen johtavat rikkomiset

1. Jos toimivaltaiset viranomaiset ovat **valvonta- tai täytäntöönpanovaltuuksien käytön yhteydessä** [...] **saaneet tietoonsa**, että keskeisen tai tärkeän toimijan **tämän direktiivin** 18 ja 20 artiklassa säädettyjen velvoitteiden laiminlyönti **saattaa** [...] aiheuttaa asetuksen (EU) 2016/679 4 artiklan 12 kohdassa määritellyn henkilötietojen tietoturvaloukkauksen, josta on ilmoitettava mainitun asetuksen 33 artiklan mukaisesti, niiden on ilmoitettava asiasta **ilman aiheetonta viivytystä** kyseisen asetuksen 55 ja 56 artiklan nojalla toimivaltaisille valvontaviranomaisille.

2. Jos asetuksen (EU) 2016/679 55 ja 56 artiklan mukaisesti toimivaltaiset valvontaviranomaiset päättävät käyttää kyseisen asetuksen 58 artiklan **2 kohdan** i alakohdan mukaisia valtuuksiaan ja määrätä hallinnollisen sakon, **tämän direktiivin 8 artiklassa tarkoitetut** toimivaltaiset viranomaiset eivät saa määrätä hallinnollista sakkoa [...] rikkomisesta tämän direktiivin 31 artiklassa säädetyin **samoin perustein**. Toimivaltaiset viranomaiset voivat kuitenkin soveltaa täytäntöönpanotoimia tai käyttää seuraamusvaltuuksiaan tämän direktiivin 29 artiklan 4 kohdan a–i alakohdan, 29 artiklan 5 kohdan ja 30 artiklan 4 kohdan a–h alakohdan mukaisesti.

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

33 artikla

Seuraamukset

1. Jäsenvaltioiden on säädettävä tämän direktiivin nojalla annettujen kansallisten säännösten rikkomiseen sovellettavista seuraamuksista ja toteutettava kaikki tarvittavat toimenpiteet sen varmistamiseksi, että ne pannaan täytäntöön. Seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia.

2. Jäsenvaltioiden on annettava komissiolle tiedoksi nämä säännökset ja toimenpiteet viimeistään [kahden] vuoden kuluttua tämän direktiivin voimaantulosta ja ilmoitettava sille ilman aiheetonta viivytystä niihin vaikuttavista myöhemmistä muutoksista.

34 artikla

Keskinäinen avunanto

1. Jos keskeinen tai tärkeä toimija tarjoaa palveluja useammassa kuin yhdessä jäsenvaltiossa tai [...] **tarjoaa palveluja useammassa kuin yhdessä** jäsenvaltiossa mutta sen verkko- ja tietojärjestelmät sijaitsevat yhdessä tai useammassa muussa jäsenvaltiossa, **asianomaisten** jäsenvaltioiden toimivaltaisten viranomais[...]**ten** [...]on tehtävä yhteistyötä ja avustettava toisiaan tarpeen mukaan. Tähän yhteistyöhön kuuluu vähintään, että

a) valvonta- tai täytäntöönpanotoimenpiteitä jäsenvaltiossa soveltavat toimivaltaiset viranomaiset informoivat ja kuulevat toteutetuista [...] valvonta- ja täytäntöönpanotoimenpiteistä keskitetyn yhteyspisteen kautta muiden asianomaisten jäsenvaltioiden toimivaltaisia viranomaisia;

b) toimivaltainen viranomainen voi pyytää toista toimivaltaista viranomaista toteuttamaan [...] valvonta- tai täytäntöönpanotoimenpiteitä;

c) toimivaltaisen viranomaisen on toisen toimivaltaisen viranomaisen perustellun pyynnön saatuaan annettava **käytettävissä olevien resurssiensa puitteissa apua** toiselle toimivaltaiselle viranomaiselle, jotta [...] valvonta- tai täytäntöönpanotoimet voidaan toteuttaa tuloksellisesti, tehokkaasti ja johdonmukaisesti. Tällainen keskinäinen avunanto voi sisältää tietopyyntöjä ja valvontatoimenpiteitä, mukaan lukien pyynnöt, jotka koskevat paikan päällä suoritettavia tarkastuksia tai muualla suoritettavaa valvontaa tai kohdennettuja turvallisuusauditointeja. Toimivaltainen viranomainen, jolle avunantopyyntö on osoitettu, ei voi evätä kyseistä pyyntöä, paitsi jos muiden asianomaisten viranomaisten [...] kanssa käydyn näkemystenvaihdon jälkeen todetaan, että [...] viranomaisella ei ole toimivaltaa antaa pyydettyä apua **tai että sillä ei ole tarvittavia resursseja** tai että pyydetty apu ei ole oikeassa suhteessa toimivaltaisen viranomaisen [...] suorittamiin valvontatehtäviin nähden **tai että pyyntö koskee sellaisia tietoja tai edellyttää sellaista toimintaa, joka on ristiriidassa kyseisen jäsenvaltion kansallisen tai yleisen turvallisuuden taikka puolustuksen kanssa**.

2. Eri jäsenvaltioiden toimivaltaiset viranomaiset voivat tarvittaessa ja yhteisestä sopimuksesta toteuttaa [...] yhteisiä valvontatoimia.

VII LUKU

Siirtymä- ja loppusäännökset

35 artikla

Uudelleentarkastelu

Komissio tarkastelee määräajoin uudelleen tämän direktiivin toimivuutta ja laatii raportin Euroopan parlamentille ja neuvostolle. Raportissa arvioidaan erityisesti liitteissä I ja II tarkoitettujen toimijoiden toimialojen, alasektoreiden, koon ja tyypin merkitystä talouden ja yhteiskunnan toiminnalle kyberturvallisuuden näkökulmasta. Komissio ottaa [...] **uudelleentarkastelussa** [...] huomioon [...] CSIRT-verkoston raportit [...] operatiivisella tasolla saaduista kokemuksista. Ensimmäinen raportti annetaan viimeistään... päivänä... kuuta... [54 kuukautta tämän direktiivin voimaantulosta].

36 artikla

[...]

[...]

[...]

37 artikla

Komiteamenettely

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

2. Kun viitataan tähän kohtaan, sovelletaan asetuksen (EU) N:o 182/2011 5 artiklaa.

3. Kun komitean lausunto on määrä hankkia kirjallista menettelyä noudattaen, tämä menettely päätetään tuloksettomana, jos komitean puheenjohtaja lausunnon antamiselle asetetussa määräajassa niin päättää tai komitean jäsen sitä pyytää.

38 artikla

Saattaminen osaksi kansallista lainsäädäntöä

1. Jäsenvaltioiden on annettava ja julkaistava [...] tämän direktiivin noudattamisen edellyttämät lait, asetukset ja hallinnolliset määräykset viimeistään [...] **24** kuukauden kuluttua tämän direktiivin voimaantulosta. Niiden on viipymättä ilmoitettava tästä komissiolle. Niiden on sovellettava näitä säännöksiä … päivästä …kuuta … [ensimmäisessä alakohdassa tarkoitettua päivää seuraavasta päivästä].

2. Näissä jäsenvaltioiden antamissa säädöksissä on viitattava tähän direktiiviin tai niihin on liitettävä tällainen viittaus, kun ne julkaistaan virallisesti. Jäsenvaltioiden on säädettävä siitä, miten viittaukset tehdään.

39 artikla

Asetuksen (EU) N:o 910/2014 muuttaminen

Kumotaan **asetuksen (EU) N:o 910/2014** 19 artikla **[siitä päivästä, johon mennessä tämä direktiivi on saatettava osaksi kansallista lainsäädäntöä].**

40 artikla

Direktiivin (EU) 2018/1972 muuttaminen

Kumotaan **direktiivin (EU) 2018/1972** 40 ja 41 [...] artikla **[siitä päivästä, johon mennessä tämä direktiivi on saatettava osaksi kansallista lainsäädäntöä].**

41 artikla

Kumoaminen

Kumotaan direktiivi (EU) 2016/1148 [siitä päivästä, johon mennessä tämä direktiivi on saatettava osaksi kansallista lainsäädäntöä].

Viittauksia direktiiviin (EU) 2016/1148 pidetään viittauksina tähän direktiiviin liitteessä II [...] olevan vastaavuustaulukon mukaisesti.

42 artikla

Voimaantulo

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

43 artikla

Osoitus

Tämä direktiivi on osoitettu kaikille jäsenvaltioille.

Tehty Brysselissä

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puhemies	*Puheenjohtaja*

LIITE I

TOIMIALAT, ALASEKTORIT JA TOIMIJATYYPIT

Toimiala	Alasektori	Toimijatyyppi
1. Energia	a) Sähkö	— Direktiivin (EU) 2019/944([39]) 2 artiklan 57 kohdassa tarkoitetut sähköalan yritykset, jotka harjoittavat kyseisen direktiivin 2 artiklan 12 kohdassa tarkoitettua 'toimittamista'
		— Direktiivin (EU) 2019/944 2 artiklan 29 kohdassa tarkoitetut jakeluverkonhaltijat
		— Direktiivin (EU) 2019/944 2 artiklan 35 kohdassa tarkoitetut siirtoverkonhaltijat
		— Direktiivin (EU) 2019/944 2 artiklan 38 kohdassa tarkoitetut tuottajat
		— Asetuksen (EU) 2019/943([40]) 2 artiklan 8 kohdassa tarkoitetut nimetyt sähkömarkkinaoperaattorit
		— Asetuksen (EU) 2019/943 2 artiklan 25 kohdassa tarkoitetut markkinaosapuolet, joka tarjoavat direktiivin (EU) 2019/944 2 artiklan 18, 20 ja 59 kohdassa tarkoitettuja aggregointi-, kulutusjousto- ja energian varastointipalveluja

---

[39] Euroopan parlamentin ja neuvoston direktiivi (EU) 2019/944, annettu 5 päivänä kesäkuuta 2019, sähkön sisämarkkinoita koskevista yhteisistä säännöistä ja direktiivin 2012/27/EU muuttamisesta (EUVL L 158, 14.6.2019, s. 125).

[40] Euroopan parlamentin ja neuvoston asetus (EU) 2019/943, annettu 5 päivänä kesäkuuta 2019, sähkön sisämarkkinoista (EUVL L 158, 14.6.2019, s. 54).

	b) Kaukolämmitys ja -jäähdytys	— Uusiutuvista lähteistä peräisin olevan energian käytön edistämisestä annetun direktiivin (EU) 2018/2001[41] 2 artiklan 19 kohdassa tarkoitettu kaukolämmitys tai kaukojäähdytys
	c) Öljy	— Öljynsiirtoputkistojen haltijat
		— Öljyn tuotanto-, jalostus- ja käsittelylaitteistojen haltijat sekä öljyn varastointia ja siirtoa hoitavat operaattorit
		— Neuvoston direktiivin 2009/119/EY(42) 2 artiklan f kohdassa tarkoitetut keskusvarastointiyksiköt
	d) Kaasu	— Direktiivin 2009/73/EY(43) 2 artiklan 8 kohdassa tarkoitetut maakaasun toimittajat
		— Direktiivin 2009/73/EY 2 artiklan 6 kohdassa tarkoitetut jakeluverkonhaltijat
		— Direktiivin 2009/73/EY 2 artiklan 4 kohdassa tarkoitetut siirtoverkonhaltijat
		— Direktiivin 2009/73/EY 2 artiklan 10 kohdassa tarkoitetut varastointilaitteiston haltijat

---

[41] Euroopan parlamentin ja neuvoston direktiivi (EU) 2018/2001, annettu 11 päivänä joulukuuta 2018, uusiutuvista lähteistä peräisin olevan energian käytön edistämisestä (EUVL L 328, 21.12.2018, s. 82).

[42] Neuvoston direktiivi 2009/119/EY, annettu 14 päivänä syyskuuta 2009, jäsenvaltioiden velvollisuudesta ylläpitää raakaöljy- ja/tai öljytuotevarastojen vähimmäistasoa (EUVL L 265, 9.10.2009, s. 9).

[43] Euroopan parlamentin ja neuvoston direktiivi 2009/73/EY, annettu 13 päivänä heinäkuuta 2009, maakaasun sisämarkkinoita koskevista yhteisistä säännöistä ja direktiivin 2003/55/EY kumoamisesta (EUVL L 211, 14.8.2009, s. 94).

		— Direktiivin 2009/73/EY 2 artiklan 12 kohdassa tarkoitetut nesteytetyn maakaasun käsittelylaitteiston haltijat
		— Direktiivin 2009/73/EY 2 artiklan 1 kohdassa tarkoitetut maakaasualan yritykset
		— Maakaasun jalostus- ja käsittelylaitteistojen haltijat
	e) Vety	Vedyn tuotantoa, varastointia ja siirtoa harjoittavat toimijat
2. Liikenne	a) Ilmaliikenne	— Asetuksen (EY) N:o 300/2008([44]) 3 artiklan 4 kohdassa tarkoitetut lentoliikenteen harjoittajat, **joita käytetään kaupallisiin tarkoituksiin**
		— Euroopan parlamentin ja neuvoston direktiivin 2009/12/EY([45])2 artiklan 2 kohdassa tarkoitetut lentoaseman pitäjät, kyseisen direktiivin 2 artiklan 1 kohdassa tarkoitetut lentoasemat, mukaan lukien Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1315/2013([46]) liitteessä II olevassa 2 jaksossa luetellut ydinverkon lentoasemat, sekä lentoasemilla sijaitsevia lisärakennelmia ja -laitteita hoitavat toimijat

---

[44] Euroopan parlamentin ja neuvoston asetus (EY) N:o 300/2008, annettu 11 päivänä maaliskuuta 2008, yhteisistä siviili-ilmailun turvaamista koskevista säännöistä ja asetuksen (EY) N:o 2320/2002 kumoamisesta (EUVL L 97, 9.4.2008, s. 72).

[45] Euroopan parlamentin ja neuvoston direktiivi 2009/12/EY, annettu 11 päivänä maaliskuuta 2009, lentoasemamaksuista (EUVL L 70, 14.3.2009, s. 11).

[46] Euroopan parlamentin ja neuvoston asetus (EU) N:o 1315/2013, annettu 11 päivänä joulukuuta 2013, unionin suuntaviivoista Euroopan laajuisen liikenneverkon kehittämiseksi ja päätöksen N:o 661/2010/EU kumoamisesta (EUVL L 348, 20.12.2013, s. 1).

		— Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 549/2004(47) 2 artiklan 1 kohdassa tarkoitettuja lennonjohtopalveluja tarjoavat liikenteenhallinnan ylläpitäjät
	b) Raideliikenne	— Direktiivin 2012/34/EU(48) 3 artiklan 2 kohdassa tarkoitetut rataverkon haltijat
		— Direktiivin 2012/34/EU 3 artiklan 1 kohdassa tarkoitetut rautatieyritykset, mukaan lukien direktiivin 2012/34/EU 3 artiklan 12 kohdassa tarkoitetut palvelupaikan ylläpitäjät
	c) Vesiliikenne	— Asetuksen (EY) N:o 725/2004(49) liitteessä I merenkulun osalta tarkoitetut sisävesillä, merillä ja rannikoilla matkustaja- ja rahtiliikennettä hoitavat yhtiöt, lukuun ottamatta tällaisten yhtiöiden liikennöimiä yksittäisiä aluksia
		— Direktiivin 2005/65/EY(50) 3 artiklan 1 kohdassa tarkoitettujen satamien hallinnointielimet, mukaan lukien niiden asetuksen (EY) N:o 725/2004 2 artiklan 11 kohdassa tarkoitetut satamarakenteet, sekä toimijat, jotka huolehtivat töistä ja laitteistoista satamien alueella

---

[47] Euroopan parlamentin ja neuvoston asetus (EY) N:o 549/2004, annettu 10 päivänä maaliskuuta 2004, yhtenäisen eurooppalaisen ilmatilan toteuttamisen puitteista (puiteasetus) (EUVL L 96, 31.3.2004, s. 1).

[48] Euroopan parlamentin ja neuvoston direktiivi 2012/34/EU, annettu 21 päivänä marraskuuta 2012, yhtenäisestä eurooppalaisesta rautatiealueesta (EUVL L 343, 14.12.2012, s. 32).

[49] Euroopan parlamentin ja neuvoston asetus (EY) N:o 725/2004, annettu 31 päivänä maaliskuuta 2004, alusten ja satamarakenteiden turvatoimien parantamisesta (EUVL L 129, 29.4.2004, s. 6).

[50] Euroopan parlamentin ja neuvoston direktiivi 2005/65/EY, annettu 26 päivänä lokakuuta 2005, satamien turvallisuuden parantamisesta (EUVL L 310, 25.11.2005, s. 28).

		— Direktiivin 2002/59/EY(51) 3 artiklan o alakohdassa tarkoitettujen alusliikennepalvelujen tarjoajat
	d) Tieliikenne	— Komission delegoidun asetuksen (EU) 2015/962(52) 2 artiklan 12 kohdassa tarkoitetut liikenteenhallinnasta vastaavat tieviranomaiset, **lukuun ottamatta julkisia toimijoita, joiden osalta älykkäiden liikennejärjestelmien ylläpitäjien liikenteenhallinta ei ole keskeinen osa niiden yleistä toimintaa**.
		— Direktiivin 2010/40/EU(53) 4 artiklan 1 kohdassa tarkoitettujen älykkäiden liikennejärjestelmien ylläpitäjät
3. Pankkitoiminta		— Asetuksen (EU) N:o 575/2013(54) 4 artiklan 1 kohdassa tarkoitetut luottolaitokset **[lukuun ottamatta direktiivin 2013/36/EU 2 artiklan 5 kohdan 8 alakohdassa tarkoitettuja luottolaitoksia, jotka on vapautettu soveltamisesta asetuksen XX [finanssialan digitaalista häiriönsietokykyä koskeva asetus] 2 artiklan 4 kohdan mukaisesti].**

---

[51] Euroopan parlamentin ja neuvoston direktiivi 2002/59/EY, annettu 27 päivänä kesäkuuta 2002, alusliikennettä koskevan yhteisön seuranta- ja tietojärjestelmän perustamisesta sekä neuvoston direktiivin 93/75/ETY kumoamisesta (EYVL L 208, 5.8.2002, s. 10).

[52] Komission delegoitu asetus (EU) 2015/962, annettu 18 päivänä joulukuuta 2014, Euroopan parlamentin ja neuvoston direktiivin 2010/40/EU täydentämisestä EU:n laajuisten tosiaikaisten liikennetietopalvelujen tarjoamisen osalta (EUVL L 157, 23.6.2015, s. 21).

[53] Euroopan parlamentin ja neuvoston direktiivi 2010/40/EU, annettu 7 päivänä heinäkuuta 2010, tieliikenteen älykkäiden liikennejärjestelmien käyttöönoton sekä tieliikenteen ja muiden liikennemuotojen rajapintojen puitteista (EUVL L 207, 6.8.2010, s. 1).

[54] Euroopan parlamentin ja neuvoston asetus (EU) N:o 575/2013, annettu 26 päivänä kesäkuuta 2013, luottolaitosten ja sijoituspalveluyritysten vakavaraisuusvaatimuksista ja asetuksen (EU) N:o 648/2012 muuttamisesta (EUVL L 176, 27.6.2013, s. 1).

4. Finanssimarkkinoiden infrastruktuurit		— Direktiivin 2014/65/EU([55]) 4 artiklan 24 kohdassa tarkoitettujen kauppapaikkojen ylläpitäjät
		— Asetuksen (EU) N:o 648/2012([56]) 2 artiklan 1 kohdassa tarkoitetut keskusvastapuolet
5. Terveys		— Direktiivin 2011/24/EU([57]) 3 artiklan g alakohdassa tarkoitetut terveydenhuollon tarjoajat
		— Vakavista rajat ylittävistä terveysuhista annetun asetuksen XXXX/XXXX[58] 15 artiklassa tarkoitetut EU:n vertailulaboratoriot
		— Direktiivin 2001/83/EY([59]) 1 artiklan 2 kohdassa tarkoitettujen lääkkeiden tutkimusta ja kehitystä harjoittavat toimijat — NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 21 tarkoitettujen farmaseuttisten perustuotteiden ja farmaseuttisten valmisteiden valmistajat

---

[55] Euroopan parlamentin ja neuvoston direktiivi 2014/65/EU, annettu 15 päivänä toukokuuta 2014, rahoitusvälineiden markkinoista sekä direktiivin 2002/92/EY ja direktiivin 2011/61/EU muuttamisesta (EUVL L 173, 12.6.2014, s. 349).

[56] Euroopan parlamentin ja neuvoston asetus (EU) N:o 648/2012, annettu 4 päivänä heinäkuuta 2012, OTC-johdannaisista, keskusvastapuolista ja kauppatietorekistereistä (EUVL L 201, 27.7.2012, s. 1).

[57] Euroopan parlamentin ja neuvoston direktiivi 2011/24/EU, annettu 9 päivänä maaliskuuta 2011, potilaiden oikeuksien soveltamisesta rajatylittävässä terveydenhuollossa (EUVL L 88, 4.4.2011, s. 45).

[58] [Euroopan parlamentin ja neuvoston asetus vakavista rajat ylittävistä terveysuhista ja päätöksen N:o 1082/2013/EU kumoamisesta, lisätään viittaus kun ehdotus COM (2020)727 final on hyväksytty]

[59] Euroopan parlamentin ja neuvoston direktiivi 2001/83/EY, annettu 6 päivänä marraskuuta 2001, ihmisille tarkoitettuja lääkkeitä koskevista yhteisön säännöistä (EYVL L 311, 28.11.2001, s. 67).

		— Asetuksen XXXX[60] 20 artiklassa tarkoitettujen vakavan kansanterveysuhan aikana kriittisiksi katsottujen lääkinnällisten laitteiden ('kansanterveyden hätätilanteessa kriittisten laitteiden luettelo') valmistajat
6. Juomavesi		Neuvoston direktiivin 98/83/EY(61) 2 artiklan 1 kohdan a alakohdassa tarkoitetun ihmisten käyttöön tarkoitetun veden toimittajat ja jakelijat, lukuun ottamatta jakelijoita, joille ihmisten käyttöön tarkoitetun veden jakelu **ei ole keskeinen** osa niiden yleistä toimintaa, joka muodostuu muiden hyödykkeiden ja tavaroiden jakelusta [...]
7. Jätevesi		Neuvoston direktiivin 91/271/ETY(62) 2 artiklan 1–3 kohdassa tarkoitettua yhdyskuntajätevettä, talousjätevettä ja teollisuusjätevettä keräävät, hävittävät tai käsittelevät toimijat **lukuun ottamatta yrityksiä, joille yhdyskuntajäteveden, talousjäteveden ja teollisuusjäteveden kerääminen, hävittäminen tai käsittely ei ole keskeinen osa niiden yleistä toimintaa**. [...]
8. Digitaalinen infrastruktuuri		Internetin yhdysliikennepisteiden ylläpitäjät
		— DNS-palveluntarjoajat **lukuun ottamatta juuripalvelinten ylläpitäjiä**

---

[60] [Euroopan parlamentin ja neuvoston asetus Euroopan lääkeviraston vahvemmasta asemasta lääkkeitä ja lääkinnällisiä laitteita koskevassa kriiseihin valmistautumisessa ja kriisinhallinnassa, lisätään viittaus kun ehdotus COM (2020)725 final on hyväksytty]

[61] Neuvoston direktiivi 98/83/EY, annettu 3 päivänä marraskuuta 1998, ihmisten käyttöön tarkoitetun veden laadusta (EYVL L 330, 5.12.1998, s. 32).

[62] Neuvoston direktiivi 91/271/ETY, annettu 21 päivänä toukokuuta 1991, yhdyskuntajätevesien käsittelystä (EYVL L 135, 30.5.1991, s. 40).

		— TLD-rekisterit
		— Pilvipalvelujen tarjoajat
		— Datakeskuspalvelujen tarjoajat
		— Sisällönjakeluverkkojen tarjoajat
		— Asetuksen (EU) N:o 910/2014([63]) 3 artiklan 19 kohdassa tarkoitetut luottamuspalvelun tarjoajat
		— Direktiivin (EU) 2018/1972([64]) 2 artiklan 8 kohdassa tarkoitettujen yleisten sähköisten viestintäverkkojen tarjoajat tai direktiivin (EU) 2018/1972 2 artiklan 4 kohdassa tarkoitettujen sähköisten viestintäpalvelujen tarjoajat siltä osin kuin niiden palvelut ovat yleisesti saatavilla
8.a IT-palvelunhallinta (IT Service Management) **(B2B)**		**— Hallintapalvelujen tarjoajat** **— Tietoturvapalveluntarjoajat**

---

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

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

9. Julkishallinnon **toimijat**		— Keskushallintojen julkiset toimijat **sellaisina kuin jäsenvaltio on ne määrittänyt kansallisen lainsäädännön mukaisesti** — [...][65][...] — [...]
10. Avaruus		— Avaruuspohjaisia palveluja tukevien, jäsenvaltioiden tai yksityisten tahojen omistamien, hallinnoimien ja operoimien maainfrastruktuurien ylläpitäjät, lukuun ottamatta direktiivin (EU) 2018/1972 2 artiklan 8 kohdassa tarkoitettuja yleisen sähköisen viestintäverkon tarjoajia

---

[65] [...]

LIITE II

TOIMIALAT, ALASEKTORIT JA TOIMIJATYYPIT

Toimiala	Alasektori	Toimijatyyppi
1. Posti- ja kuriiripalvelut		Direktiivin 97/67/EY([66]) 2 artiklan 1 [...] kohdassa tarkoitetut postipalvelujen tarjoajat, [...] **mukaan lukien** kuriiripalvelujen tarjoajat
2. Jätehuolto		Direktiivin 2008/98/EY([67]) 3 artiklan 9 kohdassa tarkoitettua jätehuoltoa harjoittavat toimijat, lukuun ottamatta toimijoita, joiden toiminnan pääasiallinen sisältö ei ole jätehuolto

---

[66] Euroopan parlamentin ja neuvoston direktiivi 97/67/EY, annettu 15 päivänä joulukuuta 1997, yhteisön postipalvelujen sisämarkkinoiden kehittämistä ja palvelun laadun parantamista koskevista yhteisistä säännöistä (EYVL L 15, 21.1.1998, s. 14), **sellaisena kuin se on muutettuna Euroopan parlamentin ja neuvoston direktiivillä 2008/6/EY, annettu 20 päivänä helmikuuta 2008, direktiivin 97/67/EY muuttamisesta yhteisön postipalvelujen sisämarkkinoiden täysimääräisen toteuttamisen osalta (EYVL L 52, 27.2.2008, s. 3).**

[67] Euroopan parlamentin ja neuvoston direktiivi 2008/98/EY, annettu 19 päivänä marraskuuta 2008, jätteistä ja tiettyjen direktiivien kumoamisesta (EUVL L 312, 22.11.2008, s. 3).

3. Kemikaalien valmistus, tuotanto ja jakelu		Asetuksen (EY) N:o 1907/2006([68]) 3 artiklan [...], 9 ja 14 kohdassa tarkoitettua aineiden ja [...] **seosten** valmistamista [...] ja jakelua harjoittavat toimijat **sekä mainitun asetuksen 3 artiklan 3 kohdassa tarkoitettua aineista tai seoksista koostuvien esineiden tuottamista harjoittavat toimijat.**
4. Elintarvikkeiden tuotanto, jalostus ja jakelu		Asetuksen (EY) N:o 178/2002([69]) 3 artiklan 2 kohdassa tarkoitetut elintarvikeyritykset, **jotka harjoittavat tukkukauppaa sekä teollista tuotantoa ja jalostusta**
5. Valmistus	a) Lääkinnällisten laitteiden ja in vitro -diagnostiikkaan tarkoitettujen lääkinnällisten laitteiden valmistus	Asetuksen (EU) 2017/745([70]) 2 artiklan 1 kohdassa tarkoitettujen lääkinnällisten laitteiden valmistajat sekä asetuksen (EU) 2017/746([71]) 2 artiklan 2 kohdassa tarkoitettujen in vitro -diagnostiikkaan tarkoitettujen lääkinnällisten laitteiden valmistajat, lukuun ottamatta liitteessä 1 olevassa 5 kohdassa mainittujen lääkinnällisten laitteiden valmistajia.

---

[68] Euroopan parlamentin ja neuvoston asetus (EY) N:o 1907/2006, annettu 18 päivänä joulukuuta 2006, kemikaalien rekisteröinnistä, arvioinnista, lupamenettelyistä ja rajoituksista (REACH), Euroopan kemikaaliviraston perustamisesta, direktiivin 1999/45/EY muuttamisesta sekä neuvoston asetuksen (ETY) N:o 793/93, komission asetuksen (EY) N:o 1488/94, neuvoston direktiivin 76/769/ETY ja komission direktiivien 91/155/ETY, 93/67/ETY, 93/105/EY ja 2000/21/EY kumoamisesta (EUVL L 396, 30.12.2006, s. 1).

[69] Euroopan parlamentin ja neuvoston asetus (EY) N:o 178/2002, annettu 28 päivänä tammikuuta 2002, elintarvikelainsäädäntöä koskevista yleisistä periaatteista ja vaatimuksista, Euroopan elintarviketurvallisuusviranomaisen perustamisesta sekä elintarvikkeiden turvallisuuteen liittyvistä menettelyistä (EYVL L 31, 1.2.2002, s. 1).

[70] Euroopan parlamentin ja neuvoston asetus (EU) 2017/745, annettu 5 päivänä huhtikuuta 2017, lääkinnällisistä laitteista, direktiivin 2001/83/EY, asetuksen (EY) N:o 178/2002 ja asetuksen (EY) N:o 1223/2009 muuttamisesta sekä neuvoston direktiivien 90/385/ETY ja 93/42/ETY kumoamisesta (EUVL L 117, 5.5.2017, s. 1).

[71] Euroopan parlamentin ja neuvoston asetus (EU) 2017/746, annettu 5 päivänä huhtikuuta 2017, in vitro -diagnostiikkaan tarkoitetuista lääkinnällisistä laitteista sekä direktiivin 98/79/EY ja komission päätöksen 2010/227/EU kumoamisesta (EUVL L 117, 5.5.2017, s. 176).

	b) Tietokoneiden sekä elektronisten ja optisten tuotteiden valmistus	NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 26 tarkoitettua taloudellista toimintaa harjoittavat toimijat
	c) Sähkölaitteiden valmistus	NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 27 tarkoitettua taloudellista toimintaa harjoittavat toimijat
	d) Muiden koneiden ja laitteiden valmistus	NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 28 tarkoitettua taloudellista toimintaa harjoittavat toimijat
	e) Moottoriajoneuvojen, perävaunujen ja puoliperävaunujen valmistus	NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 29 tarkoitettua taloudellista toimintaa harjoittavat toimijat
	f) Muiden kulkuneuvojen valmistus	NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 30 tarkoitettua taloudellista toimintaa harjoittavat toimijat
6. Digitaalisen palvelun tarjoajat		— Verkon kauppapaikkojen tarjoajat
		— Verkon hakukoneiden tarjoajat
		— Verkkoyhteisöalustojen tarjoajat