DIREKTIIVIT

EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI (EU) 2022/2555,

annettu 14 päivänä joulukuuta 2022,

toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi)

(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 keskuspankin lausunnon ([1]),

ottavat huomioon Euroopan talous- ja sosiaalikomitean lausunnon ([2]),

ovat kuulleet alueiden komiteaa,

noudattavat tavallista lainsäätämisjärjestystä ([3]),

sekä katsovat seuraavaa:

(1) Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/1148 ([4]) tavoitteena oli kehittää kyberturvallisuusvalmiuksia kaikkialla unionissa, lieventää keskeisten palvelujen tarjoamiseen keskeisillä aloilla käytettäviin verkko- ja tietojärjestelmiin kohdistuvia uhkia ja varmistaa tällaisten palvelujen jatkuvuus poikkeamatilanteissa sekä tukea näin unionin turvallisuutta ja sen talouden ja yhteiskunnan tehokasta toimintaa.

(2) Direktiivin (EU) 2016/1148 voimaantulon jälkeen unionin kyberresilienssin parantamisessa on edistytty merkittävästi. Mainitun direktiivin uudelleentarkastelu on osoittanut, että se on vauhdittanut institutionaalista ja sääntelyyn perustuvaa lähestymistapaa kyberturvallisuuteen unionissa ja tasoittanut tietä merkittävälle ajattelutavan muutokselle. Direktiivillä on varmistettu verkko- ja tietojärjestelmien turvallisuutta koskevien kansallisten kehysten täydentäminen määrittämällä kansalliset verkko- ja tietojärjestelmien turvallisuutta koskevat strategiat, luomalla kansallisia valmiuksia ja toteuttamalla sääntelytoimenpiteitä, jotka kattavat kunkin jäsenvaltion määrittämät keskeiset infrastruktuurit ja toimijat. Direktiivillä (EU) 2016/1148 on myös edistetty yhteistyötä unionin tasolla perustamalla erityinen yhteistyöryhmä ja tietoturvaloukkauksiin reagoivien ja niitä tutkivien kansallisten yksiköiden verkosto. Näistä saavutuksista huolimatta direktiivin (EU) 2016/1148 uudelleentarkastelussa on tullut esiin sisälähtöisiä puutteita, joiden vuoksi sillä ei kyetä tuloksekkaasti puuttumaan nykyisiin ja esiin nouseviin kyberturvallisuushaasteisiin.

(3) Verkko- ja tietojärjestelmät ovat kehittyneet arjen keskeiseksi osaksi yhteiskuntien digitalisaation ja verkottumisen edetessä nopeasti, myös rajatylittävässä yhteydenpidossa. Tämä kehitys on laajentanut kyberuhkaympäristöä ja tuonut mukanaan uusia haasteita, jotka edellyttävät mukautettuja, koordinoituja ja innovatiivisia hallintatoimia kaikissa jäsenvaltioissa. Poikkeamien määrä, laajuus, kehittyneisyys, esiintymistiheys ja vaikutukset lisääntyvät, ja ne muodostavat merkittävän uhkan verkko- ja tietojärjestelmien toiminnalle. Tämän seurauksena poikkeamat voivat haitata taloudellisen toiminnan harjoittamista sisämarkkinoilla, aiheuttaa taloudellisia tappioita, heikentää käyttäjien

([1]) EUVL C 233, 16.6.2022, s. 22.
([2]) EUVL C 286, 16.7.2021, s. 170.
([3]) Euroopan parlamentin kanta, vahvistettu 10. marraskuuta 2022 (ei vielä julkaistu virallisessa lehdessä), ja neuvoston päätös, tehty 28. marraskuuta 2022.
([4]) 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).

luottamusta ja aiheuttaa huomattavaa vahinkoa unionin taloudelle ja yhteiskunnalle. Kyberturvallisuusvalmius ja tehokas kyberturvallisuus ovat siksi nyt tärkeämpiä kuin koskaan sisämarkkinoiden moitteettoman toiminnan kannalta. Lisäksi kyberturvallisuus on monilla kriittisillä toimialoilla keskeinen tekijä, jotta digitaalinen siirtymä voidaan toteuttaa onnistuneesti ja digitalisaation taloudelliset, sosiaaliset ja kestävyysedut voidaan hyödyntää täysimääräisesti.

(4) Direktiivin (EU) 2016/1148 oikeusperustana oli Euroopan unionin toiminnasta tehdyn sopimuksen 114 artikla, jonka tavoitteena on sisämarkkinoiden toteuttaminen ja toiminta tehostamalla toimenpiteitä kansallisten sääntöjen lähentämiseksi. Taloudellisesti merkittäviä palveluja tarjoaville tai taloudellisesti merkittävää toimintaa harjoittaville toimijoille asetetut kyberturvallisuusvaatimukset vaihtelevat huomattavasti jäsenvaltiosta toiseen vaatimusten tyypin, yksityiskohtaisuuden ja valvontamenetelmän osalta. Nämä erot aiheuttavat lisäkustannuksia ja vaikeuksia toimijoille, jotka tarjoavat tavaroita tai palveluja yli valtioiden rajojen. Tällaiseen rajatylittävään toimintaan voi merkittävästi vaikuttaa se, jos yhden jäsenvaltion asettamat vaatimukset eroavat toisen jäsenvaltion asettamista vaatimuksista tai ovat jopa ristiriidassa niiden kanssa. Jos kyberturvallisuusvaatimusten suunnittelu tai täytäntöönpano sattuu lisäksi olemaan jossain jäsenvaltiossa puutteellista, tämä todennäköisesti vaikuttaa kyberturvallisuuden tasoon muissa jäsenvaltioissa, erityisesti kun otetaan huomioon rajatylittävien yhteyksien määrä. Direktiivin (EU) 2016/1148 uudelleentarkastelu on osoittanut, että jäsenvaltiot ovat panneet sen täytäntöön hyvin eri tavoin, myös sen soveltamisalan osalta, jonka rajaaminen jätettiin suurelta osin jäsenvaltioiden harkintaan. Direktiivin (EU) 2016/1148 mukaan jäsenvaltioilla oli myös hyvin laaja harkintavalta päättää, miten ne panevat täytäntöön siinä säädetyt turvallisuutta ja poikkeamista raportointia koskevat velvoitteet. Niinpä näiden velvoitteiden täytäntöönpanossa kansallisella tasolla on merkittäviä eroja. Valvontaa ja täytäntöönpanoa koskevien direktiivin (EU) 2016/1148 säännösten täytäntöönpanossa on samankaltaisia eroja.

(5) Kaikki nämä erot aiheuttavat sisämarkkinoiden pirstoutumista ja voivat haitata niiden toimintaa, mikä vaikuttaa erityisesti rajatylittävään palveluntarjontaan ja kyberresilienssin tasoon, kun käytössä on monenlaisia toimenpiteitä. Nämä erot saattavat viime kädessä lisätä joidenkin jäsenvaltioiden haavoittuvuutta kyberuhkille, millä voi olla heijastusvaikutuksia kaikkialla unionissa. Tällä direktiivillä pyritään poistamaan näitä jäsenvaltioiden välisiä suuria eroja erityisesti vahvistamalla vähimmäissäännöt koordinoidun sääntelykehyksen toiminnalle, vahvistamalla järjestelyt kunkin jäsenvaltion vastuuviranomaisten toimivaa yhteistyötä varten, ajantasaistamalla luettelo aloista ja toiminnoista, joihin sovelletaan kyberturvallisuusvelvoitteita, ja säätämällä tehokkaista oikeussuojakeinoista ja täytäntöönpanotoimenpiteistä, jotka ovat olennaisen tärkeitä velvoitteiden tehokkaan täytäntöönpanon kannalta. Sen vuoksi direktiivi (EU) 2016/1148 olisi kumottava ja korvattava tällä direktiivillä.

(6) Kun direktiivi (EU) 2016/1148 kumotaan, toimialoittainen soveltamisala olisi laajennettava koskemaan suurempaa osaa taloudesta, jotta sen piiriin saadaan kaikki toimialat ja palvelut, jotka ovat elintärkeitä sisämarkkinoiden yhteiskunnallisten ja taloudellisten avaintoimintojen kannalta. Tällä direktiivillä pyritään erityisesti korjaamaan puutteet, jotka liittyvät keskeisten palvelujen tarjoajien ja digitaalisten palvelujen tarjoajien väliseen erotteluun, joka on osoittautunut vanhanaikaiseksi, koska se ei kuvasta toimialojen tai palvelujen merkitystä yhteiskunnalliselle ja taloudelliselle toiminnalle sisämarkkinoilla.

(7) Direktiivin (EU) 2016/1148 mukaan oli jäsenvaltioiden tehtävä määrittää toimijat, jotka täyttävät kriteerit, joiden perusteella niitä voidaan pitää keskeisten palvelujen tarjoajina. Jotta voidaan poistaa asiaan liittyvät jäsenvaltioiden väliset suuret erot ja varmistaa oikeusvarmuus kaikkien asianomaisten toimijoiden kyberturvallisuusriskien hallintatoimenpiteiden ja raportointivelvoitteiden osalta, olisi vahvistettava yhdenmukainen kriteeri, jolla määritetään tämän direktiivin soveltamisalaan kuuluvat toimijat. Kriteerinä olisi sovellettava enimmäiskokoa koskevaa sääntöä, jonka mukaan direktiivin soveltamisalaan kuuluvat kaikki toimijat, jotka täyttävät komission suosituksen 2003/361/EY ([5]) liitteessä olevan 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset tai jotka ylittävät kyseisen artiklan 1 kohdassa säädetyt keskisuurten yritysten määrittelyssä käytettävät kynnysarvot ja

([5]) 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).

jotka toimivat sellaisilla toimialoilla ja tarjoavat sellaisia palvelutyyppejä tai harjoittavat sellaista toimintaa, jotka kuuluvat tämän direktiivin soveltamisalaan. Jäsenvaltioiden olisi myös säädettävä, että tämän direktiivin soveltamisalaan kuuluvat sellaiset kyseisessä liitteessä olevan 2 artiklan 2 ja 3 kohdassa määritellyt pienet yritykset ja mikroyritykset, jotka täyttävät erityiset kriteerit, jotka osoittavat niiden olevan avainasemassa yhteiskunnassa, taloudessa tai tietyillä toimialoilla tai tietyissä palvelutyypeissä.

(8) Julkishallinnon toimijoista olisi jätettävä tämän direktiivin soveltamisalan ulkopuolelle ne, jotka harjoittavat toimintaa pääasiassa kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla, mukaan lukien rikosten ennalta estäminen, tutkiminen, paljastaminen ja rikoksiin liittyvät syytetoimet. Niitä julkishallinnon toimijoita, joiden toiminta liittyy vain marginaalisesti mainittuihin aloihin, ei kuitenkaan olisi jätettävä tämän direktiivin soveltamisalan ulkopuolelle. Tätä direktiiviä sovellettaessa sääntelyvaltaa käyttävien toimijoiden ei katsota harjoittavan toimintaa lainvalvonnan alalla, joten niitä ei kyseisellä perusteella jätetä tämän direktiivin soveltamisalan ulkopuolelle. Julkishallinnon toimijat, jotka on perustettu yhdessä kolmannen maan kanssa kansainvälisen sopimuksen mukaisesti, eivät kuulu tämän direktiivin soveltamisalaan. Tätä direktiiviä ei sovelleta jäsenvaltioiden kolmansissa maissa sijaitseviin diplomaattisiin edustustoihin ja konsuliedustustoihin tai näiden verkko- ja tietojärjestelmiin, siltä osin kuin tällaiset järjestelmät sijaitsevat edustuston tiloissa tai niitä ylläpidetään kolmannessa maassa olevia käyttäjiä varten.

(9) Jäsenvaltioiden olisi voitava toteuttaa tarvittavat toimenpiteet keskeisten kansalliseen turvallisuuteen liittyvien etujen suojaamiseksi, yleisen järjestyksen ja turvallisuuden takaamiseksi sekä rikosten ennalta estämisen, tutkimisen, paljastamisen ja rikoksiin liittyvien syytetoimien mahdollistamiseksi. Tätä varten jäsenvaltioiden olisi voitava vapauttaa erityiset toimijat, jotka harjoittavat toimintaa kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla, mukaan lukien rikosten ennalta estäminen, tutkiminen, paljastaminen ja rikoksiin liittyvät syytetoimet, tietyistä tässä direktiivissä säädetyistä velvoitteista mainituissa toiminnoissa. Jos toimija tarjoaa palveluja yksinomaan tämän direktiivin soveltamisalan kuulumattomalle julkishallinnon toimijalle, jäsenvaltioiden olisi voitava vapauttaa kyseinen toimija tässä direktiivissä säädetyistä velvoitteista mainituissa palveluissa. Mitään jäsenvaltiota ei myöskään pitäisi vaatia antamaan tietoja, joiden luovuttaminen olisi vastoin sen keskeisiä kansalliseen turvallisuuteen, yleiseen turvallisuuteen tai puolustukseen liittyviä etuja. Tässä yhteydessä olisi otettava huomioon turvallisuusluokiteltujen tietojen suojaamista koskevat unionin tai kansalliset säännöt, salassapitosopimukset ja epäviralliset salassapitosopimukset, kuten Traffic Light Protocol -käsittelyluokitus. Traffic Light Protocol -käsittelyluokitus on keino tiedottaa mahdollisista tietojen levittämiseen liittyvistä rajoituksista. Sitä käytetään lähes kaikissa tietoturvaloukkauksiin reagoivissa ja niitä tutkivissa yksiköissä (CSIRT) ja joissakin tietojen jakamisen ja analysoinnin keskuksissa.

(10) Vaikka tätä direktiiviä sovelletaan toimijoihin, jotka toteuttavat ydinvoimaloiden sähköntuotantoon liittyviä toimintoja, jotkin kyseisistä toiminnoista voivat liittyä kansalliseen turvallisuuteen. Jos näin on, jäsenvaltion olisi voitava perussopimusten mukaisesti kantaa vastuunsa kansallisen turvallisuuden takaamisesta näiden toimintojen osalta, mukaan lukien ydinenergia-alan arvoketjuun kuuluvat toiminnot.

(11) Jotkut toimijat toimivat kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla, mukaan lukien rikosten ennalta estäminen, tutkiminen, paljastaminen ja rikoksiin liittyvät syytetoimet, ja tarjoavat lisäksi luottamuspalveluja. Luottamuspalvelun tarjoajien, jotka kuuluvat Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 ([6]) soveltamisalaan, olisi kuuluttava tämän direktiivin soveltamisalaan, jotta voidaan varmistaa sama tietoturvavaatimusten ja valvonnan taso, josta on säädetty aiemmin kyseisessä asetuksessa luottamuspalvelun tarjoajien osalta. Samoin kuin tietyt erityispalvelut eivät kuulu asetuksen (EU) N:o 910/2014 soveltamisalaan, tätä direktiiviä ei pitäisi soveltaa sellaisten luottamuspalvelujen tarjoamiseen, joita käytetään yksinomaan kansallisesta oikeudesta tai määrätyn osallistujajoukon välisistä sopimuksista johtuvissa suljetuissa järjestelmissä.

([6]) 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).

(12) Euroopan parlamentin ja neuvoston direktiivissä 97/67/EY ([7]) määriteltyjen postipalvelujen tarjoajien, myös kuriiripalvelujen tarjoajien, olisi kuuluttava tämän direktiivin soveltamisalaan, jos ne tarjoavat vähintään yhden postiketjun vaiheista, erityisesti postilähetysten keräilyn, lajittelun, kuljetuksen tai jakelun, mukaan lukien noutopalvelut, ja ottaen huomioon, missä määrin ne ovat riippuvaisia verkko- ja tietojärjestelmistä. Kuljetuspalvelut, jotka eivät koske jotain mainituista vaiheista, olisi jätettävä postipalvelujen määritelmän ulkopuolelle.

(13) Koska kyberuhkat ovat yhä runsaslukuisempia ja kehittyneempiä, jäsenvaltioiden olisi pyrittävä varmistamaan, että tämän direktiivin soveltamisalaan kuulumattomat toimijat saavuttavat korkean tason kyberturvallisuudessa, ja tukemaan vastaavien kyberturvallisuusriskien hallintatoimenpiteiden täytäntöönpanoa, joissa otetaan huomioon kyseisten toimijoiden toiminnan arkaluonteisuus.

(14) Kaikkeen tämän direktiivin mukaiseen henkilötietojen käsittelyyn sovelletaan unionin tietosuojalainsäädäntöä ja yksityisyyden suojaa koskevaa unionin lainsäädäntöä. Tällä direktiivillä ei etenkään rajoiteta Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 ([8]) ja Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY ([9]) soveltamista. Tämä direktiivi ei sen vuoksi saisi vaikuttaa muun muassa niiden viranomaisten tehtäviin ja valtuuksiin, jotka ovat toimivaltaisia valvomaan sovellettavan unionin tietosuojalainsäädännön ja yksityisyyden suojaa koskevan unionin lainsäädännön noudattamista.

(15) Kyberturvallisuusriskien hallintatoimenpiteiden ja raportointivelvoitteiden noudattamista varten tämän direktiivin soveltamisalaan kuuluvat toimijat olisi luokiteltava kahteen luokkaan, keskeisiin toimijoihin ja tärkeisiin toimijoihin, sen mukaan, kuinka kriittisiä ne ovat alallaan tai tarjoamansa palvelutyypin tarjoajina sekä kokonsa mukaan. Tältä osin olisi tapauksen mukaan otettava asianmukaisesti huomioon mahdolliset merkitykselliset alakohtaiset riskinarvioinnit tai toimivaltaisten viranomaisten antama ohjeistus. Näiden kahden toimijaluokan valvonta- ja täytäntöönpanojärjestelmät olisi eriytettävä, jotta varmistetaan oikeudenmukainen tasapaino yhtäältä riskiperusteisten vaatimusten ja velvoitteiden ja toisaalta sääntöjen noudattamisen valvonnasta aiheutuvan hallinnollisen rasitteen välillä.

(16) Jottei toimijoita, joilla on omistusyhteysyrityksiä tai jotka ovat sidosyrityksiä, pidettäisi keskeisinä tai tärkeinä toimijoina tapauksissa, joissa se olisi suhteetonta, jäsenvaltiot voivat ottaa huomioon sen, kuinka riippumaton toimija on omistusyhteysyrityksistään tai sidosyrityksistään, sovellettaessa suosituksen 2003/361/EY liitteessä olevan 6 artiklan 2 kohtaa. Jäsenvaltiot voivat erityisesti ottaa huomioon sen seikan, että toimija ei ole riippuvainen omistusyhteys- tai sidosyrityksistään palvelujensa tarjoamiseen käyttämiensä verkko- ja tietojärjestelmien osalta ja tarjoamiensa palvelujen osalta. Tämän perusteella jäsenvaltiot voivat tarvittaessa katsoa, että tällainen toimija ei täytä suosituksen 2003/361/EY liitteessä olevan 2 artiklan mukaisia keskisuuria yrityksiä koskevia edellytyksiä tai että se ei ylitä kyseisen artiklan 1 kohdassa säädettyjä keskisuurten yritysten määrittelyssä käytettäviä kynnysarvoja, jos kyseisen toimijan ei olisi sen jälkeen, kun on otettu huomioon sen riippumattomuuden aste, katsottu täyttävän keskisuuria yrityksiä koskevia edellytyksiä tai ylittävän näitä kynnysarvoja, jos ainoastaan sen omat tiedot olisi otettu huomioon. Tämä ei vaikuta tämän direktiivin soveltamisalaan kuuluvien omistusyhteys- ja sidosyritysten tässä direktiivissä säädettyihin velvoitteisiin.

(17) Jäsenvaltioiden olisi voitava päättää, että ne toimijat, jotka on ennen tämän direktiivin voimaantuloa määritetty keskeisten palvelujen tarjoajiksi direktiivin (EU) 2016/1148 mukaisesti, on katsottava keskeisiksi toimijoiksi.

([7]) 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).

([8]) 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).

([9]) 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).

(18) Jotta voidaan saada selkeä yleiskuva tämän direktiivin soveltamisalaan kuuluvista toimijoista, jäsenvaltioiden olisi laadittava luettelo keskeisistä ja tärkeistä toimijoista sekä verkkotunnusten rekisteröintipalveluja tarjoavista toimijoista. Tätä varten jäsenvaltioiden olisi vaadittava toimijoita toimittamaan toimivaltaisille viranomaisille ainakin seuraavat tiedot: toimijan nimi, osoite ja ajantasaiset yhteystiedot, mukaan lukien toimijan sähköpostiosoitteet, IP-osoitealueet ja puhelinnumerot ja tapauksen mukaan asiaankuuluva toimiala ja toimialan osa liitteiden mukaisesti sekä tapauksen mukaan luettelo jäsenvaltioista, joissa ne tarjoavat tämän direktiivin soveltamisalaan kuuluvia palveluja. Tätä varten komission olisi Euroopan unionin kyberturvallisuusviraston (ENISA) avustuksella ilman aiheetonta viivytystä annettava ohjeita ja malleja tietojen toimittamisvelvoitteen täyttämiseksi. Keskeisten ja tärkeiden toimijoiden sekä verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden luettelon laatimisen ja ajantasaistamisen helpottamiseksi jäsenvaltioiden olisi voitava perustaa kansallisia järjestelyjä, joiden ansiosta toimijat voivat itse kirjautua luetteloon. Jos kansallisella tasolla on olemassa rekistereitä, jäsenvaltiot voivat päättää asianmukaisista järjestelyistä, joiden avulla voidaan tunnistaa tämän direktiivin soveltamisalaan kuuluvat toimijat.

(19) Jäsenvaltioiden olisi vastattava siitä, että komissiolle toimitetaan vähintään kunkin liitteissä mainitun toimialan ja toimialan osan keskeisten ja tärkeiden toimijoiden lukumäärä sekä asiaankuuluvat tiedot määritettyjen toimijoiden lukumäärästä ja siitä, mihin tämän direktiivin säännökseen kunkin toimijan määrittäminen perustuu, sekä niiden tarjoaman palvelun tyyppi. Jäsenvaltioita kannustetaan vaihtamaan komission kanssa tietoja keskeisistä ja tärkeistä toimijoista sekä laajamittaisen kyberturvallisuuspoikkeaman tapauksessa asiaankuuluvia tietoja, kuten asianomaisen toimijan nimi.

(20) Komission olisi yhteistyössä yhteistyöryhmän kanssa ja asianomaisia sidosryhmiä kuultuaan annettava ohjeita mikroyrityksiin ja pieniin yrityksiin sovellettavien kriteerien käytöstä sen arvioimisessa, kuuluvatko ne tämän direktiivin soveltamisalaan. Komission olisi myös varmistettava, että tämän direktiivin soveltamisalaan kuuluville mikroyrityksille ja pienille yrityksille annetaan asianmukaista ohjeistusta. Komission olisi jäsenvaltioiden avustuksella asetettava asiaa koskevia tietoja mikroyritysten ja pienten yritysten saataville.

(21) Komissio voisi antaa ohjeistusta avustaakseen jäsenvaltioita soveltamisalaa koskevien tämän direktiivin säännösten täytäntöönpanossa ja tämän direktiivin nojalla toteutettavien toimenpiteiden oikeasuhteisuuden arvioimisessa, erityisesti kun on kyse toimijoista, jotka kompleksisen liiketoimintamallinsa tai toimintaympäristönsä vuoksi voivat samanaikaisesti täyttää sekä keskeisille että tärkeille toimijoille asetetut kriteerit tai voivat samanaikaisesti harjoittaa toimintaa, josta osa kuuluu ja osa ei kuulu tämän direktiivin soveltamisalaan.

(22) Tässä direktiivissä vahvistetaan kyberturvallisuusriskien hallintatoimenpiteiden ja raportointivelvoitteiden perustaso kaikilla direktiivin soveltamisalaan kuuluvilla toimialoilla. Jos pidetään tarpeellisena antaa täydentäviä kyberturvallisuusriskien hallintatoimenpiteisiin ja raportointivelvoitteisiin liittyviä alakohtaisia unionin säädöksiä kyberturvallisuuden korkean tason varmistamiseksi kaikkialla unionissa, komission olisi arvioitava, voitaisiinko tällaisia täydentäviä säännöksiä antaa täytäntöönpanosäädöksessä tämän direktiivin nojalla, jotta vältetään unionin säädösten kyberturvallisuussäännösten hajanaisuus. Jos tällainen täytäntöönpanosäädös ei sovi tähän tarkoitukseen, alakohtaisilla unionin säädöksillä voitaisiin edistää kyberturvallisuuden korkean tason varmistamista kaikkialla unionissa, samalla kun otetaan kaikilta osin huomioon asianomaisten toimialojen erityispiirteet ja kompleksisuus. Siksi tämä direktiivi ei estä hyväksymästä täydentäviä alakohtaisia unionin säädöksiä, jotka koskevat kyberturvallisuusriskien hallintatoimenpiteitä ja raportointivelvoitteita ja joissa otetaan asianmukaisesti huomioon kattavan ja johdonmukaisen kyberturvallisuuskehyksen tarve. Tämä direktiivi ei vaikuta nykyiseen täytäntöönpanovaltaan, joka on siirretty komissiolle useilla aloilla, mukaan lukien liikenne ja energia.

(23) Jos alakohtaisessa unionin säädöksessä on säännöksiä, joissa keskeisiä tai tärkeitä toimijoita vaaditaan ottamaan käyttöön kyberturvallisuusriskien hallintatoimenpiteitä tai ilmoittamaan merkittävistä poikkeamista, ja jos kyseiset vaatimukset ovat vaikutukseltaan vähintään tässä direktiivissä säädettyjä velvoitteita vastaavia, tällaisiin toimijoihin

olisi sovellettava kyseisiä säännöksiä, mukaan lukien valvontaa ja täytäntöönpanoa koskevat säännökset. Jos alakohtainen unionin säädös ei kata tämän direktiivin soveltamisalaan kuuluvan tietyn toimialan kaikkia toimijoita, tämän direktiivin asiaankuuluvia säännöksiä olisi edelleen sovellettava niihin toimijoihin, joita mainittu säädös ei kata.

(24) Jos alakohtaisen unionin säädöksen säännöksissä vaaditaan keskeisiä tai tärkeitä toimijoita noudattamaan raportointivelvoitteita, jotka ovat vaikutukseltaan vähintään tässä direktiivissä säädettyjä raportointivelvoitteita vastaavia, olisi varmistettava poikkeamailmoitusten käsittelyn johdonmukaisuus ja tehokkuus. Tätä varten poikkeamista ilmoittamiseen liittyvissä alakohtaisen unionin säädöksen säännöksissä olisi annettava tämän direktiivin mukaisille CSIRT-yksiköille, toimivaltaisille viranomaisille tai kyberturvallisuusalan keskitetyille yhteyspisteille, jäljempänä 'keskitetty yhteyspiste', välitön pääsy alakohtaisen unionin säädöksen mukaisesti tehtyihin poikkeamailmoituksiin. Tällainen välitön pääsy voidaan varmistaa erityisesti, jos poikkeamailmoitukset toimitetaan ilman aiheetonta viivytystä eteenpäin tämän direktiivin mukaiselle CSIRT-yksikölle, toimivaltaiselle viranomaiselle tai keskitetylle yhteyspisteelle. Jäsenvaltioiden olisi tarvittaessa otettava käyttöön automaattinen ja suora raportointimekanismi, jolla varmistetaan tällaisten poikkeamailmoitusten käsittelyä koskevien tietojen järjestelmällinen ja välitön jakaminen CSIRT-yksiköiden, toimivaltaisten viranomaisten tai keskitettyjen yhteyspisteiden kanssa. Ilmoittamisen yksinkertaistamiseksi ja automaattisen ja suoran raportointimekanismin toteuttamiseksi jäsenvaltiot voisivat alakohtaisen unionin säädöksen mukaisesti käyttää keskitettyä asiointipistettä.

(25) Alakohtaisissa unionin säädöksissä, joissa säädetään kyberturvallisuusriskien hallintatoimenpiteistä tai raportointivelvoitteista, jotka ovat vaikutukseltaan vähintään tässä direktiivissä säädettyjä toimenpiteitä ja velvoitteita vastaavia, voitaisiin säätää, että tällaisten säädösten mukaiset toimivaltaiset viranomaiset käyttävät näiden toimenpiteiden tai velvoitteiden valvonta- ja täytäntöönpanovaltuuksiaan tämän direktiivin mukaisten toimivaltaisten viranomaisten avustuksella. Kyseiset toimivaltaiset viranomaiset voisivat perustaa yhteistyöjärjestelyjä tätä tarkoitusta varten. Tällaisissa yhteistyöjärjestelyissä voitaisiin täsmentää muun muassa valvontatoimien koordinointia koskevat menettelyt, mukaan lukien kansallisen lainsäädännön mukaiset tutkintamenettelyt ja paikalla tehtävät tarkastukset sekä järjestely valvontaa ja täytäntöönpanoa koskevien asiaankuuluvien tietojen vaihtamiseksi toimivaltaisten viranomaisten välillä, myös pääsy tämän direktiivin mukaisten toimivaltaisten viranomaisten pyytämiin kyberturvallisuustietoihin.

(26) Jos alakohtaisissa unionin säädöksissä vaaditaan toimijoita ilmoittamaan tai tarjotaan toimijoille kannustimia ilmoittaa merkittävistä kyberuhkista, jäsenvaltioiden olisi myös kannustettava merkittäviä kyberuhkia koskevien tietojen jakamiseen tämän direktiivin mukaisten CSIRT-yksiköiden, toimivaltaisten viranomaisten tai keskitettyjen yhteyspisteiden kanssa, jotta voidaan varmistaa kyseisten elinten parempi tietoisuus kyberuhkaympäristöstä ja antaa niille mahdollisuus reagoida tehokkaasti ja oikea-aikaisesti, jos merkittävät kyberuhkat toteutuvat.

(27) Tulevissa alakohtaisissa unionin säädöksissä olisi otettava asianmukaisesti huomioon tässä direktiivissä säädetyt määritelmät ja valvonta- ja täytäntöönpanokehys.

(28) Euroopan parlamentin ja neuvoston asetusta (EU) 2022/2554 ([10]) olisi pidettävä tähän direktiiviin liittyvänä alakohtaisena unionin säädöksenä finanssialan toimijoiden osalta. Asetuksen (EU) 2022/2554 säännöksiä, jotka koskevat tieto- ja viestintätekniikan (TVT) riskinhallintaa, TVT:hen liittyvien poikkeamien hallintaa ja erityisesti laajavaikutteisista TVT:hen liittyvistä poikkeamista raportointia, sekä sen säännöksiä digitaalisen häiriönsietokyvyn testauksesta, tiedonjakojärjestelyistä ja TVT-palveluntarjoajana oleviin kolmansiin osapuoliin liittyvistä riskeistä olisi sovellettava tämän direktiivin säännösten asemesta. Sen vuoksi jäsenvaltioiden ei pitäisi soveltaa tämän direktiivin säännöksiä, jotka koskevat kyberturvallisuusriskien hallintaa ja raportointivelvoitteita sekä valvontaa ja täytäntöönpanoa, asetuksen (EU) 2022/2554 soveltamisalaan kuuluviin finanssialan toimijoihin. Samalla tässä direktiivissä on tärkeää säilyttää vahva yhteys finanssialaan ja tietojenvaihto finanssialan kanssa. Tätä varten asetuksessa (EU) 2022/2554 annetaan Euroopan valvontaviranomaisille ja kyseisen asetuksen mukaisille toimivaltaisille viranomaisille mahdollisuus osallistua yhteistyöryhmän toimintaan sekä vaihtaa tietoja ja tehdä yhteistyötä keskitettyjen yhteyspisteiden sekä tämän direktiivin mukaisten CSIRT-yksiköiden ja toimivaltaisten viranomaisten kanssa. Asetuksen (EU) 2022/2554 mukaisten toimivaltaisten viranomaisten olisi myös toimitettava tiedot laajavaikutteisista TVT:hen liittyvistä poikkeamista ja tapauksen mukaan merkittävistä kyberuhkista tämän direktiivin mukaisille CSIRT-yksiköille, toimivaltaisille viranomaisille tai keskitetyille yhteyspisteille. Tämä voidaan

([10]) Euroopan parlamentin ja neuvoston asetus (EU) 2022/2554, annettu 14 päivänä joulukuuta 2022, finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU) N:o 600/2014, (EU) N:o 909/2014 ja (EU) 2016/1011 muuttamisesta (ks. tämän virallisen lehden s. 1).

toteuttaa tarjoamalla välitön pääsy poikkeamailmoituksiin ja toimittamalla ne eteenpäin joko suoraan tai poikkeamailmoituksia käsittelevän keskitetyn asiointipisteen kautta. Lisäksi jäsenvaltioiden olisi edelleen sisällytettävä finanssiala kyberturvallisuusstrategioihinsa, ja CSIRT-yksiköt voivat kattaa finanssialan toiminnassaan.

(29) Jotta vältetään ilmailualan toimijoille asetettujen kyberturvallisuusvelvoitteiden väliset puutteet ja päällekkäisyydet, Euroopan parlamentin ja neuvoston asetusten (EY) N:o 300/2008 ([11]) ja (EU) 2018/1139 ([12]) mukaisten kansallisten viranomaisten ja tämän direktiivin mukaisten toimivaltaisten viranomaisten olisi tehtävä yhteistyötä kyberturvallisuusriskien hallintatoimenpiteiden täytäntöönpanon ja näiden toimenpiteiden noudattamisen kansallisen tason valvonnan osalta. Jos toimija täyttää asetuksissa (EY) N:o 300/2008 ja (EU) 2018/1139 sekä niiden nojalla hyväksytyissä asiaankuuluvissa delegoiduissa säädöksissä ja täytäntöönpanosäädöksissä säädetyt turvallisuusvaatimukset, tämän direktiivin mukaiset toimivaltaiset viranomaiset voivat katsoa sen täyttävän tässä direktiivissä säädetyt vastaavat vaatimukset.

(30) Kyberturvallisuuden ja toimijoiden fyysisen turvallisuuden välisten yhteyksien vuoksi olisi varmistettava johdonmukainen lähestymistapa Euroopan parlamentin ja neuvoston direktiivin (EU) 2022/2557 ([13]) ja tämän direktiivin välillä. Tämän saavuttamiseksi direktiivin (EU) 2022/2557 nojalla kriittisiksi toimijoiksi määritettyjä toimijoita olisi pidettävä tämän direktiivin mukaisina keskeisinä toimijoina. Kunkin jäsenvaltion olisi myös varmistettava, että sen kansallinen kyberturvallisuusstrategia sisältää toimintakehyksen koordinoinnin tehostamiselle kyseisessä jäsenvaltioissa sen tämän direktiivin mukaisten toimivaltaisten viranomaisten ja direktiivin (EU) 2022/2557 mukaisten toimivaltaisten viranomaisten välillä, kun vaihdetaan tietoja riskeistä, kyberuhkista ja poikkeamista ja muista kuin kyberturvallisuuteen liittyvistä riskeistä, uhkista ja poikkeamista sekä hoidetaan valvontatehtäviä. Tämän direktiivin ja direktiivin (EU) 2022/2557 mukaisten toimivaltaisten viranomaisten olisi tehtävä yhteistyötä ja vaihdettava tietoja ilman aiheetonta viivytystä erityisesti kriittisten toimijoiden, riskien, kyberuhkien ja poikkeamien tunnistamisesta sekä kriittisiin toimijoihin vaikuttavista muista kuin kyberturvallisuuteen liittyvistä riskeistä, uhkista ja poikkeamista, mukaan lukien kriittisten toimijoiden toteuttamat kyberturvallisuustoimenpiteet ja fyysiset toimenpiteet sekä näitä toimijoita koskevien valvontatoimien tulokset.

Lisäksi jotta valvontatoimia voitaisiin virtaviivaistaa tämän direktiivin ja direktiivin (EU) 2022/2557 mukaisten toimivaltaisten viranomaisten kesken ja jotta asianomaisille toimijoille aiheutuva hallinnollinen rasite voitaisiin minimoida, kyseisten toimivaltaisten viranomaisten olisi pyrittävä yhdenmukaistamaan poikkeamailmoitusmallit ja valvontamenettelyt. Direktiivin (EU) 2022/2557 mukaisten toimivaltaisten viranomaisten olisi voitava tarvittaessa pyytää tämän direktiivin mukaisia toimivaltaisia viranomaisia käyttämään valvonta- ja täytäntöönpanovaltuuksiaan suhteessa toimijaan, joka on määritetty kriittiseksi toimijaksi direktiivin (EU) 2022/2557 nojalla. Tämän direktiivin ja direktiivin (EU) 2022/2557 mukaisten toimivaltaisten viranomaisten olisi tehtävä yhteistyötä ja vaihdettava tietoja, mahdollisuuksien mukaan reaaliaikaisesti, tätä tarkoitusta varten.

(31) Digitaalisen infrastruktuurin toimialan toimijoiden toiminta perustuu olennaisesti verkko- ja tietojärjestelmiin, joten kyseisille toimijoille tämän direktiivin nojalla asetetuilla velvoitteilla olisi varmistettava kattavasti kyseisten järjestelmien fyysinen turvallisuus osana toimijoiden kyberturvallisuusriskien hallintatoimenpiteitä ja raportointivelvoitteita. Koska näistä seikoista säädetään tässä direktiivissä, direktiivin (EU) 2022/2557 III, IV ja VI luvussa säädettyjä velvoitteita ei sovelleta näihin toimijoihin.

([11]) 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).

([12]) 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).

([13]) Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2557, annettu 14 päivänä joulukuuta 2022, kriittisten toimijoiden häiriönsietokyvystä ja neuvoston direktiivin 2008/114/EY kumoamisesta (ks. tämän virallisen lehden s. 164).

(32) Luotettavan, häiriönsietokykyisen ja turvallisen verkkotunnusjärjestelmän (DNS) ylläpitäminen ja säilyttäminen ovat keskeisiä tekijöitä internetin eheyden säilymisen kannalta ja olennaisen tärkeitä internetin jatkuvalle ja vakaalle toiminnalle, mistä koko digitaalitalous ja -yhteiskunta ovat riippuvaisia. Sen vuoksi tätä direktiiviä olisi sovellettava aluetunnusrekistereihin ja DNS-palveluntarjoajiin, jotka on ymmärrettävä toimijoiksi, jotka tarjoavat yleisesti saatavilla olevia rekursiivisia verkkotunnusten selvityspalveluja internetin loppukäyttäjille tai auktoritatiivisia verkkotunnusten selvityspalveluja kolmansille osapuolille. Tätä direktiiviä ei pitäisi soveltaa juurinimipalvelimiin.

(33) Pilvipalveluihin olisi luettava digitaaliset palvelut, jotka tarjoavat laajaan etäkäyttöön skaalattavan ja joustavan joukon jaettavissa olevia ja tarveperusteisesti ohjattavia tietoteknisiä resursseja, myös sijainniltaan hajautettuja resursseja. 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. Pilvipalvelujen 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 tarveperusteiseksi ohjaukseksi. Ilmaisua ’laaja etäkäyttö’ käytetään kuvaamaan sitä, että pilvipalveluresursseja tarjotaan verkossa ja niitä pääsee käyttämään erilaisten prosessointivalmiuksiltaan kevyiden tai raskaiden päätelaitteiden, kuten älypuhelinten, tablettitietokoneiden, kannettavien tietokoneiden ja työasemien, käytön mahdollistavien järjestelyjen ansiosta.

Ilmaisu ’skaalautuva’ viittaa tietoteknisiin resursseihin, joita pilvipalvelujen tarjoaja jakaa joustavasti resurssien maantieteellisestä sijainnista riippumatta kysynnän vaihtelun mukaan. Ilmaisua ’joustava joukko’ käytetään kuvaamaan tietoteknisiä resursseja, joita tarjotaan ja vapautetaan käyttöön kysynnän mukaan niin, että resursseja voidaan nopeasti lisätä ja vähentää kuormituksen perusteella. Ilmaisua ’jaettavissa oleva’ käytetään kuvaamaan tietoteknisiä resursseja, joita tarjotaan useille käyttäjille, joilla on yhteinen pääsy palveluun, jossa prosessointi on kuitenkin käyttäjäkohtaista, vaikka palvelu tarjotaan saman sähköisen laitteiston kautta. Ilmaisua ’hajautettu’ käytetään kuvaamaan tietoteknisiä resursseja, jotka sijaitsevat erillisissä verkotetuissa tietokoneissa tai laitteissa ja jotka viestivät ja koordinoivat toimintaansa keskenään rakenteisella viestinvaihdolla.

(34) Innovatiivisten teknologioiden ja uusien liiketoimintamallien myötä sisämarkkinoille odotetaan tulevan uusia pilvipalvelujen palvelu- ja toimintamalleja, joilla vastataan asiakkaiden muuttuviin tarpeisiin. Pilvipalveluja voidaan tarjota pitkälle hajautetussa muodossa ja entistä lähempänä paikkaa, jossa dataa tuotetaan tai kerätään, jolloin siirrytään perinteisestä mallista pitkälle hajautettuun malliin (reunalaskentamalli).

(35) Datakeskuspalvelujen tarjoajat eivät välttämättä aina tarjoa palvelujaan pilvipalveluna. Näin ollen datakeskukset eivät välttämättä aina ole osa pilvipalveluinfrastruktuuria. Kaikkien verkko- ja tietojärjestelmien turvallisuuteen kohdistuvien riskien hallitsemiseksi tämän direktiivin olisi siksi katettava 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. Ilmaisua ’datakeskuspalvelu’ ei pitäisi käyttää toimijan omistamista ja omiin sisäisiin käyttötarkoituksiinsa operoimista datakeskuksista.

(36) Tutkimustoiminnalla on keskeinen rooli uusien tuotteiden ja prosessien kehittämisessä. Monia näistä toiminnoista suorittavat toimijat, jotka jakavat, levittävät tai hyödyntävät tutkimustuloksiaan kaupallisiin tarkoituksiin. Nämä toimijat voivat näin ollen olla tärkeitä lenkkejä arvoketjuissa, minkä johdosta niiden verkko- ja tietojärjestelmien turvallisuus on erottamaton osa sisämarkkinoiden yleistä kyberturvallisuutta. Tutkimusorganisaatioihin olisi luettava toimijat, joiden toiminnasta olennainen osa on Taloudellisen yhteistyön ja kehityksen järjestön vuonna

2015 laaditussa, tutkimus- ja kehittämistoiminnan tietojen keräämis- ja raportointiohjeita koskevassa Frascati-käsikirjassa tarkoitettua soveltavaa tutkimusta tai kokeellista kehitystyötä, joiden tuloksia ne hyödyntävät kaupallisiin tarkoituksiin, kuten tuotteen valmistamiseen tai kehittämiseen tai prosessiin, palvelun tarjoamiseen tai sen markkinointiin.

(37) Kasvavat keskinäiset riippuvuussuhteet ovat tulosta yhä useammin rajatylittävästä ja keskinäisriippuvaisesta verkostosta, jossa käytetään eri puolilla unionia sijaitsevia keskeisiä infrastruktuureja palveluntarjontaan energian, liikenteen, digitaalisen infrastruktuurin, juoma- ja jäteveden, terveyden ja julkishallinnon tiettyjen näkökohtien kaltaisilla aloilla sekä avaruustoiminnassa siinä määrin kuin on kyse sellaisten palvelujen tarjoamisesta, jotka ovat riippuvaisia joko jäsenvaltioiden tai yksityisten osapuolten omistamasta, hallinnoimasta ja operoimasta maassa sijaitsevasta infrastruktuurista, mihin ei näin ollen lueta infrastruktuuria, jonka unioni omistaa tai jota se hallinnoi tai operoi tai jota hallinnoidaan tai operoidaan sen puolesta osana sen avaruusohjelmaa. Näiden keskinäisriippuvuuksien vuoksi kaikilla häiriöillä, vaikka ne alun perin rajoittuisivatkin yhteen toimijaan tai yhteen toimialaan, voi olla laajempi, ketjureaktiona etenevä vaikutus, joka saattaa johtaa kauaskantoisiin ja pitkäkestoisiin kielteisiin vaikutuksiin palvelujen tarjontaan sisämarkkinoilla. Covid-19-pandemian aikana lisääntyneet kyberhyökkäykset ovat osoittaneet yhä voimakkaammin keskinäisriippuvaisten yhteiskuntiemme haavoittuvuuden kohdatessamme alhaisen todennäköisyyden riskejä.

(38) Jotta voidaan ottaa huomioon kansallisten hallintorakenteiden erot ja säilyttää olemassa olevat alakohtaiset järjestelyt tai unionin valvonta- ja sääntelyelimet, jäsenvaltioiden olisi voitava nimetä tai perustaa yksi tai useampi toimivaltainen viranomainen, joka vastaa kyberturvallisuudesta ja tämän direktiivin mukaisista valvontatehtävistä.

(39) Viranomaisten välisen rajatylittävän yhteistyön ja viestinnän helpottamiseksi ja tämän direktiivin tehokkaan täytäntöönpanon mahdollistamiseksi kunkin jäsenvaltion olisi nimettävä keskitetty yhteyspiste, joka vastaa verkko- ja tietojärjestelmien turvallisuuteen ja rajatylittävään yhteistyöhön liittyvien kysymysten koordinoinnista unionin tasolla.

(40) Keskitettyjen yhteyspisteiden olisi varmistettava tehokas rajatylittävä yhteistyö muiden jäsenvaltioiden asiaankuuluvien viranomaisten ja tarvittaessa komission ja ENISAn kanssa. Keskitetyille yhteyspisteille olisi sen vuoksi annettava tehtäväksi toimittaa ilmoitukset merkittävistä poikkeamista, joilla on rajatylittäviä vaikutuksia, eteenpäin niiden muiden jäsenvaltioiden keskitetyille yhteyspisteille, joihin poikkeama vaikuttaa, CSIRT-yksikön tai toimivaltaisen viranomaisen pyynnöstä. Kansallisella tasolla keskitettyjen yhteyspisteiden olisi mahdollistettava sujuva toimialarajat ylittävä yhteistyö muiden toimivaltaisten viranomaisten kanssa. Keskitetyt yhteyspisteet voisivat myös olla asetuksen (EU) 2022/2554 mukaisten toimivaltaisten viranomaisten toimittamien, finanssialan yhteisöjä koskevia poikkeamia koskevien asiaankuuluvien tietojen vastaanottajia, ja niiden olisi voitava tarvittaessa toimittaa nämä tiedot eteenpäin tämän direktiivin mukaisille CSIRT-yksiköille tai toimivaltaisille viranomaisille.

(41) Jäsenvaltioilla olisi oltava käytössään riittävät sekä tekniset että organisatoriset valmiudet, jotta voidaan ehkäistä, havaita ja hallita poikkeamia ja riskejä sekä lieventää niiden vaikutuksia. Jäsenvaltioiden olisi sen vuoksi perustettava tai nimettävä yksi tai useampi tämän direktiivin mukainen CSIRT-yksikkö ja varmistettava, että niillä on riittävät resurssit ja tarvittavat tekniset valmiudet. CSIRT-yksiköiden olisi täytettävä tässä direktiivissä säädetyt vaatimukset, jotta voidaan taata tehokkaat ja yhteensopivat valmiudet käsitellä poikkeamia ja riskejä ja varmistaa tehokas yhteistyö unionin tasolla. Jäsenvaltioiden olisi voitavat nimetä CSIRT-yksiköiksi olemassa olevia tietotekniikan kriisiryhmiä (CERT). Toimijoiden ja CSIRT-yksiköiden välisen luottamuksen lujittamiseksi tapauksissa, joissa CSIRT on osa toimivaltaista viranomaista, jäsenvaltioiden olisi voitava harkita CSIRT-yksiköiden operatiivisten tehtävien, erityisesti tietojen jakamisen ja toimijoille annettavan tuen, erottamista toiminnallisesti toimivaltaisten viranomaisten valvontatoimista.

(42) CSIRT-yksiköille annetaan tehtäväksi poikkeamien käsittely. Tämä edellyttää suurten tietomäärien käsittelyä, ja nämä tiedot ovat toisinaan arkaluonteisia. Jäsenvaltioiden olisi varmistettava, että CSIRT-yksiköillä on infrastruktuuri tietojen jakamiseen ja käsittelyyn sekä hyvin varustettu henkilöstö, jotta voidaan varmistaa näiden yksiköiden toimintojen luottamuksellisuus ja luotettavuus. CSIRT-yksiköt voivat myös hyväksyä asiaa koskevia käytännesääntöjä.

(43) Henkilötietojen osalta CSIRT-yksiköiden olisi voitava tarjota asetuksen (EU) 2016/679 mukaisesti keskeisen tai tärkeän toimijan pyynnöstä niiden verkko- ja tietojärjestelmien ennakoiva skannaus, joita kyseinen toimija käyttää palvelujensa tarjoamiseen. Jäsenvaltioiden olisi tapauksen mukaan pyrittävä varmistamaan, että kaikilla toimialakohtaisilla CSIRT-yksiköillä on yhtäläiset tekniset valmiudet. Jäsenvaltioiden olisi voitava pyytää ENISAa avustamaan CSIRT-yksiköidensä kehittämisessä.

(44) CSIRT-yksiköiden olisi voitava keskeisen tai tärkeän toimijan pyynnöstä seurata toimijan internetiin yhteydessä olevia resursseja sekä tämän toimitiloissa että niiden ulkopuolella, jotta voidaan tunnistaa, ymmärtää ja hallita toimijan yleisiä organisaatioriskejä, jotka liittyvät äskettäin havaittuihin toimitusketjun vaarantumisiin tai kriittisiin haavoittuvuuksiin. Toimijaa olisi kannustettava ilmoittamaan CSIRT-yksikölle, onko sillä käytössä etuoikeutettu hallintarajapinta, koska tämä voi vaikuttaa siihen, miten nopeasti lieventäviä toimia voidaan toteuttaa.

(45) Kun otetaan huomioon kyberturvallisuutta koskevan kansainvälisen yhteistyön tärkeys, CSIRT-yksiköiden olisi voitava osallistua kansainvälisiin yhteistyöverkostoihin tällä direktiivillä perustettavan CSIRT-verkoston lisäksi. Sen vuoksi CSIRT-yksiköiden ja toimivaltaisten viranomaisten olisi voitava tehtäviensä suorittamiseksi vaihtaa tietoja, myös henkilötietoja, kolmansien maiden tietoturvaloukkauksiin reagoivien ja niitä tutkivien kansallisten yksiköiden tai toimivaltaisten viranomaisten kanssa edellyttäen, että unionin tietosuojalainsäädännön mukaiset edellytykset henkilötietojen siirrolle kolmansiin maihin, muun muassa asetuksen (EU) 2016/679 49 artiklassa säädetyt edellytykset, täyttyvät.

(46) On olennaisen tärkeää varmistaa riittävät resurssit tämän direktiivin tavoitteiden saavuttamiseksi ja sen mahdollistamiseksi, että toimivaltaiset viranomaiset ja CSIRT-yksiköt voivat suorittaa tässä säädetyt tehtävänsä. Jäsenvaltiot voivat ottaa kansallisella tasolla käyttöön rahoitusmekanismin, jolla katetaan tarpeelliset menot, jotka liittyvät kyberturvallisuudesta jäsenvaltiossa tämän direktiivin nojalla vastaavien julkisten toimijoiden tehtävien hoitamiseen. Tällaisen mekanismin olisi oltava unionin oikeuden mukainen, sen olisi oltava oikeasuhteinen ja syrjimätön, ja siinä olisi otettava huomioon erilaiset lähestymistavat turvallisten palvelujen tarjoamiseen.

(47) CSIRT-verkoston olisi jatkossakin edistettävä luottamuksen vahvistumista sekä ripeää ja toimivaa operatiivista yhteistyötä jäsenvaltioiden välillä. Unionin tason operatiivisen yhteistyön parantamiseksi CSIRT-verkoston olisi harkittava kyberturvallisuuspolitiikkaan osallistuvien unionin elinten ja virastojen, kuten Europolin, kutsumista osallistumaan sen työhön.

(48) Kyberturvallisuuden korkean tason saavuttamiseksi ja ylläpitämiseksi tässä direktiivissä edellytettävien kansallisten kyberturvallisuusstrategioiden olisi sisällettävä yhtenäinen kehys, jossa määritetään kyberturvallisuutta koskevat strategiset tavoitteet ja painopisteet ja hallintokehys niiden saavuttamiseksi. Nämä strategiat voivat koostua yhdestä tai useammasta lainsäädännöllisestä tai muusta välineestä.

(49) Kyberhygieniaperiaatteet laskevat perustan toimille, joilla suojataan verkko- ja tietojärjestelmien infrastruktuuri, laitteistojen, ohjelmistojen ja verkkosovellusten turvallisuus sekä yritys- tai loppukäyttäjätiedot, joita toimijat hyödyntävät. Kyberhygieniaperiaatteet, joihin kuuluvat yhteiset perustason käytännöt, kuten ohjelmisto- ja laitteistopäivitykset, salasanojen vaihtaminen, uusien asennusten hallinta, ylläpitäjän käyttöoikeuksia edellyttävien tilien rajoittaminen ja tietojen varmuuskopiointi, tarjoavat ennakoivan kehyksen, jossa varautua poikkeamiin ja kyberuhkiin ja varmistaa yleinen turvallisuus niiden toteutuessa. ENISAn olisi seurattava ja analysoitava jäsenvaltioiden kyberhygieniaperiaatteita.

(50) Kyberturvallisuustietoisuus ja kyberhygienia ovat olennaisen tärkeitä kyberturvallisuuden tason nostamiseksi unionissa, etenkin kun verkkoon liitettyjä laitteita on yhä enemmän ja niitä käytetään yhä useammin kyberhyökkäyksissä. Yleistä tietoisuutta tällaisiin laitteisiin liittyvistä riskeistä olisi pyrittävä lisäämään, ja unionin tason arvioinnit voisivat auttaa varmistamaan, että nämä riskit tiedostetaan yleisesti sisämarkkinoilla.

(51) Jäsenvaltioiden olisi kannustettava käyttämään mitä tahansa innovatiivista teknologiaa, myös tekoälyä, jonka käyttö voisi parantaa kyberhyökkäysten havaitsemista ja ehkäisemistä ja mahdollistaa resurssien tehokkaamman kohdentamisen kyberhyökkäyksiin. Jäsenvaltioiden olisi sen vuoksi edistettävä kansallisissa kyberturvallisuusstrategioissaan tutkimus- ja kehitystoimia, joilla helpotetaan tällaisten teknologioiden, erityisesti automatisoituihin tai puoliautomaattisiin kyberturvallisuustyökaluihin liittyvien teknologioiden, käyttöä sekä tarvittaessa tällaisen teknologian käyttäjien kouluttamiseen ja sen parantamiseen tarvittavien tietojen jakamista. Käytettäessä mitä tahansa innovatiivista teknologiaa, myös tekoälyä, olisi noudatettava unionin tietosuojalainsäädäntöä ja tietosuojaperiaatteita, joita ovat tietojen täsmällisyys, tietojen minimointi, asianmukaisuus ja läpinäkyvyys, ja varmistettava tietoturva, esimerkiksi viimeisintä kehitystä edustavan salaustekniikan käyttäminen. Asetuksessa (EU) 2016/679 vahvistettuja sisäänrakennetun ja oletusarvoisen tietosuojan vaatimuksia olisi hyödynnettävä täysimääräisesti.

(52) Avoimen lähdekoodin kyberturvallisuustyökalut ja -sovellukset voivat osaltaan lisätä avoimuutta, ja niillä voi olla myönteinen vaikutus teollisen innovoinnin tehokkuuteen. Avoimet standardit helpottavat turvallisuustyökalujen yhteentoimivuutta, mikä edistää teollisuuden sidosryhmien turvallisuutta. Avoimen lähdekoodin kyberturvallisuustyökaluissa ja -sovelluksissa voidaan hyödyntää laajempaa kehittäjäyhteisöä, minkä ansiosta toimijat voivat monipuolistaa toimittajapohjaansa. Avoimen lähdekoodin käyttö voi tehdä kyberturvallisuustyökalujen varmennusprosessista läpinäkyvämmän ja haavoittuvuuksien havaitsemisesta yhteisövetoista. Jäsenvaltioiden olisi siksi voitava edistää avoimen lähdekoodin ohjelmistojen ja avointen standardien käyttöä toimintaperiaatteilla, jotka liittyvät avoimen datan ja avoimen lähdekoodin käyttöön osana avoimuuteen perustuvaa turvallisuutta. Toimintaperiaatteet, joilla edistetään avoimen lähdekoodin kyberturvallisuustyökalujen käyttöönottoa ja kestävää käyttöä, ovat erityisen tärkeitä pienille ja keskisuurille yrityksille, joille täytäntöönpanosta aiheutuu huomattavia kustannuksia, jotka voitaisiin minimoida vähentämällä erityisten sovellusten tai työkalujen tarvetta.

(53) Julkiset laitokset liitetään kaupungeissa yhä useammin digitaalisiin verkkoihin, jotta voidaan parantaa kaupunkiliikenneverkkoja, vesihuoltoa ja jätehuoltoa sekä tehostaa valaistusta ja rakennusten lämmitystä. Nämä digitalisoidut laitokset ovat alttiita kyberhyökkäyksille ja saattavat kyberhyökkäyksen onnistuessa aiheuttaa kansalaisille suuren mittakaavan haittaa keskinäisten yhteyksiensä vuoksi. Jäsenvaltioiden olisi kehitettävä kansallisessa kyberturvallisuusstrategiassaan toimintaperiaatteita, joilla käsitellään tällaisten verkkoon liitettyjen eli älykkäiden kaupunkien kehittymistä ja niiden mahdollisia vaikutuksia yhteiskuntaan.

(54) Kiristyshaittaohjelmahyökkäykset, joissa haittaohjelma salaa tietoja ja järjestelmiä ja vaatii lunnaita salauksen purkamisesta, ovat viime vuosina lisääntyneet unionissa räjähdysmäisesti. Kiristyshaittaohjelmahyökkäysten esiintymistiheyttä ja vakavuutta voivat lisätä useat tekijät, kuten erilaiset hyökkäyskuviot, ”kiristyshaittaohjelma-palveluun” ja kryptovaluuttoihin liittyvät rikolliset liiketoimintamallit, lunnasvaatimukset ja toimitusketjuun kohdistuvien hyökkäysten yleistyminen. Jäsenvaltioiden olisi kehitettävä kansallisissa kyberturvallisuusstrategioissaan toimintaperiaatteet, joilla puututaan kiristyshaittaohjelmahyökkäysten lisääntymiseen.

(55) Julkisen ja yksityisen sektorin kyberturvallisuusalan kumppanuudet voivat tarjota tarkoituksenmukaiset puitteet osaamisen vaihdolle, parhaiden käytäntöjen jakamiselle ja yleisen tietoisuuden lisäämiselle sidosryhmien keskuudessa. Jäsenvaltioiden olisi edistettävä toimintaperiaatteita, joilla tuetaan julkisen ja yksityisen sektorin kyberturvallisuuskumppanuuksien perustamista. Näissä toimintaperiaatteissa olisi selvennettävä muun muassa soveltamisala, mukana olevat sidosryhmät, hallintomalli, käytettävissä olevat rahoitusvaihtoehdot ja osallistuvien sidosryhmien vuorovaikutus julkisen ja yksityisen sektorin kumppanuuksien kanssa. Julkisen ja yksityisen sektorin kumppanuudet voivat hyödyntää yksityisen sektorin toimijoiden asiantuntemusta auttaakseen toimivaltaisia viranomaisia kehittämään viimeisintä kehitystä edustavia palveluja ja prosesseja, muun muassa tietojenvaihdon, ennakkovaroitusten, kyberuhka- ja poikkeamaharjoitusten, kriisinhallinnan ja resilienssisuunnittelun aloilla.

(56) Jäsenvaltioiden olisi käsiteltävä kansallisissa kyberturvallisuusstrategioissaan pienten ja keskisuurten yritysten erityisiä kyberturvallisuustarpeita. Pienten ja keskisuurten yritysten prosenttiosuus teollisen ja liiketoiminnan markkinoilla on suuri eri puolilla unionia, ja niillä on usein vaikeuksia mukautua uusiin liiketoimintakäytäntöihin yhä tiiviimpien yhteyksien maailmassa ja digitaaliseen toimintaympäristöön, jossa työntekijät työskentelevät kotoa käsin ja liiketoimintaa harjoitetaan yhä enemmän verkossa. Joillakin pienillä ja keskisuurilla yrityksillä on erityisiä kyberturvallisuushaasteita, kuten vähäinen kybertietoisuus, etätietoturvan puuttuminen, kyberturvallisuusratkaisujen korkeat kustannukset ja esimerkiksi kiristyshaittaohjelmista johtuva kohonnut uhkataso, minkä takia niiden olisi saatava ohjausta ja tukea. Pienet ja keskisuuret yritykset joutuvat yhä useammin toimitusketjuun kohdistuvien hyökkäysten kohteeksi, koska niiden kyberturvallisuusriskien hallintatoimenpiteet ja kyberhyökkäysten hallinta eivät ole yhtä kehittyneitä ja koska niillä on rajalliset turvallisuusresurssit. Tällaiset toimitusketjuun kohdistuvat hyökkäykset vaikuttavat yksittäisiin pieniin ja keskisuuriin yrityksiin ja niiden toimintoihin, mutta ne voivat myös laajentua ketjureaktiona sellaisiin toimijoihin kohdistuviksi hyökkäyksiksi,

joiden toimittajia yritykset ovat. Jäsenvaltioiden olisi kansallisten kyberturvallisuusstrategioidensa välityksellä autettava pieniä ja keskisuuria yrityksiä vastaamaan toimitusketjujensa haasteisiin. Jäsenvaltioilla olisi oltava pieniä ja keskisuuria yrityksiä kansallisella tai alueellisella tasolla palveleva yhteyspiste, joka joko antaa ohjausta ja tukea pienille ja keskisuurille yrityksille tai ohjaa ne ottamaan yhteyttä asianmukaisiin elimiin, jotka antavat ohjausta ja tukea kyberturvallisuuteen liittyvissä kysymyksissä. Jäsenvaltioita kannustetaan myös tarjoamaan sellaisia palveluja kuin verkkosivuston konfigurointi ja lokikirjanpidon aktivointi mikroyrityksille ja pienille yrityksille, joilta puuttuvat tällaiset valmiudet.

(57) Jäsenvaltioiden olisi otettava kansallisissa kyberturvallisuusstrategioissaan käyttöön toimintaperiaatteita, jotka koskevat aktiivisen kybersuojauksen edistämistä osana laajempaa puolustusstrategiaa. Reaktiivisen reagoinnin vastakohtana aktiivisella kybersuojauksella tarkoitetaan verkon tietoturvaloukkausten aktiivista ehkäisemistä, havaitsemista, seurantaa, analysointia ja lieventämistä, joihin yhdistyy valmiuksien käyttö hyökkäyksen uhriksi joutuneessa verkossa ja sen ulkopuolella. Tähän voisivat kuulua jäsenvaltioiden tietyille toimijoille maksutta tarjoamat palvelut tai työkalut, mukaan lukien itsepalveluna tehtävät tarkastukset, havaitsemisvälineet ja poistopalvelut. Kyky jakaa ja ymmärtää nopeasti ja automaattisesti uhkatietoja ja -analyyseja, kyberaktiivisuushälytyksiä ja hallintatoimia on ratkaisevan tärkeä, jotta mahdollistetaan toimien yhtenäisyys verkko- ja tietojärjestelmiin kohdistuvien hyökkäysten onnistunutta ehkäisemistä, havaitsemista, käsittelyä ja estämistä varten. Aktiivinen kybersuojaus perustuu puolustusstrategiaan, johon ei sisälly hyökkääviä toimenpiteitä.

(58) Koska verkko- ja tietojärjestelmien haavoittuvuuksien hyödyntäminen voi aiheuttaa merkittäviä häiriöitä ja haittoja, tällaisten haavoittuvuuksien nopea tunnistaminen ja korjaaminen on tärkeä tekijä riskin vähentämisessä. Verkko- ja tietojärjestelmiä kehittävien tai hallinnoivien toimijoiden olisi sen vuoksi otettava käyttöön asianmukaiset menettelyt haavoittuvuuksien käsittelemiseksi, kun niitä havaitaan. Koska haavoittuvuuksia havaitsevat ja julkistavat usein kolmannet osapuolet, TVT-tuotteiden valmistajan tai TVT-palvelujen 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 julkistamisesta. On erityisen tärkeää lujittaa toimien koordinointia raportoivien luonnollisten henkilöiden ja oikeushenkilöiden ja TVT-tuotteiden tai TVT-palvelujen valmistajien tai tarjoajien välillä, jotta voidaan edistää haavoittuvuuksien julkistamisen vapaaehtoista kehystä. Koordinoitu haavoittuvuuksien julkistaminen on jäsennelty prosessi, jossa haavoittuvuuksista ilmoitetaan mahdollisesti haavoittuvien TVT-tuotteiden tai TVT-palvelujen valmistajalle tai tarjoajalle, jotta se voi diagnosoida haavoittuvuuden ja korjata sen ennen kuin yksityiskohtaiset haavoittuvuustiedot julkistetaan kolmansille osapuolille tai yleisölle. Koordinoituun haavoittuvuuksien julkistamiseen olisi kuuluttava myös haavoittuvuuksien korjaamisen ja julkistamisen aikataulua koskeva raportoivan luonnollisen henkilön tai oikeushenkilön ja mahdollisesti haavoittuvien TVT-tuotteiden tai TVT-palvelujen valmistajan tai tarjoajan välinen yhteensovittaminen.

(59) Komission, ENISAn ja jäsenvaltioiden olisi edelleen edistettävä mukautumista kansainvälisiin standardeihin ja toimialan nykyisiin parhaisiin käytäntöihin kyberturvallisuusriskien hallinnan alalla, esimerkiksi toimitusketjujen turvallisuusarvioinneissa, tietojenvaihdossa ja haavoittuvuuksien julkistamisessa.

(60) Jäsenvaltioiden olisi yhteistyössä ENISAn kanssa toteutettava toimenpiteitä koordinoidun haavoittuvuuksien julkistamisen helpottamiseksi laatimalla asiaa koskevat kansalliset toimintaperiaatteet. Jäsenvaltioiden olisi kansallisissa toimintaperiaatteissaan pyrittävä mahdollisuuksien mukaan ratkaisemaan haavoittuvuuksia tutkivien kohtaamat haasteet, myös rikosoikeudelliseen vastuuseen joutumisen mahdollisuus, kansallisen lainsäädäntönsä mukaisesti. Koska haavoittuvuuksia tutkivat luonnolliset henkilöt ja oikeushenkilöt voisivat joissakin jäsenvaltioissa joutua rikosoikeudelliseen ja siviilioikeudelliseen vastuuseen, jäsenvaltioita kannustetaan antamaan ohjeita tietoturvaa tutkivien syyttämättä jättämisestä ja vapauttamisesta siviilioikeudellisesta vastuusta niiden toiminnan osalta.

(61) Jäsenvaltioiden olisi nimettävä yksi CSIRT-yksiköistään koordinaattoriksi, joka toimii tarvittaessa luotettuna välittäjänä raportoivien luonnollisten henkilöiden tai oikeushenkilöiden ja sellaisten TVT-tuotteiden tai TVT-palvelujen valmistajien tai tarjoajien, joihin haavoittuvuus todennäköisesti vaikuttaa, välillä. Koordinaattoriksi nimetyn CSIRT-yksikön tehtäviin olisi kuuluttava asianomaisten toimijoiden tunnistaminen ja yhteyden ottaminen niihin, haavoittuvuudesta ilmoittavien luonnollisten henkilöiden tai oikeushenkilöiden avustaminen, julkistamisen

aikataulusta neuvotteleminen ja useisiin toimijoihin vaikuttavien haavoittuvuuksien hallinta (monenvälinen koordinoitu haavoittuvuuden julkistaminen). Jos ilmoitetulla haavoittuvuudella voi olla merkittävä vaikutus useamman kuin yhden jäsenvaltion toimijoihin, koordinaattoriksi nimettyjen CSIRT-yksiköiden olisi tarvittaessa tehtävä yhteistyötä CSIRT-verkostossa.

(62) Nopea paikkansapitävien tietojen saanti TVT-tuotteisiin ja TVT-palveluihin vaikuttavista haavoittuvuuksista parantaa kyberturvallisuusriskien hallintaa. Julkisesti saatavilla olevat haavoittuvuuksia koskevat tietolähteet ovat tärkeä apuväline toimijoille ja niiden palvelujen käyttäjille mutta myös toimivaltaisille viranomaisille ja CSIRT-yksiköille. Tästä syystä ENISAn olisi perustettava Euroopan haavoittuvuustietokanta, johon toimijat riippumatta siitä, kuuluvatko ne tämän direktiivin soveltamisalaan, ja niiden verkko- ja tietojärjestelmien toimittajat sekä toimivaltaiset viranomaiset ja CSIRT-yksiköt voivat vapaaehtoisesti ilmoittaa ja kirjata julkisesti tiedossa olevia haavoittuvuuksia, jotta käyttäjät voivat toteuttaa asianmukaisia lieventäviä toimenpiteitä. Tietokannan tarkoituksena on ratkoa riskien unionin toimijoille aiheuttamia ainutlaatuisia haasteita. ENISAn olisi lisäksi otettava käyttöön julkistamisprosessia koskeva asianmukainen menettely, jotta toimijoilla on aikaa toteuttaa haavoittuvuuksiaan lieventäviä toimenpiteitä, ja sovellettava viimeisintä kehitystä edustavia kyberturvallisuusriskien hallintatoimenpiteitä sekä käytettävä koneluettavia tietoaineistoja ja vastaavia rajapintoja. Jotta voidaan edistää toimintakulttuuria, jossa haavoittuvuudet julkistetaan, julkistamisesta ei saisi aiheutua haittaa raportoivalle luonnolliselle henkilölle tai oikeushenkilölle.

(63) Vaikka vastaavia haavoittuvuusrekistereitä tai -tietokantoja on olemassa, niitä hallinnoivat ja ylläpitävät tahot, jotka eivät ole sijoittautuneet unioniin. ENISAn ylläpitämä Euroopan haavoittuvuustietokanta lisäisi julkistamisprosessin läpinäkyvyyttä ennen haavoittuvuuden julkistamista yleisölle ja häiriönsietokykyä tilanteissa, joissa samankaltaisten palvelujen tarjonta häiriintyy tai keskeytyy. Jotta voidaan mahdollisimman pitkälle välttää toimien päällekkäisyyttä ja lisätä täydentävyyttä, ENISAn olisi tutkittava mahdollisuutta tehdä sopimuksia jäsennellystä yhteistyöstä kolmannen maan lainkäyttövaltaan kuuluvien vastaavien rekisterien tai tietokantojen kanssa. ENISAn olisi erityisesti tutkittava mahdollisuutta tehdä tiivistä yhteistyötä CVE-järjestelmän (Common Vulnerabilities and Exposures, tunnetut haavoittuvuudet ja tietoturvapuutteet) ylläpitäjien kanssa.

(64) Yhteistyöryhmän olisi tuettava ja helpotettava strategista yhteistyötä ja tietojenvaihtoa sekä vahvistettava jäsenvaltioiden keskinäistä luottamusta. Yhteistyöryhmän olisi laadittava joka toinen vuosi työohjelma. Työohjelman olisi sisällettävä toimet, jotka yhteistyöryhmän on määrä toteuttaa tavoitteidensa saavuttamiseksi ja tehtäviensä hoitamiseksi. Tämän direktiivin mukaisen ensimmäisen työohjelman aikataulu olisi sovitettava direktiivin (EU) 2016/1148 mukaisesti laaditun viimeisen työohjelman aikatauluun, jotta vältetään mahdolliset häiriöt yhteistyöryhmän työssä.

(65) Laatiessaan ohjeasiakirjoja yhteistyöryhmän olisi säännönmukaisesti kartoitettava kansallisia ratkaisuja ja kokemuksia, arvioitava yhteistyöryhmän tulosten vaikutusta kansallisiin lähestymistapoihin, keskusteltava täytäntöönpanon haasteista ja laadittava erityisiä suosituksia etenkin siitä, miten voidaan helpottaa tämän direktiivin yhdenmukaista saattamista osaksi kansallista lainsäädäntöä jäsenvaltioissa, olemassa olevien sääntöjen täytäntöönpanon parantamiseksi. Yhteistyöryhmä voisi myös kartoittaa kansalliset ratkaisut edistääkseen kullakin toimialalla eri puolilla unionia sovellettavien kyberturvallisuusratkaisujen yhteensopivuutta. Tämä koskee varsinkin toimialoja, joilla toiminta on kansainvälistä tai rajatylittävää.

(66) Yhteistyöryhmän olisi pysyttävä joustavana foorumina, ja sen olisi voitava reagoida muuttuviin ja uusiin poliittisiin painopisteisiin ja haasteisiin ottaen samalla huomioon käytettävissä olevat resurssit. Se voisi järjestää eri puolilta unionia tulevien asiaankuuluvien yksityisten sidosryhmien kanssa säännöllisiä yhteisiä kokouksia, joissa keskusteltaisiin yhteistyöryhmän toteuttamista toimista ja kerättäisiin tietoja ja näkemyksiä uusista toimintapoliittisista haasteista. Lisäksi yhteistyöryhmän olisi esitettävä säännöllisesti tilannearvio kyberuhkista tai poikkeamista, kuten kiristyshaittaohjelmista. Unionin tason yhteistyön tehostamiseksi yhteistyöryhmän olisi harkittava kyberturvallisuuspolitiikkaan osallistuvien asiaankuuluvien unionin toimielinten, elinten, laitosten ja

virastojen, kuten Euroopan parlamentin, Europolin, Euroopan tietosuojaneuvoston, asetuksella (EU) 2018/1139 perustetun Euroopan unionin lentoturvallisuusviraston ja Euroopan parlamentin ja neuvoston asetuksella (EU) 2021/696 ([14]) perustetun Euroopan unionin avaruusohjelmaviraston, kutsumista osallistumaan sen työhön.

(67) Jäsenvaltioiden keskinäisen yhteistyön parantamiseksi ja luottamuksen lujittamiseksi toimivaltaisten viranomaisten ja CSIRT-yksiköiden olisi voitava osallistua muiden jäsenvaltioiden virkamiesvaihtojärjestelmiin erityisjärjestelyjen mukaisesti ja kun tällaisiin vaihtojärjestelmiin osallistuville virkamiehille on tarpeen mukaan tehty vaadittava turvallisuusselvitys. Toimivaltaisten viranomaisten olisi toteutettava tarvittavat toimenpiteet, jotta muiden jäsenvaltioiden virkamiehet voivat tuloksekkaasti osallistua vastaanottavan toimivaltaisen viranomaisen tai vastaanottavan CSIRT-yksikön toimintaan.

(68) Jäsenvaltioiden olisi osallistuttava komission suosituksessa (EU) 2017/1584 ([15]) esitetyn EU:n kyberturvallisuuden kriisinhallintakehyksen perustamiseen olemassa olevien yhteistyöverkostojen, erityisesti EU-CyCLONen, CSIRT-verkoston ja yhteistyöryhmän, välityksellä. Euroopan kyberkriisien yhteysorganisaatioiden verkoston (EU-CyCLONe) ja CSIRT-verkoston olisi tehtävä yhteistyötä sellaisten menettelytapajärjestelyjen pohjalta, joissa täsmennetään kyseisen yhteistyön yksityiskohdat, ja vältettävä tehtävien päällekkäisyyttä. EU-CyCLONen työjärjestyksessä olisi täsmennettävä tarkemmin verkoston toimintatavat, mukaan lukien verkoston roolit, yhteistyökeinot, vuorovaikutus muiden asiaankuuluvien toimijoiden kanssa ja tietojenvaihdon mallit sekä viestintäkeinot. Unionin tason kriisinhallinnassa asianomaisten osapuolten olisi hyödynnettävä EU:n poliittisen kriisitoiminnan integroituja järjestelyjä, joista säädetään neuvoston täytäntöönpanopäätöksessä (EU) 2018/1993 ([16]), jäljempänä 'IPCR-järjestelyt'. Komission olisi käytettävä tähän tarkoitukseen ARGUS-järjestelmän korkean tason monialaista kriisinkoordinointiprosessia. Jos kriisiin liittyy merkittävä ulkoinen tai yhteisen turvallisuus- ja puolustuspolitiikan ulottuvuus, olisi aktivoitava Euroopan ulkosuhdehallinnon kriisinhallintamekanismi.

(69) Suosituksen (EU) 2017/1584 liitteen mukaisesti laajamittaisella kyberturvallisuuspoikkeamalla olisi tarkoitettava poikkeamaa, joka aiheuttaa niin laajan häiriön, ettei yksittäisellä jäsenvaltiolla ole valmiuksia hallita sitä, tai jolla on merkittävä vaikutus vähintään kahteen jäsenvaltioon. Laajamittaiset kyberturvallisuuspoikkeamat voivat aiheuttajasta ja vaikutuksista riippuen kärjistyä ja kehittyä todellisiksi kriiseiksi, jotka estävät sisämarkkinoiden moitteettoman toiminnan tai aiheuttavat vakavia yleiseen turvallisuuteen kohdistuvia riskejä toimijoille tai kansalaisille useissa jäsenvaltioissa tai koko unionissa. Kun otetaan huomioon tällaisten poikkeamien laaja vaikuttavuus ja useimmissa tapauksissa rajatylittävä luonne, jäsenvaltioiden ja asiaankuuluvien unionin toimielinten, elinten, laitosten ja virastojen olisi tehtävä yhteistyötä teknisellä, operatiivisella ja poliittisella tasolla, jotta eri puolilla unionia toteutettavia hallintatoimia voidaan koordinoida asianmukaisesti.

(70) Toimialojen ja jäsenvaltioiden suuren keskinäisriippuvuuden vuoksi unionin tason laajamittaiset kyberturvallisuuspoikkeamat ja kriisit edellyttävät koordinoituja toimia nopeiden ja vaikuttavien hallintatoimien varmistamiseksi. Kyberresilienttien verkko- ja tietojärjestelmien saatavuus sekä datan saatavuus, luottamuksellisuus ja eheys ovat elintärkeitä unionin turvallisuuden kannalta ja sen kansalaisten, yritysten ja instituutioiden suojelemiseksi poikkeamilta ja kyberuhkilta ja jotta voidaan lujittaa yksilöiden ja organisaatioiden luottamusta unionin kykyyn edistää ja suojella maailmanlaajuista, avointa, vapaata, vakaata ja turvallista kybertoimintaympäristöä, joka perustuu ihmisoikeuksiin, perusvapauksiin, demokratiaan ja oikeusvaltioon.

([14]) Euroopan parlamentin ja neuvoston asetus (EU) 2021/696, annettu 28 päivänä huhtikuuta 2021, unionin avaruusohjelman ja Euroopan unionin avaruusohjelmaviraston perustamisesta sekä asetusten (EU) N:o 912/2010, (EU) N:o 1285/2013 ja (EU) N:o 377/2014 ja päätöksen N:o 541/2014/EU kumoamisesta (EUVL L 170, 12.5.2021, s. 69).

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

([16]) Neuvoston täytäntöönpanopäätös (EU) 2018/1993, annettu 11 päivänä joulukuuta 2018, EU:n poliittisen kriisitoiminnan integroiduista järjestelyistä (EUVL L 320, 17.12.2018, s. 28).

(71) EU-CyCLONen olisi toimittava teknisen ja poliittisen tason välisenä yhdyssiteenä laajamittaisten kyberturvallisuuspoikkeamien ja kriisien aikana, ja sen olisi tehostettava operatiivisen tason yhteistyötä ja tuettava poliittisen tason päätöksentekoa. EU-CyCLONen olisi hyödynnettävä CSIRT-verkoston havaintoja ja omia valmiuksiaan, kun se analysoi laajamittaisten kyberturvallisuuspoikkeamien ja kriisien vaikutuksia yhteistyössä komission kanssa ottaen huomioon komission kompetenssin kriisinhallinnan alalla.

(72) Kyberhyökkäykset ovat luonteeltaan rajatylittäviä, ja merkittävä poikkeama voi häiritä ja vahingoittaa kriittisiä tietoinfrastruktuureja, joista sisämarkkinoiden moitteeton toiminta on riippuvainen. Suosituksessa (EU) 2017/1584 käsitellään kaikkien asianomaisten toimijoiden roolia. Komissio vastaa Euroopan parlamentin ja neuvoston päätöksellä N:o 1313/2013/EU ([17]) perustetun unionin pelastuspalvelumekanismin puitteissa yleisistä valmiustoimista, joihin kuuluvat hätäavun koordinointikeskuksen ja yhteisen hätäviestintä- ja tietojärjestelmän hallinnointi, tilannetietoisuus- ja -analyysivalmiuden ylläpito ja edelleen kehittäminen sekä valmiuksien luominen ja ylläpito niin, että voidaan koota ja lähettää paikan päälle asiantuntijaryhmiä, jos jäsenvaltio tai kolmas maa esittää avunpyynnön. Komissio vastaa lisäksi analyysiraporttien laatimisesta täytäntöönpanopäätöksen (EU) 2018/1993 mukaisia IPCR-järjestelyjä varten, mukaan lukien kyberturvallisuustilannekuva ja -valmiudet, sekä tilannekuvasta ja kriisitoiminnasta maatalouden, vaikeiden sääolojen, konfliktien kartoituksen ja ennustamisen, luonnonkatastrofeja koskevien ennakkovaroitusjärjestelmien, terveysuhkien, tartuntatautien seurannan, kasvien terveyden, kemiallisten vaaratilanteiden, elintarvikkeiden ja rehujen turvallisuuden, eläinten terveyden, muuttoliikkeen, tullin, ydinvoima- ja säteilyhätätilanteiden ja energian aloilla.

(73) Unioni voi tarvittaessa tehdä Euroopan unionin toiminnasta tehdyn sopimuksen 218 artiklan mukaisesti kolmansien maiden tai kansainvälisten järjestöjen kanssa kansainvälisiä sopimuksia, joilla mahdollistetaan ja järjestetään niiden osallistuminen tiettyihin yhteistyöryhmän, CSIRT-verkoston EU-CyCLONen toimintoihin. Tällaisilla sopimuksilla olisi varmistettava unionin edut ja riittävä tietosuoja. Tämä ei vaikuta jäsenvaltioiden oikeuteen tehdä kolmansien maiden kanssa yhteistyötä haavoittuvuuksien hallinnassa ja kyberturvallisuusriskien hallinnassa, jotta voidaan helpottaa raportointia ja yleistä tietojenvaihtoa unionin oikeuden mukaisesti.

(74) Jotta voidaan helpottaa tässä direktiivissä säädettyjen, muun muassa haavoittuvuuksien hallintaa, kyberturvallisuusriskien hallintatoimenpiteitä, raportointivelvoitteita ja kyberturvallisuustietojen jakamisjärjestelyjä koskevien säännösten tehokasta täytäntöönpanoa, jäsenvaltiot voivat tehdä yhteistyötä kolmansien maiden kanssa ja toteuttaa tätä varten tarkoituksenmukaisina pitämiään toimia, jollaisia ovat esimerkiksi tietojen vaihto kyberuhkista, poikkeamista, haavoittuvuuksista, työkaluista ja menetelmistä, taktiikasta, tekniikoista ja menettelyistä, kyberturvallisuuskriisien hallintaan valmistautuminen ja kriisinhallintaharjoitukset, koulutus, luottamuksen lujittamistoimet ja jäsennellyt tiedonjakojärjestelyt.

(75) Olisi otettava käyttöön vertaisarviointeja, jotta voidaan oppia yhteisistä kokemuksista, lujittaa keskinäistä luottamusta ja saavuttaa kyberturvallisuuden yhteinen korkea taso. Vertaisarvioinnit voivat tuottaa tulokseksi arvokkaita näkemyksiä ja suosituksia, joilla lujitetaan yleisiä kyberturvallisuusvalmiuksia, luodaan uusi toimintamalli parhaiden käytäntöjen jakamiselle jäsenvaltioiden kesken ja edistetään jäsenvaltioiden kyberturvallisuuden kehitystasoa. Vertaisarvioinneissa olisi myös otettava huomioon tulokset, joita on saatu vastaavista mekanismeista, kuten CSIRT-verkoston vertaisarviointijärjestelmästä, ja niissä olisi tuotettava lisäarvoa ja vältettävä päällekkäisyydet. Vertaisarviointien toteuttaminen ei saisi rajoittaa luottamuksellisten tai turvallisuusluokiteltujen tietojen suojaa koskevan unionin oikeuden tai kansallisen lainsäädännön soveltamista.

(76) Yhteistyöryhmän olisi vahvistettava jäsenvaltioille itsearviointimenetelmät, joiden on tarkoitus kattaa sellaisia tekijöitä kuin kyberturvallisuusriskien hallintatoimenpiteiden ja raportointivelvoitteiden täytäntöönpanoaste, toimivaltaisten viranomaisten valmiuksien taso ja tuloksekkuus tehtäviensä hoidossa, CSIRT-yksiköiden operatiiviset valmiudet, keskinäisen avunannon toteutusaste, kyberturvallisuustietojen jakamisjärjestelyjen täytäntöönpanoaste taikka rajatylittävät tai useaa toimialaa koskevat erityiskysymykset. Jäsenvaltioita olisi kannustettava tekemään säännöllisesti itsearviointeja sekä esittelemään niiden tulokset ja keskustelemaan näistä yhteistyöryhmässä.

([17]) Euroopan parlamentin ja neuvoston päätös N:o 1313/2013/EU, annettu 17 päivänä joulukuuta 2013, unionin pelastuspalvelumekanismista (EUVL L 347, 20.12.2013, s. 924).

(77) Vastuu verkko- ja tietojärjestelmän turvallisuuden varmistamisesta lankeaa suurelta osin keskeisille ja tärkeille toimijoille. Olisi edistettävä ja kehitettävä riskinhallintakulttuuria, johon sisältyy riskinarviointi ja riskeihin suhteutettujen kyberturvallisuusriskien hallintatoimenpiteiden toteuttaminen.

(78) Kyberturvallisuusriskien hallintatoimenpiteissä olisi otettava huomioon se, missä määrin keskeinen tai tärkeä toimija on riippuvainen verkko- ja tietojärjestelmistä, ja niihin olisi sisällyttävä toimenpiteitä, joilla tunnistetaan poikkeamariskit, ehkäistään, havaitaan ja hallitaan poikkeamia, palaudutaan niistä ja lievennetään niiden vaikutuksia. Verkko- ja tietojärjestelmien turvallisuuden olisi katettava säilytettävien, siirrettävien ja käsiteltävien tietojen turvallisuus. Kyberturvallisuusriskien hallintatoimenpiteisiin olisi kuuluttava järjestelmäanalyysi, jossa otetaan huomioon inhimilliset tekijät, jotta saadaan täydellinen kuva verkko- ja tietojärjestelmän turvallisuudesta.

(79) Koska verkko- ja tietojärjestelmien turvallisuuteen kohdistuvien uhkien aiheuttajia on monenlaisia, kyberturvallisuusriskien hallintatoimenpiteiden olisi perustuttava kaikki vaaratekijät huomioivaan toimintamalliin, jolla pyritään suojaamaan verkko- ja tietojärjestelmät ja näiden järjestelmien fyysinen ympäristö sellaisilta tapahtumilta kuin varkaus, tulipalo, tulva, televiestintä- tai sähkökatko sekä luvattomalta fyysiseltä pääsyltä keskeisen tai tärkeän toimijan tietoihin tai tietojenkäsittely-ympäristöön ja niille aiheutuvalta vahingolta ja häirinnältä, jotka saattaisivat vaarantaa verkko- ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden. Kyberturvallisuusriskien hallintatoimenpiteillä olisi näin ollen varmistettava myös verkko- ja tietojärjestelmien fyysinen ja ympäristön turvallisuus sisällyttämällä niihin toimenpiteitä, joilla suojataan tällaiset järjestelmät järjestelmähäiriöiltä, inhimillisiltä virheiltä, vihamielisiltä teoilta tai luonnonilmiöiltä eurooppalaisten tai kansainvälisten standardien, kuten ISO/IEC 27000 -sarjaan kuuluvien standardien, mukaisesti. Tähän liittyen keskeisten ja tärkeiden toimijoiden olisi käsiteltävä kyberturvallisuusriskien hallintatoimenpiteissään myös henkilöstöturvallisuutta ja otettava käyttöön asianmukaiset pääsynhallintaperiaatteet. Näiden toimenpiteiden olisi oltava direktiivin (EU) 2022/2557 mukaisia.

(80) Jotta voidaan näyttää toteen kyberturvallisuusriskien hallintatoimenpiteiden noudattaminen ja jos saatavilla ei ole Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 ([18]) mukaisesti hyväksyttyä asianmukaista eurooppalaista kyberturvallisuuden sertifiointijärjestelmää, jäsenvaltioiden olisi yhteistyöryhmää ja Euroopan kyberturvallisuuden sertifiointiryhmää kuullen edistettävä asiaa koskevien eurooppalaisten ja kansainvälisten standardien käyttöä keskeisten ja tärkeiden toimijoiden keskuudessa tai ne voivat vaatia toimijoita käyttämään sertifioituja TVT-tuotteita, TVT-palveluja ja TVT-prosesseja.

(81) Jotta keskeisille ja tärkeille toimijoille ei aiheutuisi kohtuutonta taloudellista ja hallinnollista rasitetta, kyberturvallisuusriskien hallintatoimenpiteiden olisi oltava oikeassa suhteessa asianomaiselle verkko- ja tietojärjestelmälle aiheutuviin riskeihin ja niissä olisi otettava huomioon tällaisten toimenpiteiden viimeisin kehitys sekä tapauksen mukaan asiaa koskevat eurooppalaiset ja kansainväliset standardit ja niiden täytäntöönpanokustannukset.

(82) Kyberturvallisuusriskien hallintatoimenpiteiden olisi oltava oikeassa suhteessa keskeisen tai tärkeän toimijan altistumiseen riskeille ja niihin yhteiskunnallisiin ja taloudellisiin vaikutuksiin, joita poikkeamalla olisi. Kun vahvistetaan keskeisille ja tärkeille toimijoille sovitettuja kyberturvallisuusriskien hallintatoimenpiteitä, olisi otettava asianmukaisesti huomioon keskeisten ja tärkeiden toimijoiden erilainen altistuminen riskeille, kuten toimijan kriittisyys, ne – myös yhteiskunnalliset – riskit, joille se altistuu, toimijan koko sekä poikkeamien esiintymisen todennäköisyys ja niiden vakavuus, mukaan lukien niiden yhteiskunnalliset ja taloudelliset vaikutukset.

([18]) 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).

(83) Keskeisten ja tärkeiden toimijoiden olisi varmistettava toiminnassaan käyttämiensä verkko- ja tietojärjestelmien turvallisuus. Kyseiset järjestelmät ovat pääasiassa yksityisiä verkko- ja tietojärjestelmiä, joita hallinnoi keskeisen tai tärkeän toimijan oma tietotekniikkahenkilöstö tai joiden turvallisuuspalvelut on ulkoistettu. Tässä direktiivissä säädettyjä kyberturvallisuusriskien hallintatoimenpiteitä ja raportointivelvoitteita olisi sovellettava asiaankuuluviin keskeisiin ja tärkeisiin toimijoihin riippumatta siitä, hoitavatko kyseiset toimijat verkko- ja tietojärjestelmiensä ylläpidon sisäisesti vai ovatko ne ulkoistaneet sen.

(84) Kun otetaan huomioon DNS-palveluntarjoajien, aluetunnusrekisterien, pilvipalvelujen tarjoajien, datakeskuspalvelujen tarjoajien, sisällönjakeluverkkojen tarjoajien, hallintapalvelun tarjoajien, tietoturvapalveluntarjoajien, verkossa toimivien markkinapaikkojen tarjoajien, verkossa toimivien hakukoneiden tarjoajien ja verkkoyhteisöalustojen tarjoajien sekä luottamuspalvelun tarjoajien toiminnan rajatylittävä luonne, niihin olisi sovellettava unionin tasolla pitkälle yhdenmukaistettuja sääntöjä. Kyseisiä toimijoita koskevien kyberturvallisuusriskien hallintatoimenpiteiden toteuttamista olisi siksi helpotettava täytäntöönpanosäädöksellä.

(85) On erityisen tärkeää puuttua riskeihin, jotka johtuvat toimijan toimitusketjusta ja suhteesta toimittajiinsa, kuten datan tallennus- ja käsittelypalvelujen tarjoajiin tai tietoturvapalveluntarjoajiin ja ohjelmistotoimittajiin, kun otetaan huomioon sellaisten poikkeamien yleisyys, jossa toimija on joutunut kyberhyökkäyksen uhriksi ja vihamieliset hyökkääjät ovat onnistuneet vaarantamaan toimijan verkko- ja tietojärjestelmien turvallisuuden hyödyntämällä kolmansien osapuolten tuotteisiin ja palveluihin vaikuttavia haavoittuvuuksia. Keskeisten ja tärkeiden toimijoiden olisi sen vuoksi arvioitava ja otettava huomioon toimittajiensa tuotteiden ja palveluntarjoajiensa palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet ja toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt, mukaan lukien tuotekehityksen suojausmenettelyt. Keskeisiä ja tärkeitä toimijoita olisi erityisesti kannustettava sisällyttämään kyberturvallisuusriskien hallintatoimenpiteitä sopimusjärjestelyihin, joita ne tekevät välittömien toimittajiensa ja palveluntarjoajiensa kanssa. Kyseiset toimijat voisivat käsitellä myös alemman tason toimittajistaan ja palveluntarjoajistaan johtuvia riskejä.

(86) Palveluntarjoajista erityisen tärkeällä sijalla ovat muun muassa poikkeamanhallintaa, tunkeutumisenestotestausta, turvallisuusauditointeja ja konsultointia tarjoavat tietoturvapalveluntarjoajat, jotka avustavat toimijoita niiden pyrkiessä ehkäisemään, havaitsemaan ja hallitsemaan poikkeamia tai palautumaan niistä. Tietoturvapalveluntarjoajat ovat kuitenkin itsekin joutuneet kyberhyökkäysten kohteeksi, ja niiden tiivis integroituminen toimijoiden toimintoihin aiheuttaa erityisen riskin. Keskeisten ja tärkeiden toimijoiden olisi sen vuoksi noudatettava erityisen suurta huolellisuutta tietoturvapalveluntarjoajaa valitessaan.

(87) Toimivaltaiset viranomaiset voivat hyödyntää valvontatehtävissään myös kyberturvallisuuspalveluja, kuten turvallisuusauditointeja, tunkeutumisenestotestausta ja poikkeamanhallintaa.

(88) Keskeisten ja tärkeiden toimijoiden olisi puututtava myös riskeihin, jotka johtuvat niiden vuorovaikutuksesta ja suhteista muihin sidosryhmiin laajemmassa ekosysteemissä, myös teollisuusvakoilun torjumiseksi ja liikesalaisuuksien suojaamiseksi. Toimijoiden olisi erityisesti varmistettava asianmukaisin toimenpitein, että niiden yhteistyössä akateemisten laitosten ja tutkimuslaitosten kanssa noudatetaan toimijoiden kyberturvallisuusperiaatteita ja hyviä käytäntöjä, jotka koskevat yleensä tiedon suojattua saatavuutta ja levittämistä ja etenkin teollis- ja tekijänoikeuksien suojaa. Kun otetaan huomioon datan merkitys ja arvo keskeisten ja tärkeiden toimijoiden toiminnalle, kyseisten toimijoiden olisi samoin toteutettava kaikki asianmukaiset kyberturvallisuusriskien hallintatoimenpiteet hankkiessaan tietojen muuntamispalveluja ja data-analytiikkapalveluja kolmansilta osapuolilta.

(89) Keskeisten ja tärkeiden toimijoiden olisi otettava käyttöön monenlaisia perustason kyberhygieniakäytäntöjä, kuten nollaluottamuksen periaate, ohjelmistopäivitykset, laitteiden konfigurointi, verkon segmentointi, identiteetin- ja pääsynhallinta ja käyttäjien tietoisuuden lisääminen, ja järjestettävä henkilöstölleen koulutusta kyberuhkista, verkkourkinnasta ja käyttäjän manipuloinnista. Kyseisten toimijoiden olisi lisäksi arvioitava omat kyberturvallisuusvalmiutensa ja tapauksen mukaan otettava käyttöön kyberturvallisuutta parantavia teknologioita, kuten tekoäly- tai koneoppimisjärjestelmiä, parantaakseen valmiuksiaan ja verkko- ja tietojärjestelmien turvallisuutta.

(90) Jotta voidaan paremmin puuttua keskeisiin toimitusketjun riskeihin ja auttaa tämän direktiivin soveltamisalaan kuuluvien toimialojen keskeisiä ja tärkeitä toimijoita hallitsemaan asianmukaisesti toimitusketjuihin ja toimittajiin liittyviä riskejä, yhteistyöryhmän olisi yhteistyössä komission ja ENISAn kanssa ja kuultuaan tarvittaessa asiaankuuluvia sidosryhmiä, myös toimialan sidosryhmiä, suoritettava kriittisiä toimitusketjuja koskevia koordinoituja turvallisuusriskinarviointeja, jollaisia tehdään 5G-verkkojen osalta komission suosituksen (EU) 2019/534 ([19]) mukaisesti, jotta voidaan määrittää kullakin alalla kriittiset TVT-palvelut, TVT-järjestelmät tai TVT-tuotteet sekä kyseeseen tulevat uhkat ja haavoittuvuudet. Tällaisissa koordinoiduissa turvallisuusriskinarvioinneissa olisi yksilöitävä toimenpiteitä, lieventämissuunnitelmia ja parhaita käytäntöjä, joilla ehkäistään kriittisiä riippuvuuksia, mahdollisia koko toiminnan lamauttavia yksittäisiä vikaantumispisteitä, uhkia, haavoittuvuuksia ja muita toimitusketjuun liittyviä riskejä, ja niissä olisi selvitettävä keinoja kannustaa niiden laajempaan käyttöönottoon keskeisten ja tärkeiden toimijoiden keskuudessa. Mahdollisia muita kuin teknisiä riskitekijöitä, kuten se, että kolmas maa vaikuttaa sopimattomasti toimittajiin ja palveluntarjoajiin, erityisesti vaihtoehtoisten hallintomallien tapauksessa, ovat salatut haavoittuvuudet tai takaportit ja mahdolliset järjestelmätason toimitushäiriöt, etenkin jos on ajauduttu teknologialukkiutumaan tai toimittajariippuvuuteen.

(91) Kriittisiä toimitusketjuja koskevissa koordinoiduissa turvallisuusriskinarvioinneissa olisi otettava asianomaisen toimialan erityispiirteiden perusteella huomioon sekä tekniset että tarvittaessa muut kuin tekniset tekijät, mukaan lukien suosituksessa (EU) 2019/534, 5G-verkkojen kyberturvallisuutta koskevassa koordinoidussa EU-tason riskinarvioinnissa ja yhteistyöryhmän hyväksymässä 5G-kyberturvallisuutta koskevassa EU:n välineistössä määritetyt tekijät. Koordinoitua turvallisuusriskinarviointia edellyttävien toimitusketjujen määrittämisessä olisi otettava huomioon seuraavat kriteerit: i) missä määrin keskeiset ja tärkeät toimijat käyttävät tiettyjä kriittisiä TVT-palveluja, TVT-järjestelmiä tai TVT-tuotteita ja ovat riippuvaisia niistä; ii) tiettyjen kriittisten TVT-palvelujen, TVT-järjestelmien tai TVT-tuotteiden merkitys kriittisten tai arkaluonteisten toimintojen suorittamisessa, myös henkilötietojen käsittelyssä; iii) vaihtoehtoisten TVT-palvelujen, TVT-järjestelmien tai TVT-tuotteiden saatavuus; iv) TVT-palvelujen, TVT-järjestelmien tai TVT-tuotteiden koko toimitusketjun häiriönsietokyky häiriötilanteissa niiden koko elinkaaren ajan; ja v) käyttöön tulevien uusien TVT-palvelujen, TVT-järjestelmien tai TVT-tuotteiden mahdollinen tuleva merkitys toimijoiden toiminnalle. Lisäksi olisi kiinnitettävä erityistä huomiota sellaisiin TVT-palveluihin, TVT-järjestelmiin tai TVT-tuotteisiin, joihin sovelletaan kolmansista maista johtuvia erityisvaatimuksia.

(92) Jotta voidaan virtaviivaistaa yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajille ja luottamuspalvelun tarjoajille asetettuja velvoitteita, jotka liittyvät niiden verkko- ja tietojärjestelmien turvallisuuteen, sekä antaa näille toimijoille ja Euroopan parlamentin ja neuvoston direktiivin (EU) 2018/1972 ([20]) ja asetuksen (EU) N:o 910/2014 mukaisille toimivaltaisille viranomaisille mahdollisuus hyötyä tällä direktiivillä perustetusta oikeudellisesta kehyksestä, mukaan lukien poikkeamien käsittelystä vastaavan CSIRT-yksikön nimeäminen sekä asianomaisten toimivaltaisten viranomaisten osallistuminen yhteistyöryhmän ja CSIRT-verkoston toimintaan, kyseiset toimijat olisi sisällytettävä tämän direktiivin soveltamisalaan. Asetuksessa (EU) N:o 910/2014 ja direktiivissä (EU) 2018/1972 vahvistetut vastaavat säännökset tämän tyyppisille toimijoille asetettavista turvallisuus- ja ilmoitusvaatimuksista olisi sen vuoksi kumottava. Tässä direktiivissä säädetyt raportointivelvoitteita koskevat säännöt eivät saisi rajoittaa asetuksen (EU) 2016/679 ja direktiivin 2002/58/EY soveltamista.

(93) Tässä direktiivissä säädettyjen kyberturvallisuusvelvoitteiden olisi katsottava täydentävän asetuksessa (EU) N:o 910/2014 luottamuspalvelun tarjoajille asetettuja vaatimuksia. Luottamuspalvelun tarjoajia olisi vaadittava toteuttamaan kaikki asianmukaiset ja oikeasuhteiset toimenpiteet palveluihinsa kohdistuvien riskien hallitsemiseksi, myös suhteessa asiakkaisiinsa ja palveluihinsa tukeutuviin kolmansiin osapuoliin, ja raportoimaan tämän direktiivin mukaisista poikkeamista. Näiden kyberturvallisuus- ja raportointivelvoitteiden olisi koskettava myös tarjottujen palvelujen fyysistä suojaamista. Asetuksen (EU) N:o 910/2014 24 artiklassa säädettyjä hyväksyttyjä luottamuspalvelun tarjoajia koskevia vaatimuksia sovelletaan edelleen.

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

([20]) 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).

(94) Jäsenvaltiot voivat antaa luottamuspalvelujen suhteen toimivaltaisten viranomaisten tehtävän asetuksen (EU) N:o 910/2014 mukaisille valvontaelimille, jotta voidaan varmistaa nykyisten käytäntöjen jatkuminen ja hyödyntää mainitun asetuksen soveltamisesta saatua tietämystä ja kokemusta. Tällaisessa tapauksessa tämän direktiivin mukaisten toimivaltaisten viranomaisten olisi tehtävä tiivistä ja oikea-aikaista yhteistyötä kyseisten valvontaelinten kanssa vaihtamalla asiaankuuluvia tietoja sen varmistamiseksi, että valvonta on tehokasta ja että luottamuspalvelun tarjoajat noudattavat tässä direktiivissä ja asetuksessa (EU) N:o 910/2014 säädettyjä vaatimuksia. Tapauksen mukaan tämän direktiivin mukaisen CSIRT-yksikön tai toimivaltaisen viranomaisen olisi tiedotettava asetuksen (EU) N:o 910/2014 mukaiselle valvontaelimelle välittömästi kaikista sille ilmoitetuista merkittävistä kyberuhkista ja poikkeamista, jotka vaikuttavat luottamuspalveluihin, sekä luottamuspalvelun tarjoajan mahdollisesta tämän direktiivin rikkomisesta. Jäsenvaltiot voivat tarvittaessa käyttää raportointiin keskitettyä asiointipistettä, joka on perustettu turvaamaan yhteinen ja automaattinen poikkeamista raportointi sekä asetuksen (EU) N:o 910/2014 mukaiselle valvontaelimelle että tämän direktiivin mukaiselle CSIRT-yksikölle tai toimivaltaiselle viranomaiselle.

(95) Tarkoituksenmukaisissa tapauksissa ja tarpeettomien katkosten välttämiseksi olisi tätä direktiiviä kansallisen lainsäädännön osaksi saatettaessa otettava huomioon olemassa olevat kansalliset ohjeet direktiivin (EU) 2018/1972 40 ja 41 artiklassa säädettyjen turvallisuustoimenpiteitä koskevien sääntöjen saattamisesta osaksi kansallista lainsäädäntöä, jotta voidaan hyödyntää direktiivin (EU) 2018/1972 soveltamisesta turvallisuustoimenpiteiden ja poikkeamien ilmoittamisen alalla saatua tietämystä ja ammattitaitoa. ENISA voi myös laatia yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajille ohjeistusta turvallisuusvaatimuksista ja raportointivelvoitteista yhdenmukaistamisen ja siirtymän helpottamiseksi ja häiriöiden minimoimiseksi. Jäsenvaltiot voivat antaa sähköisen viestinnän suhteen toimivaltaisten viranomaisten tehtävän direktiivin (EU) 2018/1972 mukaisille kansallisille sääntelyviranomaisille, jotta voidaan varmistaa nykyisten käytäntöjen jatkuminen ja hyödyntää kyseisen direktiivin täytäntöönpanosta saatua tietämystä ja kokemusta.

(96) Kun otetaan huomioon direktiivissä (EU) 2018/1972 määriteltyjen numeroista riippumattomien henkilöiden välisten viestintäpalvelujen kasvava merkitys, on tarpeen varmistaa, että myös tällaisiin palveluihin sovelletaan asianmukaisia turvallisuusvaatimuksia niiden erityisen luonteen ja taloudellisen merkityksen mukaisesti. Hyökkäyspinnan koko ajan kasvaessa numeroista riippumattomista henkilöiden välisistä viestintäpalveluista, kuten sanomanvälityspalveluista, on tulossa laajalti käytettyjä hyökkäysvektoreita. Vihamieliset hyökkääjät käyttävät alustoja viestiäkseen uhreille ja saadakseen heidät avaamaan turvallisuudeltaan vaarantuneita verkkosivuja, mikä lisää sellaisten poikkeamien todennäköisyyttä, joissa käytetään hyväksi henkilötietoja ja jotka siten vaikuttavat verkko- ja tietojärjestelmien turvallisuuteen. Numeroista riippumattomien henkilöiden välisten viestintäpalvelujen tarjoajien olisi varmistettava, että verkko- ja tietojärjestelmien turvallisuuden taso on oikeassa suhteessa aiheutuviin riskeihin. Koska numeroista riippumattomien henkilöiden välisten viestintäpalvelujen tarjoajat eivät yleensä tosiasiallisesti valvo signaalinsiirtoa verkoissa, tällaisille palveluille aiheutuvia riskejä voidaan joiltakin osin pitää perinteisiä sähköisiä viestintäpalveluja alhaisempina. Sama koskee sellaisia direktiivissä (EU) 2018/1972 määriteltyjä henkilöiden välisiä viestintäpalveluja, jotka perustuvat numeroihin mutta joissa palveluntarjoaja ei tosiasiallisesti valvo signaalinsiirtoa.

(97) Sisämarkkinat ovat entistä riippuvaisempia internetin toiminnasta. Lähes kaikkien keskeisten ja tärkeiden toimijoiden palvelut ovat riippuvaisia internetin kautta tarjottavista palveluista. Keskeisten ja tärkeiden toimijoiden tarjoamien palvelujen sujuvan tarjonnan varmistamiseksi on tärkeää, että kaikilla yleisten sähköisten viestintäverkkojen tarjoajilla on käytössä asianmukaiset kyberturvallisuusriskien hallintatoimenpiteet ja että ne raportoivat kyberturvallisuuteen liittyvistä merkittävistä poikkeamista. Jäsenvaltioiden olisi varmistettava, että yleisten sähköisten viestintäverkkojen turvallisuus säilyy ja että niiden elintärkeät turvallisuusedut suojataan sabotaasilta ja vakoilulta. Koska kansainväliset yhteydet parantavat ja nopeuttavat kilpailuun perustuvaa digitalisaatiota unionissa ja sen taloudessa, merenalaisiin tietoliikennekaapeleihin vaikuttavista poikkeamista olisi raportoitava CSIRT-yksikölle tai tapauksen mukaan toimivaltaiselle viranomaiselle. Kansallisessa kyberturvallisuusstrategiassa olisi tarvittaessa otettava huomioon merenalaisten tietoliikennekaapelien kyberturvallisuus, ja siihen olisi sisällyttävä mahdollisten kyberturvallisuusriskien kartoitus ja toimenpiteitä vaikutusten lieventämiseksi, jotta voidaan varmistaa tietoliikennekaapelien mahdollisimman korkeatasoinen suojaus.

(98) Yleisten sähköisten viestintäverkkojen ja yleisesti saatavilla olevien sähköisten viestintäpalvelujen turvallisuuden takaamiseksi olisi edistettävä salaustekniikoiden, erityisesti päästä päähän -salauksen, käyttöä sekä datakeskeisiä turvallisuuskonsepteja, kuten kartografiaa, segmentointia, tunnisteita, käyttöoikeusperiaatteita ja pääsynhallintaa sekä automatisoituja käyttöoikeuspäätöksiä. Salauksen, erityisesti päästä päähän -salauksen, käytön olisi tarvittaessa oltava pakollista yleisten sähköisten viestintäverkkojen tarjoajille ja yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajille oletusarvoisen ja sisäänrakennetun turvallisuuden ja yksityisyyden suojan periaatteiden mukaisesti tätä direktiiviä sovellettaessa. Päästä päähän -salauksen käyttö olisi sovitettava jäsenvaltioiden toimivaltaan varmistaa keskeisten turvallisuusetujensa ja yleisen turvallisuuden suojelu ja mahdollistaa rikosten ennalta estäminen, tutkiminen, paljastaminen ja rikoksiin liittyvät syytetoimet unionin oikeuden mukaisesti. Tämä ei kuitenkaan saisi heikentää päästä päähän -salausta, joka on tehokkaan tietosuojan, yksityisyyden suojan ja viestinnän turvallisuuden kannalta kriittinen teknologia.

(99) Yleisten sähköisten viestintäverkkojen ja yleisesti saatavilla olevien sähköisten viestintäpalvelujen turvallisuuden takaamiseksi ja niiden väärinkäytön ja manipuloinnin estämiseksi olisi edistettävä suojatun reitityksen standardien käyttöä, jotta voidaan varmistaa reititystoimintojen eheys ja luotettavuus koko internetyhteyspalvelun tarjoajien ekosysteemissä.

(100) Jotta voidaan taata internetin toimivuus ja eheys ja edistää DNS-järjestelmän turvallisuutta ja häiriönsietokykyä, asiaankuuluvia sidosryhmiä, mukaan lukien unionin yksityisen sektorin toimijat, yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat, etenkin internetyhteyspalvelun tarjoajat, ja verkossa toimivien hakukoneiden tarjoajat, olisi kannustettava hyväksymään DNS-selvityksen monipuolistamisstrategia. Jäsenvaltioita olisi myös kannustettava kehittämään julkinen ja suojattu eurooppalainen DNS-selvittäjäpalvelu ja käyttämään sitä.

(101) Tässä direktiivissä säädetään merkittävien poikkeamien ilmoittamista koskevasta monivaiheisesta lähestymistavasta, jotta löydetään oikea tasapaino yhtäältä nopean ilmoittamisen, joka auttaa lieventämään merkittävien poikkeamien mahdollista leviämistä ja antaa keskeisille ja tärkeille toimijoille mahdollisuuden pyytää apua, ja toisaalta sellaisen perusteellisemman raportoinnin välillä, jonka ansiosta saadaan arvokasta kokemusta yksittäisistä poikkeamista ja parannetaan ajan mittaan yksittäisten toimijoiden ja kokonaisten toimialojen kyberresilienssiä. Tältä osin tähän direktiiviin olisi sisällytettävä sellaisista poikkeamista raportoiminen, jotka voivat asianomaisen toimijan suorittaman alustavan arvioinnin perusteella johtaa vakaviin palvelun toimintahäiriöihin tai aiheuttaa kyseiselle toimijalle suuria taloudellisia tappioita tai vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista ja aineetonta vahinkoa. Tällaisessa alustavassa arvioinnissa olisi otettava huomioon muun muassa verkko- ja tietojärjestelmät, joihin poikkeama vaikuttaa, ja erityisesti niiden merkitys toimijan palvelujen tarjoamisessa, kyberuhkan vakavuus ja tekniset ominaisuudet sekä mahdolliset taustalla olevat haavoittuvuudet, joita käytetään hyväksi, sekä toimijan kokemukset samanlaisista poikkeamista. Indikaattorit, kuten palvelun häiriintymisen laajuus, poikkeaman kesto tai niiden palvelun vastaanottajien lukumäärä, joihin poikkeama vaikuttaa, voivat olla tärkeitä määritettäessä, onko palvelun toimintahäiriö vakava.

(102) Kun keskeinen tai tärkeä toimija tulee tietoiseksi merkittävästä poikkeamasta, sillä olisi oltava velvollisuus antaa ennakkovaroitus ilman aiheetonta viivytystä ja joka tapauksessa 24 tunnin kuluessa. Ennakkovaroituksen jälkeen olisi tehtävä poikkeamailmoitus. Asianomaisten toimijoiden olisi tehtävä poikkeamailmoitus ilman aiheetonta viivytystä ja joka tapauksessa 72 tunnin kuluessa siitä, kun ne tulevat tietoisiksi merkittävästä poikkeamasta, ja pyrittävä erityisesti pitämään ennakkovaroituksessa annetut tiedot ajantasaisina ja esittämään alustava arvio merkittävästä poikkeamasta, myös sen vakavuudesta ja vaikutuksista, sekä vaarantumista kuvaavat indikaattorit eli IoC-tieto, jäljempänä 'vaarantumisindikaattorit', jos sellaisia on saatavilla. Lopullinen raportti olisi toimitettava viimeistään kuukauden kuluttua poikkeamailmoituksesta. Ennakkovaroituksen olisi sisällettävä vain ne tiedot, jotka ovat välttämättömiä, jotta CSIRT-yksikkö tai tapauksen mukaan toimivaltainen viranomainen tulee tietoiseksi merkittävästä poikkeamasta ja jotta asianomainen toimija voi tarvittaessa pyytää apua. Tällaisessa ennakkovaroituksessa olisi tapauksen mukaan ilmoitettava, epäilläänkö merkittävän poikkeaman johtuvan lainvastaisista tai vihamielisistä teoista ja onko sillä todennäköisesti rajatylittäviä vaikutuksia. Jäsenvaltioiden olisi varmistettava, että velvollisuus antaa kyseinen ennakkovaroitus tai sen jälkeinen poikkeamailmoitus ei vie ilmoituksen tehneen toimijan resursseja pois poikkeamien käsittelyyn liittyvistä toiminnoista, jotka olisi asetettava etusijalle, jotta voidaan estää se, että poikkeamaraportointivelvoitteet joko vievät resursseja pois merkittävien poikkeamien

hallintatoimista tai muulla tavoin vaarantavat toimijan asiaan liittyvät ponnistelut. Jos poikkeama on edelleen meneillään silloin, kun lopullinen raportti pitäisi toimittaa, jäsenvaltioiden olisi varmistettava, että asianomaiset toimijat toimittavat tuolloin edistymisraportin ja lopullisen raportin kuukauden kuluessa siitä, kun ne ovat käsitelleet merkittävän poikkeaman.

(103) Keskeisten ja tärkeiden toimijoiden olisi tarvittaessa tiedotettava palvelunsa vastaanottajille ilman aiheetonta viivytystä kaikista toimenpiteistä tai korjaavista toimista, joita he voivat toteuttaa lieventääkseen merkittävästä kyberuhkasta johtuvia riskejä. Kyseisten toimijoiden olisi tarvittaessa ja erityisesti silloin, kun merkittävä kyberuhka todennäköisesti toteutuu, tiedotettava palvelunsa vastaanottajille myös itse uhkasta. Kyseisten toimijoiden olisi täytettävä vaatimus tiedottaa merkittävistä kyberuhkista palvelunsa vastaanottajille parhaansa mukaan, mutta tämä ei saisi vapauttaa niitä velvollisuudesta toteuttaa omalla kustannuksellaan asianmukaisia ja välittömiä toimenpiteitä uhkien ehkäisemiseksi tai korjaamiseksi ja palvelun normaalin turvallisuustason palauttamiseksi. Merkittäviä kyberuhkia koskevat tiedot olisi annettava palvelun vastaanottajille maksutta, ja ne olisi ilmaistava helppotajuisesti.

(104) Yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajien olisi pantava täytäntöön sisäänrakennettu ja oletusarvoinen turvallisuus sekä tiedotettava palvelunsa vastaanottajille merkittävistä kyberuhkista ja toimenpiteistä, joita he voivat toteuttaa laitteidensa ja viestintänsä turvallisuuden suojaamiseksi esimerkiksi käyttämällä tietyntyyppisiä ohjelmistoja tai salaustekniikoita.

(105) Ennakoiva lähestymistapa kyberuhkiin on ratkaiseva osa kyberturvallisuusriskien hallintaa, jonka avulla toimivaltaisten viranomaisten olisi pystyttävä estämään tehokkaasti kyberuhkien toteutuminen poikkeamina, jotka voivat aiheuttaa huomattavaa aineellista ja aineetonta vahinkoa. Tätä varten kyberuhkista ilmoittaminen on erittäin tärkeää. Siksi toimijoita kannustetaan raportoimaan vapaaehtoisesti kyberuhkista.

(106) Tässä direktiivissä edellytettävien tietojen raportoinnin yksinkertaistamiseksi ja toimijoille aiheutuvan hallinnollisen rasitteen vähentämiseksi jäsenvaltioiden olisi tarjottava tekniset keinot, kuten keskitetty asiointipiste, automatisoidut järjestelmät, verkkolomakkeet, käyttäjäystävälliset käyttöliittymät, mallit ja erityiset alustat, joita toimijat riippumatta siitä, kuuluvatko ne tämän direktiivin soveltamisalaan, voivat käyttää asiaankuuluvien raportoitavien tietojen toimittamiseen. Tämän direktiivin täytäntöönpanoa tukevaan unionin rahoitukseen, erityisesti Euroopan parlamentin ja neuvoston asetuksella (EU) 2021/694 ([21]) perustetusta Digitaalinen Eurooppa -ohjelmasta annettavaan rahoitukseen, voisi sisältyä tuki keskitetyille asiointipisteille. Toimijat ovat lisäksi usein tilanteessa, jossa tietystä poikkeamasta on sen ominaisuuksien vuoksi ilmoitettava useille viranomaisille eri säädöksiin sisältyvien ilmoitusvelvoitteiden vuoksi. Tällaiset tapaukset aiheuttavat hallinnollista lisärasitteita ja saattavat myös synnyttää epävarmuutta tällaisten ilmoitusten muodosta ja menettelyistä. Kun keskitetty asiointipiste on perustettu, jäsenvaltioita kannustetaan käyttämään kyseistä keskitettyä asiointipistettä myös turvapoikkeamien ilmoittamiseen muun unionin lainsäädännön, kuten asetuksen (EU) 2016/679 ja direktiivin 2002/58/EY, nojalla. Tällaisen keskitetyn asiointipisteen käyttö turvapoikkeamien ilmoittamiseen asetuksen (EU) 2016/679 ja direktiivin 2002/58/EY nojalla ei saisi vaikuttaa asetuksen (EU) 2016/679 ja direktiivin 2002/58/EY säännösten soveltamiseen, etenkään niiden säännösten, jotka koskevat niissä tarkoitettujen viranomaisten riippumattomuutta. ENISAn olisi yhteistyössä yhteistyöryhmän kanssa kehitettävä yhteiset ilmoitusmallit antamalla ohjeita, joilla yksinkertaistetaan ja virtaviivaistetaan unionin lainsäädännössä edellytettyjä raportoitavia tietoja ja vähennetään ilmoituksen tehneille toimijoille aiheutuvaa hallinnollista rasitetta.

(107) Jos epäillään, että poikkeama liittyy unionin oikeudessa tai kansallisessa lainsäädännössä tarkoitettuun vakavaan rikolliseen toimintaan, jäsenvaltioiden olisi kannustettava keskeisiä ja tärkeitä toimijoita raportoimaan vakaviksi rikoksiksi epäillyistä poikkeamista asiaankuuluville lainvalvontaviranomaisille sovellettavien rikosoikeudellisia menettelyjä koskevien sääntöjen perusteella unionin oikeuden mukaisesti. Tarvittaessa ja rajoittamatta Europoliin sovellettavien henkilötietojen suojaa koskevien sääntöjen soveltamista on suotavaa, että eri jäsenvaltioiden toimivaltaisten viranomaisten ja lainvalvontaviranomaisten välinen koordinointi tapahtuu Euroopan kyberrikostorjuntakeskuksen (EC3) ja ENISAn myötävaikutuksella.

([21]) Euroopan parlamentin ja neuvoston asetus (EU) 2021/694, annettu 29 päivänä huhtikuuta 2021, Digitaalinen Eurooppa -ohjelman perustamisesta ja päätöksen (EU) 2015/2240 kumoamisesta (EUVL L 166, 11.5.2021, s. 1).

(108) Poikkeamat vaarantavat monissa tapauksissa henkilötietojen suojan. Niinpä toimivaltaisten viranomaisten olisi tehtävä yhteistyötä ja vaihdettava tietoja kaikista merkityksellisistä asioista asetuksessa (EU) 2016/679 ja direktiivissä 2002/58/EY tarkoitettujen viranomaisten kanssa.

(109) Verkkotunnusten rekisteröintitietojen (WHOIS-tietojen) tarkkojen ja kattavien tietokantojen ylläpitäminen ja laillisen pääsyn tarjoaminen tällaisiin tietoihin on olennaisen tärkeää, jotta voidaan varmistaa DNS-järjestelmän turvallisuus, vakaus ja häiriönsietokyky, mikä puolestaan edistää kyberturvallisuuden yhteistä korkeaa tasoa kaikkialla unionissa. Tätä nimenomaista tarkoitusta varten aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat olisi velvoitettava käsittelemään tiettyjä, tähän tarkoitukseen tarvittavia tietoja. Tällaista käsittelyä olisi pidettävä asetuksen (EU) 2016/679 6 artiklan 1 kohdan c alakohdassa tarkoitettuna lakisääteisenä velvoitteena. Tämä velvoite ei rajoita mahdollisuutta kerätä verkkotunnusten rekisteröintitietoja muihin tarkoituksiin, esimerkiksi sopimusjärjestelyjen tai muussa unionin oikeudessa tai kansallisessa lainsäädännössä vahvistettujen oikeudellisten vaatimusten perusteella. Tällä velvoitteella pyritään varmistamaan, että rekisteröintitiedot ovat täydelliset ja tarkat, eikä sen pitäisi johtaa samojen tietojen keräämiseen moneen kertaan. Aluetunnusrekisterien ja verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden olisi tehtävä yhteistyötä päällekkäisen keruun välttämiseksi.

(110) Verkkotunnusten rekisteröintitietojen saatavuus ja nopea käytettävyys niihin pääsyä oikeutetusti pyytäville on olennaisen tärkeää DNS-järjestelmän väärinkäytön ehkäisemiseksi ja torjumiseksi sekä poikkeamien ehkäisemiseksi, havaitsemiseksi ja hallitsemiseksi. Pääsyä oikeutetusti pyytävillä tarkoitetaan kaikkia luonnollisia henkilöitä tai oikeushenkilöitä, jotka esittävät pyynnön unionin oikeuden tai kansallisen lainsäädännön nojalla. Niihin voi kuulua viranomaisia, jotka ovat toimivaltaisia tämän direktiivin mukaisesti, sekä viranomaisia, joilla on unionin oikeuden tai kansallisen lainsäädännön nojalla toimivalta rikosten ennalta estämiseen, tutkimiseen, paljastamiseen tai rikoksiin liittyviin syytetoimiin, ja CERT-ryhmiä tai CSIRT-yksiköitä. Aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat olisi velvoitettava antamaan laillinen pääsy tarkasti määrättyihin verkkotunnusten rekisteröintitietoihin, joita tarvitaan esitettyä pyyntöä varten, niille, jotka pyytävät pääsyä oikeutetusti unionin oikeuden ja kansallisen lainsäädännön mukaisesti. Pääsyä oikeutetusti pyytävän olisi liitettävä pyyntöönsä perustelut, joiden avulla voidaan arvioida, onko tietoihin pääsy tarpeen.

(111) Tarkkojen ja täydellisten verkkotunnusten rekisteröintitietojen saatavuuden varmistamiseksi aluetunnusrekisterien ja verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden olisi kerättävä verkkotunnusten rekisteröintitiedot ja taattava niiden eheys ja saatavuus. Aluetunnusrekisterien ja verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden olisi erityisesti vahvistettava toimintaperiaatteet ja menettelyt, joiden mukaisesti kerätään ja ylläpidetään tarkkoja ja täydellisiä verkkotunnusten rekisteröintitietoja sekä ehkäistään ja korjataan virheellisiä rekisteröintitietoja unionin tietosuojalainsäädännön mukaisesti. Näissä toimintaperiaatteissa ja menettelyissä olisi mahdollisuuksien mukaan otettava huomioon monisidosryhmäisten hallintorakenteiden kansainvälisellä tasolla kehittämät standardit. Aluetunnusrekisterien ja verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden olisi hyväksyttävä ja pantava täytäntöön oikeasuhteiset menettelyt verkkotunnusten rekisteröintitietojen tarkistamiseksi. Näiden menettelyjen olisi kuvastettava toimialan parhaita käytäntöjä ja mahdollisuuksien mukaan sähköisen tunnistamisen alalla saavutettua edistystä. Esimerkkejä tarkastusmenettelyistä voivat olla rekisteröintihetkellä suoritettavat ennakkotarkastukset ja rekisteröinnin jälkeen suoritettavat jälkitarkastukset. Aluetunnusrekisterien ja verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden olisi erityisesti varmennettava ainakin yksi keino ottaa yhteyttä verkkotunnuksen rekisteröijään.

(112) Aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat olisi velvoitettava asettamaan julkisesti saataville verkkotunnusten rekisteröintitiedot, jotka eivät kuulu unionin tietosuojalainsäädännön soveltamisalaan, kuten oikeushenkilöitä koskevat tiedot, asetuksen (EU) 2016/679 johdanto-osan mukaisesti. Oikeushenkilöiden osalta aluetunnusrekisterien ja verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden olisi asetettava julkisesti saataville ainakin verkkotunnuksen rekisteröijän nimi ja yhteyspuhelinnumero. Yhteyssähköpostiosoite olisi myös julkaistava edellyttäen, että se ei sisällä henkilötietoja, kuten käyttämällä vaihtoehtoisia sähköpostiosoitteita (alias) tai asiointiosoitteita. Aluetunnusrekisterien ja verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden olisi myös unionin tietosuojalainsäädännön mukaisesti annettava pääsyä oikeutetusti pyytäville laillinen pääsy tarkasti määrättyihin luonnollisia henkilöitä koskeviin verkkotunnusten rekisteröintitietoihin. Jäsenvaltioiden olisi edellytettävä, että aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat vastaavat ilman aiheetonta viivytystä pääsyä oikeutetusti pyytävien esittämiin verkkotunnusten rekisteröintitietojen luovuttamispyyntöihin. Aluetunnusrekisterien ja verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden olisi vahvistettava toimintaperiaatteet ja menettelyt rekisteröintitietojen julkaisemista ja luovuttamista varten, mukaan lukien palvelutasosopimukset pääsyä oikeutetusti pyytävien esittämien pyyntöjen

käsittelemiseksi. Näissä toimintaperiaatteissa ja menettelyissä olisi mahdollisuuksien mukaan otettava huomioon mahdollinen ohjeistus ja monisidosryhmäisten hallintorakenteiden kansainvälisellä tasolla kehittämät standardit. Tietojenluovutusmenettelyssä voidaan käyttää rajapintaa, portaalia tai muuta teknistä välinettä tehokkaan järjestelyn tarjoamiseksi rekisteröintitietojen pyytämistä ja niihin pääsyä varten. Edistääkseen yhdenmukaisia käytäntöjä sisämarkkinoilla komissio voi Euroopan tietosuojaneuvoston toimivaltaa rajoittamatta antaa tällaisia menettelyjä koskevia ohjeita, joissa otetaan mahdollisuuksien mukaan huomioon monisidosryhmäisten hallintorakenteiden kansainvälisellä tasolla kehittämät standardit. Jäsenvaltioiden olisi varmistettava, että kaikenlainen pääsy verkkotunnusten rekisteröintitietoihin, sekä henkilötietoihin että muihin kuin henkilötietoihin, on maksutonta.

(113) Tämän direktiivin soveltamisalaan kuuluvien toimijoiden olisi katsottava kuuluvan sen jäsenvaltion lainkäyttövaltaan, johon ne ovat sijoittautuneet. Yleisten sähköisten viestintäverkkojen tarjoajien tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajien olisi kuitenkin katsottava kuuluvan sen jäsenvaltion lainkäyttövaltaan, jossa ne tarjoavat palvelujaan. DNS-palveluntarjoajien, aluetunnusrekisterien, verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden, pilvipalvelujen tarjoajien, datakeskuspalvelujen tarjoajien, sisällönjakeluverkkojen tarjoajien, hallintapalvelun tarjoajien, tietoturvapalveluntarjoajien sekä verkossa toimivien markkinapaikkojen tarjoajien, verkossa toimivien hakukoneiden tarjoajien ja verkkoyhteisöalustojen tarjoajien olisi katsottava kuuluvan sen jäsenvaltion lainkäyttövaltaan, jossa niiden päätoimipaikka on unionissa. Julkishallinnon toimijoiden olisi kuuluttava sen jäsenvaltion lainkäyttövaltaan, joka ne on perustanut. Jos toimija tarjoaa palveluja useammassa kuin yhdessä jäsenvaltiossa tai on sijoittautunut useampaan kuin yhteen jäsenvaltioon, sen olisi kuuluttava asianomaisten jäsenvaltioiden erilliseen ja rinnakkaiseen lainkäyttövaltaan. Näiden jäsenvaltioiden toimivaltaisten viranomaisten olisi tehtävä yhteistyötä, annettava toisilleen keskinäistä apua ja tarvittaessa toteutettava yhteisiä valvontatoimia. Käyttäessään lainkäyttövaltaansa jäsenvaltiot eivät *ne bis in idem* -periaatteen mukaisesti saisi määrätä täytäntöönpanotoimenpiteitä tai seuraamuksia useammin kuin kerran samasta toiminnasta.

(114) Jotta voidaan ottaa huomioon DNS-palveluntarjoajien, aluetunnusrekisterien, verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden, pilvipalvelujen tarjoajien, datakeskuspalvelujen tarjoajien, sisällönjakeluverkkojen tarjoajien, hallintapalvelun tarjoajien, tietoturvapalveluntarjoajien sekä verkossa toimivien markkinapaikkojen tarjoajien, verkossa toimivien hakukoneiden tarjoajien ja verkkoyhteisöalustojen tarjoajien palvelujen ja toimintojen rajatylittävä luonne, vain yhdellä jäsenvaltiolla olisi oltava lainkäyttövalta näihin toimijoihin nähden. Lainkäyttövalta olisi oltava sillä jäsenvaltiolla, jossa asianomaisen toimijan päätoimipaikka sijaitsee unionissa. Tätä direktiiviä sovellettaessa sijoittautumiskriteerin täyttyminen edellyttää tosiasiallista toimintaa ja kiinteää toimipaikkaa. 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 määrätyssä paikassa; tällaisten järjestelmien sijainti ja käyttö tietyssä paikassa eivät itsessään tee siitä päätoimipaikkaa, eivätkä ne näin ollen ole ratkaisevia perusteita päätoimipaikan määrittämisessä. Päätoimipaikan olisi katsottava olevan unionissa siinä jäsenvaltiossa, jossa kyberturvallisuusriskien hallintatoimenpiteisiin liittyvät päätökset pääsääntöisesti tehdään. Tämä vastaa tyypillisesti toimijan keskushallinnon sijaintipaikkaa unionissa. Jos tällaista jäsenvaltiota ei voida määrittää tai jos tällaisia päätöksiä ei tehdä unionissa, päätoimipaikan olisi katsottava sijaitsevan jäsenvaltiossa, jossa kyberturvallisuustoiminnot toteutetaan. Jos tällaista jäsenvaltiota ei voida määrittää, päätoimipaikan olisi katsottava sijaitsevan jäsenvaltiossa, jossa toimijalla on eniten työntekijöitä työllistävä toimipaikka unionissa. Jos palvelut suorittaa yritysryhmä, sen päätoimipaikaksi olisi katsottava määräysvaltaa käyttävän yrityksen päätoimipaikka.

(115) Jos yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoaja tarjoaa yleisesti saatavilla olevaa rekursiivista DNS-palvelua ainoastaan internetyhteyspalvelun osana, kyseisen toimijan olisi katsottava kuuluvan kaikkien niiden jäsenvaltioiden lainkäyttövaltaan, joissa se tarjoaa palvelujaan.

(116) Kun DNS-palveluntarjoaja, aluetunnusrekisteri, verkkotunnusten rekisteröintipalveluja tarjoava toimija, pilvipalvelujen tarjoaja, datakeskuspalvelujen tarjoaja, sisällönjakeluverkkojen tarjoaja, hallintapalvelun tarjoaja, tietoturvapalveluntarjoaja taikka verkossa toimivien markkinapaikkojen, verkossa toimivien hakukoneiden tai verkkoyhteisöalustojen tarjoaja, joka ei ole sijoittautunut unioniin, tarjoaa palveluja unionissa, sen olisi nimettävä itselleen edustaja unioniin. Jotta voidaan määrittää, tarjoaako tällainen toimija palveluja unionissa, olisi varmistettava, aikooko se tarjota palveluja henkilöille yhdessä tai useammassa jäsenvaltiossa. Pelkkää toimijan tai välittäjän verkkosivuston tai sähköpostiosoitteen tai muiden yhteystietojen saatavuutta unionissa taikka sitä, että käytetään toimijan sijoittautumispaikkana olevassa kolmannessa maassa yleisesti käytettävää kieltä, olisi pidettävä riittämättömänä osoituksena tällaisesta aikomuksesta. Kuitenkin esimerkiksi yhdessä tai useammassa jäsenvaltiossa yleisesti käytettävän kielen tai rahayksikön käyttäminen ja mahdollisuus tilata palveluja kyseisellä kielellä taikka unionissa olevien asiakkaiden tai käyttäjien mainitseminen voivat 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 nimettävä nimenomaisesti toimijan antamalla kirjallisella valtuutuksella hoitamaan tämän puolesta tässä direktiivissä säädetyt velvoitteet, myös poikkeamista raportointi.

(117) Jotta saadaan selkeä yleiskuva DNS-palveluntarjoajista, aluetunnusrekistereistä, verkkotunnusten rekisteröinti-palveluja tarjoavista toimijoista, pilvipalvelujen tarjoajista, datakeskuspalvelujen tarjoajista, sisällönjakeluverkkojen tarjoajista, hallintapalvelun tarjoajista, tietoturvapalveluntarjoajista sekä verkossa toimivien markkinapaikkojen tarjoajista, verkossa toimivien hakukoneiden tarjoajista ja verkkoyhteisöalustojen tarjoajista, jotka tarjoavat tämän direktiivin soveltamisalaan kuuluvia palveluja eri puolilla unionia, ENISAn olisi perustettava tällaisten toimijoiden rekisteri ja ylläpidettävä sitä käyttäen tietoja, joita jäsenvaltiot saavat, tapauksen mukaan toimijoiden rekisteröitymistä varten perustettujen kansallisten järjestelyjen välityksellä. Keskitettyjen yhteyspisteiden olisi toimitettava nämä tiedot ja niihin mahdollisesti tehdyt muutokset ENISAlle. Jotta voidaan varmistaa tähän rekisteriin sisällytettävien tietojen tarkkuus ja täydellisyys, jäsenvaltiot voivat toimittaa ENISAlle mahdollisissa kansallisissa rekistereissään saatavilla olevat tiedot kyseisistä toimijoista. ENISAn ja jäsenvaltioiden olisi toteutettava toimenpiteitä, joilla edistetään tällaisten rekisterien yhteentoimivuutta, ja varmistettava samalla luottamuksellisten tai turvallisuusluokiteltujen tietojen suoja. ENISAn olisi laadittava asianmukaisia tietojen luokitus- ja hallintaprotokollia luovutettujen tietojen turvallisuuden ja luottamuksellisuuden varmistamiseksi ja rajattava pääsy tällaisiin tietoihin ja niiden tallentaminen ja siirtäminen vain aiotuille käyttäjille.

(118) Jos unionin oikeuden tai kansallisen lainsäädännön mukaisesti turvallisuusluokiteltuja tietoja vaihdetaan, ilmoitetaan tai muutoin jaetaan tämän direktiivin nojalla, olisi sovellettava vastaavia turvallisuusluokiteltujen tietojen käsittelyä koskevia sääntöjä. ENISAlla olisi lisäksi oltava käytössään infrastruktuuri, menettelyt ja säännöt, joiden avulla se voi käsitellä arkaluonteisia ja turvallisuusluokiteltuja tietoja EU:n turvallisuusluokiteltuihin tietojen suojaamiseen sovellettavien turvallisuussääntöjen mukaisesti.

(119) Koska kyberuhkat ovat yhä monimutkaisempia ja kehittyneempiä, tällaisten uhkien onnistunut havaitseminen ja ehkäisytoimenpiteet ovat pitkälti riippuvaisia uhkiin ja haavoittuvuuksiin liittyvän tiedon säännöllisestä jakamisesta toimijoiden kesken. Tietojenvaihto lisää tietoisuutta kyberuhkista, mikä puolestaan parantaa toimijoiden valmiuksia estää näitä uhkia kehittymästä poikkeamiksi ja auttaa niitä rajoittamaan paremmin poikkeamien vaikutuksia ja palautumaan niistä tehokkaammin. Koska unionin tasolla ei ole annettu ohjeistusta, vaikuttaa siltä, että erilaiset tekijät, erityisesti epävarmuus yhteensopivuudesta kilpailu- ja vastuusääntöjen kanssa, ovat estäneet tällaisen tietojen jakamisen.

(120) Jäsenvaltioiden olisi kannustettava ja avustettava toimijoita hyödyntämään kollektiivisesti kunkin tietämystä ja käytännön kokemusta strategisella, taktisella ja operatiivisella tasolla, jotta voidaan parantaa niiden valmiuksia ehkäistä, havaita ja hallita poikkeamia tai palautua niistä tai lieventää niiden vaikutuksia asianmukaisesti. Sen vuoksi on tarpeen mahdollistaa vapaaehtoisuuteen perustuvat kyberturvallisuustietojen jakamisjärjestelyt unionin tasolla. Tätä varten jäsenvaltioiden olisi aktiivisesti avustettava ja kannustettava toimijoita, kuten kyberturvallisuuspalveluja ja -tutkimusta tarjoavia toimijoita sekä sellaisia asiaankuuluvia toimijoita, jotka eivät kuulu tämän direktiivin soveltamisalaan, osallistumaan tällaisiin kyberturvallisuustietojen jakamisjärjestelyihin. Nämä järjestelyt olisi toteutettava unionin kilpailusääntöjen ja unionin tietosuojalainsäädännön mukaisesti.

(121) Keskeisten ja tärkeiden toimijoiden suorittamaa henkilötietojen käsittelyä, siinä määrin kuin se on tarpeen ja oikeasuhteista verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi, voidaan pitää lainmukaisena sillä perusteella, että se on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi asetuksen (EU) 2016/679 6 artiklan 1 kohdan c alakohdan ja 6 artiklan 3 kohdan vaatimusten mukaisesti. Henkilötietojen käsittely voi olla tarpeen myös keskeisten ja tärkeiden toimijoiden sekä niiden puolesta toimivien turvallisuusteknologioiden ja -palvelujen tarjoajien oikeutettujen etujen toteuttamiseksi asetuksen (EU) 2016/679 6 artiklan 1 kohdan f alakohdan mukaisesti, myös silloin, kun tällainen käsittely on tarpeen tämän direktiivin mukaisia kyberturvallisuustietojen jakamisjärjestelyjä tai asiaankuuluvien tietojen vapaaehtoista ilmoittamista varten. Toimenpiteet, jotka liittyvät poikkeamien ehkäisemiseen, havaitsemiseen, tunnistamiseen, rajoittamiseen, analysointiin ja hallitsemiseen, toimenpiteet yksittäisistä kyberuhkista tiedottamiseksi, haavoittuvuuden korjaamiseen ja koordinoituun haavoittuvuuden julkistamiseen liittyvä tietojenvaihto sekä vapaaehtoinen tietojenvaihto kyseisistä poikkeamista, kyberuhkista ja haavoittuvuuksista, vaarantumisindikaattoreista, taktiikasta, tekniikoista ja menettelyistä, kyberturvallisuushälytyksistä ja konfigurointityökaluista, saattavat edellyttää tiettyjen henkilötietoryhmien, kuten IP-osoitteiden, URL-osoitteiden, verkkotunnusten, sähköpostiosoitteiden ja, sikäli kuin niistä käy ilmi henkilötietoja, aikaleimojen käsittelyä. Toimivaltaisten viranomaisten, keskitettyjen yhteyspisteiden ja CSIRT-yksiköiden suorittamaa henkilötietojen käsittelyä voidaan pitää lakisääteisenä velvoitteena tai sen voidaan katsoa olevan tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi asetuksen (EU) 2016/679 6 artiklan 1 kohdan c tai e alakohdan ja 6 artiklan 3 kohdan mukaisesti taikka keskeisten ja tärkeiden toimijoiden oikeutettujen etujen toteuttamiseksi asetuksen (EU) 2016/679 6 artiklan 1 kohdan f alakohdan mukaisesti. Lisäksi kansallisessa lainsäädännössä voitaisiin vahvistaa säännöt, joiden nojalla toimivaltaiset viranomaiset, keskitetyt yhteyspisteet ja CSIRT-yksiköt voivat, siinä määrin kuin se on tarpeen ja oikeasuhteista keskeisten ja tärkeiden toimijoiden verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi, käsitellä erityisiä henkilötietoryhmiä asetuksen (EU) 2016/679 9 artiklan mukaisesti, erityisesti säätämällä asianmukaisista erityistoimenpiteistä luonnollisten henkilöiden perusoikeuksien ja etujen suojaamiseksi, myös tällaisten tietojen uudelleenkäyttöä koskevista teknisistä rajoituksista sekä viimeisintä kehitystä edustavien turvallisuustoimenpiteiden ja yksityisyyden suojan säilyttävien toimenpiteiden, kuten pseudonymisoinnin, käytöstä tai salauksen käytöstä, jos anonymisointi voi vaikuttaa merkittävästi aiottuun käyttötarkoitukseen.

(122) Jotta voidaan vahvistaa valvontavaltuuksia ja -toimenpiteitä, jotka auttavat varmistamaan sääntöjen tosiasiallisen noudattamisen, tässä direktiivissä olisi vahvistettava vähimmäisluettelo valvontatoimenpiteistä ja -keinoista, joiden avulla toimivaltaiset viranomaiset voivat valvoa keskeisiä ja tärkeitä toimijoita. Lisäksi tässä direktiivissä olisi säädettävä eri valvontajärjestelmästä keskeisille ja tärkeille toimijoille, jotta voidaan varmistaa kyseisten toimijoiden ja toimivaltaisten viranomaisten velvoitteiden oikeudenmukainen tasapaino. Sen vuoksi keskeisiin toimijoihin olisi sovellettava kattavaa valvontajärjestelmää, johon kuuluu etukäteis- ja jälkikäteisvalvonta, ja tärkeisiin toimijoihin olisi sovellettava kevyttä valvontajärjestelmää, johon kuuluu vain jälkikäteisvalvonta. Näin ollen tärkeitä toimijoita ei pitäisi vaatia dokumentoimaan järjestelmällisesti kyberturvallisuusriskien hallintatoimenpiteiden noudattamista, ja toimivaltaisten viranomaisten olisi harjoitettava reaktiivista jälkikäteisvalvontaa eikä niillä olisi oltava yleistä velvoitetta valvoa kyseisiä toimijoita. Tärkeiden toimijoiden jälkikäteisvalvonta voidaan käynnistää, jos toimivaltaisten viranomaisten tietoon tulee näyttöä, viitteitä tai tietoja, joiden perusteella kyseiset viranomaiset epäilevät, että tätä direktiiviä on ehkä rikottu. Tällaista näyttöä, viitteitä tai tietoja voivat olla esimerkiksi muiden viranomaisten, toimijoiden, kansalaisten, tiedotusvälineiden tai muiden lähteiden toimivaltaisille viranomaisille toimittamat tai julkisesti saatavilla olevat tiedot, tai toimivaltaisten viranomaiset voivat saada ne tietoonsa hoitaessaan tehtäviään.

(123) Toimivaltaisten viranomaisten valvontatehtävien suorittaminen ei saisi tarpeettomasti haitata asianomaisen toimijan liiketoimintaa. Kun toimivaltaiset viranomaiset suorittavat keskeisiin toimijoihin liittyviä valvontatehtäviään, kuten paikalla tehtäviä tarkastuksia ja muuta kuin paikalla toteutettavaa valvontaa, tämän direktiivin rikkomisten tutkintaa, turvallisuusauditointia tai turvallisuusskannausta, niiden olisi minimoitava vaikutus asianomaisen toimijan liiketoimintaan.

(124) Kun toimivaltaiset viranomaiset harjoittavat etukäteisvalvontaa, niiden olisi voitava päättää käytettävissään olevien valvontatoimenpiteiden ja -keinojen käytön etusijajärjestyksestä oikeasuhteisella tavalla. Tämä tarkoittaa, että toimivaltaiset viranomaiset voivat päättää etusijajärjestyksestä sellaisten valvontamenetelmien perusteella, joissa olisi sovellettava riskiperusteista lähestymistapaa. Tällaiset menetelmät voivat erityisesti sisältää kriteerejä tai vertailuarvoja, joiden mukaan keskeiset toimijat luokitellaan riskiluokkiin ja kullekin riskiluokalle määritetään suositeltavat valvontatoimenpiteet ja -keinot, kuten paikalla tehtävien tarkastusten, kohdennettujen turvallisuusauditointien tai turvallisuusskannausten käyttö, aikaväli ja tyypit sekä pyydettävien tietojen tyyppi ja yksityiskohtaisuus.

Tällaisten valvontamenetelmien ohella voitaisiin käyttää työohjelmia, ja niitä voitaisiin arvioida ja tarkastella uudelleen säännöllisesti, myös esimerkiksi resurssien jakamisen ja tarpeiden osalta. Julkishallinnon toimijoiden suhteen valvontavaltuuksia olisi käytettävä kansallisten lainsäädäntö- ja toimielinkehysten mukaisesti.

(125) Toimivaltaisten viranomaisten olisi varmistettava, että niille kuuluvia keskeisten ja tärkeiden toimijoiden valvontatehtäviä hoitavat koulutetut ammattilaiset, joilla olisi oltava kyseisten tehtävien suorittamiseen vaadittavat taidot, etenkin paikalla tehtäviä tarkastuksia ja muuta kuin paikalla toteutettavaa valvontaa, kuten tietokantojen, laitteistojen, palomuurien, salauksen ja verkkojen heikkouksien tunnistamista, varten. Nämä tarkastukset ja tämä valvonta olisi toteutettava objektiivisesti.

(126) Asianmukaisesti perustelluissa tapauksissa, joissa toimivaltainen viranomainen on tietoinen merkittävästä kyberuhkasta tai välittömästä riskistä, toimivaltaisen viranomaisen olisi voitava tehdä välittömästi täytäntöönpanopäätöksiä, joiden tarkoituksena on ehkäistä poikkeama tai hallita sitä.

(127) Jotta valvonta olisi tuloksekasta, olisi vahvistettava vähimmäisluettelo täytäntöönpanovaltuuksista, joita voidaan käyttää tässä direktiivissä säädettyjen kyberturvallisuusriskien hallintatoimenpiteiden ja raportointivelvoitteiden laiminlyönnin tapauksessa, ja vahvistettava selkeä ja johdonmukainen kehys tällaiselle täytäntöönpanolle kaikkialla unionissa. Olisi otettava asianmukaisesti huomioon tämä direktiivin rikkomisen luonne, vakavuus ja kesto, aiheutettu aineellinen tai aineeton vahinko, rikkomisen tahallisuus tai tuottamuksellisuus, aineellisen tai aineettoman vahingon ehkäisemiseksi tai lieventämiseksi toteutetut toimet, vastuun aste tai mahdolliset vastaavat aiemmat rikkomiset, yhteistyöhalukkuus toimivaltaisen viranomaisen kanssa ja mahdolliset muut raskauttavat tai lieventävät tekijät. Täytäntöönpanotoimenpiteiden, myös hallinnollisten sakkojen, olisi oltava oikeasuhteisia, ja niiden määräämiseen olisi sovellettava asianmukaisia menettelytakeita unionin oikeuden ja Euroopan unionin perusoikeuskirjan, jäljempänä ’perusoikeuskirja’, yleisten periaatteiden mukaisesti, mukaan lukien oikeus tehokkaisiin oikeussuojakeinoihin ja puolueettomaan tuomioistuimeen, syyttömyysolettama ja oikeus puolustukseen.

(128) Tässä direktiivissä ei edellytetä jäsenvaltioiden säätävän, että luonnolliset henkilöt, joiden tehtävänä on varmistaa, että toimija noudattaa tätä direktiiviä, ovat rikosoikeudellisessa tai siviilioikeudellisessa vastuussa vahingosta, jota kolmansille osapuolille on aiheutunut tämän direktiivin rikkomisen tuloksena.

(129) Tässä direktiivissä säädettyjen velvoitteiden tehokkaan täytäntöönpanon varmistamiseksi kullakin toimivaltaisella viranomaisella olisi oltava valtuudet määrätä tai pyytää määräämään hallinnollisia sakkoja.

(130) Jos hallinnollinen sakko määrätään keskeiselle tai tärkeälle toimijalle, joka on yritys, yritys olisi ymmärrettävä Euroopan unionin toiminnasta tehdyn sopimuksen 101 ja 102 artiklan mukaiseksi yritykseksi. Jos hallinnollinen sakko määrätään henkilölle, joka ei ole yritys, toimivaltaisen viranomaisen olisi otettava sakon sopivan määrän harkinnassa huomioon jäsenvaltion yleinen tulotaso ja asianomaisen henkilön taloudellinen tilanne. Olisi oltava jäsenvaltioiden vastuulla määrittää, onko viranomaisille määrättävä hallinnollisia sakkoja ja missä määrin. Hallinnollisen sakon määrääminen ei vaikuta toimivaltaisten viranomaisten muiden valtuuksien soveltamiseen eikä muihin seuraamuksiin, joista säädetään kansallisissa säännöksissä, joilla tämä direktiivi saatetaan osaksi kansallista lainsäädäntöä.

(131) Jäsenvaltioiden olisi voitava antaa säännöksiä rikosoikeudellisista seuraamuksista, joita määrätään niiden kansallisten säännösten rikkomisesta, joilla tämä direktiivi saatetaan osaksi kansallista lainsäädäntöä. Näiden kansallisten säännösten rikkomisesta määrättävien rikosoikeudellisten seuraamusten ja niihin liittyvien hallinnollisten seuraamusten määrääminen ei kuitenkaan saisi johtaa *ne bis in idem* -periaatteen, sellaisena kuin unionin tuomioistuin on sitä tulkinnut, rikkomiseen.

(132) Sikäli kuin tässä direktiivissä ei yhdenmukaisteta hallinnollisia seuraamuksia tai tarvittaessa muissa tapauksissa, esimerkiksi silloin, kun kyseessä on tämän direktiivin vakava rikkominen, jäsenvaltioiden olisi pantava täytäntöön järjestelmä, jossa määrätään tehokkaista, oikeasuhteisista ja varoittavista seuraamuksista. Tällaisten seuraamusten luonne ja se, ovatko ne rikosoikeudellisia vai hallinnollisia, olisi määriteltävä kansallisessa lainsäädännössä.

(133) Jotta voidaan edelleen vahvistaa tämän direktiivin rikkomiseen sovellettavien täytäntöönpanotoimenpiteiden vaikuttavuutta ja varoittavuutta, toimivaltaisilla viranomaisilla olisi oltava valtuudet keskeyttää tai pyytää keskeyttämään väliaikaisesti sertifiointi tai lupa, joka koskee keskeisen toimijan tarjoamia kaikkia asiaankuuluvia palveluja tai toimintoja tai osaa niistä, sekä pyytää kieltämään ketä tahansa luonnollista henkilöä, joka hoitaa johtotehtäviä toimitusjohtajan tai laillisen edustajan tasolla, hoitamasta johtotehtäviä. Kun otetaan huomioon tällaisten väliaikaisten keskeyttämisten tai kieltojen vakavuus ja vaikutus toimijoiden toimintaan ja viime kädessä niiden palvelujen käyttäjiin, niitä olisi sovellettava ainoastaan suhteessa rikkomisen vakavuuteen ja ottaen huomioon kunkin yksittäisen tapauksen olosuhteet, mukaan lukien rikkomisen tahallisuus tai tuottamuksellisuus, sekä mahdolliset aineellisen tai aineettoman vahingon ehkäisemiseksi tai lieventämiseksi toteutetut toimet. Tällaisia väliaikaisia keskeyttämisiä tai kieltoja olisi sovellettava vasta viimeisenä keinona eli sen jälkeen, kun muut tässä direktiivissä säädetyt asiaankuuluvat täytäntöönpanotoimenpiteet on käytetty, ja ainoastaan siihen asti, kun asianomainen toimija toteuttaa tarvittavat toimet korjatakseen ne puutteet tai noudattaakseen niitä toimivaltaisen viranomaisen vaatimuksia, joiden johdosta väliaikaisia keskeyttämisiä tai kieltoja sovellettiin. Tällaisten väliaikaisten keskeyttämisten tai kieltojen määräämiseen olisi sovellettava asianmukaisia menettelytakeita unionin oikeuden ja perusoikeuskirjan yleisten periaatteiden mukaisesti, mukaan lukien oikeus tehokkaisiin oikeussuojakeinoihin ja puolueettomaan tuomioistuimeen, syyttömyysolettama ja oikeus puolustukseen.

(134) Sen varmistamiseksi, että toimijat noudattavat tässä direktiivissä säädettyjä velvoitteitaan, jäsenvaltioiden olisi tehtävä yhteistyötä ja avustettava toisiaan valvonta- ja täytäntöönpanotoimenpiteissä, etenkin kun toimija tarjoaa palveluja useammassa kuin yhdessä jäsenvaltiossa tai kun sen verkko- ja tietojärjestelmät sijaitsevat muussa jäsenvaltiossa kuin siinä, jossa se tarjoaa palveluja. Avunantopyynnön saaneen toimivaltaisen viranomaisen olisi apua antaessaan toteutettava valvonta- tai täytäntöönpanotoimenpiteitä kansallisen lainsäädännön mukaisesti. Tämän direktiivin mukaisen keskinäisen avunannon sujuvuuden varmistamiseksi toimivaltaisten viranomaisten olisi käytettävä yhteistyöryhmää foorumina, jolla keskustellaan tapauksista ja yksittäisistä avunantopyynnöistä.

(135) Jotta voidaan varmistaa tehokas valvonta ja täytäntöönpano, erityisesti silloin kun tilanteella on rajatylittävä ulottuvuus, keskinäistä avunantoa koskevan pyynnön saaneen jäsenvaltion olisi kyseisen pyynnön asettamissa rajoissa toteutettava asianmukaisia valvonta- ja täytäntöönpanotoimenpiteitä suhteessa pyynnön kohteena olevaan toimijaan, joka tarjoaa palveluja tai jolla on verkko- ja tietojärjestelmä kyseisen jäsenvaltion alueella.

(136) Tässä direktiivissä olisi vahvistettava säännöt toimivaltaisten viranomaisten ja asetuksen (EU) 2016/679 mukaisten valvontaviranomaisten välistä yhteistyötä varten henkilötietoihin liittyvien tämän direktiivin rikkomisten käsittelemiseksi.

(137) Tällä direktiivillä olisi pyrittävä varmistamaan, että vastuu kyberturvallisuusriskien hallintatoimenpiteistä ja raportointivelvoitteista on keskeisten ja tärkeiden toimijoiden organisaatiossa korkealla tasolla. Sen vuoksi keskeisten ja tärkeiden toimijoiden hallintoelinten olisi hyväksyttävä kyberturvallisuusriskien hallintatoimenpiteet ja valvottava niiden täytäntöönpanoa.

(138) Jotta tämän direktiivin perusteella voidaan varmistaa kyberturvallisuuden yhteinen korkea taso kaikkialla unionissa, komissiolle olisi siirrettävä valta hyväksyä Euroopan unionin toiminnasta tehdyn sopimuksen 290 artiklan mukaisesti säädösvallan siirron nojalla annettavia delegoituja säädöksiä, joilla täydennetään tätä direktiiviä täsmentämällä ne keskeisten ja tärkeiden toimijoiden luokat, jotka on velvoitettava käyttämään tiettyjä sertifioituja TVT-tuotteita, TVT-palveluja ja TVT-prosesseja tai hankkimaan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän myöntämä sertifiointi. On erityisen tärkeää, että komissio asiaa valmistellessaan toteuttaa asianmukaiset kuulemiset, myös asiantuntijatasolla, ja että nämä kuulemiset toteutetaan paremmasta lainsäädännöstä 13 päivänä huhtikuuta 2016 tehdyssä toimielinten välisessä sopimuksessa ([22]) vahvistettujen periaatteiden mukaisesti. Jotta voitaisiin erityisesti varmistaa tasavertainen osallistuminen delegoitujen säädösten valmisteluun, Euroopan parlamentille ja neuvostolle toimitetaan kaikki asiakirjat samaan aikaan kuin jäsenvaltioiden asiantuntijoille, ja Euroopan parlamentin ja neuvoston asiantuntijoilla on järjestelmällisesti oikeus osallistua komission asiantuntijaryhmien kokouksiin, joissa valmistellaan delegoituja säädöksiä.

([22]) EUVL L 123, 12.5.2016, s. 1.

(139) Jotta voidaan varmistaa tämän direktiivin yhdenmukainen täytäntöönpano, komissiolle olisi siirrettävä täytäntöönpanovaltaa vahvistaa yhteistyöryhmän toiminnan edellyttämät menettelytapajärjestelyt ja kyberturvallisuusriskien hallintatoimenpiteitä koskevat tekniset, menetelmiin liittyvät ja alakohtaiset vaatimukset sekä täsmentää poikkeamista, kyberuhkista ja läheltä piti -tilanteista tehtävien ilmoitusten sekä merkittävistä kyberuhkista annettavien tiedonantojen tietosisältö, muoto ja ilmoitusmenettely sekä tapaukset, joissa poikkeama katsotaan merkittäväksi. Tätä valtaa olisi käytettävä Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 182/2011 ([23]) mukaisesti.

(140) Komission olisi tarkasteltava tätä direktiiviä määräajoin uudelleen sidosryhmiä kuultuaan, erityisesti sen selvittämiseksi, onko aiheellista ehdottaa yhteiskunnan, politiikan, tekniikan ja markkinaolojen kehitykseen perustuvia muutoksia. Komission olisi osana näitä uudelleentarkasteluja arvioitava asianomaisten toimijoiden koon sekä tämän direktiivin liitteissä tarkoitettujen toimialojen, toimialan osien ja toimijatyyppien merkitystä talouden ja yhteiskunnan toiminnalle kyberturvallisuuden näkökulmasta. Komission olisi arvioitava muun muassa sitä, voitaisiinko tämän direktiivin soveltamisalaan kuuluvat palveluntarjoajat, jotka on nimetty Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2065 ([24]) 33 artiklan mukaisiksi erittäin suuriksi verkkoalustoiksi, määrittää tämän direktiivin mukaisiksi keskeisiksi toimijoiksi.

(141) Tällä direktiivillä annetaan ENISAlle uusia tehtäviä ja siten merkittävämpi rooli, minkä johdosta sitä saatetaan vaatia suorittamaan asetuksen (EU) 2019/881 mukaiset nykyiset tehtävänsä aiempaa korkeammalla vaatimustasolla. Sen varmistamiseksi, että ENISAlla on tarvittavat taloudelliset ja henkilöresurssit, jotta se voi suorittaa nykyiset ja uudet tehtävänsä ja selviytyä niistä entistä merkittävämmästä roolistaan johtuvalla, mahdollisesti korkeammalla vaatimustasolla, sen määrärahoja olisi vastaavasti lisättävä. Resurssien tehokkaan käytön varmistamiseksi ENISAlle olisi lisäksi jätettävä enemmän joustovaraa sen suhteen, miten se voi kohdentaa resursseja sisäisesti suorittaakseen tehtävänsä tehokkaasti ja vastatakseen odotuksiin.

(142) Jäsenvaltiot eivät voi riittävällä tavalla saavuttaa tämän direktiivin tavoitetta eli saavuttaa kyberturvallisuuden yhteinen korkea taso kaikkialla 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 kyseisen tavoitteen saavuttamiseksi.

(143) Tässä direktiivissä kunnioitetaan perusoikeuskirjassa tunnustettuja perusoikeuksia ja noudatetaan siinä tunnustettuja periaatteita, erityisesti oikeutta yksityiselämän ja viestien kunnioittamiseen, henkilötietojen suojaa, elinkeinovapautta, omistusoikeutta, oikeutta tehokkaisiin oikeussuojakeinoihin ja puolueettomaan tuomioistuimeen, syyttömyysolettamaa ja oikeutta puolustukseen. Oikeus tehokkaisiin oikeussuojakeinoihin on myös keskeisten ja tärkeiden toimijoiden tarjoamien palvelujen vastaanottajilla. Tämä direktiivi olisi pantava täytäntöön näiden oikeuksien ja periaatteiden mukaisesti.

(144) Euroopan tietosuojavaltuutettua on kuultu Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1725 ([25]) 42 artiklan 1 kohdan mukaisesti, ja hän on antanut lausuntonsa 11 päivänä maaliskuuta 2021 ([26]),

([23]) 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).

([24]) Euroopan parlamentin ja neuvoston asetus (EU) 2022/2065, annettu 19 päivänä lokakuuta 2022, digitaalisten palvelujen sisämarkkinoista ja direktiivin 2000/31/EY muuttamisesta (digipalvelusäädös) (EUVL L 277, 27.10.2022, s. 1).

([25]) Euroopan parlamentin ja neuvoston asetus (EU) 2018/1725, annettu 23 päivänä lokakuuta 2018, luonnollisten henkilöiden suojelusta unionin toimielinten, elinten ja laitosten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta sekä asetuksen (EY) N:o 45/2001 ja päätöksen N:o 1247/2002/EY kumoamisesta (EUVL L 295, 21.11.2018, s. 39).

([26]) EUVL C 183, 11.5.2021, s. 3.

OVAT HYVÄKSYNEET TÄMÄN DIREKTIIVIN:

I LUKU

YLEISET SÄÄNNÖKSET

1 artikla

Kohde

1. Tässä direktiivissä säädetään toimenpiteistä, joilla pyritään saavuttamaan kyberturvallisuuden yhteinen korkea taso kaikkialla unionissa sisämarkkinoiden toiminnan parantamiseksi.

2. Tätä varten tässä direktiivissä vahvistetaan

a) jäsenvaltioiden velvoitteet hyväksyä kansalliset kyberturvallisuusstrategiat sekä nimetä tai perustaa toimivaltaiset viranomaiset, kyberkriisinhallintaviranomaiset, kyberturvallisuusalan keskitetyt yhteyspisteet, jäljempänä 'keskitetyt yhteyspisteet', ja tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt, jäljempänä 'CSIRT-yksiköt';

b) kyberturvallisuusriskien hallintatoimenpiteet ja raportointivelvoitteet liitteessä I tai II tarkoitettua toimijatyyppiä oleville toimijoille ja direktiivissä (EU) 2022/2557 kriittisiksi toimijoiksi määritetyille toimijoille;

c) kyberturvallisuustietojen jakamista koskevat säännöt ja velvoitteet;

d) jäsenvaltioiden valvonta- ja täytäntöönpanovelvoitteet.

2 artikla

Soveltamisala

1. Tätä direktiiviä sovelletaan liitteissä I ja II tarkoitettua toimijatyyppiä oleviin julkisiin ja yksityisiin toimijoihin, jotka täyttävät suosituksen 2003/361/EY liitteessä olevan 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset tai ylittävät kyseisen artiklan 1 kohdassa säädetyt keskisuurten yritysten määrittelyssä käytettävät kynnysarvot ja jotka tarjoavat palvelujaan tai harjoittavat toimintaansa unionissa.

Mainitun suosituksen liitteessä olevan 3 artiklan 4 kohtaa ei sovelleta tätä direktiiviä sovellettaessa.

2. Tätä direktiiviä sovelletaan liitteessä I tai II tarkoitettua toimijatyyppiä oleviin toimijoihin niiden koosta riippumatta myös, kun

a) palvelujen tarjoajat ovat

   i) yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajia;

   ii) luottamuspalvelun tarjoajia;

   iii) aluetunnusrekisterejä ja DNS-palveluntarjoajia;

b) toimija tarjoaa ainoana jäsenvaltiossa palvelua, joka on yhteiskunnan tai talouden kriittisten toimintojen ylläpitämisen kannalta keskeinen;

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

d) häiriö toimijan tarjoamassa palvelussa voisi aiheuttaa merkittävän systeemisen riskin erityisesti aloilla, joilla tällaisella häiriöllä voisi olla rajatylittäviä vaikutuksia;

e) toimija on kriittinen, koska sillä on erityisen suuri merkitys kansallisella tai alueellisella tasolla kyseisen toimialan tai palvelutyypin tai jäsenvaltion muiden keskinäisriippuvaisten toimialojen kannalta;

f) toimija on julkishallinnon toimija,

i) jonka jäsenvaltio on kansallisen lainsäädäntönsä mukaisesti määritellyt keskustason julkishallinnon toimijaksi;

ii) jonka jäsenvaltio on kansallisen lainsäädäntönsä mukaisesti määritellyt aluetason julkishallinnon toimijaksi ja joka riskiperusteisen arvioinnin perusteella tarjoaa palveluja, joiden häiriintymisellä voisi olla merkittävä vaikutus yhteiskunnan tai talouden kriittisiin toimintoihin.

3. Tätä direktiiviä sovelletaan direktiivin (EU) 2022/2557 nojalla kriittisiksi toimijoiksi määritettyihin toimijoihin niiden koosta riippumatta.

4. Tätä direktiiviä sovelletaan verkkotunnusten rekisteröintipalveluja tarjoaviin toimijoihin niiden koosta riippumatta.

5. Jäsenvaltiot voivat säätää, että tätä direktiiviä sovelletaan

a) paikallistason julkishallinnon toimijoihin;

b) opetus- ja koulutusalan laitoksiin, etenkin kun niissä harjoitetaan olennaisen tärkeää tutkimustoimintaa.

6. Tämä direktiivi ei vaikuta jäsenvaltioiden velvollisuuteen taata kansallinen turvallisuus eikä niiden valtuuksiin huolehtia muista keskeisistä valtion tehtävistä, myös valtion alueellisen koskemattomuuden turvaamisesta ja yleisen järjestyksen ylläpitämisestä.

7. Tätä direktiiviä ei sovelleta julkishallinnon toimijoihin, jotka harjoittavat toimintaa kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla, mukaan lukien rikosten ennalta estäminen, tutkiminen, paljastaminen ja rikoksiin liittyvät syytetoimet.

8. Jäsenvaltiot voivat vapauttaa erityiset toimijat, jotka harjoittavat toimintaa kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla, mukaan lukien rikosten ennalta estäminen, tutkiminen, paljastaminen ja rikoksiin liittyvät syytetoimet, tai jotka tarjoavat palveluja yksinomaan tämän artiklan 7 kohdassa tarkoitetuille julkishallinnon toimijoille, 21 tai 23 artiklassa säädetyistä velvoitteista mainituissa toiminnoissa tai palveluissa. Tällöin VII luvussa tarkoitettuja valvonta- ja täytäntöönpanotoimenpiteitä ei sovelleta kyseisiin erityisiin toimintoihin ja palveluihin. Jos toimijoiden harjoittama toiminta tai tarjoamat palvelut ovat yksinomaan tässä kohdassa tarkoitettua tyyppiä, jäsenvaltiot voivat myös päättää vapauttaa kyseiset toimijat 3 ja 27 artiklassa säädetyistä velvoitteista.

9. Edellä olevia 7 ja 8 kohtaa ei sovelleta, jos toimija toimii luottamuspalvelun tarjoajana.

10. Tätä direktiiviä ei sovelleta toimijoihin, jotka jäsenvaltiot ovat jättäneet asetuksen (EU) 2022/2554 soveltamisalan ulkopuolelle mainitun asetuksen 2 artiklan 4 kohdan mukaisesti.

11. Tässä direktiivissä säädettyihin velvoitteisiin ei kuulu sellaisten tietojen antaminen, joiden luovuttaminen olisi vastoin jäsenvaltioiden keskeisiä kansalliseen turvallisuuteen, yleiseen turvallisuuteen tai puolustukseen liittyviä etuja.

12. Tämän direktiivin soveltaminen ei rajoita asetuksen (EU) 2016/679, direktiivin 2002/58/EY, Euroopan parlamentin ja neuvoston direktiivien 2011/93/EU ([27]) ja 2013/40/EU ([28]) eikä direktiivin (EU) 2022/2557 soveltamista.

13. Tietoja, jotka katsotaan luottamuksellisiksi unionin tai kansallisten sääntöjen, kuten liikesalaisuuksia koskevien sääntöjen, mukaisesti, saa vaihtaa komission ja muiden asiaankuuluvien 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. Tietojenvaihdossa on säilytettävä kyseisten tietojen luottamuksellisuus sekä suojeltava asianomaisten toimijoiden turvallisuusetuja ja kaupallisia etuja.

([27]) 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).

([28]) 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).

14. Toimijat, toimivaltaiset viranomaiset, keskitetyt yhteyspisteet ja CSIRT-yksiköt käsittelevät henkilötietoja, siinä määrin kuin se on tarpeen tämän direktiivin soveltamiseksi ja asetuksen (EU) 2016/679 mukaisesti, ja tällaisen käsittelyn on oltava erityisesti mainitun asetuksen 6 artiklan mukaista.

Yleisten sähköisten viestintäverkkojen tarjoajien tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajien tämän direktiivin nojalla suorittamassa henkilötietojen käsittelyssä on noudatettava unionin tietosuojalainsäädäntöä ja yksityisyyden suojaa koskevaa unionin lainsäädäntöä, erityisesti direktiiviä 2002/58/EY.

3 artikla

Keskeiset ja tärkeät toimijat

1. Tätä direktiiviä sovellettaessa seuraavia toimijoita pidetään keskeisinä toimijoina:

a) liitteessä I tarkoitettua toimijatyyppiä olevat toimijat, jotka ylittävät suosituksen 2003/361/EY liitteessä olevan 2 artiklan 1 kohdassa säädetyt keskisuurten yritysten määrittelyssä käytettävät kynnysarvot;

b) hyväksytyt luottamuspalvelun tarjoajat ja aluetunnusrekisterit sekä DNS-palveluntarjoajat niiden koosta riippumatta;

c) yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat, jotka täyttävät suosituksen 2003/361/EY liitteessä olevan 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset;

d) 2 artiklan 2 kohdan f alakohdan i alakohdassa tarkoitetut julkishallinnon toimijat;

e) muut liitteessä I tai II tarkoitettua toimijatyyppiä olevat toimijat, jotka jäsenvaltio on määrittänyt keskeisiksi toimijoiksi 2 artiklan 2 kohdan b–e alakohdan nojalla;

f) tämän direktiivin 2 artiklan 3 kohdassa tarkoitetut toimijat, jotka on määritetty kriittisiksi toimijoiksi direktiivin (EU) 2022/2557 nojalla;

g) jos jäsenvaltio niin säätää, toimijat, jotka kyseinen jäsenvaltio on ennen 16 päivää tammikuuta 2023 määrittänyt keskeisten palvelujen tarjoajiksi direktiivin (EU) 2016/1148 tai kansallisen lainsäädännön mukaisesti.

2. Tätä direktiiviä sovellettaessa liitteessä I tai II tarkoitettua toimijatyyppiä olevia toimijoita, joita ei pidetä keskeisinä toimijoina tämän artiklan 1 kohdan nojalla, pidetään tärkeinä toimijoina. Niihin luetaan myös toimijat, jotka jäsenvaltiot ovat määrittäneet tärkeiksi toimijoiksi 2 artiklan 2 kohdan b–e alakohdan nojalla.

3. Jäsenvaltioiden on viimeistään 17 päivänä huhtikuuta 2025 laadittava luettelo keskeisistä ja tärkeistä toimijoista sekä verkkotunnusten rekisteröintipalveluja tarjoavista toimijoista. Jäsenvaltioiden on tarkasteltava luetteloa uudelleen säännöllisesti ja vähintään kahden vuoden välein ja saatettava se tarvittaessa ajan tasalle.

4. Edellä 3 kohdassa tarkoitetun luettelon laatimiseksi jäsenvaltioiden on vaadittava kyseisessä kohdassa tarkoitettuja toimijoita toimittamaan toimivaltaisille viranomaisille ainakin seuraavat tiedot:

a) toimijan nimi;

b) osoite ja ajantasaiset yhteystiedot, mukaan lukien sähköpostiosoitteet, IP-osoitealueet ja puhelinnumerot;

c) tapauksen mukaan liitteessä I tai II tarkoitettu asiaankuuluva toimiala ja toimialan osa; ja

d) tapauksen mukaan luettelo jäsenvaltioista, joissa ne tarjoavat tämän direktiivin soveltamisalaan kuuluvia palveluja.

Edellä 3 kohdassa tarkoitettujen toimijoiden on ilmoitettava kaikista muutoksista tämän kohdan ensimmäisen alakohdan nojalla toimitettuihin tietoihin viipymättä ja joka tapauksessa kahden viikon kuluessa muutospäivästä.

Komissio antaa Euroopan unionin kyberturvallisuusviraston (ENISA) avustuksella ilman aiheetonta viivytystä ohjeita ja malleja tässä kohdassa säädettyjen velvoitteiden täyttämiseksi.

Jäsenvaltiot voivat perustaa kansallisia järjestelyjä, joiden ansiosta toimijat voivat itse kirjautua luetteloon.

5. Toimivaltaisten viranomaisten on viimeistään 17 päivänä huhtikuuta 2025 ja sen jälkeen kahden vuoden välein ilmoitettava

a) komissiolle ja yhteistyöryhmälle luetteloon 3 kohdan nojalla kirjattujen keskeisten ja tärkeiden toimijoiden lukumäärä kullakin liitteessä I tai II tarkoitetulla toimialalla ja toimialan osalla; ja

b) komissiolle asiaankuuluvat tiedot 2 artiklan 2 kohdan b–e alakohdan nojalla määritettyjen keskeisten ja tärkeiden toimijoiden lukumäärästä, näiden toimijoiden liitteessä I tai II tarkoitetusta toimialasta ja toimialan osasta, niiden tarjoaman palvelun tyypistä sekä siitä, minkä 2 artiklan 2 kohdan b–e alakohdan säännöksen nojalla ne on määritetty.

6. Jäsenvaltiot voivat 17 päivään huhtikuuta 2025 saakka ja komission pyynnöstä ilmoittaa komissiolle 5 kohdan b alakohdassa tarkoitettujen keskeisten ja tärkeiden toimijoiden nimet.

4 artikla

Alakohtaiset unionin säädökset

1. Jos alakohtaisissa unionin säädöksissä edellytetään, että keskeiset tai tärkeät toimijat ottavat käyttöön kyberturvallisuusriskien hallintatoimenpiteitä tai ilmoittavat merkittävistä poikkeamista, ja jos kyseiset vaatimukset ovat vaikutukseltaan vähintään tässä direktiivissä säädettyjä velvoitteita vastaavia, tällaisiin toimijoihin ei sovelleta tämän direktiivin asiaankuuluvia säännöksiä, myöskään VII luvun säännöksiä valvonnasta ja täytäntöönpanosta. Jos alakohtaiset unionin säädökset eivät kata tämän direktiivin soveltamisalaan kuuluvan toimialan kaikkia toimijoita, tämän direktiivin asiaankuuluvia säännöksiä sovelletaan edelleen niihin toimijoihin, joita kyseiset alakohtaiset unionin säädökset eivät kata.

2. Tämän artiklan 1 kohdassa tarkoitettujen vaatimusten katsotaan olevan vaikutukseltaan tässä direktiivissä säädettyjä velvoitteita vastaavia, kun

a) kyberturvallisuusriskien hallintatoimenpiteet ovat vaikutukseltaan vähintään 21 artiklan 1 ja 2 kohdassa säädettyjä toimenpiteitä vastaavia; tai

b) alakohtaisessa unionin säädöksessä säädetään tämän direktiivin mukaisten CSIRT-yksiköiden, toimivaltaisten viranomaisten tai keskitettyjen yhteyspisteiden välittömästä, tarvittaessa automaattisesta ja suorasta, pääsystä poikkeamailmoituksiin, jos merkittävistä poikkeamista ilmoittamista koskevat vaatimukset ovat vaikutukseltaan vähintään tämän direktiivin 23 artiklan 1–6 kohdassa säädettyjä vaatimuksia vastaavia.

3. Komissio antaa viimeistään 17 päivänä heinäkuuta 2023 ohjeita, joissa selvennetään 1 ja 2 kohdan soveltamista. Komissio tarkistaa näitä ohjeita säännöllisesti. Komissio ottaa kyseisiä ohjeita laatiessaan huomioon yhteistyöryhmän ja ENISAn mahdollisesti esittämät huomautukset.

5 artikla

Vähimmäistason yhdenmukaistaminen

Tällä direktiivillä ei estetä jäsenvaltioita antamasta tai pitämästä voimassa säännöksiä, joilla varmistetaan kyberturvallisuuden korkeampi taso, edellyttäen, että tällaiset säännökset ovat unionin oikeudessa säädettyjen jäsenvaltioiden velvoitteiden mukaisia.

6 artikla

Määritelmät

Tässä direktiivissä tarkoitetaan:

1) ’verkko- ja tietojärjestelmällä’

   a) direktiivin (EU) 2018/1972 2 artiklan 1 alakohdassa määriteltyä sähköistä viestintäverkkoa;

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

c) digitaalisia tietoja, joita a ja b alakohdassa tarkoitetuissa järjestelmissä säilytetään, käsitellään, haetaan tai siirretään näiden järjestelmien 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 tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden;

3) 'kyberturvallisuudella' asetuksen (EU) 2019/881 2 artiklan 1 alakohdassa määriteltyä kyberturvallisuutta;

4) 'kansallisella kyberturvallisuusstrategialla' jäsenvaltion yhtenäistä kehystä, jossa määritetään kyberturvallisuusalan strategiset tavoitteet ja painopisteet kyseisessä jäsenvaltiossa ja hallintotapa niiden saavuttamiseksi;

5) 'läheltä piti -tilanteella' tapahtumaa, joka olisi voinut vaarantaa verkko- ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden mutta jonka toteutuminen onnistuttiin estämään tai joka ei toteutunut;

6) 'poikkeamalla' tapahtumaa, joka vaarantaa verkko- ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden;

7) 'laajamittaisella kyberturvallisuuspoikkeamalla' poikkeamaa, joka aiheuttaa niin laajan häiriön, ettei yksittäisellä jäsenvaltiolla ole valmiuksia hallita sitä, tai jolla on merkittävä vaikutus vähintään kahteen jäsenvaltioon;

8) 'poikkeaman käsittelyllä' mitä tahansa toimia ja menettelyjä, joilla pyritään ehkäisemään ja havaitsemaan poikkeama, analysoimaan, rajoittamaan tai hallitsemaan sitä ja palautumaan siitä;

9) 'riskillä' poikkeaman aiheuttamien menetysten tai häiriön mahdollisuutta, joka ilmaistaan tällaisten menetysten tai häiriön suuruuden ja kyseisen poikkeaman toteutumisen todennäköisyyden yhdistelmänä;

10) 'kyberuhkalla' asetuksen (EU) 2019/881 2 artiklan 8 alakohdassa määriteltyä kyberuhkaa;

11) 'merkittävällä kyberuhkalla' kyberuhkaa, jonka voidaan sen teknisten ominaisuuksien perusteella olettaa vaikuttavan mahdollisesti vakavasti toimijan verkko- ja tietojärjestelmiin tai toimijan palvelujen käyttäjiin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa;

12) 'TVT-tuotteella' asetuksen (EU) 2019/881 2 artiklan 12 alakohdassa määriteltyä tieto- ja viestintätekniikan tuotetta;

13) 'TVT-palvelulla' asetuksen (EU) 2019/881 2 artiklan 13 alakohdassa määriteltyä tieto- ja viestintätekniikan palvelua;

14) 'TVT-prosessilla' asetuksen (EU) 2019/881 2 artiklan 14 alakohdassa määriteltyä tieto- ja viestintätekniikan prosessia;

15) 'haavoittuvuudella' TVT-tuotteiden tai TVT-palvelujen heikkoutta, alttiutta tai vikaa, jota kyberuhka voi hyödyntää;

16) 'standardilla' Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1025/2012 ([29]) 2 artiklan 1 alakohdassa määriteltyä standardia;

17) 'teknisellä eritelmällä' asetuksen (EU) N:o 1025/2012 2 artiklan 4 alakohdassa määriteltyä teknistä eritelmää;

([29]) 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).

18) 'internetin yhdysliikennepisteellä' verkkoinfrastruktuurin osaa, joka mahdollistaa useamman kuin kahden riippumattoman verkon (autonomisen järjestelmän) yhdistämisen pääasiassa internetliikenteen välittämisen helpottamiseksi, joka tarjoaa yhteenliitäntää ainoastaan autonomisille järjestelmille ja joka ei edellytä minkään yhteenliittämänsä kahden autonomisen järjestelmän väliseltä internetliikenteeltä kulkemista minkään kolmannen autonomisen järjestelmän kautta eikä muokkaa tällaista liikennettä tai muutoin puutu siihen;

19) 'verkkotunnusjärjestelmällä' tai 'DNS-järjestelmällä' hierarkkista hajautettua nimipalvelujärjestelmää, joka mahdollistaa internetpalvelujen ja -resurssien yksilöimisen niin, että loppukäyttäjien laitteet voivat käyttää internetin reititys- ja yhteyspalveluja kyseisten palvelujen ja resurssien saavuttamiseen;

20) 'DNS-palveluntarjoajalla' toimijaa, joka tarjoaa

a) yleisesti saatavilla olevia rekursiivisia verkkotunnusten selvityspalveluja internetin loppukäyttäjille; tai

b) auktoritatiivisia verkkotunnusten selvityspalveluja kolmansille osapuolille, lukuun ottamatta juurinimipalvelimia;

21) 'aluetunnusrekisterillä' toimijaa, jolle on myönnetty oikeus hallinnoida tiettyä aluetunnusta ja joka kyseistä aluetunnusta hallinnoidessaan vastaa muun muassa verkkotunnusten rekisteröinnistä kyseisen aluetunnuksen alle sekä kyseisen aluetunnuksen teknisestä toiminnasta, myös siihen liittyvien nimipalvelinten toiminnasta, sen tietokantojen ylläpidosta ja aluetunnuksen vyöhyketiedostojen jakelusta nimipalvelimille, riippumatta siitä, suorittaako toimija kyseiset toiminnot itse vai ulkoistaako se ne, ja lukuun ottamatta tilanteita, joissa rekisteri käyttää aluetunnuksia vain omiin tarkoituksiinsa;

22) 'verkkotunnusten rekisteröintipalveluja tarjoavalla toimijalla' verkkotunnusvälittäjää tai verkkotunnusvälittäjien puolesta toimivaa tahoa, kuten yksityisyys- tai välityspalvelujen tarjoajaa tai jälleenmyyjää;

23) 'digitaalisella palvelulla' Euroopan parlamentin ja neuvoston direktiivin (EU) 2015/1535 ([30]) 1 artiklan 1 kohdan b alakohdassa tarkoitettua palvelua;

24) 'luottamuspalvelulla' asetuksen (EU) N:o 910/2014 3 artiklan 16 alakohdassa määriteltyä luottamuspalvelua;

25) 'luottamuspalvelun tarjoajalla' asetuksen (EU) N:o 910/2014 3 artiklan 19 alakohdassa määriteltyä luottamuspalvelu tarjoajaa;

26) 'hyväksytyllä luottamuspalvelulla' asetuksen (EU) N:o 910/2014 3 artiklan 17 alakohdassa määriteltyä hyväksyttyä luottamuspalvelua;

27) 'hyväksytyllä luottamuspalvelun tarjoajalla' asetuksen (EU) N:o 910/2014 3 artiklan 20 alakohdassa määriteltyä hyväksyttyä luottamuspalvelun tarjoajaa;

28) 'verkossa toimivalla markkinapaikalla' Euroopan parlamentin ja neuvoston direktiivin 2005/29/EY ([31]) 2 artiklan n alakohdassa määriteltyä verkossa toimivaa markkinapaikkaa;

29) 'verkossa toimivalla hakukoneella' Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/1150 ([32]) 2 artiklan 5 alakohdassa tarkoitettua verkossa toimivaa hakukonetta;

30) 'pilvipalvelulla' digitaalista palvelua, joka tarjoaa laajaan etäkäyttöön skaalattavan ja joustavan joukon jaettavissa olevia ja tarveperusteisesti ohjattavia tietoteknisiä resursseja, myös sijainniltaan hajautettuja resursseja;

([30]) 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).

([31]) 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).

([32]) 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).

31) ’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;

32) ’sisällönjakeluverkolla’ maantieteellisesti hajautettujen palvelimien verkkoa, jonka tarkoituksena on varmistaa digitaalisen sisällön ja digitaalisten palvelujen hyvä saatavuus, käytettävyys ja nopea jakelu internetin käyttäjille sisällön ja palvelujen tarjoajien puolesta;

33) ’verkkoyhteisöalustalla’ alustaa, jonka avulla loppukäyttäjät voivat olla yhteydessä toisiinsa, jakaa sisältöä, hakea tietoa ja viestiä keskenään monenlaisilla päätelaitteilla, erityisesti pikaviestikeskustelujen, julkaisujen, videoiden ja suositusten muodossa;

34) ’edustajalla’ unioniin sijoittautunutta luonnollista henkilöä tai oikeushenkilöä, joka on nimenomaisesti nimetty toimimaan unioniin sijoittautumattoman DNS-palveluntarjoajan, aluetunnusrekisterin, verkkotunnusten rekisteröinti-palveluja tarjoavan toimijan, pilvipalveluntarjoajan, datakeskuspalvelun tarjoajan, sisällönjakeluverkon tarjoajan, hallintapalvelun tarjoajan, tietoturvapalveluntarjoajan tai verkossa toimivan markkinapaikan tarjoajan, verkossa toimivan hakukoneen tarjoajan tai verkkoyhteisöalustan tarjoajan puolesta ja johon toimivaltainen viranomainen tai CSIRT-yksikkö voi ottaa yhteyttä kyseisen toimijan sijasta, kun on kyse toimijan tämän direktiivin mukaisista velvoitteista;

35) ’julkishallinnon toimijalla’ jäsenvaltiossa kansallisen lainsäädännön mukaisesti julkishallinnon toimijaksi tunnustettua toimijaa, lukuun ottamatta oikeuslaitosta, parlamentteja ja keskuspankkeja, 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) sitä rahoittavat pääosin valtio, alueviranomaiset tai muut julkisoikeudelliset laitokset, sen johto on näiden viranomaisten tai laitosten valvonnan alainen taikka 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 henkilöiden, tavaroiden, palvelujen tai pääoman rajatylittävässä liikkuvuudessa;

36) ’yleisellä sähköisellä viestintäverkolla’ direktiivin (EU) 2018/1972 2 artiklan 8 alakohdassa määriteltyä yleistä sähköistä viestintäverkkoa;

37) ’sähköisellä viestintäpalvelulla’ direktiivin (EU) 2018/1972 2 artiklan 4 alakohdassa määriteltyä sähköistä viestintä-palvelua;

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

39) ’hallintapalvelun tarjoajalla’ toimijaa, joka tarjoaa TVT-tuotteiden, verkkojen, infrastruktuurin, sovellusten tai muiden verkko- ja tietojärjestelmien asentamiseen, hallintaan, käyttöön tai ylläpitoon liittyviä palveluja joko asiakkaan tiloissa tai etäyhteyden välityksellä toteutettavan tuen tai aktiivisen ylläpidon muodossa;

40) ’tietoturvapalveluntarjoajalla’ hallintapalvelun tarjoajaa, joka toteuttaa kyberturvallisuusriskien hallintatoimia tai antaa tukea niitä varten;

41) ’tutkimusorganisaatiolla’ toimijaa, jonka ensisijaisena tavoitteena on harjoittaa soveltavaa tutkimusta tai kokeellista kehitystyötä kyseisen tutkimuksen tulosten hyödyntämiseksi kaupallisiin tarkoituksiin mutta joka ei ole opetus- ja koulutusalan laitos.

II LUKU

KOORDINOIDUT KYBERTURVALLISUUSKEHYKSET

7 artikla

Kansallinen kyberturvallisuusstrategia

1. Kunkin jäsenvaltion on hyväksyttävä kansallinen kyberturvallisuusstrategia, jossa määritetään strategiset tavoitteet, kyseisten tavoitteiden saavuttamiseksi tarvittavat resurssit sekä asianmukaiset politiikka- ja sääntelytoimenpiteet kyberturvallisuuden korkean tason saavuttamiseksi ja ylläpitämiseksi. Kansalliseen kyberturvallisuusstrategiaan on sisällyttävä:

a) jäsenvaltion kyberturvallisuusstrategian tavoitteet ja painopisteet, jotka kattavat erityisesti liitteissä I ja II tarkoitetut toimialat;

b) hallintokehys tämän kohdan a alakohdassa tarkoitettujen tavoitteiden ja painopisteiden saavuttamiseksi, mukaan lukien 2 kohdassa tarkoitetut toimintaperiaatteet;

c) hallintokehys, jossa selvennetään asiaankuuluvien kansallisen tason sidosryhmien tehtävät ja vastuut ja joka tukee tämän direktiivin mukaisten toimivaltaisten viranomaisten, keskitettyjen yhteyspisteiden ja CSIRT-yksiköiden välistä yhteistyötä ja koordinointia kansallisella tasolla sekä kyseisten elinten ja alakohtaisten unionin säädösten mukaisten toimivaltaisten viranomaisten välistä koordinointia ja yhteistyötä;

d) menettely asiaankuuluvien toimintojen määrittämiseksi ja arvio riskeistä kyseisessä jäsenvaltiossa;

e) toimenpiteet, joilla varmistetaan poikkeamiin varautuminen, kyky hallita niitä ja niistä palautuminen, mukaan lukien julkisen ja yksityisen sektorin yhteistyö;

f) luettelo kansallisen kyberturvallisuusstrategian täytäntöönpanoon osallistuvista eri viranomaisista ja sidosryhmistä;

g) toimintakehys tämän direktiivin mukaisten toimivaltaisten viranomaisten ja direktiivin (EU) 2022/2557 mukaisten toimivaltaisten viranomaisten välisen koordinoinnin tehostamiseksi, jotta ne voivat tarvittaessa vaihtaa tietoja riskeistä, kyberuhkista ja poikkeamista ja muista kuin kyberturvallisuuteen liittyvistä riskeistä, uhkista ja poikkeamista sekä hoitaa valvontatehtävänsä;

h) suunnitelma ja tarvittavat toimenpiteet kansalaisten yleisen kyberturvallisuustietoisuuden parantamiseksi.

2. Jäsenvaltioiden on erityisesti vahvistettava kansallisessa kyberturvallisuusstrategiassaan toimintaperiaatteet, joilla

a) huolehditaan kyberturvallisuudesta sellaisten TVT-tuotteiden ja TVT-palvelujen toimitusketjussa, joita toimijat käyttävät palvelujensa tarjoamiseen;

b) otetaan käyttöön ja määritetään julkisissa hankinnoissa TVT-tuotteita ja TVT-palveluja koskevat kyberturvallisuusvaatimukset, mukaan lukien kyberturvallisuussertifiointiin, salaukseen ja avoimen lähdekoodin kyberturvallisuustuotteiden käyttöön liittyvät vaatimukset;

c) hallitaan haavoittuvuuksia, myös edistämällä ja helpottamalla 12 artiklan 1 kohdan mukaista koordinoitua haavoittuvuuksien julkistamista;

d) ylläpidetään avoimen internetin yleisen ydinverkon yleistä saatavuutta, eheyttä ja luottamuksellisuutta, tarvittaessa myös merenalaisten tietoliikennekaapelien kyberturvallisuutta;

e) edistetään sellaisten asiaankuuluvien kehittyneiden teknologioiden kehittämistä ja integrointia, joilla pyritään panemaan täytäntöön viimeisintä kehitystä edustavia kyberturvallisuusriskien hallintatoimenpiteitä;

f) edistetään ja kehitetään kyberturvallisuutta koskevaa valistusta ja koulutusta, kyberturvallisuustaitoja, kyberturvallisuutta koskevia tietoisuuden lisäämistä ja tutkimus- ja kehitysaloitteita sekä kansalaisille, sidosryhmille ja toimijoille suunnattua ohjeistusta hyvistä kyberhygieniakäytännöistä ja -hallintakeinoista;

g) tuetaan akateemisia ja tutkimuslaitoksia niiden kehittäessä ja parantaessa kyberturvallisuustyökaluja ja suojattua verkkoinfrastruktuuria ja edistäessä niiden käyttöönottoa;

h) tuetaan asiaankuuluvien menettelyjen ja asianmukaisten tiedonjakovälineiden avulla vapaaehtoista kyberturvallisuustietojen jakamista toimijoiden välillä unionin oikeuden mukaisesti;

i) vahvistetaan pienten ja keskisuurten yritysten, erityisesti tämän direktiivin soveltamisalaan kuulumattomien yritysten, kyberresilienssiä ja kyberhygienian perustasoa tarjoamalla niiden erityistarpeisiin sovitettua helposti saatavilla olevaa ohjausta ja tukea;

j) edistetään aktiivista kybersuojausta.

3. Jäsenvaltioiden on annettava kansalliset kyberturvallisuusstrategiansa komissiolle tiedoksi kolmen kuukauden kuluessa niiden hyväksymisestä. Jäsenvaltiot voivat jättää pois kansalliseen turvallisuuteensa liittyviä tietoja tällaisista tiedonannoista.

4. Jäsenvaltioiden on arvioitava kansallista kyberturvallisuusstrategiaansa säännöllisesti ja vähintään viiden vuoden välein keskeisten suorituskykyindikaattorien perusteella ja tarvittaessa ajantasaistettava strategiansa. ENISA avustaa jäsenvaltioita niiden pyynnöstä kansallisen kyberturvallisuusstrategian ja sen arvioinnissa käytettävien keskeisten suorituskykyindikaattorien kehittämisessä tai ajantasaistamisessa, jotta strategia vastaisi tässä direktiivissä säädettyjä vaatimuksia ja velvoitteita.

8 artikla

Toimivaltaiset viranomaiset ja keskitetyt yhteyspisteet

1. Kunkin jäsenvaltion on nimettävä tai perustettava yksi tai useampi toimivaltainen viranomainen, joka vastaa kyberturvallisuudesta ja VII luvussa tarkoitetuista valvontatehtävistä, jäljempänä ’toimivaltaiset viranomaiset’.

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

3. Kunkin jäsenvaltion on nimettävä tai perustettava keskitetty yhteyspiste. Jos jäsenvaltio nimeää tai perustaa 1 kohdan nojalla vain yhden toimivaltaisen viranomaisen, kyseinen toimivaltainen viranomainen toimii myös kyseisen jäsenvaltion keskitettynä yhteyspisteenä.

4. Kunkin keskitetyn yhteyspisteen on huolehdittava yhteydenpidosta ja varmistettava jäsenvaltionsa viranomaisten rajatylittävä yhteistyö muiden jäsenvaltioiden asiaankuuluvien viranomaisten ja tarvittaessa komission ja ENISAn kanssa sekä varmistettava toimialarajat ylittävä yhteistyö jäsenvaltionsa muiden toimivaltaisten viranomaisten kanssa.

5. Jäsenvaltioiden on varmistettava, että niiden toimivaltaisilla viranomaisilla ja keskitetyllä yhteyspisteellä on riittävät resurssit suorittaa niille osoitetut tehtävät tuloksekkaasti ja tehokkaasti ja siten saavuttaa tämän direktiivin tavoitteet.

6. Kunkin jäsenvaltion on ilmoitettava komissiolle ilman aiheetonta viivytystä 1 kohdassa tarkoitetun toimivaltaisen viranomaisen ja 3 kohdassa tarkoitetun keskitetyn yhteyspisteen nimi, kyseisten viranomaisten tehtävät ja näiden tietojen mahdolliset myöhemmät muutokset. Kunkin jäsenvaltion on julkistettava toimivaltaisen viranomaisensa nimi. Komissio asettaa julkisesti saataville luettelon keskitetyistä yhteyspisteistä.

9 artikla

Kansalliset kyberkriisinhallintakehykset

1. Kunkin jäsenvaltion on nimettävä tai perustettava yksi tai useampi toimivaltainen viranomainen, joka vastaa laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallinnasta, jäljempänä ’kyberkriisinhallintaviranomaiset’. Jäsenvaltioiden on varmistettava, että kyseisillä viranomaisilla on riittävät resurssit suorittaa niille osoitetut tehtävät tuloksekkaasti ja tehokkaasti. Jäsenvaltioiden on varmistettava johdonmukaisuus käytössä olevien yleisten kansallisten kriisinhallintakehysten kanssa.

2. Jos jäsenvaltio nimeää tai perustaa 1 kohdan nojalla useamman kuin yhden kyberkriisinhallintaviranomaisen, sen on selkeästi ilmoitettava, mikä näistä viranomaisista toimii koordinaattorina laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallinnassa.

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

4. Kunkin jäsenvaltion on laadittava kansallinen laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallintasuunnitelma, jossa vahvistetaan laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallinnan tavoitteet ja järjestelyt. Kyseisessä suunnitelmassa on vahvistettava erityisesti seuraavat seikat:

a) kansallisten varautumiskeinojen ja -toimien tavoitteet;

b) kyberkriisinhallintaviranomaisten tehtävät ja vastuut;

c) kyberkriisien hallintamenettelyt, mukaan lukien niiden sisällyttäminen yleiseen kansalliseen kriisinhallintakehykseen, ja tiedonvaihtokanavat;

d) kansalliset varautumiskeinot, mukaan lukien harjoitukset ja koulutustoimenpiteet;

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

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

5. Kunkin jäsenvaltion on ilmoitettava komissiolle kolmen kuukauden kuluessa 1 kohdassa tarkoitetun kyberkriisinhallintaviranomaisen nimeämisestä tai perustamisesta viranomaisensa nimi ja sen mahdolliset myöhemmät muutokset. Jäsenvaltioiden on toimitettava komissiolle ja Euroopan kyberkriisien yhteysorganisaatioiden verkostolle (EU-CyCLONe) 4 kohdan vaatimuksiin liittyvät asiaankuuluvat tiedot kansallisista laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallintasuunnitelmistaan kolmen kuukauden kuluessa kyseisten suunnitelmien hyväksymisestä. Jäsenvaltiot voivat tässä yhteydessä jättää pois tietoja, jos ja siinä määrin kuin se on kansallisen turvallisuuden kannalta välttämätöntä.

10 artikla

Tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (CSIRT-yksiköt)

1. Kunkin jäsenvaltion on nimettävä tai perustettava yksi tai useampi CSIRT-yksikkö. CSIRT-yksikkö voidaan nimetä tai perustaa toimivaltaisen viranomaisen yhteyteen. CSIRT-yksikön on täytettävä 11 artiklan 1 kohdassa säädetyt vaatimukset, katettava ainakin liitteissä I ja II tarkoitetut toimialat, toimialan osat ja toimijatyypit ja vastattava poikkeamien käsittelystä tarkasti määrättyä prosessia noudattaen.

2. Jäsenvaltioiden on varmistettava, että kullakin CSIRT-yksiköllä on riittävät resurssit suorittaa 11 artiklan 3 kohdassa säädetyt tehtävänsä tuloksekkaasti.

3. Jäsenvaltioiden on varmistettava, että kullakin CSIRT-yksiköllä on käytössään asianmukainen, suojattu ja häiriönsietokykyinen viestintä- ja tietoinfrastruktuuri tietojen vaihtamiseen keskeisten ja tärkeiden toimijoiden ja muiden asiaankuuluvien sidosryhmien kanssa. Tätä varten jäsenvaltioiden on varmistettava, että kukin CSIRT-yksikkö edistää suojattujen tiedonjakovälineiden käyttöönottoa.

4. CSIRT-yksiköiden on tehtävä yhteistyötä ja tarvittaessa vaihdettava asiaankuuluvia tietoja 29 artiklan mukaisesti keskeisten ja tärkeiden toimijoiden alakohtaisten tai monialaisten yhteisöjen kanssa.

5. CSIRT-yksiköiden on osallistuttava 19 artiklan mukaisesti järjestettäviin vertaisarviointeihin.

6. Jäsenvaltioiden on varmistettava, että niiden CSIRT-yksiköt tekevät tuloksekasta, tehokasta ja suojattua yhteistyötä CSIRT-verkostossa.

7. CSIRT-yksiköt voivat luoda yhteistyösuhteita kolmansien maiden tietoturvaloukkauksiin reagoiviin ja niitä tutkiviin kansallisiin yksiköihin. Jäsenvaltioiden on tällaisia yhteistyösuhteita varten helpotettava tuloksekasta, tehokasta ja suojattua tietojenvaihtoa kyseisten kolmansien maiden tietoturvaloukkauksiin reagoivien ja niitä tutkivien kansallisten yksiköiden kanssa käyttäen asiaankuuluvia tiedonjakoprotokollia, mukaan lukien Traffic Light Protocol -käsittelyluokitus. CSIRT-yksiköt voivat vaihtaa asiaankuuluvia tietoja kolmansien maiden tietoturvaloukkauksiin reagoivien ja niitä tutkivien kansallisten yksiköiden kanssa, myös henkilötietoja unionin tietosuojalainsäädännön mukaisesti.

8. CSIRT-yksiköt voivat tehdä yhteistyötä kolmansien maiden tietoturvaloukkauksiin reagoivien ja niitä tutkivien kansallisten yksiköiden tai vastaavien kolmansien maiden elinten kanssa erityisesti avustaakseen niitä kyberturvallisuus-asioissa.

9. Kunkin jäsenvaltion on ilmoitettava komissiolle ilman aiheetonta viivytystä tämän artiklan 1 kohdassa tarkoitetun CSIRT-yksikön ja 12 artiklan 1 kohdan nojalla koordinaattoriksi nimetyn CSIRT-yksikön nimi, kunkin yksikön keskeisiin ja tärkeisiin toimijoihin liittyvät tehtävät ja näiden tietojen mahdolliset myöhemmät muutokset.

10. Jäsenvaltiot voivat pyytää ENISAa avustamaan CSIRT-yksiköidensä toiminnan kehittämisessä.

11 artikla

CSIRT-yksiköiden vaatimukset, tekniset valmiudet ja tehtävät

1. CSIRT-yksiköiden on täytettävä seuraavat vaatimukset:

a) CSIRT-yksiköiden on varmistettava viestintäkanaviensa kattava saatavuus välttäen viestinnän täysin katkaisevia yksittäisiä vikaantumispisteitä ja ylläpidettävä useita viestintäkeinoja, joilla muut voivat ottaa niihin ja ne voivat ottaa muihin yhteyttä milloin tahansa. CSIRT-yksiköiden on määritettävä selkeästi viestintäkanavat ja tiedotettava niistä kohderyhmilleen ja yhteistyökumppaneilleen;

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

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

d) CSIRT-yksiköiden on varmistettava toimintojensa luottamuksellisuus ja luotettavuus;

e) CSIRT-yksiköillä on oltava riittävä henkilöstö palvelujensa jatkuvan saatavuuden varmistamiseksi, ja niiden on varmistettava henkilöstönsä asianmukainen koulutus;

f) CSIRT-yksiköillä on oltava varajärjestelmät ja -työtilat palvelujensa jatkuvuuden varmistamiseksi.

CSIRT-yksiköt voivat osallistua kansainvälisiin yhteistyöverkostoihin.

2. Jäsenvaltioiden on varmistettava, että niiden CSIRT-yksiköillä on yhdessä tarvittavat tekniset valmiudet suorittaa 3 kohdassa tarkoitetut tehtävät. Jäsenvaltioiden on varmistettava, että niiden CSIRT-yksiköille osoitetaan riittävät resurssit, jotta niillä olisi riittävästi henkilöstöä teknisten valmiuksiensa kehittämisen mahdollistamiseksi.

3. CSIRT-yksiköiden tehtävänä on

a) seurata ja analysoida kyberuhkia, haavoittuvuuksia ja poikkeamia kansallisella tasolla ja avustaa pyynnöstä asianomaisia keskeisiä ja tärkeitä toimijoita näiden verkko- ja tietojärjestelmien reaaliaikaisessa tai lähes reaaliaikaisessa seurannassa;

b) antaa kyberuhkia, haavoittuvuuksia ja poikkeamia koskevia ennakkovaroituksia, hälytyksiä, ilmoituksia ja tietoja keskeisille ja tärkeille toimijoille sekä toimivaltaisille viranomaisille ja muille asianomaisille sidosryhmille, mahdollisuuksien mukaan lähes reaaliaikaisesti;

c) reagoida poikkeamiin ja avustaa tapauksen mukaan asianomaisia keskeisiä ja tärkeitä toimijoita;

d) kerätä ja analysoida forensisia tietoja ja laatia dynaamisia riski- ja poikkeama-analyysejä ja ylläpitää kyberturvallisuuden tilannekuvaa;

e) suorittaa keskeisen tai tärkeän toimijan pyynnöstä asianomaisen toimijan verkko- ja tietojärjestelmien ennakoiva skannaus sellaisten haavoittuvuuksien havaitsemiseksi, joilla voi olla merkittävä vaikutus;

f) osallistua CSIRT-verkostoon ja antaa valmiuksiensa ja osaamistasonsa mukaan keskinäistä apua muille CSIRT-verkoston jäsenille näiden pyynnöstä;

g) toimia tapauksen mukaan koordinaattorina 12 artiklan 1 kohdan mukaista koordinoitua haavoittuvuuksien julkistamisprosessia varten;

h) edistää suojattujen tiedonjakovälineiden käyttöönottoa 10 artiklan 3 kohdan mukaisesti.

CSIRT-yksiköt voivat suorittaa keskeisten ja tärkeiden toimijoiden yleisesti saatavilla olevien verkko- ja tietojärjestelmien ennakoivaa, ei-intrusiivista skannausta. Tällaisen skannauksen tarkoituksena on havaita haavoittuvat tai epäturvallisesti konfiguroidut verkko- ja tietojärjestelmät ja ilmoittaa niistä asianomaisille toimijoille. Skannaus ei saa haitata asianomaisten toimijoiden palvelujen toimintaa.

Suorittaessaan ensimmäisessä alakohdassa tarkoitettuja tehtäviä CSIRT-yksiköt voivat asettaa etusijalle tiettyjä tehtäviä soveltaen riskiperusteista lähestymistapaa.

4. CSIRT-yksiköiden on luotava yhteistyösuhteet asiaankuuluviin yksityisen sektorin sidosryhmiin, jotta tämän direktiivin tavoitteet voidaan saavuttaa.

5. CSIRT-yksiköiden on 4 kohdassa tarkoitetun yhteistyön helpottamiseksi edistettävä yhteisten tai standardoitujen käytäntöjen, luokitusjärjestelmien ja taksonomioiden hyväksymistä ja käyttöä seuraavien osalta:

a) poikkeamien käsittelymenettelyt;

b) kriisinhallinta; ja

c) 12 artiklan 1 kohdan mukainen koordinoitu haavoittuvuuksien julkistaminen.

12 artikla

Koordinoitu haavoittuvuuden julkistaminen ja Euroopan haavoittuvuustietokanta

1. Kunkin jäsenvaltion on nimettävä yksi CSIRT-yksiköistään koordinaattoriksi koordinoitua haavoittuvuuksien julkistamista varten. Koordinaattoriksi nimetty CSIRT-yksikkö toimii luotettuna välittäjänä ja edesauttaa tarvittaessa vuorovaikutusta haavoittuvuudesta ilmoittavan luonnollisen henkilön tai oikeushenkilön ja mahdollisesti haavoittuvien TVT-tuotteiden tai TVT-palvelujen valmistajan tai tarjoajan välillä kumman tahansa osapuolen pyynnöstä. Koordinaattoriksi nimetyn CSIRT-yksikön tehtäviin kuuluvat

a) asianomaisten toimijoiden määrittäminen ja yhteyden ottaminen niihin;

b) haavoittuvuudesta ilmoittavien luonnollisten henkilöiden tai oikeushenkilöiden avustaminen; ja

c) haavoittuvuuden julkistamisen aikataulusta neuvotteleminen ja useisiin toimijoihin vaikuttavien haavoittuvuuksien hallinta.

Jäsenvaltioiden on varmistettava, että luonnolliset henkilöt tai oikeushenkilöt, jotka sitä pyytävät, voivat ilmoittaa haavoittuvuudesta koordinaattoriksi nimetylle CSIRT-yksikölle nimettömästi. Koordinaattoriksi nimetyn CSIRT-yksikön on varmistettava, että ilmoitetun haavoittuvuuden johdosta toteutetaan huolelliset jatkotoimet, ja taattava haavoittuvuudesta ilmoittavan luonnollisen henkilön tai oikeushenkilön nimettömyys. Jos ilmoitetulla haavoittuvuudella voi olla merkittävä vaikutus useamman kuin yhden jäsenvaltion toimijoihin, kunkin asianomaisen jäsenvaltion koordinaattoriksi nimetyn CSIRT-yksikön on tarvittaessa tehtävä yhteistyötä muiden koordinaattoreiksi nimettyjen CSIRT-yksiköiden kanssa CSIRT-verkostossa.

2. ENISA perustaa yhteistyöryhmää kuultuaan Euroopan haavoittuvuustietokannan ja ylläpitää sitä. Tätä varten ENISA luo asianmukaiset tietojärjestelmät, toimintaperiaatteet ja menettelyt ja pitää niitä yllä sekä hyväksyy tarvittavat tekniset ja organisatoriset toimenpiteet Euroopan haavoittuvuustietokannan turvallisuuden ja eheyden varmistamiseksi, etenkin siksi, että toimijat riippumatta siitä, kuuluvatko ne tämän direktiivin soveltamisalaan, ja niiden verkko- ja tietojärjestelmien toimittajat voisivat julkistaa ja kirjata vapaaehtoisesti yleisessä tiedossa olevia TVT-tuotteiden tai TVT-palvelujen haavoittuvuuksia. Kaikille sidosryhmille on annettava pääsy Euroopan haavoittuvuustietokannan sisältämiin haavoittuvuuksia koskeviin tietoihin. Kyseisen tietokannan on sisällettävä

a) tiedot, jotka sisältävät kuvauksen haavoittuvuudesta;

b) TVT-tuotteet tai TVT-palvelut, joihin haavoittuvuus vaikuttaa, sekä haavoittuvuuden vakavuus niiden olosuhteiden perusteella, joissa sitä voidaan hyödyntää;

c) asiaan liittyvien ohjelmistokorjausten saatavuus ja, jos niitä ei ole saatavilla, toimivaltaisten viranomaisten tai CSIRT-yksiköiden antama ohjeistus haavoittuvien TVT-tuotteiden ja TVT-palvelujen käyttäjille siitä, miten julkistetusta haavoittuvuudesta johtuvia riskejä voidaan lieventää.

13 artikla

Kansallisen tason yhteistyö

1. Jos saman jäsenvaltion toimivaltaiset viranomaiset, keskitetty yhteyspiste ja CSIRT-yksiköt ovat toisistaan erillisiä, niiden on tehtävä yhteistyötä keskenään tässä direktiivissä säädettyjen velvoitteiden täyttämiseksi.

2. Jäsenvaltioiden on varmistettava, että niiden CSIRT-yksiköt tai tapauksen mukaan niiden toimivaltaiset viranomaiset saavat 23 artiklan nojalla tehdyt ilmoitukset merkittävistä poikkeamista ja 30 artiklan nojalla tehdyt ilmoitukset poikkeamista, kyberuhkista ja läheltä piti -tilanteista.

3. Jäsenvaltioiden on varmistettava, että niiden CSIRT-yksiköt tai tapauksen mukaan niiden toimivaltaiset viranomaiset tiedottavat niiden keskitetylle yhteyspisteelle tämän direktiivin nojalla tehdyistä poikkeamia, kyberuhkia ja läheltä piti -tilanteita koskevista ilmoituksista.

4. Jotta voidaan varmistaa toimivaltaisten viranomaisten, keskitettyjen yhteyspisteiden ja CSIRT-yksiköiden tehtävien ja velvoitteiden tehokas suorittaminen, jäsenvaltioiden on mahdollisuuksien mukaan varmistettava, että kyseiset elimet tekevät asianmukaista yhteistyötä kyseisen jäsenvaltion lainvalvontaviranomaisten, tietosuojaviranomaisten, asetusten (EY) N:o 300/2008 ja (EU) 2018/1139 mukaisten kansallisten viranomaisten, asetuksen (EU) N:o 910/2014 mukaisten valvontaelinten, asetuksen (EU) 2022/2554 mukaisten toimivaltaisten viranomaisten, direktiivin (EU) 2018/1972 mukaisten kansallisten sääntelyviranomaisten, direktiivin (EU) 2022/2557 mukaisten toimivaltaisten viranomaisten sekä muiden alakohtaisten unionin säädösten mukaisten toimivaltaisten viranomaisten kanssa.

5. Jäsenvaltioiden on varmistettava, että niiden tämän direktiivin mukaiset toimivaltaiset viranomaiset ja niiden direktiivin (EU) 2022/2557 mukaiset toimivaltaiset viranomaiset tekevät yhteistyötä ja vaihtavat säännöllisesti tietoja kriittisten toimijoiden määrittämisestä sekä riskeistä, kyberuhkista ja poikkeamista ja muista kuin kyberturvallisuuteen liittyvistä riskeistä, uhkista ja poikkeamista, jotka vaikuttavat direktiivin (EU) 2022/2557 nojalla kriittisiksi toimijoiksi määritettyihin keskeisiin toimijoihin, sekä tällaisten riskien, uhkien ja poikkeamien hallitsemiseksi toteutetuista toimenpiteistä. Jäsenvaltioiden on myös varmistettava, että niiden tämän direktiivin mukaiset toimivaltaiset viranomaiset ja niiden asetuksen (EU) N:o 910/2014, asetuksen (EU) 2022/2554 ja direktiivin (EU) 2018/1972 mukaiset toimivaltaiset viranomaiset vaihtavat säännöllisesti asiaankuuluvia tietoja, myös merkityksellisistä poikkeamista ja kyberuhkista.

6. Jäsenvaltioiden on yksinkertaistettava teknisesti 23 ja 30 artiklassa tarkoitettujen ilmoitusten tekemistä.

III LUKU

UNIONIN JA KANSAINVÄLISEN TASON YHTEISTYÖ

14 artikla

Yhteistyöryhmä

1. Perustetaan yhteistyöryhmä tukemaan ja helpottamaan jäsenvaltioiden välistä strategista yhteistyötä ja tietojenvaihtoa sekä lujittamaan luottamusta.

2. Yhteistyöryhmä suorittaa tehtävänsä 7 kohdassa tarkoitettujen kaksivuotisten työohjelmien pohjalta.

3. Yhteistyöryhmä koostuu jäsenvaltioiden, komission ja ENISAn edustajista. Euroopan ulkosuhdehallinto osallistuu yhteistyöryhmän toimintaan tarkkailijana. Euroopan valvontaviranomaiset ja asetuksen (EU) 2022/2554 mukaiset toimivaltaiset viranomaiset voivat osallistua yhteistyöryhmän toimintaan mainitun asetuksen 47 artiklan 1 kohdan mukaisesti.

Yhteistyöryhmä voi tarvittaessa kutsua Euroopan parlamentin ja asiaankuuluvien sidosryhmien edustajia osallistumaan työhönsä.

Komissio huolehtii sihteeristötehtävistä.

4. Yhteistyöryhmän tehtävänä on

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

b) opastaa toimivaltaisia viranomaisia 7 artiklan 2 kohdan c alakohdassa tarkoitettujen koordinoitua haavoittuvuuksien julkistamista koskevien toimintaperiaatteiden laadinnassa ja täytäntöönpanossa;

c) vaihtaa parhaita käytäntöjä ja tietoja, jotka liittyvät tämän direktiivin täytäntöönpanoon, muun muassa kyberuhkiin, poikkeamiin, haavoittuvuuksiin, läheltä piti -tilanteisiin, tietoisuuden lisäämishankkeisiin, koulutukseen, harjoituksiin ja osaamiseen, valmiuksien kehittämiseen, standardeihin ja teknisiin eritelmiin sekä keskeisten ja tärkeiden toimijoiden määrittämiseen 2 artiklan 2 kohdan b–e alakohdan nojalla;

d) vaihtaa neuvoja ja tehdä yhteistyötä komission kanssa, kun kyse on uusista kyberturvallisuuspoliittisista aloitteista ja alakohtaisten kyberturvallisuusvaatimusten yleisestä johdonmukaisuudesta;

e) vaihtaa neuvoja ja tehdä yhteistyötä komission kanssa, kun kyse on ehdotuksista tämän direktiivin nojalla annettaviksi delegoiduiksi säädöksiksi tai täytäntöönpanosäädöksiksi;

f) vaihtaa parhaita käytäntöjä ja tietoja asiaankuuluvien unionin toimielinten, elinten, laitosten ja virastojen kanssa;

g) vaihtaa näkemyksiä sellaisten alakohtaisten unionin säädösten täytäntöönpanosta, joissa on kyberturvallisuutta koskevia säännöksiä;

h) keskustella tarvittaessa 19 artiklan 9 kohdassa tarkoitetuista vertaisarviointiraporteista ja laatia päätelmiä ja suosituksia;

i) tehdä kriittisiä toimitusketjuja koskevia koordinoituja turvallisuusriskinarviointeja 22 artiklan 1 kohdan mukaisesti;

j) keskustella keskinäisen avunannon tapauksista, myös 37 artiklassa tarkoitetuista rajatylittävistä yhteisistä valvontatoimista saaduista kokemuksista ja näiden valvontatoimien tuloksista;

k) keskustella yhden tai useamman asianomaisen jäsenvaltion pyynnöstä yksittäisistä 37 artiklassa tarkoitettua keskinäistä avunantoa koskevista pyynnöistä;

l) antaa CSIRT-verkostolle ja EU-CyCLONelle strategista ohjausta erityisissä esiin nousevissa kysymyksissä;

m) vaihtaa CSIRT-verkostosta ja EU-CyCLONesta saatujen kokemusten pohjalta näkemyksiä toimintaperiaatteista, jotka koskevat laajamittaisten kyberturvallisuuspoikkeamien ja kriisien jälkeisiä jatkotoimia;

n) edesauttaa kyberturvallisuusvalmiuksien kehittymistä unionissa helpottamalla kansallisten virkamiesten vaihtoa valmiuksien kehittämisohjelmassa, johon osallistuu toimivaltaisten viranomaisten tai CSIRT-yksiköiden henkilöstöä;

o) järjestää eri puolilta unionia tulevien asiaankuuluvien yksityisten sidosryhmien kanssa säännöllisiä yhteisiä kokouksia, joissa keskustellaan yhteistyöryhmän toteuttamista toimista ja kerätään näkemyksiä esiin nousevista toimintapoliittisista haasteista;

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

q) vahvistaa 19 artiklan 1 kohdassa tarkoitetut vertaisarviointien menetelmät ja organisatoriset näkökohdat sekä vahvistaa 19 artiklan 5 kohdan mukaisesti jäsenvaltioiden itsearviointimenetelmät komission ja ENISAn avustuksella ja laatia 19 artiklan 6 kohdan mukaisesti yhteistyössä komission ja ENISAn kanssa käytännesäännöt nimettyjen kyberturvallisuusasiantuntijoiden työmenetelmien tueksi;

r) laatia 40 artiklassa tarkoitettua uudelleentarkastelua varten kertomuksia strategisella tasolla ja vertaisarvioinneista saaduista kokemuksista;

s) keskustella ja esittää säännöllisesti tilannearvio kyberuhkista tai poikkeamista, kuten kiristyshaittaohjelmista.

Yhteistyöryhmä toimittaa ensimmäisen alakohdan r alakohdassa tarkoitetut kertomukset komissiolle, Euroopan parlamentille ja neuvostolle.

5. Jäsenvaltioiden on varmistettava edustajiensa tuloksekas, tehokas ja suojattu yhteistyö yhteistyöryhmässä.

6. Yhteistyöryhmä voi pyytää CSIRT-verkostolta teknistä raporttia haluamistaan aiheista.

7. Yhteistyöryhmä laatii viimeistään 1 päivänä helmikuuta 2024 ja sen jälkeen kahden vuoden välein työohjelman toteutettavista toimista, joilla pannaan täytäntöön sen tavoitteet ja tehtävät.

8. Komissio voi hyväksyä täytäntöönpanosäädöksiä, joilla vahvistetaan tarvittavat menettelytapajärjestelyt yhteistyöryhmän toimintaa varten.

Nämä täytäntöönpanosäädökset hyväksytään 39 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

Komissio vaihtaa neuvoja ja tekee yhteistyötä yhteistyöryhmän kanssa 4 kohdan e alakohdan mukaisesti, kun kyse on tämän kohdan ensimmäisessä alakohdassa tarkoitetuista ehdotuksista täytäntöönpanosäädöksiksi.

9. Yhteistyöryhmä kokoontuu säännöllisesti ja joka tapauksessa vähintään kerran vuodessa direktiivillä (EU) 2022/2557 perustetun kriittisten toimijoiden häiriönsietokykyä käsittelevän ryhmän kanssa edistääkseen ja helpottaakseen strategista yhteistyötä ja tietojenvaihtoa.

15 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 10 artiklan nojalla nimettyjen tai perustettujen CSIRT-yksiköiden ja unionin toimielinten, elinten ja virastojen tietotekniikan kriisiryhmän (CERT-EU) edustajista. Komissio osallistuu CSIRT-verkostoon tarkkailijana. ENISA huolehtii sihteeristötehtävistä ja avustaa aktiivisesti CSIRT-yksiköiden keskinäisessä yhteistyössä.

3. CSIRT-verkoston tehtävänä on

a) vaihtaa tietoja CSIRT-yksiköiden valmiuksista;

b) helpottaa teknologian sekä asiaankuuluvien toimenpiteiden, toimintaperiaatteiden, työkalujen, prosessien, parhaiden käytäntöjen ja toimintakehysten jakamista, siirtoa ja vaihtoa CSIRT-yksiköiden kesken;

c) vaihtaa asiaankuuluvia tietoja poikkeamista, läheltä piti -tilanteista, kyberuhkista, riskeistä ja haavoittuvuuksista;

d) vaihtaa tietoja kyberturvallisuutta koskevista julkaisuista ja suosituksista;

e) varmistaa tiedonjakoeritelmien ja -protokollien yhteentoimivuus;

f) vaihtaa tietoja ja keskustella poikkeamasta ja siihen liittyvistä kyberuhkista, riskeistä ja haavoittuvuuksista sellaisen CSIRT-verkoston jäsenen pyynnöstä, johon poikkeama mahdollisesti vaikuttaa;

g) keskustella CSIRT-verkoston jäsenen pyynnöstä kyseisen jäsenvaltion lainkäyttöalueella havaitun poikkeaman koordinoiduista hallintatoimista ja mahdollisuuksien mukaan toteuttaa ne;

h) avustaa jäsenvaltioita rajatylittävien poikkeamien käsittelyssä tämän direktiivin nojalla;

i) tehdä yhteistyötä, vaihtaa parhaita käytäntöjä ja avustaa 12 artiklan 1 kohdan nojalla koordinaattoriksi nimettyjä CSIRT-yksiköitä sellaisten haavoittuvuuksien koordinoidun julkistamisen hoitamisessa, joilla voisi olla merkittävä vaikutus useamman kuin yhden jäsenvaltion toimijoihin;

j) keskustella uusista operatiivisen yhteistyön muodoista ja tunnistaa niitä, myös seuraavien osalta:

   i) kyberuhkien ja poikkeamien luokat;

   ii) ennakkovaroitukset;

   iii) keskinäinen avunanto;

   iv) rajatylittävien riskien ja poikkeamien hallintatoimien koordinoinnin periaatteet ja järjestelyt;

   v) osallistuminen jäsenvaltion pyynnöstä 9 artiklan 4 kohdassa tarkoitetun kansallisen laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallintasuunnitelman laadintaan;

k) tiedottaa yhteistyöryhmälle verkoston toiminnasta ja muista operatiivisen yhteistyön muodoista, joista on keskusteltu j alakohdan mukaisesti, ja pyytää tarvittaessa asiaan liittyvää ohjeistusta;

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

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

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

o) keskustella tarvittaessa 19 artiklan 9 kohdassa tarkoitetuista vertaisarviointiraporteista;

p) antaa ohjeita, joilla helpotetaan operatiivisten käytäntöjen lähentymistä sovellettaessa tämän artiklan säännöksiä operatiivisesta yhteistyöstä.

4. CSIRT-verkoston on 40 artiklassa tarkoitettua uudelleentarkastelua varten ja viimeistään 17 päivänä tammikuuta 2025 ja sen jälkeen kahden vuoden välein arvioitava edistymistä operatiivisessa yhteistyössä ja annettava siitä kertomus. Kertomuksessa on erityisesti laadittava päätelmiä ja suosituksia kansallisista CSIRT-yksiköistä tehtyjen 19 artiklassa tarkoitettujen vertaisarviointien tulosten pohjalta. Kertomus toimitetaan yhteistyöryhmälle.

5. CSIRT-verkosto vahvistaa työjärjestyksensä.

6. CSIRT-verkoston ja EU-CyCLONen on sovittava menettelytapajärjestelyistä ja tehtävä yhteistyötä niiden pohjalta.

16 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 asiaankuuluvien tietojen vaihto jäsenvaltioiden ja unionin toimielinten, elinten, laitosten ja virastojen välillä.

2. EU-CyCLONe koostuu jäsenvaltioiden kyberkriisinhallintaviranomaisten edustajista sekä komission edustajista tapauksissa, joissa mahdollisella tai meneillään olevalla laajamittaisella kyberturvallisuuspoikkeamalla on tai todennäköisesti on merkittävä vaikutus tämän direktiivin soveltamisalaan kuuluviin palveluihin ja toimintoihin. Muissa tapauksissa komissio osallistuu EU-CyCLONen toimintaan tarkkailijana.

ENISA huolehtii EU-CyCLONen sihteeristötehtävistä ja tukee suojattua tietojenvaihtoa sekä tarjoaa käyttöön tarvittavat välineet, joilla tuetaan jäsenvaltioiden yhteistyötä varmistaen suojattu tietojenvaihto.

EU-CyCLONe voi tarvittaessa kutsua asiaankuuluvien sidosryhmien edustajia osallistumaan työhönsä tarkkailijoina.

3. EU-CyCLONen tehtävänä on

a) parantaa varautumista laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallintaan;

b) kehittää yhteistä tilannekuvaa laajamittaisista kyberturvallisuuspoikkeamista ja kriiseistä;

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

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

e) keskustella 9 artiklan 4 kohdassa tarkoitetuista kansallisista laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallintasuunnitelmista asianomaisen jäsenvaltion pyynnöstä.

4. EU-CyCLONe vahvistaa työjärjestyksensä.

5. EU-CyCLONe raportoi säännöllisesti yhteistyöryhmälle laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallinnasta sekä alan suuntauksista keskittyen erityisesti niiden vaikutuksiin keskeisiin ja tärkeisiin toimijoihin.

6. EU-CyCLONen tekee CSIRT-verkoston kanssa yhteistyötä 15 artiklan 6 kohdassa säädettyjen menettelytapajärjestelyjen pohjalta.

7. EU-CyCLONe antaa viimeistään 17 päivänä heinäkuuta 2024 ja sen jälkeen 18 kuukauden välein Euroopan parlamentille ja neuvostolle kertomuksen, jossa arvioidaan sen työtä.

17 artikla

Kansainvälinen yhteistyö

Unioni voi tarvittaessa tehdä Euroopan unionin toiminnasta tehdyn sopimuksen 218 artiklan mukaisesti kolmansien maiden tai kansainvälisten järjestöjen kanssa kansainvälisiä sopimuksia, joilla mahdollistetaan ja järjestetään niiden osallistuminen yhteistyöryhmän, CSIRT-verkoston ja EU-CyCLONen tiettyihin toimintoihin. Tällaisten sopimusten on oltava unionin tietosuojalainsäädännön mukaisia.

18 artikla

Kertomus kyberturvallisuuden tilasta unionissa

1. ENISA antaa yhteistyössä komission ja yhteistyöryhmän kanssa joka toinen vuosi kyberturvallisuuden tilaa unionissa käsittelevän kertomuksen, jonka se toimittaa ja esittelee Euroopan parlamentille. Kertomus on muun muassa asetettava saataville koneluettavana datana, ja siihen on sisällyttävä seuraavat:

a) unionin tasolla tehtävä kyberturvallisuusriskien arviointi, jossa otetaan huomioon kyberuhkaympäristö;

b) arvio kyberturvallisuusvalmiuksien kehittymisestä julkisella ja yksityisellä sektorilla unionissa;

c) arvio kansalaisten ja toimijoiden, myös pienten ja keskisuurten yritysten, kyberturvallisuustietoisuuden ja kyberhygienian yleisestä tasosta;

d) kokonaisarvio 19 artiklassa tarkoitettujen vertaisarviointien tuloksista;

e) kokonaisarvio kyberturvallisuusvalmiuksien ja -resurssien kehitystasosta unionissa, mukaan lukien alakohtaiset valmiudet ja resurssit, sekä siitä, miten yhdenmukaisia jäsenvaltioiden kansalliset kyberturvallisuusstrategiat ovat.

2. Kertomuksen on sisällettävä erityisiä toimintapoliittisia suosituksia, jotta voidaan korjata puutteita ja nostaa kyberturvallisuuden tasoa kaikkialla unionissa, sekä yhteenveto kyseistä kautta koskevista havainnoista, jotka sisältyvät ENISAn asetuksen (EU) 2019/881 7 artiklan 6 kohdan mukaisesti laatimiin poikkeamia ja kyberuhkia koskeviin unionin kyberturvallisuuden teknisiin tilanneraportteihin.

3. ENISA kehittää yhteistyössä komission, yhteistyöryhmän ja CSIRT-verkoston kanssa menetelmät, mukaan lukien 1 kohdan e alakohdassa tarkoitetussa kokonaisarviossa käytettävät asiaankuuluvat muuttujat, kuten määrälliset ja laadulliset indikaattorit.

19 artikla

Vertaisarvioinnit

1. Yhteistyöryhmä vahvistaa komission ja ENISAn sekä tarvittaessa CSIRT-verkoston avustuksella viimeistään 17 päivänä tammikuuta 2025 vertaisarviointien menetelmät ja organisatoriset näkökohdat, jotta voidaan oppia yhteisistä kokemuksista, lujittaa keskinäistä luottamusta ja saavuttaa kyberturvallisuuden yhteinen korkea taso sekä kehittää jäsenvaltioiden kyberturvallisuusvalmiuksia ja tämän direktiivin täytäntöönpanon edellyttämiä toimintaperiaatteita. Vertaisarviointeihin osallistuminen on vapaaehtoista. Vertaisarvioinnin suorittavat kyberturvallisuusasiantuntijat. Kyberturvallisuusasiantuntijoiden on oltava vähintään kahden jäsenvaltion nimeämiä, ja arvioitava jäsenvaltio ei voi nimetä asiantuntijoita.

Vertaisarvioinnin on katettava vähintään yksi seuraavista seikoista:

a) 21 artiklassa säädettyjen kyberturvallisuusriskien hallintatoimenpiteiden ja 23 artiklassa säädettyjen raportointivelvoitteiden täytäntöönpanoaste;

b) toimivaltaisten viranomaisten valmiuksien taso, mukaan lukien käytettävissä olevat taloudelliset, tekniset ja henkilöresurssit, sekä toimivaltaisten viranomaisten tuloksekkuus tehtäviensä hoidossa;

c) CSIRT-yksiköiden operatiiviset valmiudet;

d) 37 artiklassa tarkoitetun keskinäisen avunannon toteutusaste;

e) 29 artiklassa tarkoitettujen kyberturvallisuustietojen jakamisjärjestelyjen täytäntöönpanoaste;

f) rajatylittävät tai useaa toimialaa koskevat erityiskysymykset.

2. Edellä 1 kohdassa tarkoitettuihin menetelmiin sisältyvät objektiiviset, syrjimättömät, oikeudenmukaiset ja läpinäkyvät kriteerit, joiden perusteella jäsenvaltiot nimeävät kyberturvallisuusasiantuntijat, joille voidaan antaa tehtäväksi suorittaa vertaisarvioinnit. Komissio ja ENISA osallistuvat vertaisarviointeihin tarkkailijoina.

3. Jäsenvaltiot voivat yksilöidä 1 kohdan f alakohdassa tarkoitettuja erityiskysymyksiä vertaisarviointia varten.

4. Ennen 1 kohdassa tarkoitetun vertaisarvioinnin aloittamista jäsenvaltioiden on ilmoitettava osallistuville jäsenvaltioille vertaisarvioinnin laajuudesta, 3 kohdan nojalla yksilöidyt erityiskysymykset mukaan lukien.

5. Ennen vertaisarvioinnin aloittamista jäsenvaltiot voivat itse tehdä arvioitavista seikoista arvioinnin ja toimittaa kyseisen itsearvioinnin nimetyille kyberturvallisuusasiantuntijoille. Yhteistyöryhmä vahvistaa komission ja ENISAn avustuksella menetelmät jäsenvaltioiden tekemää itsearviointia varten.

6. Vertaisarviointeihin sisältyy fyysisiä tai virtuaalisia vierailuja toimipaikoissa ja muuta kuin paikalla toteutettavaa tietojenvaihtoa. Vertaisarvioinnin kohteena olevan jäsenvaltion on hyvän yhteistyön hengessä annettava nimetyille kyberturvallisuusasiantuntijoille arviointiin tarvittavat tiedot, sanotun kuitenkaan rajoittamatta luottamuksellisten tai turvallisuusluokiteltujen tietojen suojaamista koskevan unionin oikeuden tai kansallisen lainsäädännön soveltamista ja keskeisistä valtion tehtävistä, kuten kansallisesta turvallisuudesta, huolehtimista. Yhteistyöryhmä laatii yhteistyössä komission ja ENISAn kanssa asianmukaiset käytännesäännöt nimettyjen kyberturvallisuusasiantuntijoiden työmenetelmien tueksi. Vertaisarvioinnin yhteydessä saatuja tietoja saa käyttää ainoastaan tähän tarkoitukseen. Vertaisarviointiin osallistuvat kyberturvallisuusasiantuntijat eivät saa paljastaa vertaisarvioinnin aikana saatuja arkaluonteisia tai luottamuksellisia tietoja ulkopuolisille.

7. Vertaisarvioinnin kohteena olleessa jäsenvaltiossa arvioiduista seikoista ei tehdä uutta vertaisarviointia kyseisessä jäsenvaltiossa kahteen vuoteen vertaisarvioinnin päättymisestä, ellei kyseinen jäsenvaltio toisin pyydä tai yhteistyöryhmän ehdotuksesta toisin päätetä.

8. Jäsenvaltioiden on varmistettava, että nimettyjä kyberturvallisuusasiantuntijoita koskevien mahdollisten eturistiriitojen riskeistä ilmoitetaan muille jäsenvaltioille, yhteistyöryhmälle, komissiolle ja ENISAlle ennen vertaisarvioinnin aloittamista. Vertaisarvioinnin kohteena oleva jäsenvaltio voi vastustaa tiettyjen kyberturvallisuusasiantuntijoiden nimeämistä asianmukaisesti perustelluista syistä, jotka sen on ilmoitettava nimeäjänä olevalle jäsenvaltiolle.

9. Vertaisarviointeihin osallistuvien kyberturvallisuusasiantuntijoiden on laadittava luonnokset raporteiksi vertaisarviointien tuloksista ja päätelmistä. Vertaisarvioinnin kohteena olevat jäsenvaltiot voivat esittää huomautuksia itseään koskevista raporttiluonnoksista, ja tällaiset huomautukset liitetään raportteihin. Raportteihin on sisällytettävä suosituksia, jotta vertaisarviointiprosessin piiriin kuuluvia seikkoja voidaan kehittää. Raportit on toimitettava yhteistyöryhmälle ja tarvittaessa CSIRT-verkostolle. Vertaisarvioinnin kohteena oleva jäsenvaltio voi päättää asettaa raporttinsa tai sen muokatun version julkisesti saataville.

IV LUKU

KYBERTURVALLISUUSRISKIEN HALLINTATOIMENPITEET JA RAPORTOINTIVELVOITTEET

20 artikla

Hallinnointi

1. Jäsenvaltioiden on varmistettava, että keskeisten ja tärkeiden toimijoiden hallintoelimet hyväksyvät näiden toimijoiden 21 artiklan noudattamiseksi toteuttamat kyberturvallisuusriskien hallintatoimenpiteet ja valvovat mainitun artiklan täytäntöönpanoa ja että nämä hallintoelimet voidaan saattaa vastuuseen, jos toimijat rikkovat kyseistä artiklaa.

Tämän kohdan soveltaminen ei rajoita kansallisen lainsäädännön soveltamista, kun on kyse julkisiin laitoksiin sovellettavista vastuusäännöistä taikka virkamiesten tai vaalilla valittujen tai nimettyjen toimenhaltijoiden vastuusta.

2. Jäsenvaltioiden on varmistettava, että keskeisten ja tärkeiden toimijoiden hallintoelinten jäsenillä on velvollisuus osallistua koulutukseen, ja kannustettava keskeisiä ja tärkeitä toimijoita tarjoamaan säännöllisesti vastaavaa koulutusta työntekijöilleen, jotta he voivat hankkia riittävät tiedot ja taidot kyetäkseen tunnistamaan riskejä ja arvioimaan kyberturvallisuusriskien hallintakäytäntöjä ja niiden vaikutusta toimijan tarjoamiin palveluihin.

21 artikla

Kyberturvallisuusriskien hallintatoimenpiteet

1. Jäsenvaltioiden on varmistettava, että keskeiset ja tärkeät toimijat toteuttavat asianmukaiset ja oikeasuhteiset tekniset, operatiiviset ja organisatoriset toimenpiteet hallitakseen riskejä, joita niiden toiminnoissaan tai palveluntarjonnassaan käyttämien verkko- ja tietojärjestelmien turvallisuuteen kohdistuu, ja estääkseen tai minimoidakseen poikkeamien vaikutuksen palvelujensa vastaanottajiin ja muihin palveluihin.

Kun otetaan huomioon viimeisin kehitys ja tapauksen mukaan asiaa koskevat eurooppalaiset ja kansainväliset standardit sekä täytäntöönpanokustannukset, ensimmäisessä alakohdassa tarkoitetuilla toimenpiteillä on varmistettava, että verkko- ja tietojärjestelmien turvallisuuden taso on oikeassa suhteessa riskeihin. Näiden toimenpiteiden oikeasuhteisuutta arvioitaessa on otettava asianmukaisesti huomioon se, missä määrin toimija altistuu riskeille, toimijan koko ja poikkeamien esiintymisen todennäköisyys ja niiden vakavuus, mukaan lukien niiden yhteiskunnalliset ja taloudelliset vaikutukset.

2. Edellä 1 kohdassa tarkoitettujen toimenpiteiden on perustuttava kaikki vaaratekijät huomioivaan toimintamalliin, jolla pyritään suojaamaan verkko- ja tietojärjestelmät ja näiden järjestelmien fyysinen ympäristö poikkeamilta, ja niihin on sisällyttävä vähintään seuraavat:

a) riskianalyysejä ja tietojärjestelmien turvallisuutta koskevat politiikat;

b) poikkeamien käsittely;

c) toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisinhallinta;

d) toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat;

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

f) toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta;

g) perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus;

h) toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä;

i) henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta;

j) tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa.

3. Jäsenvaltioiden on varmistettava, että toimijoiden harkitessa, mitkä tämän artiklan 2 kohdan d alakohdassa tarkoitetuista toimenpiteistä ovat asianmukaisia, toimijat ottavat huomioon kullekin välittömälle toimittajalle ja palveluntarjoajalle ominaiset haavoittuvuudet, niiden tuotteiden yleisen laadun sekä toimittajiensa ja palveluntarjoajiensa kyberturvallisuuskäytännöt, mukaan lukien tuotekehityksen suojausmenettelyt. Jäsenvaltioiden on myös varmistettava, että toimijoiden harkitessa, mitkä kyseisessä alakohdassa tarkoitetuista toimenpiteistä ovat asianmukaisia, toimijoita vaaditaan ottamaan huomioon 22 artiklan 1 kohdan mukaisesti tehtyjen kriittisiä toimitusketjuja koskevien koordinoitujen riskinarviointien tulokset.

4. Jäsenvaltioiden on varmistettava, että toimija, joka toteaa, ettei se noudata 2 kohdassa säädettyjä toimenpiteitä, toteuttaa ilman aiheetonta viivytystä kaikki tarvittavat, asianmukaiset ja oikeasuhteiset korjaavat toimenpiteet.

5. Komissio hyväksyy viimeistään 17 päivänä lokakuuta 2024 täytäntöönpanosäädöksiä, joilla vahvistetaan 2 kohdassa tarkoitettujen toimenpiteiden tekniset ja menetelmiin liittyvät vaatimukset, jotka koskevat DNS-palveluntarjoajia, aluetunnusrekistereitä, pilvipalvelujen tarjoajia, datakeskuspalvelujen tarjoajia, sisällönjakeluverkkojen tarjoajia, hallintapalvelun tarjoajia, tietoturvapalveluntarjoajia, verkossa toimivien markkinapaikkojen tarjoajia, verkossa toimivien hakukoneiden tarjoajia, verkkoyhteisöalustojen tarjoajia ja luottamuspalvelun tarjoajia.

Komissio voi hyväksyä täytäntöönpanosäädöksiä, joilla vahvistetaan 2 kohdassa tarkoitettujen toimenpiteiden tekniset ja menetelmiin liittyvät vaatimukset sekä tarvittaessa alakohtaiset vaatimukset, jotka koskevat muita keskeisiä ja tärkeitä toimijoita kuin tämän kohdan ensimmäisessä alakohdassa tarkoitettuja toimijoita.

Valmistellessaan tämän kohdan ensimmäisessä ja toisessa alakohdassa tarkoitettuja täytäntöönpanosäädöksiä komissio noudattaa mahdollisimman pitkälle eurooppalaisia ja kansainvälisiä standardeja sekä asiaankuuluvia teknisiä eritelmiä. Komissio vaihtaa neuvoja ja tekee yhteistyötä yhteistyöryhmän ja ENISAn kanssa 14 artiklan 4 kohdan e alakohdan mukaisesti, kun kyse on ehdotuksista täytäntöönpanosäädöksiksi.

Nämä täytäntöönpanosäädökset hyväksytään 39 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

22 artikla

Kriittisiä toimitusketjuja koskevat unionin tason koordinoidut turvallisuusriskinarvioinnit

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

2. Komissio määrittää yhteistyöryhmää ja ENISAa sekä tarvittaessa asiaankuuluvia sidosryhmiä kuultuaan ne kriittiset TVT-palvelut, TVT-järjestelmät tai TVT-tuotteet, joista voidaan tehdä 1 kohdassa tarkoitettu koordinoitu turvallisuusriskinarviointi.

23 artikla

Raportointivelvoitteet

1. Kunkin jäsenvaltion on varmistettava, että keskeiset ja tärkeät toimijat ilmoittavat ilman aiheetonta viivytystä sen CSIRT-yksikölle tai tapauksen mukaan sen toimivaltaiselle viranomaiselle 4 kohdan mukaisesti mistä tahansa poikkeamasta, jolla on 3 kohdan mukainen merkittävä vaikutus niiden palvelujen tarjoamiseen (merkittävä poikkeama). Asianomaisten toimijoiden on tarvittaessa ilmoitettava ilman aiheetonta viivytystä palvelujensa vastaanottajille merkittävistä poikkeamista, jotka todennäköisesti vaikuttavat haitallisesti kyseisten palvelujen tarjoamiseen. Kunkin jäsenvaltion on varmistettava, että kyseiset toimijat ilmoittavat muun muassa kaikki tiedot, joiden avulla CSIRT-yksikkö tai tapauksen mukaan toimivaltainen viranomainen voi määrittää poikkeaman mahdolliset rajatylittävät vaikutukset. Ilmoittaminen ei itsessään lisää ilmoituksen tehneen toimijan vastuuta.

Jos asianomaiset toimijat ilmoittavat toimivaltaiselle viranomaiselle merkittävästä poikkeamasta ensimmäisen alakohdan nojalla, jäsenvaltion on varmistettava, että kyseinen toimivaltainen viranomainen heti ilmoituksen saatuaan toimittaa sen eteenpäin CSIRT-yksikölle.

Rajatylittävän tai useaa toimialaa koskevan merkittävän poikkeaman tapauksessa jäsenvaltioiden on varmistettava, että niiden keskitetyt yhteyspisteet saavat hyvissä ajoin 4 kohdan mukaisesti ilmoitetut asiaankuuluvat tiedot.

2. Jäsenvaltioiden on tapauksen mukaan varmistettava, että keskeiset ja tärkeät toimijat tiedottavat ilman aiheetonta viivytystä niille palvelujensa vastaanottajille, joihin merkittävä kyberuhka saattaa vaikuttaa, kaikista toimenpiteistä tai korjaavista toimista, joita kyseiset palvelun vastaanottajat voivat uhkan hallitsemiseksi toteuttaa. Toimijoiden on tarvittaessa myös tiedotettava kyseisille palvelun vastaanottajille merkittävästä kyberuhkasta itsestään.

3. Poikkeama katsotaan merkittäväksi, jos

a) se on aiheuttanut tai voi aiheuttaa palvelujen vakavan toimintahäiriön tai asianomaiselle toimijalle taloudellisia tappioita;

b) poikkeama on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa.

4. Jäsenvaltioiden on varmistettava, että 1 kohdan nojalla tehtävää ilmoittamista varten asianomaiset toimijat toimittavat CSIRT-yksikölle tai tapauksen mukaan toimivaltaiselle viranomaiselle

a) ilman aiheetonta viivytystä ja joka tapauksessa 24 tunnin kuluessa siitä, kun ne ovat tulleet tietoisiksi poikkeamasta, ennakkovaroituksen, jossa on tapauksen mukaan ilmoitettava, epäilläänkö merkittävän poikkeaman johtuvan lainvastaisista tai vihamielisistä teoista tai voiko sillä olla rajatylittäviä vaikutuksia;

b) ilman aiheetonta viivytystä ja joka tapauksessa 72 tunnin kuluessa siitä, kun ne ovat tulleet tietoisiksi merkittävästä poikkeamasta, poikkeamailmoituksen, jossa on tapauksen mukaan ajantasaistettava a alakohdassa tarkoitetut tiedot ja esitettävä ensimmäinen arvio merkittävästä poikkeamasta, sen vakavuudesta ja vaikutuksista sekä vaarantumisindikaattorit, jos sellaisia on saatavilla;

c) CSIRT-yksikön tai tapauksen mukaan toimivaltaisen viranomaisen pyynnöstä väliraportin asiaan liittyvistä tilannepäivityksistä;

d) viimeistään kuukauden kuluttua b alakohdan mukaisen poikkeamailmoituksen toimittamisesta lopullisen raportin, joka sisältää seuraavat tiedot:

   i) yksityiskohtainen kuvaus poikkeamasta, sen vakavuus ja vaikutukset mukaan lukien;

   ii) poikkeaman todennäköisesti aiheuttaneen uhkan tai juurisyyn tyyppi;

   iii) toteutetut ja meneillään olevat toimenpiteet vaikutusten lieventämiseksi;

   iv) tapauksen mukaan poikkeaman rajatylittävät vaikutukset;

e) jos poikkeama on edelleen meneillään silloin, kun d alakohdassa tarkoitettu lopullinen raportti pitäisi toimittaa, jäsenvaltioiden on varmistettava, että asianomaiset toimijat toimittavat tuolloin edistymisraportin ja lopullisen raportin kuukauden kuluessa siitä, kun ne ovat käsitelleet poikkeaman.

Poiketen siitä, mitä ensimmäisen alakohdan b alakohdassa säädetään, luottamuspalvelun tarjoajan on ilmoitettava merkittävistä poikkeamista, jotka vaikuttavat sen luottamuspalvelujen tarjontaan, CSIRT-yksikölle tai tapauksen mukaan toimivaltaiselle viranomaiselle ilman aiheetonta viivytystä ja joka tapauksessa 24 tunnin kuluessa siitä, kun se on tullut tietoiseksi merkittävästä poikkeamasta.

5. CSIRT-yksikön tai toimivaltaisen viranomaisen on ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 24 tunnin kuluessa 4 kohdan a alakohdassa tarkoitetun ennakkovaroituksen vastaanottamisesta annettava ilmoituksen tehneelle toimijalle vastaus, johon sisältyy alustava palaute merkittävästä poikkeamasta sekä kyseisen toimijan pyynnöstä ohjeita tai operatiivisia neuvoja mahdollisten vaikutuksia lieventävien toimenpiteiden täytäntöönpanoa varten. Jos CSIRT-yksikkö ei ole 1 kohdassa tarkoitetun ilmoituksen alkuperäinen vastaanottaja, toimivaltaisen viranomaisen on annettava ohjeet yhteistyössä CSIRT-yksikön kanssa. CSIRT-yksikkö antaa täydentävää teknistä tukea, jos asianomainen toimija sitä pyytää. Jos merkittävää poikkeamaa epäillään rikokseksi, CSIRT-yksikön tai toimivaltaisen viranomaisen on myös annettava ohjeita merkittävän poikkeaman ilmoittamisesta lainvalvontaviranomaisille.

6. CSIRT-yksikön, toimivaltaisen viranomaisen tai keskitetyn yhteyspisteen on tarvittaessa ja erityisesti silloin, kun merkittävä poikkeama koskee vähintään kahta jäsenvaltiota, tiedotettava merkittävästä poikkeamasta ilman aiheetonta viivytystä niille muille jäsenvaltioille, joihin poikkeama vaikuttaa, ja ENISAlle. Tällöin annettaviin tietoihin on sisällyttävä sen tyyppisiä tietoja kuin on vastaanotettu 4 kohdan mukaisesti. Näin tehdessään CSIRT-yksikön, toimivaltaisen viranomaisen tai keskitetyn yhteyspisteen on unionin oikeuden tai kansallisen lainsäädännön mukaisesti säilytettävä toimijan turvallisuusedut ja kaupalliset edut sekä annettujen tietojen luottamuksellisuus.

7. Jos yleinen tietoisuus on tarpeen merkittävän poikkeaman estämiseksi tai meneillään olevan merkittävän poikkeaman käsittelemiseksi tai jos merkittävän poikkeaman julkistaminen on muutoin yleisen edun mukaista, jäsenvaltion CSIRT-yksikkö tai tapauksen mukaan sen toimivaltainen viranomainen sekä tarvittaessa muiden asianomaisten jäsenvaltioiden CSIRT-yksiköt tai toimivaltaiset viranomaiset voivat asianomaista toimijaa kuultuaan tiedottaa merkittävästä poikkeamasta yleisölle tai vaatia toimijaa tekemään niin.

8. Keskitetyn yhteyspisteen on CSIRT-yksikön tai toimivaltaisen viranomaisen pyynnöstä toimitettava 1 kohdan mukaisesti saadut ilmoitukset eteenpäin niiden muiden jäsenvaltioiden keskitetyille yhteyspisteille, joihin poikkeama vaikuttaa.

9. Keskitetyn yhteyspisteen on toimitettava ENISAlle kolmen kuukauden välein yhteenvetoraportti, joka sisältää anonymisoidut koontitiedot merkittävistä poikkeamista, poikkeamista, kyberuhkista ja läheltä piti -tilanteista, joista on ilmoitettu tämän artiklan 1 kohdan ja 30 artiklan mukaisesti. Edistääkseen toimitettavien tietojen vertailukelpoisuutta ENISA voi antaa teknisiä ohjeita yhteenvetoraporttiin sisällytettävien tietojen parametreista. ENISA tiedottaa kuuden kuukauden välein yhteistyöryhmälle ja CSIRT-verkostolle saatuja ilmoituksia koskevista havainnoistaan.

10. CSIRT-yksiköiden tai tapauksen mukaan toimivaltaisten viranomaisten on toimitettava direktiivin (EU) 2022/2557 mukaisille toimivaltaisille viranomaisille tietoa merkittävistä poikkeamista, poikkeamista, kyberuhkista ja läheltä piti -tilanteista, joista direktiivin (EU) 2022/2557 nojalla kriittisiksi toimijoiksi määritetyt toimijat ovat ilmoittaneet tämän artiklan 1 kohdan ja 30 artiklan mukaisesti.

11. Komissio voi hyväksyä täytäntöönpanosäädöksiä, joissa täsmennetään tämän artiklan 1 kohdan ja 30 artiklan nojalla tehtävän ilmoituksen sekä tämän artiklan 2 kohdan nojalla annettavan tiedonannon tietosisältö, muoto ja ilmoitusmenettely.

Komissio hyväksyy viimeistään 17 päivänä lokakuuta 2024 DNS-palveluntarjoajia, aluetunnusrekistereitä, pilvipalvelujen tarjoajia, datakeskuspalvelujen tarjoajia, sisällönjakeluverkkojen tarjoajia, hallintapalvelun tarjoajia, tietoturvapalvelun-tarjoajia sekä verkossa toimivien markkinapaikkojen tarjoajia, verkossa toimivien hakukoneiden tarjoajia ja verkkoyhteisöalustojen tarjoajia koskevia täytäntöönpanosäädöksiä, joissa täsmennetään tapaukset, joissa poikkeama katsotaan merkittäväksi 3 kohdan mukaisesti. Komissio voi hyväksyä tällaisia täytäntöönpanosäädöksiä muitakin keskeisiä ja tärkeitä toimijoita varten.

Komissio vaihtaa neuvoja ja tekee yhteistyötä yhteistyöryhmän kanssa 14 artiklan 4 kohdan e alakohdan mukaisesti, kun kyse on tämän kohdan ensimmäisessä ja toisessa alakohdassa tarkoitetuista ehdotuksista täytäntöönpanosäädöksiksi.

Nämä täytäntöönpanosäädökset hyväksytään 39 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

24 artikla

Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien käyttö

1. Tiettyjen 21 artiklan vaatimusten noudattamisen osoittamiseksi jäsenvaltiot voivat vaatia keskeisiä ja tärkeitä toimijoita käyttämään määrättyjä, keskeisen tai tärkeän toimijan itse kehittämiä tai kolmansilta osapuolilta hankittavia TVT-tuotteita, TVT-palveluja ja TVT-prosesseja, jotka on sertifioitu asetuksen (EU) 2019/881 49 artiklan nojalla hyväksyttyjen eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukaisesti. Lisäksi jäsenvaltioiden on kannustettava keskeisiä ja tärkeitä toimijoita käyttämään hyväksyttyjä luottamuspalveluja.

2. Siirretään komissiolle valta antaa 38 artiklan mukaisesti delegoituja säädöksiä, joilla täydennetään tätä direktiiviä täsmentämällä, mitä keskeisten ja tärkeiden toimijoiden luokkia on vaadittava käyttämään tiettyjä sertifioituja TVT-tuotteita, TVT-palveluja ja TVT-prosesseja tai hankkimaan sertifiointi asetuksen (EU) 2019/881 49 artiklan nojalla hyväksytyn eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti. Tällaisia delegoituja säädöksiä annetaan, kun on havaittu, että kyberturvallisuus ei ole riittävän korkealla tasolla, ja niissä säädetään täytäntöönpano-kaudesta.

Ennen tällaisten delegoitujen säädösten hyväksymistä komissio tekee vaikutustenarvioinnin ja toteuttaa kuulemisia asetuksen (EU) 2019/881 56 artiklan mukaisesti.

3. Jos tämän artiklan 2 kohdan soveltamiseksi ei ole saatavilla asianmukaista eurooppalaista kyberturvallisuuden sertifiointijärjestelmää, komissio voi yhteistyöryhmää ja Euroopan kyberturvallisuuden sertifiointiryhmää kuultuaan pyytää ENISAa valmistelemaan ehdolla olevan järjestelmän asetuksen (EU) 2019/881 48 artiklan 2 kohdan nojalla.

25 artikla

Standardointi

1. Jäsenvaltioiden on 21 artiklan 1 ja 2 kohdan yhdenmukaisen täytäntöönpanon edistämiseksi kannustettava käyttämään verkko- ja tietojärjestelmien turvallisuuden kannalta merkityksellisiä eurooppalaisia ja kansainvälisiä standardeja ja teknisiä eritelmiä ilman, että ne määräävät käyttämään jotain tiettyä teknologiaa tai harjoittavat syrjintää jonkin tietyn teknologian käytön suosimiseksi.

2. ENISA antaa yhteistyössä jäsenvaltioiden kanssa ja tarvittaessa asiaankuuluvia sidosryhmiä kuultuaan neuvoja ja ohjeita teknisistä osa-alueista, jotka on otettava huomioon 1 kohtaa sovellettaessa, sekä jo olemassa olevista, myös kansallisista, standardeista, joiden avulla nämä osa-alueet tulisivat katetuiksi.

V LUKU

LAINKÄYTTÖVALTA JA REKISTERÖINTI

26 artikla

Lainkäyttövalta ja alueellisuus

1. Tämän direktiivin soveltamisalaan kuuluvien toimijoiden katsotaan kuuluvan sen jäsenvaltion lainkäyttövaltaan, johon ne ovat sijoittautuneet, lukuun ottamatta seuraavia:

a) yleisten sähköisten viestintäverkkojen tarjoajat tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat, joiden katsotaan kuuluvan sen jäsenvaltion lainkäyttövaltaan, jossa ne tarjoavat palvelujaan;

b) DNS-palveluntarjoajat, aluetunnusrekisterit, verkkotunnusten rekisteröintipalveluja tarjoavat toimijat, pilvipalvelujen tarjoajat, datakeskuspalvelujen tarjoajat, sisällönjakeluverkkojen tarjoajat, hallintapalvelun tarjoajat, tietoturvapalvelun-tarjoajat sekä verkossa toimivien markkinapaikkojen, verkossa toimivien hakukoneiden tai verkkoyhteisöalustojen tarjoajat, joiden katsotaan kuuluvan sen jäsenvaltion lainkäyttövaltaan, jossa niiden päätoimipaikka on unionissa 2 kohdan mukaisesti;

c) julkishallinnon toimijat, joiden katsotaan kuuluvan sen jäsenvaltion lainkäyttövaltaan, joka ne on perustanut.

2. Tätä direktiiviä sovellettaessa 1 kohdan b alakohdassa tarkoitetun toimijan päätoimipaikan katsotaan olevan unionissa siinä jäsenvaltiossa, jossa kyberturvallisuusriskien hallintatoimenpiteisiin liittyvät päätökset pääsääntöisesti tehdään. Jos tällaista jäsenvaltiota ei voida määrittää tai jos tällaisia päätöksiä ei tehdä unionissa, päätoimipaikan katsotaan sijaitsevan jäsenvaltiossa, jossa kyberturvallisuustoiminnot toteutetaan. Jos tällaista jäsenvaltiota ei voida määrittää, päätoimipaikan katsotaan sijaitsevan jäsenvaltiossa, jossa asianomaisella toimijalla on eniten työntekijöitä työllistävä toimipaikka unionissa.

3. Jos 1 kohdan b alakohdassa tarkoitettu toimija ei ole sijoittautunut unioniin mutta tarjoaa palveluja unionissa, sen on nimettävä itselleen edustaja unioniin. Edustajan on oltava sijoittautunut johonkin niistä jäsenvaltioista, joissa palveluja tarjotaan. Tällaisen toimijan katsotaan kuuluvan sen jäsenvaltion lainkäyttövaltaan, johon sen edustaja on sijoittautunut. Jos toimijalla ei ole unionissa tämän kohdan nojalla nimettyä edustajaa, mikä tahansa jäsenvaltio, jossa toimija tarjoaa palveluja, voi ryhtyä oikeustoimiin toimijaa vastaan tämän direktiivin rikkomisen vuoksi.

4. Se, että 1 kohdan b alakohdassa tarkoitettu toimija nimeää edustajan, ei rajoita oikeustoimia, joita voidaan panna vireille toimijaa itseään vastaan.

5. Jäsenvaltiot, jotka ovat saaneet 1 kohdan b alakohdassa tarkoitettuun toimijaan liittyvän keskinäistä avunantoa koskevan pyynnön, voivat kyseisen pyynnön asettamissa rajoissa toteuttaa asianmukaisia valvonta- ja täytäntöönpanotoimenpiteitä suhteessa asianomaiseen toimijaan, joka tarjoaa palveluja tai jolla on verkko- ja tietojärjestelmä niiden alueella.

27 artikla

Toimijoiden rekisteri

1. ENISA perustaa DNS-palveluntarjoajien, aluetunnusrekisterien, verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden, pilvipalvelujen tarjoajien, datakeskuspalvelujen tarjoajien, sisällönjakeluverkkojen tarjoajien, hallintapalvelun tarjoajien, tietoturvapalveluntarjoajien sekä verkossa toimivien markkinapaikkojen tarjoajien, verkossa toimivien hakukoneiden tarjoajien ja verkkoyhteisöalustojen tarjoajien rekisterin ja ylläpitää sitä käyttäen keskitetyiltä yhteyspisteiltä saatuja tietoja 4 kohdan mukaisesti. ENISA antaa pyynnöstä toimivaltaisille viranomaisille pääsyn kyseiseen rekisteriin ja varmistaa tarvittaessa tietojen luottamuksellisuuden suojaamisen.

2. Jäsenvaltioiden on edellytettävä, että 1 kohdassa tarkoitetut toimijat toimittavat viimeistään 17 päivänä tammikuuta 2025 toimivaltaisille viranomaisille seuraavat tiedot:

a) toimijan nimi;

b) tapauksen mukaan liitteessä I tai II tarkoitettu asiaankuuluva toimiala, toimialan osa ja toimijatyyppi;

c) toimijan päätoimipaikan ja muiden unionissa sijaitsevien laillisten toimipaikkojen osoite tai, jos toimija ei ole sijoittautunut unioniin, sen 26 artiklan 3 kohdan nojalla nimetyn edustajan osoite;

d) toimijan ja tarvittaessa sen 26 artiklan 3 kohdan nojalla nimetyn edustajan ajantasaiset yhteystiedot, mukaan lukien sähköpostiosoitteet ja puhelinnumerot;

e) jäsenvaltiot, joissa toimija tarjoaa palveluja; ja

f) toimijan IP-osoitealueet.

3. Jäsenvaltioiden on varmistettava, että 1 kohdassa tarkoitetut toimijat ilmoittavat toimivaltaiselle viranomaiselle kaikista muutoksista 2 kohdan mukaisesti toimittamiinsa tietoihin viipymättä ja joka tapauksessa kolmen kuukauden kuluessa muutospäivästä.

4. Kun asianomaisen jäsenvaltion keskitetty yhteyspiste saa 2 ja 3 kohdassa tarkoitetut tiedot, lukuun ottamatta 2 kohdan f alakohdassa tarkoitettuja tietoja, sen on toimitettava ne ilman aiheetonta viivytystä ENISAlle.

5. Tämän artiklan 2 ja 3 kohdassa tarkoitetut tiedot on tapauksen mukaan toimitettava 3 artiklan 4 kohdan neljännessä alakohdassa tarkoitettujen kansallisten järjestelyjen välityksellä.

28 artikla

Verkkotunnusten rekisteröintitietojen tietokanta

1. DNS-järjestelmän turvallisuuden, vakauden ja häiriönsietokyvyn edistämiseksi jäsenvaltioiden on edellytettävä, että aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat keräävät ja ylläpitävät tarkkoja ja täydellisiä verkkotunnusten rekisteröintitietoja erityisessä tietokannassa noudattaen unionin tietosuojalainsäädännön mukaisesti asianmukaista huolellisuutta henkilötietojen suhteen.

2. Edellä olevan 1 kohdan soveltamiseksi jäsenvaltioiden on edellytettävä, että verkkotunnusten rekisteröintitietojen tietokanta sisältää tarvittavat tiedot, jotta verkkotunnusten haltijat ja aluetunnusrekistereissä verkkotunnuksia hallinnoivat yhteyspisteet voidaan tunnistaa ja niihin voidaan ottaa yhteyttä. Näihin tietoihin on sisällyttävä

a) verkkotunnus;

b) rekisteröintipäivä;

c) verkkotunnuksen rekisteröijän nimi, yhteyssähköpostiosoite ja puhelinnumero;

d) verkkotunnusta hallinnoivan yhteyspisteen yhteyssähköpostiosoite ja puhelinnumero, jos ne eivät ole samat kuin verkkotunnuksen rekisteröijän.

3. Jäsenvaltioiden on edellytettävä, että aluetunnusrekistereillä ja verkkotunnusten rekisteröintipalveluja tarjoavilla toimijoilla on käytössä toimintaperiaatteet ja menettelyt, myös tarkastusmenettelyt, joilla varmistetaan, että 1 kohdassa tarkoitetut tietokannat sisältävät tarkat ja täydelliset tiedot. Jäsenvaltioiden on edellytettävä, että tiedot tällaisista toimintaperiaatteista ja menettelyistä asetetaan julkisesti saataville.

4. Jäsenvaltioiden on edellytettävä, että aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat asettavat julkisesti saataville ilman aiheetonta viivytystä verkkotunnuksen rekisteröinnin jälkeen muut verkkotunnuksen rekisteröintitiedot kuin henkilötiedot.

5. Jäsenvaltioiden on edellytettävä, että aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat antavat pääsyn tarkasti määrättyihin verkkotunnusten rekisteröintitietoihin unionin tietosuojalainsäädännön mukaisesti, kun pääsyä oikeutetusti pyytävä esittää lainmukaisen ja asianmukaisesti perustellun pyynnön. Jäsenvaltioiden on edellytettävä, että aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat vastaavat tietoihin pääsyä koskeviin pyyntöihin ilman aiheetonta viivytystä ja joka tapauksessa 72 tunnin kuluessa pyynnön vastaanottamisesta. Jäsenvaltioiden on edellytettävä, että tällaisten tietojen luovuttamista koskevat toimintaperiaatteet ja menettelyt asetetaan julkisesti saataville.

6. Edellä 1–5 kohdassa säädettyjen velvoitteiden noudattaminen ei saa johtaa päällekkäisyyksiin verkkotunnusten rekisteröintitietojen keruussa. Tätä varten jäsenvaltioiden on edellytettävä, että aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat tekevät yhteistyötä keskenään.

VI LUKU

TIETOJENVAIHTO

29 artikla

Kyberturvallisuustietojen jakamisjärjestelyt

1) Jäsenvaltioiden on varmistettava, että tämän direktiivin soveltamisalaan kuuluvat toimijat ja tapauksen mukaan muut toimijat, jotka eivät kuulu tämän direktiivin soveltamisalaan, voivat vapaaehtoisesti vaihtaa keskenään asiaankuuluvia kyberturvallisuustietoja, mukaan lukien tietoja kyberuhkista, läheltä piti -tilanteista, haavoittuvuuksista, tekniikoista ja menettelyistä, vaarantumisindikaattoreista, kyberhyökkäystaktiikoista, yksittäisistä uhkatoimijoista, kyberturvallisuushälytyksistä ja suosituksista, jotka koskevat kyberhyökkäysten havaitsemiseen käytettävien kyberturvallisuustyökalujen konfigurointia, kun tällaisella tietojenvaihdolla

a) pyritään ehkäisemään, havaitsemaan ja hallitsemaan poikkeamia tai palautumaan niistä tai lieventämään niiden vaikutuksia;

b) parannetaan kyberturvallisuuden tasoa erityisesti lisäämällä tietoisuutta kyberuhkista, rajoittamalla tai estämällä tällaisten uhkien kykyä levitä, tukemalla erilaisia puolustusvalmiuksia, haavoittuvuuden korjaamista ja julkistamista, uhkien havaitsemis-, rajoittamis- ja ehkäisemistekniikoita, lieventämisstrategioita tai hallinta- ja palautumisvaiheita tai edistämällä julkisten ja yksityisten toimijoiden yhteistyöhön perustuvaa kyberuhkatutkimusta.

2. Jäsenvaltioiden on varmistettava, että tietojenvaihto tapahtuu keskeisten ja tärkeiden toimijoiden sekä tarvittaessa niiden toimittajien tai palveluntarjoajien yhteisöjen sisällä. Tällainen tietojenvaihto on toteutettava kyberturvallisuustietojen jakamisjärjestelyillä, joissa otetaan huomioon jaettujen tietojen mahdollinen arkaluonteisuus.

3. Jäsenvaltioiden on helpotettava tämän artiklan 2 kohdassa tarkoitettujen kyberturvallisuustietojen jakamisjärjestelyjen perustamista. Tällaisissa järjestelyissä voidaan täsmentää tiedonjakojärjestelyjen operatiiviset osat, mukaan lukien tiettyjen TVT-alustojen ja automatisointityökalujen käyttö, sisältö ja edellytykset. Vahvistaessaan viranomaisten tällaisiin järjestelyihin osallistumisen yksityiskohtia jäsenvaltiot voivat asettaa tiettyjä ehtoja toimivaltaisten viranomaisten tai CSIRT-yksiköiden saataville asettamille tiedoille. Jäsenvaltioiden on tarjouduttava avustamaan tällaisten järjestelyjen soveltamisessa 7 artiklan 2 kohdan h alakohdassa tarkoitettujen toimintaperiaatteidensa mukaisesti.

4. Jäsenvaltioiden on varmistettava, että keskeiset ja tärkeät toimijat ilmoittavat toimivaltaisille viranomaisille osallistumisestaan 2 kohdassa tarkoitettuihin kyberturvallisuustietojen jakamisjärjestelyihin, kun ne liittyvät tällaisiin järjestelyihin, tai tapauksen mukaan vetäytymisestään tällaisista järjestelyistä, kun vetäytyminen tulee voimaan.

5. ENISA avustaa 2 kohdassa tarkoitettujen kyberturvallisuustietojen jakamisjärjestelyjen perustamisessa vaihtamalla parhaita käytäntöjä ja antamalla ohjeistusta.

30 artikla

Asiaankuuluvien tietojen vapaaehtoinen ilmoittaminen

1. Jäsenvaltioiden on varmistettava, että 23 artiklassa säädetyn ilmoitusvelvoitteen lisäksi CSIRT-yksiköille tai tapauksen mukaan toimivaltaisille viranomaisille voivat vapaaehtoisesti tehdä ilmoituksia

a) keskeiset ja tärkeät toimijat poikkeamista, kyberuhkista ja läheltä piti -tilanteista;

b) muut kuin a alakohdassa tarkoitetut toimijat riippumatta siitä, kuuluvatko ne tämän direktiivin soveltamisalaan, merkittävistä poikkeamista, kyberuhkista ja läheltä piti -tilanteista.

2. Jäsenvaltioiden on käsiteltävä tämän artiklan 1 kohdassa tarkoitetut ilmoitukset 23 artiklassa säädettyä menettelyä noudattaen. Jäsenvaltiot voivat asettaa etusijalle pakollisten ilmoitusten käsittelyn vapaaehtoisten ilmoitusten käsittelyyn nähden.

CSIRT-yksiköiden on tarvittaessa ja toimivaltaisten viranomaisten on tapauksen mukaan toimitettava keskitetyille yhteyspisteille tiedot tämän artiklan nojalla saaduista ilmoituksista varmistaen ilmoituksen tehneen toimijan toimittamien tietojen luottamuksellisuuden ja asianmukaisen suojan. Vapaaehtoinen raportointi ei saa johtaa sellaisten lisävelvoitteiden asettamiseen ilmoituksen tehneelle toimijalle, joita siihen ei olisi sovellettu, jos se ei olisi antanut kyseistä ilmoitusta, sanotun kuitenkaan rajoittamatta rikosten ennalta estämistä, tutkimista, paljastamista ja rikoksiin liittyviä syytetoimia.

VII LUKU

VALVONTA JA TÄYTÄNTÖÖNPANO

31 artikla

Valvontaa ja täytäntöönpanoa koskevat yleiset näkökohdat

1. Jäsenvaltioiden on varmistettava, että niiden toimivaltaiset viranomaiset valvovat tosiasiallisesti tämän direktiivin noudattamista ja toteuttavat tarvittavat toimenpiteet sen varmistamiseksi.

2. Jäsenvaltiot voivat sallia sen, että niiden toimivaltaiset viranomaiset asettavat valvontatoimenpiteitä etusijalle. Tällaisessa etusijalle asettamisessa on sovellettava riskiperusteista lähestymistapaa. Toimivaltaiset viranomaiset voivat 32 ja 33 artiklassa säädettyjä valvontatehtäviään suorittaessaan vahvistaa valvontamenetelmiä, joiden ansiosta tällaisia tehtäviä voidaan asettaa etusijalle soveltaen riskiperusteista lähestymistapaa.

3. Toimivaltaisten viranomaisten on tehtävä tiivistä yhteistyötä asetuksen (EU) 2016/679 mukaisten valvontaviranomaisten kanssa käsitellessään henkilötietojen tietoturvaloukkauksiin johtaneita poikkeamia, sanotun kuitenkaan rajoittamatta kyseisen asetuksen mukaisten valvontaviranomaisten toimivaltaa ja tehtäviä.

4. Jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on valvoessaan julkishallinnon toimijoita tämän direktiivin noudattamisessa ja määrätessään tämän direktiivin rikkomista koskevia täytäntöönpanotoimenpiteitä asianmukaiset valtuudet tällaisten tehtävien suorittamiseksi ja että ne ovat toiminnallisesti riippumattomia valvomistaan julkishallinnon toimijoista, sanotun kuitenkaan rajoittamatta kansallisten lainsäädäntö- ja toimielinkehysten soveltamista. Jäsenvaltiot voivat päättää määrätä kyseisiä toimijoita koskevia asianmukaisia, oikeasuhteisia ja tehokkaita valvonta- ja täytäntöönpanotoimenpiteitä kansallisten lainsäädäntö- ja toimielinkehysten mukaisesti.

32 artikla

Keskeisiin toimijoihin liittyvät valvonta- ja täytäntöönpanotoimenpiteet

1. Jäsenvaltioiden on varmistettava, että keskeisiä toimijoita koskevat tässä direktiivissä säädettyjen velvoitteiden noudattamisen valvonta- tai täytäntöönpanotoimenpiteet ovat vaikuttavia, oikeasuhteisia ja varoittavia ja että niissä otetaan huomioon kunkin yksittäisen tapauksen olosuhteet.

2. Jäsenvaltioiden on varmistettava, että hoitaessaan keskeisiä toimijoita koskevia valvontatehtäviään toimivaltaisilla viranomaisilla on valtuudet ainakin seuraaviin:

a) koulutettujen ammattilaisten toteuttamat paikalla tehtävät tarkastukset ja muu kuin paikalla toteutettava valvonta, mukaan lukien satunnaistarkastukset;

b) riippumattoman elimen tai toimivaltaisen viranomaisen suorittamat säännölliset ja kohdennetut turvallisuusauditoinnit;

c) tapauskohtaiset auditoinnit, myös kun perusteena on merkittävä poikkeama tai se, että keskeinen toimija on rikkonut tätä direktiiviä;

d) objektiivisiin, syrjimättömiin, oikeudenmukaisiin ja läpinäkyviin riskinarviointikriteereihin perustuvat turvallisuusskannaukset, tarvittaessa yhteistyössä asianomaisen toimijan kanssa;

e) pyynnöt saada tietoja, jotka ovat tarpeen asianomaisen toimijan hyväksymien kyberturvallisuusriskien hallintatoimenpiteiden arvioimiseksi, mukaan lukien dokumentoidut kyberturvallisuusperiaatteet, sekä tietojen toimittamista toimivaltaisille viranomaisille 27 artiklan nojalla koskevan velvoitteen noudattamisen arvioimiseksi;

f) pyynnöt saada pääsy dataan, asiakirjoihin ja tietoihin, joita ne tarvitsevat valvontatehtäviensä suorittamiseksi;

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

Ensimmäisen alakohdan b alakohdassa tarkoitettujen kohdennettujen turvallisuusauditointien on perustuttava toimivaltaisen viranomaisen tai auditoinnin kohteena olevan toimijan tekemiin riskinarviointeihin tai muihin riskeistä saatavilla oleviin tietoihin.

Kohdennetun turvallisuusauditoinnin tulokset on asetettava toimivaltaisen viranomaisen saataville. Auditoinnin kohteena oleva toimija vastaa riippumattoman elimen suorittaman kohdennetun turvallisuusauditoinnin kustannuksista, jollei toimivaltainen viranomainen asianmukaisesti perustelluissa tapauksissa päätä toisin.

3. Käyttäessään 2 kohdan e, f tai g alakohtaan perustuvia valtuuksiaan toimivaltaisten viranomaisten on ilmoitettava pyynnön tarkoitus ja täsmennettävä pyydetyt tiedot.

4. Jäsenvaltioiden on varmistettava, että niiden toimivaltaisilla viranomaisilla on käyttäessään täytäntöönpanovaltuuksiaan keskeisten toimijoiden suhteen ainakin valtuudet

a) antaa varoituksia, kun asianomaiset toimijat rikkovat tätä direktiiviä;

b) antaa asianomaisille toimijoille sitovia ohjeita, myös poikkeaman ehkäisemiseksi tai korjaamiseksi tarvittavista toimenpiteistä sekä tällaisten toimenpiteiden täytäntöönpanon määräajoista ja täytäntöönpanosta raportoinnin määräajoista, tai määräys, joissa tai jossa ne velvoitetaan korjaamaan havaitut puutteet tai tämän direktiivin rikkominen;

c) määrätä asianomaiset toimijat lopettamaan tämän direktiivin vastainen toiminta ja pidättäytymään tästä toiminnasta vastaisuudessa;

d) määrätä asianomaiset toimijat varmistamaan, että niiden kyberturvallisuusriskien hallintatoimenpiteet ovat 21 artiklan mukaisia, tai täyttämään 23 artiklassa säädetyt raportointivelvoitteensa määrätyllä tavalla ja määrätyn ajan kuluessa;

e) määrätä asianomaiset toimijat tiedottamaan niille luonnollisille henkilöille tai oikeushenkilöille, joille ne tarjoavat palvelujaan tai toimintojaan ja joihin merkittävä kyberuhka saattaa vaikuttaa, uhkan luonteesta sekä mahdollisista suojatoimenpiteistä tai korjaavista toimenpiteistä, joita kyseiset luonnolliset henkilöt tai oikeushenkilöt voivat uhkan hallitsemiseksi toteuttaa;

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

g) nimetä valvova virkamies, joka valvoo tarkoin määriteltyjen tehtävien puitteissa määräkauden ajan, että asianomaiset toimijat noudattavat 21 ja 23 artiklaa;

h) määrätä asianomaiset toimijat julkistamaan määrätyllä tavalla seikat, jotka liittyvät tämän direktiivin rikkomiseen;

i) määrätä tai pyytää asiaankuuluvia elimiä tai tuomioistuimia määräämään kansallisen lainsäädännön mukaisesti hallinnollisia sakkoja 34 artiklan nojalla minkä tahansa tämän kohdan a–h alakohdassa tarkoitetun toimenpiteen lisäksi.

5. Jos 4 kohdan a–d ja f alakohdan nojalla toteutetut täytäntöönpanotoimenpiteet 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 väliaikaisesti tai pyytää sertifiointi- tai lupaelintä tai tuomioistuinta keskeyttämään väliaikaisesti kansallisen lainsäädännön mukaisesti sertifiointi tai lupa, joka koskee keskeisen toimijan tarjoamia kaikkia asiaankuuluvia palveluja tai toimintoja tai osaa niistä;

b) pyytää asiaankuuluvia elimiä tai tuomioistuimia kieltämään väliaikaisesti kansallisen lainsäädännön mukaisesti ketä tahansa luonnollista henkilöä, joka hoitaa keskeisen toimijan johtotehtäviä toimitusjohtajan tai laillisen edustajan tasolla, hoitamasta kyseisen toimijan johtotehtäviä.

Tämän kohdan nojalla määrättyjä väliaikaisia keskeyttämisiä tai kieltoja on sovellettava ainoastaan siihen asti, kun asianomainen toimija toteuttaa tarvittavat toimet korjatakseen ne puutteet tai noudattaakseen niitä toimivaltaisen viranomaisen vaatimuksia, joiden johdosta seuraamukset määrättiin. Tällaisten väliaikaisten keskeyttämisten tai kieltojen määräämiseen on sovellettava asianmukaisia menettelytakeita unionin oikeuden yleisten periaatteiden ja perusoikeuskirjan mukaisesti, mukaan lukien oikeus tehokkaisiin oikeussuojakeinoihin ja puolueettomaan tuomioistuimeen, syyttömyysolettama ja oikeus puolustukseen.

Tässä kohdassa säädettyjä seuraamuksia ei sovelleta tämän direktiivin soveltamisalaan kuuluviin julkishallinnon toimijoihin.

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 hallinnoida sitä, on valta varmistaa, että toimija noudattaa tätä direktiiviä. Jäsenvaltioiden on varmistettava, että nämä luonnolliset henkilöt voidaan saattaa vastuuseen, jos he ovat laiminlyöneet velvollisuutensa varmistaa tämän direktiivin noudattaminen.

Julkishallinnon toimijoiden osalta tämä kohta ei rajoita kansallisen lainsäädännön soveltamista, kun on kyse virkamiesten tai vaalilla valittujen tai nimettyjen toimenhaltijoiden vastuusta.

7. Toimivaltaisten viranomaisten on toteuttaessaan 4 kohdassa tarkoitettuja täytäntöönpanotoimenpiteitä tai määrätessään 5 kohdassa tarkoitettuja seuraamuksia kunnioitettava oikeutta puolustukseen ja otettava huomioon kunkin yksittäisen tapauksen olosuhteet sekä vähintään seuraavat seikat:

a) rikkomisen vakavuus ja rikottujen säännösten tärkeys siten, että vakavina rikkomisina pidetään joka tapauksessa muun muassa seuraavia:

   i) toistuvat väärinkäytökset;

   ii) merkittävien poikkeamien jättäminen ilmoittamatta tai korjaamatta;

   iii) puutteiden jättäminen korjaamatta toimivaltaisten viranomaisten sitovista ohjeista huolimatta;

   iv) toimivaltaisen viranomaisen todetun rikkomisen johdosta määräämien auditointien tai seurantatoimien estäminen;

   v) 21 artiklassa säädettyihin riskinhallintatoimenpiteisiin tai 23 artiklassa säädettyihin raportointivelvoitteisiin liittyvien väärien tai erittäin virheellisten tietojen antaminen;

b) rikkomisen kesto;

c) asianomaisen toimijan mahdolliset vastaavat aiemmat rikkomiset;

d) aiheutunut aineellinen tai aineeton vahinko, mukaan lukien rahoitukseen liittyvät tai taloudelliset tappiot, vaikutukset muihin palveluihin sekä niiden käyttäjien lukumäärä, joihin rikkominen vaikuttaa;

e) rikkojan toiminnan mahdollinen tahallisuus tai tuottamuksellisuus;

f) toimenpiteet, jotka toimija on toteuttanut aineellisen tai aineettoman vahingon ehkäisemiseksi tai lieventämiseksi;

g) hyväksyttyjen käytännesääntöjen tai hyväksyttyjen sertifiointimekanismien noudattaminen;

h) vastuullisina pidettyjen luonnollisten henkilöiden tai oikeushenkilöiden halukkuus tehdä yhteistyötä toimivaltaisten viranomaisten kanssa.

8. Toimivaltaisten viranomaisten on esitettävä yksityiskohtaiset perustelut täytäntöönpanotoimenpiteilleen. Toimivaltaisten viranomaisten on ennen tällaisten toimenpiteiden hyväksymistä ilmoitettava asianomaisille toimijoille alustavista havainnoistaan. Niiden on myös varattava kyseisille toimijoille riittävästi aikaa esittää huomautuksia, lukuun ottamatta asianmukaisesti perusteltuja tapauksia, joissa välittömät toimet poikkeamien ehkäisemiseksi tai hallitsemiseksi muuten estyisivät.

9. Jäsenvaltioiden on varmistettava, että niiden tämän direktiivin mukaiset toimivaltaiset viranomaiset ilmoittavat asiasta direktiivin (EU) 2022/2557 mukaisille saman jäsenvaltion asiaankuuluville toimivaltaisille viranomaisille, kun ne käyttävät valvonta- ja täytäntöönpanovaltuuksiaan varmistaakseen, että direktiivin (EU) 2022/2557 nojalla kriittiseksi toimijaksi määritetty toimija noudattaa tätä direktiiviä. Direktiivin (EU) 2022/2557 mukaiset toimivaltaiset viranomaiset voivat tarvittaessa pyytää tämän direktiivin mukaisia toimivaltaisia viranomaisia käyttämään valvonta- ja täytäntöönpanovaltuuksiaan suhteessa toimijaan, joka on määritetty kriittiseksi toimijaksi direktiivin (EU) 2022/2557 nojalla.

10. Jäsenvaltioiden on varmistettava, että niiden tämän direktiivin mukaiset toimivaltaiset viranomaiset tekevät yhteistyötä asianomaisen jäsenvaltion asetuksen (EU) 2022/2554 mukaisten asiaankuuluvien toimivaltaisten viranomaisten kanssa. Jäsenvaltioiden on erityisesti varmistettava, että niiden tämän direktiivin mukaiset toimivaltaiset viranomaiset ilmoittavat asiasta asetuksen (EU) 2022/2554 32 artiklan 1 kohdan nojalla perustetulle valvontafoorumille, kun ne käyttävät valvonta- ja täytäntöönpanovaltuuksiaan varmistaakseen, että tämän direktiivin soveltamisalaan kuuluva keskeinen toimija, joka on nimetty kriittiseksi TVT-palveluntarjoajana olevaksi kolmanneksi osapuoleksi asetuksen (EU) 2022/2554 31 artiklan nojalla, noudattaa tätä direktiiviä.

33 artikla

Tärkeitä toimijoita koskevat valvonta- ja täytäntöönpanotoimenpiteet

1. Jos jäsenvaltiot saavat näyttöä, viitteitä tai tietoja, joiden mukaan tärkeä toimija ei väitetysti noudata tätä direktiiviä ja erityisesti sen 21 ja 23 artiklaa, niiden on varmistettava, että toimivaltaiset viranomaiset puuttuvat tilanteeseen tarpeen mukaan jälkikäteen toteutettavin valvontatoimenpitein. Jäsenvaltioiden on varmistettava, että kyseiset toimenpiteet ovat vaikuttavia, oikeasuhteisia ja varoittavia ja että niissä otetaan huomioon kunkin yksittäisen tapauksen olosuhteet.

2. Jäsenvaltioiden on varmistettava, että hoitaessaan tärkeitä toimijoita koskevia valvontatehtäviään toimivaltaisilla viranomaisilla on valtuudet ainakin seuraaviin:

a) koulutettujen ammattilaisten toteuttamat paikalla tehtävät tarkastukset ja muu kuin paikalla toteutettava jälkikäteisvalvonta;

b) riippumattoman elimen tai toimivaltaisen viranomaisen suorittamat kohdennetut turvallisuusauditoinnit;

c) objektiivisiin, syrjimättömiin, oikeudenmukaisiin ja läpinäkyviin riskinarviointikriteereihin perustuvat turvallisuusskannaukset, tarvittaessa yhteistyössä asianomaisen toimijan kanssa;

d) pyynnöt saada tietoja, jotka ovat tarpeen asianomaisen toimijan hyväksymien kyberturvallisuusriskien hallintatoimenpiteiden arvioimiseksi jälkikäteen, mukaan lukien dokumentoidut kyberturvallisuusperiaatteet, sekä 27 artiklaan perustuvan toimivaltaisille viranomaisille ilmoittamista koskevan velvoitteen noudattamisen arvioimiseksi;

e) pyynnöt saada pääsy dataan, asiakirjoihin ja tietoihin, joita ne tarvitsevat valvontatehtäviensä suorittamiseksi;

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

Ensimmäisen alakohdan b alakohdassa tarkoitettujen kohdennettujen turvallisuusauditointien on perustuttava toimivaltaisen viranomaisen tai auditoinnin kohteena olevan toimijan tekemiin riskinarviointeihin tai muihin riskeistä saatavilla oleviin tietoihin.

Kohdennetun turvallisuusauditoinnin tulokset on asetettava toimivaltaisen viranomaisen saataville. Auditoinnin kohteena oleva toimija vastaa riippumattoman elimen suorittaman kohdennetun turvallisuusauditoinnin kustannuksista, jollei toimivaltainen viranomainen asianmukaisesti perustellussa tapauksessa päätä toisin.

3. Käyttäessään 2 kohdan d, e tai f alakohtaan perustuvia valtuuksiaan toimivaltaisten viranomaisten on ilmoitettava pyynnön tarkoitus ja täsmennettävä pyydetyt tiedot.

4. Jäsenvaltioiden on varmistettava, että käyttäessään täytäntöönpanovaltuuksiaan tärkeiden toimijoiden suhteen toimivaltaisilla viranomaisilla on ainakin valtuudet

a) antaa varoituksia, kun asianomaiset toimijat rikkovat tätä direktiiviä;

b) antaa asianomaisille toimijoille sitovia ohjeita tai määräys, joissa tai jossa ne velvoitetaan korjaamaan havaitut puutteet tai tämän direktiivin rikkominen;

c) määrätä asianomaiset toimijat lopettamaan tämän direktiivin vastainen toiminta ja pidättäytymään tästä toiminnasta vastaisuudessa;

d) määrätä asianomaiset toimijat varmistamaan, että niiden kybertuvallisuusriskien hallintatoimenpiteet ovat 21 artiklan mukaisia, tai täyttämään 23 artiklassa säädetyt raportointivelvoitteensa määrätyllä tavalla ja määrätyn ajan kuluessa;

e) määrätä asianomaiset toimijat tiedottamaan niille luonnollisille henkilöille tai oikeushenkilöille, joihin liittyen ne tarjoavat palveluja tai harjoittavat toimintaa ja joihin merkittävä kyberuhka saattaa vaikuttaa, uhkan luonteesta sekä mahdollisista suojatoimenpiteistä tai korjaavista toimenpiteistä, joita kyseiset luonnolliset henkilöt tai oikeushenkilöt voivat uhkan hallitsemiseksi toteuttaa;

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

g) määrätä asianomaiset toimijat julkistamaan määrätyllä tavalla seikat, jotka liittyvät tämän direktiivin rikkomiseen;

h) määrätä tai pyytää asiaankuuluvia elimiä tai tuomioistuimia määräämään kansallisen lainsäädännön mukaisesti hallinnollisia sakkoja 34 artiklan nojalla minkä tahansa tämän kohdan a–g alakohdassa tarkoitetun toimenpiteen lisäksi.

5. Tämän asetuksen 32 artiklan 6, 7 ja 8 kohtaa sovelletaan soveltuvin osin tässä artiklassa säädettyihin tärkeitä toimijoita koskeviin valvonta- ja täytäntöönpanotoimenpiteisiin.

6. Jäsenvaltioiden on varmistettava, että niiden tämän direktiivin mukaiset toimivaltaiset viranomaiset tekevät yhteistyötä asianomaisen jäsenvaltion asetuksen (EU) 2022/2554 mukaisten asiaankuuluvien toimivaltaisten viranomaisten kanssa. Jäsenvaltioiden on erityisesti varmistettava, että niiden tämän direktiivin mukaiset toimivaltaiset viranomaiset ilmoittavat asiasta asetuksen (EU) 2022/2554 32 artiklan 1 kohdan nojalla perustetulle valvontafoorumille, kun ne käyttävät valvonta- ja täytäntöönpanovaltuuksiaan varmistaakseen, että tämän direktiivin soveltamisalaan kuuluva tärkeä toimija, joka on nimetty kriittiseksi TVT-palveluntarjoajana olevaksi kolmanneksi osapuoleksi asetuksen (EU) 2022/2554 31 artiklan nojalla, noudattaa tätä direktiiviä.

34 artikla

Yleiset edellytykset hallinnollisten sakkojen määräämiselle keskeisille ja tärkeille toimijoille

1. Jäsenvaltioiden on varmistettava, että tämän artiklan nojalla keskeisille ja tärkeille toimijoille tämän direktiivin rikkomisesta määrättävät hallinnolliset sakot ovat vaikuttavia, oikeasuhteisia ja varoittavia ja että niissä otetaan huomioon kunkin yksittäisen tapauksen olosuhteet.

2. Hallinnolliset sakot määrätään minkä tahansa 32 artiklan 4 kohdan a–h alakohdassa, 32 artiklan 5 kohdassa ja 33 artiklan 4 kohdan a–g alakohdassa tarkoitetun toimenpiteen lisäksi.

3. Päätettäessä hallinnollisen sakon määräämisestä ja sen suuruudesta kussakin yksittäisessä tapauksessa on otettava asianmukaisesti huomioon vähintään 32 artiklan 7 kohdassa säädetyt seikat.

4. Jäsenvaltioiden on varmistettava, että keskeisille toimijoille määrätään 21 tai 23 artiklan rikkomisesta tämän artiklan 2 ja 3 kohdan mukaisesti hallinnollinen sakko, joka on enimmillään vähintään 10 000 000 euroa tai enimmillään vähintään 2 prosenttia sen yrityksen, johon keskeinen toimija kuuluu, edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

5. Jäsenvaltioiden on varmistettava, että tärkeille toimijoille määrätään 21 tai 23 artiklan rikkomisesta tämän artiklan 2 ja 3 kohdan mukaisesti hallinnollinen sakko, joka on enimmillään vähintään 7 000 000 euroa tai enimmillään vähintään 1,4 prosenttia sen yrityksen, johon tärkeä toimija kuuluu, edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

6. Jäsenvaltiot voivat säätää valtuudesta määrätä uhkasakkoja, jotta keskeinen tai tärkeä toimija saadaan lopettamaan tämän direktiivin rikkominen toimivaltaisen viranomaisen aiemman päätöksen mukaisesti.

7. Kukin jäsenvaltio voi vahvistaa säännöt siitä, voidaanko julkishallinnon toimijoille määrätä hallinnollisia sakkoja ja missä määrin, sanotun kuitenkaan rajoittamatta toimivaltaisten viranomaisten 32 ja 33 artiklaan perustuvia valtuuksia.

8. Jos jäsenvaltion oikeusjärjestelmässä ei säädetä hallinnollisista sakoista, kyseisen jäsenvaltion on varmistettava, että tätä artiklaa sovelletaan 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. Jäsenvaltion on ilmoitettava tämän kohdan nojalla antamansa säännökset komissiolle viimeistään 17 päivänä lokakuuta 2024 ja ilmoitettava sille kaikki niitä koskevat myöhemmät muutokset viipymättä.

35 artikla

Henkilötietojen tietoturvaloukkaukseen johtavat rikkomiset

1. Jos toimivaltaiset viranomaiset saavat valvonnan tai täytäntöönpanon yhteydessä tietoonsa, että keskeisen tai tärkeän toimijan tämän direktiivin 21 ja 23 artiklassa säädettyjen velvoitteiden laiminlyönti voi johtaa asetuksen (EU) 2016/679 4 artiklan 12 kohdassa määriteltyyn henkilötietojen tietoturvaloukkaukseen, josta on ilmoitettava mainitun asetuksen 33 artiklan nojalla, niiden on ilmoitettava asiasta ilman aiheetonta viivytystä mainitun asetuksen 55 ja 56 artiklan mukaisille valvontaviranomaisille.

2. Jos asetuksen (EU) 2016/679 55 tai 56 artiklan mukaiset valvontaviranomaiset määräävät hallinnollisen seuraamusmaksun mainitun asetuksen 58 artiklan 2 kohdan i alakohdan nojalla, toimivaltaiset viranomaiset eivät saa määrätä hallinnollista sakkoa tämän direktiivin 34 artiklan nojalla tämän artiklan 1 kohdassa tarkoitetusta rikkomisesta, joka johtuu samasta toiminnasta kuin se, josta on määrätty hallinnollinen seuraamusmaksu asetuksen (EU) 2016/679 58 artiklan 2 kohdan i alakohdan nojalla. Toimivaltaiset viranomaiset voivat kuitenkin määrätä täytäntöönpanotoimenpiteitä, joista säädetään tämän direktiivin 32 artiklan 4 kohdan a–h alakohdassa, 32 artiklan 5 kohdassa ja 33 artiklan 4 kohdan a–g alakohdassa.

3. Jos asetuksen (EU) 2016/679 nojalla toimivaltainen valvontaviranomainen on sijoittautunut toiseen jäsenvaltioon kuin toimivaltainen viranomainen, toimivaltaisen viranomaisen on ilmoitettava asiasta omaan jäsenvaltioonsa sijoittautuneelle valvontaviranomaiselle 1 kohdassa tarkoitetusta mahdollisesta tietoturvaloukkauksesta.

36 artikla

Seuraamukset

Jäsenvaltioiden on säädettävä tämän direktiivin nojalla annettujen kansallisten toimenpiteiden rikkomiseen sovellettavista seuraamuksista ja toteutettava kaikki tarvittavat toimenpiteet niiden täytäntöönpanon varmistamiseksi. Seuraamusten on oltava tehokkaita, oikeasuhteisia ja varoittavia. Jäsenvaltioiden on ilmoitettava nämä säännökset ja toimenpiteet komissiolle viimeistään 17 päivänä tammikuuta 2025, ja jäsenvaltioiden on ilmoitettava komissiolle kaikki niitä koskevat myöhemmät muutokset viipymättä.

37 artikla

Keskinäinen avunanto

1. Jos toimija tarjoaa palveluja useammassa kuin yhdessä jäsenvaltiossa tai tarjoaa palveluja yhdessä tai useammassa jäsenvaltiossa mutta sen verkko- ja tietojärjestelmät sijaitsevat yhdessä tai useammassa muussa jäsenvaltiossa, asianomaisten jäsenvaltioiden toimivaltaisten viranomaisten on tehtävä yhteistyötä keskenään ja avustettava toisiaan tarpeen mukaan. Tähän yhteistyöhön kuuluu vähintään, että

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

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

c) toimivaltainen viranomainen antaa heti toisen toimivaltaisen viranomaisen perustellun pyynnön saatuaan tälle toiselle toimivaltaiselle viranomaiselle keskinäistä apua oikeassa suhteessa omiin resursseihinsa, jotta valvonta- tai täytäntöönpanotoimenpiteet voidaan toteuttaa tuloksekkaasti, tehokkaasti ja johdonmukaisesti.

Ensimmäisen alakohdan c alakohdassa tarkoitettu keskinäinen avunanto voi kattaa tietopyyntöjä ja valvontatoimenpiteitä, myös pyyntöjä suorittaa paikalla tehtäviä tarkastuksia tai muuta kuin paikalla toteutettavaa valvontaa tai kohdennettuja turvallisuusauditointeja. Toimivaltainen viranomainen, jolle avunantopyyntö on osoitettu, ei saa kieltäytyä pyynnöstä, paitsi jos todetaan, ettei sillä ole toimivaltaa antaa pyydettyä apua, että pyydetty apu ei ole oikeassa suhteessa toimivaltaisen viranomaisen valvontatehtäviin tai että pyyntö koskee tietoja tai käsittää toimintoja, joiden paljastaminen tai toteuttaminen olisi vastoin jäsenvaltion keskeisiä kansalliseen turvallisuuteen, yleiseen turvallisuuteen tai puolustukseen liittyviä etuja. Ennen tällaisesta pyynnöstä kieltäytymistä toimivaltaisen viranomaisen on kuultava muita asianomaisia toimivaltaisia viranomaisia sekä, jos jokin asianomaisista jäsenvaltioista sitä pyytää, komissiota ja ENISAa.

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

VIII LUKU

DELEGOIDUT SÄÄDÖKSET JA TÄYTÄNTÖÖNPANOSÄÄDÖKSET

38 artikla

Siirretyn säädösvallan käyttäminen

1. Komissiolle siirrettyä valtaa antaa delegoituja säädöksiä koskevat tässä artiklassa säädetyt edellytykset.

2. Siirretään komissiolle 16 päivästä tammikuuta 2023 viiden vuoden ajaksi 24 artiklan 2 kohdassa tarkoitettu valta antaa delegoituja säädöksiä.

3. Euroopan parlamentti tai neuvosto voi milloin tahansa peruuttaa 24 artiklan 2 kohdassa tarkoitetun säädösvallan siirron. Peruuttamispäätöksellä lopetetaan tuossa päätöksessä mainittu säädösvallan siirto. Peruuttaminen tulee voimaan sitä päivää seuraavana päivänä, jona sitä koskeva päätös julkaistaan *Euroopan unionin virallisessa lehdessä*, tai jonakin myöhempänä, kyseisessä päätöksessä mainittuna päivänä. Peruuttamispäätös ei vaikuta jo voimassa olevien delegoitujen säädösten pätevyyteen.

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

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

6. Edellä olevan 24 artiklan 2 kohdan nojalla annettu delegoitu säädös tulee voimaan ainoastaan, jos Euroopan parlamentti tai neuvosto ei ole kahden kuukauden kuluessa siitä, kun asianomainen säädös on annettu tiedoksi Euroopan parlamentille ja neuvostolle, ilmaissut vastustavansa sitä tai jos sekä Euroopan parlamentti että neuvosto ovat ennen mainitun määräajan päättymistä ilmoittaneet komissiolle, että ne eivät vastusta säädöstä. Euroopan parlamentin tai neuvoston aloitteesta tätä määräaikaa jatketaan kahdella kuukaudella.

39 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.

IX LUKU

LOPPUSÄÄNNÖKSET

40 artikla

Uudelleentarkastelu

Viimeistään 17 päivänä lokakuuta 2027 ja sen jälkeen 36 kuukauden välein komissio tarkastelee uudelleen tämän direktiivin toimivuutta ja antaa siitä kertomuksen Euroopan parlamentille ja neuvostolle. Kertomuksessa arvioidaan erityisesti asianomaisten toimijoiden koon sekä liitteissä I ja II tarkoitettujen toimialojen, toimialan osien ja toimijatyyppien merkitystä talouden ja yhteiskunnan toiminnalle kyberturvallisuuden näkökulmasta. Tätä tarkoitusta varten ja strategisen ja operatiivisen yhteistyön edistämiseksi edelleen komissio ottaa huomioon yhteistyöryhmän ja CSIRT-verkoston kertomukset strategisella ja operatiivisella tasolla saaduista kokemuksista. Komission kertomukseen liitetään tarvittaessa lainsäädäntöehdotus.

41 artikla

Saattaminen osaksi kansallista lainsäädäntöä

1. Jäsenvaltioiden on annettava ja julkaistava tämän direktiivin noudattamisen edellyttämät säännökset viimeistään 17 päivänä lokakuuta 2024. Niiden on viipymättä ilmoitettava tästä komissiolle.

Jäsenvaltioiden on sovellettava kyseisiä säännöksiä 18 päivänä lokakuuta 2024.

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

42 artikla

Asetuksen (EU) N:o 910/2014 muuttaminen

Kumotaan asetuksen (EU) N:o 910/2014 19 artikla 18 päivänä lokakuuta 2024.

43 artikla

Direktiivin (EU) 2018/1972 muuttaminen

Kumotaan direktiivin (EU) 2018/1972 40 ja 41 artikla 18 päivänä lokakuuta 2024.

44 artikla

Kumoaminen

Kumotaan direktiivi (EU) 2016/1148 18 päivänä lokakuuta 2024.

Viittauksia kumottuun direktiiviin pidetään viittauksina tähän direktiiviin liitteessä III olevan vastaavuustaulukon mukaisesti.

45 artikla

Voimaantulo

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

46 artikla

Osoitus

Tämä direktiivi on osoitettu kaikille jäsenvaltioille.

Tehty Strasbourgissa 14 päivänä joulukuuta 2022.

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puhemies	*Puheenjohtaja*
R. METSOLA	M. BEK

LIITE I

ERITTÄIN KRIITTISET TOIMIALAT

Toimiala	Toimialan osa	Toimijatyyppi
1. Energia	a) Sähkö	— Euroopan parlamentin ja neuvoston direktiivin (EU) 2019/944 ([1]) 2 artiklan 57 alakohdassa määritellyt sähköalan yritykset, jotka harjoittavat mainitun direktiivin 2 artiklan 12 alakohdassa määriteltyä 'toimittamista'
		— Direktiivin (EU) 2019/944 2 artiklan 29 alakohdassa määritellyt jakeluverkonhaltijat
		— Direktiivin (EU) 2019/944 2 artiklan 35 alakohdassa määritellyt siirtoverkonhaltijat
		— Direktiivin (EU) 2019/944 2 artiklan 38 alakohdassa määritellyt tuottajat
		— Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/943 ([2]) 2 artiklan 8 alakohdassa määritellyt nimitetyt sähkömarkkinaoperaattorit — Asetuksen (EU) 2019/943 2 artiklan 25 alakohdassa määritellyt markkinaosapuolet, joka tarjoavat direktiivin (EU) 2019/944 2 artiklan 18 alakohdassa määriteltyä aggregointia, 20 alakohdassa määriteltyä kulutusjoustoa tai 59 alakohdassa määriteltyä energian varastointia — Latauspisteiden operaattorit, jotka vastaavat latauspalvelua loppukäyttäjille tarjoavan latauspisteen hallinnoinnista ja toiminnasta, myös liikennepalvelun tarjoajan nimissä ja puolesta
	b) Kauko-lämmitys ja -jäähdytys	— Euroopan parlamentin ja neuvoston direktiivin (EU) 2018/2001 ([3]) 2 kohdan 19 alakohdassa määritellyn kaukolämmityksen tai kaukojäähdytyksen haltijat
	c) Öljy	— Öljynsiirtoputkistojen haltijat
		— Öljyn tuotanto-, jalostus- ja käsittelylaitteistojen haltijat sekä öljyn varastointia ja siirtoa hoitavat operaattorit
		— Neuvoston direktiivin 2009/119/EY ([4]) 2 kohdan f alakohdassa määritellyt keskusvarastointiyksiköt
	d) Kaasu	— Euroopan parlamentin ja neuvoston direktiivin 2009/73/EY ([5]) 2 artiklan 8 alakohdassa määritellyt maakaasun toimittajat
		— Direktiivin 2009/73/EY 2 artiklan 6 alakohdassa määritellyt jakeluverkonhaltijat
		— Direktiivin 2009/73/EY 2 artiklan 4 alakohdassa määritellyt siirtoverkonhaltijat
		— Direktiivin 2009/73/EY 2 artiklan 10 alakohdassa määritellyt varastointilaitteiston haltijat
		— Direktiivin 2009/73/EY 2 artiklan 12 alakohdassa määritellyt nesteytetyn maakaasun käsittelylaitteiston haltijat
		— Direktiivin 2009/73/EY 2 artiklan 1 alakohdassa määritellyt maakaasualan yritykset
		— Maakaasun jalostus- ja käsittelylaitteistojen haltijat
	e) Vety	— Vedyn tuotantoa, varastointia ja siirtoa harjoittavat toimijat

Toimiala	Toimialan osa	Toimijatyyppi
2. Liikenne	a) Ilmaliikenne	— Asetuksen (EY) N:o 300/2008 3 artiklan 4 alakohdassa määritellyt lentoliikenteen harjoittajat, joiden toiminta on kaupallista
		— Euroopan parlamentin ja neuvoston direktiivin 2009/12/EY ([6]) 2 artiklan 2 alakohdassa määritellyt lentoaseman pitäjät, mainitun direktiivin 2 artiklan 1 alakohdassa määritellyt lentoasemat, mukaan lukien Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1315/2013 ([7]) liitteessä II olevassa 2 jaksossa luetellut ydinverkon lentoasemat, sekä lentoasemilla sijaitsevia lisärakennelmia ja -laitteita hoitavat toimijat
		— Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 549/2004 ([8]) 2 artiklan 1 alakohdassa määriteltyä lennonjohtopalvelua tarjoavat lennonjohtopalvelun tarjoajat
	b) Raideliikenne	— Euroopan parlamentin ja neuvoston direktiivin 2012/34/EU ([9]) 3 artiklan 2 alakohdassa määritellyt rataverkon haltijat
		— Direktiivin 2012/34/EU 3 artiklan 1 alakohdassa määritellyt rautatieyritykset, mukaan lukien kyseisen direktiivin 3 artiklan 12 alakohdassa määritellyt palvelupaikan ylläpitäjät
	c) Vesiliikenne	— Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 725/2004 ([10]) liitteessä I merenkulun osalta määritellyt sisävesillä, merillä ja rannikoilla matkustaja- ja rahtiliikennettä hoitavat yhtiöt, lukuun ottamatta tällaisten yhtiöiden liikennöimiä yksittäisiä aluksia
		— Euroopan parlamentin ja neuvoston direktiivin 2005/65/EY ([11]) 3 artiklan 1 alakohdassa määriteltyjen satamien hallinnointielimet, mukaan lukien niiden asetuksen (EY) N:o 725/2004 2 artiklan 11 alakohdassa määritellyt satamarakenteet, sekä toimijat, jotka huolehtivat rakenteista ja varusteista satamien alueella
		— Euroopan parlamentin ja neuvoston direktiivin 2002/59/EY ([12]) 3 artiklan o alakohdassa määriteltyjen alusliikennepalvelujen tarjoajat
	d) Tieliikenne	— Komission delegoidun asetuksen (EU) 2015/962 ([13]) 2 artiklan 12 alakohdassa tarkoitetut, liikenteenhallinnasta vastaavat tieviranomaiset, lukuun ottamatta julkishallinnon toimijoita, joille liikenteenhallinta tai älykkäiden liikennejärjestelmien ylläpitäminen ei ole keskeinen osa niiden yleistä toimintaa
		— Euroopan parlamentin ja neuvoston direktiivin 2010/40/EU ([14]) 4 artiklan 1 alakohdassa määriteltyjen älykkäiden liikennejärjestelmien ylläpitäjät
3. Pankkitoiminta		Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 575/2013 ([15]) 4 artiklan 1 alakohdassa määritellyt luottolaitokset
4. Finanssimarkkinoiden infrastruktuurit		— Euroopan parlamentin ja neuvoston direktiivin 2014/65/EU ([16]) 4 artiklan 24 alakohdassa määriteltyjen kauppapaikkojen ylläpitäjät
		— Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 648/2012 ([17]) 2 artiklan 1 alakohdassa määritellyt keskusvastapuolet

Toimiala	Toimialan osa	Toimijatyyppi
5. Terveys		— Euroopan parlamentin ja neuvoston direktiivin 2011/24/EU ([18]) 3 artiklan g alakohdassa määritellyt terveydenhuollon tarjoajat
		— Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2371 ([19]) 15 artiklassa tarkoitetut EU:n vertailulaboratoriot
		— Euroopan parlamentin ja neuvoston direktiivin 2001/83/EY ([20]) 1 artiklan 2 alakohdassa määriteltyjen lääkkeiden tutkimusta ja kehitystä harjoittavat toimijat — NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 21 tarkoitettua lääkeaineiden ja lääkkeiden valmistusta harjoittavat toimijat — Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/123 ([21]) 22 artiklassa tarkoitettuja vakavan kansanterveysuhan aikana kriittisiksi katsottuja lääkinnällisiä laitteita (kansanterveysuhan aikana kriittisten lääkinnällisten laitteiden luettelo) valmistavat toimijat
6. Juomavesi		Euroopan parlamentin ja neuvoston direktiivin (EU) 2020/2184 ([22]) 2 artiklan 1 alakohdan a alakohdassa määritellyn 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 ([23]) 2 artiklan 1, 2 ja 3 alakohdassa määriteltyä yhdyskuntajätevettä, talousjätevettä tai teollisuusjätevettä keräävät, hävittävät tai käsittelevät yritykset, lukuun ottamatta yrityksiä, joille yhdyskuntajäteveden, talousjäteveden tai teollisuusjäteveden kerääminen, hävittäminen tai käsittely ei ole keskeinen osa niiden yleistä toimintaa
8. Digitaalinen infrastruktuuri		— Internetin yhdysliikennepisteiden ylläpitäjät
		— DNS-palveluntarjoajat, lukuun ottamatta juurinimipalvelinten ylläpitäjiä
		— Aluetunnusrekisterit
		— Pilvipalvelujen tarjoajat
		— Datakeskuspalvelujen tarjoajat
		— Sisällönjakeluverkkojen tarjoajat
		— Luottamuspalvelun tarjoajat
		— Yleisten sähköisten viestintäverkkojen tarjoajat
		— Yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat
9. TVT-palvelujen hallinta (yritysten välinen)		— Hallintapalvelun tarjoajat — Tietoturvapalveluntarjoajat

Toimiala	Toimialan osa	Toimijatyyppi
10. Julkishallinto		— Keskustason julkishallinnon toimijat, sellaisina kuin jäsenvaltio on ne kansallisen lainsäädännön mukaisesti määrittänyt
		— Aluetason julkishallinnon toimijat, sellaisina kuin jäsenvaltio on ne kansallisen lainsäädännön mukaisesti määrittänyt
11. Avaruus		Avaruuspohjaisten palvelujen tarjoamista tukevan, jäsenvaltioiden tai yksityisten tahojen omistaman, hallinnoiman ja operoiman maassa sijaitsevan infrastruktuurin ylläpitäjät, lukuun ottamatta yleisten sähköisten viestintäverkkojen tarjoajia

([1]) 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).

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

([3]) 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).

([4]) 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).

([5]) 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).

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

([7]) 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).

([8]) 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).

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

([10]) 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).

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

([12]) 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).

([13]) 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).

([14]) 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).

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

([16]) 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).

([17]) 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).

([18]) 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).

(19) Euroopan parlamentin ja neuvoston asetus (EU) 2022/2371, annettu 23 päivänä marraskuuta 2022, rajat ylittävistä vakavista terveysuhkista ja päätöksen N:o 1082/2013/EU kumoamisesta (EUVL L 314, 6.12.2022, s. 26).

(20) 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).

(21) Euroopan parlamentin ja neuvoston asetus (EU) 2022/123, annettu 25 päivänä tammikuuta 2022, Euroopan lääkeviraston roolin vahvistamisesta kriisivalmiudessa ja -hallinnassa lääkkeiden ja lääkinnällisten laitteiden osalta (EUVL L 20, 31.1.2022, s. 1).

(22) Euroopan parlamentin ja neuvoston direktiivi (EU) 2020/2184, annettu 16 päivänä joulukuuta 2020, ihmisten käyttöön tarkoitetun veden laadusta (EUVL L 435, 23.12.2020, s. 1).

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

LIITE II

MUUT KRIITTISET TOIMIALAT

Toimiala	Toimialan osa	Toimijatyyppi
1. Posti- ja kuriiripalvelut		Direktiivin 97/67/EY 2 artiklan 1 a alakohdassa määritellyt postipalvelujen tarjoajat, mukaan lukien kuriiripalvelujen tarjoajat
2. Jätehuolto		Euroopan parlamentin ja neuvoston direktiivin 2008/98/EY ([1]) 3 artiklan 9 alakohdassa määriteltyä jätehuoltoa harjoittavat yritykset, lukuun ottamatta yrityksiä, joille jätehuolto ei ole niiden pääasiallista taloudellista toimintaa
3. Kemikaalien valmistus, tuotanto ja jakelu		Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 1907/2006 ([2]) 3 artiklan 9 alakohdassa tarkoitettua aineiden valmistusta ja 14 alakohdassa tarkoitettua aineiden tai seosten jakelua harjoittavat yritykset sekä yritykset, jotka tuottavat mainitun asetuksen 3 artiklan 3 alakohdassa määriteltyjä esineitä aineista tai seoksista
4. Elintarvikkeiden tuotanto, jalostus ja jakelu		Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 178/2002 ([3]) 3 artiklan 2 alakohdassa määritellyt elintarvikeyritykset, jotka harjoittavat tukkukauppaa sekä teollista tuotantoa ja jalostusta
5. Valmistus	a) Lääkinnällisten laitteiden ja *in vitro* -diagnostiikkaan tarkoitettujen lääkinnällisten laitteiden valmistus	Euroopan parlamentin ja neuvoston asetuksen (EU) 2017/745 ([4]) 2 artiklan 1 alakohdassa määriteltyjä lääkinnällisiä laitteita valmistavat toimijat sekä Euroopan parlamentin ja neuvoston asetuksen (EU) 2017/746 ([5]) 2 artiklan 2 alakohdassa määriteltyjä *in vitro* -diagnostiikkaan tarkoitettuja lääkinnällisiä laitteita valmistavat toimijat, lukuun ottamatta tämän direktiivin liitteessä I olevan 5 kohdan viidennessä luetelmakohdassa mainittuja lääkinnällisiä laitteita valmistavia toimijoita
	b) Tietokoneiden sekä elektronisten ja optisten tuotteiden valmistus	NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 26 tarkoitettua taloudellista toimintaa harjoittavat yritykset
	c) Sähkölaitteiden valmistus	NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 27 tarkoitettua taloudellista toimintaa harjoittavat yritykset
	d) Muiden koneiden ja laitteiden valmistus	NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 28 tarkoitettua taloudellista toimintaa harjoittavat yritykset
	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

Toimiala	Toimialan osa	Toimijatyyppi
6. Digitaalisen palvelun tarjoajat		— Verkossa toimivien markkinapaikkojen tarjoajat
		— Verkossa toimivien hakukoneiden tarjoajat
		— Verkkoyhteisöalustojen tarjoajat
7. Tutkimustoiminta		Tutkimusorganisaatiot

([1]) 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).

([2]) 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).

([3]) 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).

([4]) 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).

([5]) 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).

LIITE III

VASTAAVUUSTAULUKKO

Direktiivi (EU) 2016/1148	Tämä direktiivi
1 artiklan 1 kohta	1 artiklan 1 kohta
1 artiklan 2 kohta	1 artiklan 2 kohta
1 artiklan 3 kohta	–
1 artiklan 4 kohta	2 artiklan 12 kohta
1 artiklan 5 kohta	2 artiklan 13 kohta
1 artiklan 6 kohta	2 artiklan 6 ja 11 kohta
1 artiklan 7 kohta	4 artikla
2 artikla	2 artiklan 14 kohta
3 artikla	5 artikla
4 artikla	6 artikla
5 artikla	–
6 artikla	–
7 artiklan 1 kohta	7 artiklan 1 ja 2 kohta
7 artiklan 2 kohta	7 artiklan 4 kohta
7 artiklan 3 kohta	7 artiklan 3 kohta
8 artiklan 1–5 kohta	8 artiklan 1–5 kohta
8 artiklan 6 kohta	13 artiklan 4 kohta
8 artiklan 7 kohta	8 artiklan 6 kohta
9 artiklan 1, 2 ja 3 kohta	10 artiklan 1, 2 ja 3 kohta
9 artiklan 4 kohta	10 artiklan 9 kohta
9 artiklan 5 kohta	10 artiklan 10 kohta
10 artiklan 1 ja 2 kohta ja 3 kohdan ensimmäinen alakohta	13 artiklan 1, 2 ja 3 kohta
10 artiklan 3 kohdan toinen alakohta	23 artiklan 9 kohta
11 artiklan 1 kohta	14 artiklan 1 ja 2 kohta
11 artiklan 2 kohta	14 artiklan 3 kohta
11 artiklan 3 kohta	14 artiklan 4 kohdan ensimmäisen alakohdan a–q alakohta ja s alakohta ja 7 kohta
11 artiklan 4 kohta	14 artiklan 4 kohdan ensimmäisen alakohdan r alakohta ja toinen alakohta
11 artiklan 5 kohta	14 artiklan 8 kohta
12 artiklan 1–5 kohta	15 artiklan 1–5 kohta
13 artikla	17 artikla
14 artiklan 1 ja 2 kohta	21 artiklan 1–4 kohta
14 artiklan 3 kohta	23 artiklan 1 kohta
14 artiklan 4 kohta	23 artiklan 3 kohta
14 artiklan 5 kohta	23 artiklan 5, 6 ja 8 kohta

Direktiivi (EU) 2016/1148	Tämä direktiivi
14 artiklan 6 kohta	23 artiklan 7 kohta
14 artiklan 7 kohta	23 artiklan 11 kohta
15 artiklan 1 kohta	31 artiklan 1 kohta
15 artiklan 2 kohdan ensimmäisen alakohdan a alakohta	32 artiklan 2 kohdan e alakohta
15 artiklan 2 kohdan ensimmäisen alakohdan b alakohta	32 artiklan 2 kohdan g alakohta
15 artiklan 2 kohdan toinen alakohta	32 artiklan 3 kohta
15 artiklan 3 kohta	32 artiklan 4 kohdan b alakohta
15 artiklan 4 kohta	31 artiklan 3 kohta
16 artiklan 1 ja 2 kohta	21 artiklan 1–4 kohta
16 artiklan 3 kohta	23 artiklan 1 kohta
16 artiklan 4 kohta	23 artiklan 3 kohta
16 artiklan 5 kohta	–
16 artiklan 6 kohta	23 artiklan 6 kohta
16 artiklan 7 kohta	23 artiklan 7 kohta
16 artiklan 8 ja 9 kohta	21 artiklan 5 kohta ja 23 artiklan 11 kohta
16 artiklan 10 kohta	–
16 artiklan 11 kohta	2 artiklan 1, 2 ja 3 kohta
17 artiklan 1 kohta	33 artiklan 1 kohta
17 artiklan 2 kohdan a alakohta	32 artiklan 2 kohdan e alakohta
17 artiklan 2 kohdan b alakohta	32 artiklan 4 kohdan b alakohta
17 artiklan 3 kohta	37 artiklan 1 kohdan a ja b alakohta
18 artiklan 1 kohta	26 artiklan 1 kohdan b alakohta ja 2 kohta
18 artiklan 2 kohta	26 artiklan 3 kohta
18 artiklan 3 kohta	26 artiklan 4 kohta
19 artikla	25 artikla
20 artikla	30 artikla
21 artikla	36 artikla
22 artikla	39 artikla
23 artikla	40 artikla
24 artikla	–
25 artikla	41 artikla
26 artikla	45 artikla
27 artikla	46 artikla
Liitteessä I oleva 1 alakohta	11 artiklan 1 kohta
Liitteessä I olevan 2 alakohdan a alakohdan i–iv alakohta	11 artiklan 2 kohdan a–d alakohta

Direktiivi (EU) 2016/1148	Tämä direktiivi
Liitteessä I olevan 2 alakohdan a alakohdan v alakohta	11 artiklan 2 kohdan f alakohta
Liitteessä I olevan 2 alakohdan b alakohta	11 artiklan 4 kohta
Liitteessä I olevan 2 alakohdan c alakohdan i ja ii alakohta	11 artiklan 5 kohdan a alakohta
Liite II	Liite I
Liitteessä III olevat 1 ja 2 alakohta	Liitteessä II oleva 6 alakohta
Liitteessä III oleva 3 alakohta	Liitteessä I oleva 8 alakohta