U 9/2021 vp

Valtioneuvoston kirjelmä eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi (COM (2020) 823 final) kyberturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella ja direktiivin 2016/1148 kumoamisesta (verkko- ja tietoturvadirektiivi)

Perustuslain 96 §:n 2 momentin perusteella lähetetään eduskunnalle Euroopan komission 16 päivänä joulukuuta 2020 tekemä ehdotus Euroopan parlamentin ja neuvoston direktiiviksi (COM(2020) 823 final) kyberturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella ja direktiivin 2016/1148 kumoamisesta (verkko- ja tietoturvadirektiivi) sekä ehdotuksesta laadittu muistio.

Helsingissä 11.2.2021

Liikenne- ja viestintäministeri Timo Harakka

Erityisasiantuntija Marième Korhonen

LIIKENNE- JA VIESTINTÄMINISTERIÖ | MUISTIO | EU/2020/0359

11.2.2021

VALTIONEUVOSTON KIRJELMÄ EDUSKUNNALLE KOMISSION EHDOTUKSESTA EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVIKSI (COM (2020) 823 FINAL) KYBERTURVALLISUUDEN KORKEAN TASON VARMISTAMISEKSI EUROOPAN UNIONIN ALUEELLA JA DIREKTIIVIN 2016/1148 KUMOAMISESTA (VERKKO- JA TIETOTURVADIREKTIIVI)

1 Tausta

Komissio antoi 16.12.2020 ehdotuksen Euroopan parlamentin ja neuvoston direktiiviksi (COM(2020) 823 final) kyberturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella ja direktiivin (EU) 2016/1148 kumoamisesta.

Tämä ehdotus pohjautuu ensimmäiseen EU:n laajuiseen säädösinstrumenttiin, verkko- ja tietoturvadirektiiviin (EU) 2016/1148, jäljempänä NIS-direktiivi), jonka tavoitteena oli kehittää EU:n yhteistä kyberturvallisuuden tasoa. Suomessa NIS-direktiivi implementoitiin sektorikohtaiseen sääntelyyn lisäämällä säännökset keskeisten palveluntarjoajien velvollisuudesta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta tietoyhteiskuntakaareen (nykyisin laki sähköisen viestinnän palveluista), ilmailulakiin, rautatielakiin, alusliikennepalvelulakiin, eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annettuun lakiin, liikenteen palveluista annettuun lakiin, sähkömarkkinalakiin, maakaasumarkkinalakiin ja vesihuoltolakiin. Muiden NIS-direktiivin mukaisten kriittisten sektoreiden keskeisiä palveluntarjoajia sääntelevät kansalliset lait olivat tietoturvasääntelyn osalta ensimmäisen NIS-direktiivin tasolla tai tarkempia, eikä niitä tarvinnut muuttaa.

Komissio uudelleenarvioi vuoden 2020 aikana NIS-direktiiviä ja sen soveltamiskokemuksia jäsenvaltioissa. Komissio järjesti lisäksi direktiivistä julkisen kuulemisen vuoden 2020 aikana. Suomi vastasi osaltaan julkiseen kuulemiseen ennakkovaikuttamislinjausten pohjalta (E 107/2020 vp).

2 Ehdotuksen tavoite

Komissio toteaa 16.12.2020 antamassaan ehdotuksessa, että yhteiskuntien digitaalinen kehitys, jota COVID-19 –pandemia on vauhdittanut, on muuttanut oleellisesti nykyistä toimintaympäristöä ja tuonut mukanaan uusia haasteita, jotka edellyttävät innovatiivisia ratkaisuja. Kyberloukkausten määrä on kasvanut ja nämä ovat olleet entistä kehittyneempiä. Kyberturvallisuushäiriöt vaikeuttavat sisämarkkinoiden toimintaa, aiheuttavat taloudellisia menetyksiä ja heikentävät käyttäjien luottamusta unionin talous- ja yhteiskuntaelämään. Komission mukaan ehdotus uudeksi direktiiviksi uudistaisi olemassa olevaa lainsäädäntökehystä ottaen huomioon sisämarkkinoiden toimintaympäristön muutokset. Ehdotus on osa komission painopistettä edistää Euroopan digitaalista valmiutta.

Ehdotuksen tavoitteena on vahvistaa sekä EU:n yhteistä että jäsenvaltioiden kansallista kyberturvallisuuden tasoa kriittisiksi katsottujen sektoreiden ja toimijoiden osalta asettamalla riskienhallintatoimia kyberturvallisuushäiriöiden varalta. Ehdotus yhdenmukaistaisi toimijoiden tunnistamista EU:n laajuisesti ja vähentäisi tämän osalta jäsenvaltioiden hallinnollista taakkaa. Li-

säksi ehdotus yhdenmukaistaisi kyberturvallisuus- ja raportointivelvoitteita ja laajentaisi soveltamisalaa koskettamaan uusia sektoreita ja toimijoita. Valvoville viranomaisille muodostuisi myös olemassa olevien tehtävien jatkumisen lisäksi uusia valvontatehtäviä, kuten soveltamisalaan lisättyjen toimijoiden valvonta.

3 Ehdotuksen pääasiallinen sisältö

3.1 Keskeisten toimijoiden tunnistaminen

Ensimmäisen NIS-direktiivin mukaan jäsenvaltiot olivat vastuussa toimijoiden identifioinnista keskeisiksi palveluntarjoajiksi. Komission mukaan aiempi tapa aiheutti laajaa hajanaisuutta jäsenvaltioiden soveltamisessa keskeisten palveluntarjoajien identifioinnissa, mistä syystä uudella ehdotuksella pyrittäisiin vastaamaan tähän komission tunnistamaan ongelmaan poistamalla erillinen identifiointiprosessi.

Uuden direktiiviehdotuksen mukaan jäsenvaltioiden ei tarvitsisi enää kansallisesti tunnistaa keskeisiä toimijoita, koska kriteerejä yhdenmukaistettaisiin koko EU:n laajuisesti siten, että kaikki kriittisten sektoreiden suuret ja keskisuuret toimijat olisivat jokaisen jäsenmaan osalta sääntelyn piirissä. Näistä jäsenvaltioiden ei tarvitsisi toimittaa listausta komissiolle, vaan ENISA pitäisi jatkossa yllä listaa keskeisistä palveluntarjoajista ja valvovista viranomaisista jäsenvaltioiden osalta EU-tasoisesti.

Pienet ja mikroyritykset jäisivät lähtökohtaisesti ehdotetun sääntelyn ulkopuolelle. Jäsenvaltiot voisivat kuitenkin tietyissä tapauksissa tunnistaa keskeisiksi myös pieniä ja mikrotoimijoita, mikäli näiden tuottamat palvelut voidaan katsoa yhteiskunnan toiminnan jatkuvuuden kannalta keskeisiksi. Komissio julkaisisi yhteistyössä NIS-direktiivin asettaman yhteistyöryhmän (jäljempänä NIS-yhteistyöryhmä) kanssa ohjeet identifiointikriteerien soveltamiseksi näiden toimijoiden osalta. Jäsenvaltioiden tulisi toimittaa komissiolle listaus tunnistetuista pienistä ja mikrotoimijoista.

3.2 Toimijoiden kategorisointi

Toimijoiden kategorisointi jaettaisiin ehdotuksen mukaan keskeisiin (*essential*) ja tärkeisiin (*important*) riippuen toimijan kriittisyydestä ja keskinäisriippuvuudesta muihin sektoreihin ja toimijoihin. Sekä keskeisiin että tärkeisiin kategorioihin kuuluviin toimijoihin sovellettaisiin samoja riskienhallinta- ja raportointivelvollisuuksia. Kuitenkin valvonta- ja seuraamusjärjestelmät olisivat tiukempia keskeisten toimijoiden kuin tärkeiden osalta. Aiemmassa direktiivissä ei tehty eroja kriittisten toimijoiden välillä.

3.3 Soveltamisalan laajentaminen

Ehdotuksen mukaan direktiivin soveltamisalaa laajennettaisiin aiemmasta soveltamisalan laajuudesta koskemaan keskeisten sektoreiden osalta myös energiasektorilla vetytuotannon ja kaukolämmön ja -jäähdytyksen tuottajia. Terveydenhuoltosektorin osalta soveltamisalaa laajennettaisiin koskettamaan EU:n vertailulaboratorioita, lääkealan tutkimus- ja kehitystoimijoita sekä lääkkeiden ja lääkinnällisten laitteiden tuotannon toimijoita. Lisäksi soveltamisala koskettaisi uusina lisäyksinä jätevesihuoltoa sekä avaruussektorin toimijoita. Soveltamisalaan keskeisiin sektoreihin lisättäisiin myös uutena julkishallinto, kuten keskushallinnon toimijat sekä alueelliset hallinnot sellaisina kuin ne on määritelty asetuksessa (EU) 1059/2003 liitteessä I esitettyjen luokitustasojen NUTS 1 ja NUTS 2 tavalla. Asetuksen (EU) 1059/2003 liitteiden II ja III mukaan luokitustasot koskettaisivat Suomessa valtionhallintoa ja sen alaisia valtakunnallisia virastoja ja laitoksia sekä maakuntia ja kuntia.

Ehdotuksen 4 artiklan 23 kohdan mukaan ne julkishallinnon toimijat, jotka toimivat yleisen turvallisuuden, lainvalvonnan, puolustuksen ja kansallisen turvallisuuden aloilla eivät lukeudu soveltamisalaan. Lisäksi direktiiviehdotuksen 2 artiklan 3 kohdan mukaisesti direktiivi ei vaikuta jäsenvaltioiden toimivaltaan, joka koskee yleisen turvallisuuden, puolustuksen ja kansallisen turvallisuuden ylläpitämistä.

Digitaalisen infrastruktuurin toimijat kuuluisivat keskeisten toimijoiden kategoriaan ja näihin lisättäisiin uusina toimijoina datakeskuspalveluntarjoajat, sisällönjakeluverkkojen tarjoajat, luottamuspalveluiden tarjoajat, yleisten sähköisten viestinnän verkkojen ja palvelujen tarjoajat sekä pilvipalveluiden tarjoajat.

Soveltamisalaa laajennettaisiin tärkeinä toimijoina koskemaan posti- ja kuriiripalvelujen toimijoita, jätehuoltotoimijoita, kemikaalien valmistuksen, tuotannon ja jakelun toimijoita sekä elintarviketuotannon ja -jakelun toimijoita. Tärkeiden toimijoiden osalta laajempana sektorilisäyksenä tulisi valmistusprosessit (*manufacturing*), johon lukeutuisi lääkinnällisten laitteiden valmistus, tietokoneiden, elektronisten ja optisten laitteiden valmistus, sähkölaitteiden valmistus, muiden koneiden ja laitteiden valmistus sekä moottoriajoneuvojen ja täys- ja puoliperävaunujen valmistus. Lisäksi digitaalisiin palveluntarjoajiin lisättäisiin tärkeinä toimijoina verkkoyhteisöpalvelujen tarjoajat, verkossa toimivat markkinapaikat sekä verkossa toimivat hakukoneet.

3.4 Kyberturvallisuusvalmiuksien kehittäminen EU:ssa ja kansallisesti jäsenvaltioissa

EU:n tasolla ehdotus sisältää toimia, jotka kehittäisivät yhteistä tilannekuvan ylläpitämistä sekä tiivistä yhteistyötä ja tietojenvaihtoa EU:n resilienssin kehittämiseksi kyberturvallisuuden saralla. Jäsenvaltioiden tasolla ehdotus sisältää toimia, joiden tavoitteena on kehittää valmiuksia korkean kyberturvallisuuden tason varmistamiseksi.

Ensimmäinen NIS-direktiivi loi pohjan kyberturvallisuusvalmiuksien kehittämiselle edellyttämällä jäsenvaltioita laatimaan kansalliset tietoturvastrategiat ja edellyttämällä keskeisiltä palveluntarjoajilta tietoturvallisuusvelvoitteiden noudattamista. Lisäksi direktiivi asetti valvoville viranomaisille uusia tehtäviä keskeisten toimijoiden valvomiseksi ja yhteistyön tiivistämiseksi sekä kansallisesti että EU:ssa. Suomessa laadittiin verkko- ja tietoturvadirektiivin pohjalta kansallinen tietoturvastrategia sekä asetettiin verkko- ja tietoturvavelvoitteita keskeisiksi tunnistetuille toimijoille.

Komission uuden ehdotuksen mukaan jäsenvaltioiden tulisi laatia kansalliset kyberturvallisuusstrategiat 5 artiklan mukaisesti, vahvistaa valvovien viranomaisten valvontatehtäviä ja toimijoiden tulisi lisäksi ottaa käyttöön ehdotuksessa esitettyjä riskienhallintatoimia.

3.5 Haavoittuvuuksien tunnistaminen

Ehdotus asettaisi uutena elementtinä toimintatavat haavoittuvuuksien tunnistamiselle 6 artiklan mukaisesti, jossa CSIRT –toimija (*computer security incident response teams*) toimisi koordinoivana tahona. Ehdotuksen mukaan toimijan haavoittuvuuksista tulisi ilmoittaa CSIRT-toimijalle, jotta nämä haavoittuvuudet voitaisiin korjata. Haavoittuvuuksien tunnistamiseksi jäsenvaltioiden tulisi tarkastella ja asettaa tarvittavia toimintalinjauksia. Euroopan unionin verkko- ja tietoturvaviraston (jäljempänä ENISA) tulisi kerätä ja ylläpitää haavoittuvuusrekisteriä löydetyistä haavoittuvuuksista läpinäkyvyyden varmistamiseksi ja tilannekuvan ylläpitämiseksi.

3.6 Varautuminen laajamittaisten kyberturvallisuushäiriöiden ja –kriisien varalle

Ehdotuksen 7 artiklan mukaan jäsenvaltioiden tulisi perustaa toimintalinjaukset laajamittaisten kyberturvallisuusriskien varalle.

Jäsenvaltioiden tulisi määrittää yksi tai useampi valvova viranomainen, joka olisi vastuussa laajamittaisten kyberturvallisuushäiriöiden ja –kriisien operatiivisesta johtamisesta. Jäsenvaltioiden tulisi varmistaa, että valvovilla viranomaisilla on näihin tehtäviin riittävät resurssit. Jokaisen jäsenvaltion tulisi tunnistaa valmiudet, resurssit ja prosessit, jotka voidaan käynnistää ja ottaa käyttöön ehdotuksen mukaisissa tilanteissa.

Komissiota tulisi informoida tehtävien hoitamiseen valituista valvovista viranomaisista sekä toimintalinjausten hyväksymisestä kolmen kuukauden kuluessa niiden laadinnasta.

3.7 Riskienhallintatoimien kehittäminen

Riskienhallintatoimenpiteiden tulisi ehdotuksen 17 ja 18 artiklojen mukaan sisältää toimet, joilla voidaan tunnistaa riskit mahdollisiin häiriöihin sekä tunnistaa ja käsitellä näitä ja lieventää niiden vaikutuksia. Näitä toimia olisi ehdotuksen mukaan riskianalyysit ja tietojärjestelmien turvallisuustoimet, häiriöiden käsittely (ennaltaehkäisy, tunnistaminen ja häiriöihin vastaaminen), liiketoiminnan jatkuvuus ja kriisinhallinta, tuotantoketjujen kyberturvallisuus, kyberturvallisuus verkko- ja tietojärjestelmien hankinnoissa sekä niiden kehityksessä ja ylläpidossa. Lisäksi näihin riskienhallintatoimiin kuuluisi haavoittuvuuksien käsittely ja tunnistaminen, toimintalinjaukset ja prosessit, kuten testaus ja auditointi, joiden avulla arvioidaan kyberturvallisuuden riskienhallintatoimien tehokkuutta sekä kryptografian ja salauksen hyödyntäminen.

Ehdotuksen mukaan erityisesti päästä päähän salausta tulisi kehittää, hyödyntää ja tarpeen mukaan olla pakollista viestintäverkkojen tarjoajien turvallisuuden edistämiseksi. Ehdotuksen mukaan lainvalvontaviranomaisten tehtävien ja tehokkaan salauksen hyödyntämisen välille on löydettävä tasapainoinen ratkaisu.

Komissio esittää ehdotuksessaan, että kyberturvallisuuden riskienhallintavelvoitteiden tulisi olla suhteessa kunkin toimijan kohdalla arvioituihin riskeihin. Verkko- ja tietojärjestelmien turvaamisessa riskienhallintatoimet ja raportointivelvoitteet tulisi ottaa käyttöön riippumatta siitä, onko järjestelmien ylläpitotoimet ulkoistettu. 17 artiklan mukaan toimijoiden johtoportaan tulisi hyväksyä 18 artiklan mukaiset riskienhallintatoimet, valvoa niiden toimeenpanoa ja vastata velvoitteiden noudattamatta jättämisestä. Ehdotus laajentaisi riskienhallintatoimia koskettamaan myös toimijoiden tuotantoketjuja. NIS-yhteistyöryhmän tulisi relevanttien kansallisten viranomaisten, komission ja ENISAn kanssa arvioida yhteistyössä tuotantoketjujen osalta kriittisten ICT-palvelujen, -tuotteiden, -järjestelmien mahdollisia uhkia ja haavoittuvuuksia 19 artiklassa esitetyn mukaisesti.

Ehdotuksen 3 artiklan mukaan jäsenvaltiot voisivat ehdotuksessa esitettyjen velvoitteiden lisäksi ottaa käyttöön säännöksiä, jotka takaavat kansallisesti korkean kyberturvallisuustason.

3.8 Raportointivelvoitteet

Ehdotus asettaisi 20 artiklan mukaisesti kaksiportaisen raportoinnin nopean tiedonkulun sekä syvällisemmän raportoinnin varmistamiseksi. Toimijoiden tulisi raportoida valvovalle viranomaiselle ensimmäisen kerran 24 tunnin kuluessa siitä, kun merkittäväksi arvioitu häiriö tai kyberloukkauksen uhka on tullut toimijan tietoon. Tämän jälkeen toimijan tulisi toimittaa valvovalle viranomaiselle loppuraportti kuukauden kuluessa häiriöstä. Lisäksi ehdotuksen 27 artikla mahdollistaisi tämän direktiiviehdotuksen soveltamisalan ulkopuolelle jäävien toimijoiden mahdollisuudesta raportoida häiriöistä vapaaehtoisuuden pohjalta.

3.9 Valvovien viranomaisten tehtävät

Ehdotuksen 28 artiklan mukaan jäsenvaltioiden tulee varmistaa, että valvovat viranomaiset valvovat tehokkaasti ja ottavat käyttöön vaaditut toimet varmistaakseen toimijoille asetettujen velvoitteiden noudattamisen. Ehdotus esittäisi keskeisille toimijoille ennakko- ja jälkivalvontaa ja tärkeille toimijoille vain jälkivalvontaa. Valvovien viranomaisten tulee tehdä tiivistä yhteistyötä tietosuojaviranomaisten kanssa käsitellessään henkilötietoja koskettavia tietoturvamurtoja.

Ehdotuksessa ehdotetaan lukuisia tarkempia tehtäviä valvontaviranomaisille. Näitä toimia ovat toimijoilla paikan päällä tehtävät tarkastukset sekä etävalvonta. Näiden lisäksi tulisi toimijoihin kohdistuvat sattumanvaraiset tarkastukset, säännölliset auditoinnit, kohdennetut turvallisuusauditoinnit perustuen riskien arviointiin tai riskiperustaiseen informaatioon, turvallisuusskannaukset, tietopyynnöt toimijoiden kyberturvallisuustoimien arviointiin, pääsy tarvittaviin tietoihin valvontatehtävien suorittamiseksi, todisteiden pyytäminen toimijoiden kyberturvallisuustoimien täytäntöön panemisesta.

Jäsenvaltioiden tulisi varmistaa, että valvovilla viranomaisilla on mahdollisuus antaa varoituksia toimijoille direktiiviehdotuksessa asetettujen velvoitteiden laiminlyönnistä, antaa määräyksiä laiminlyönnin korjaamiseksi, antaa määräyksiä toimijoille informoida relevantteja tahoja ja henkilöitä mahdollisista suojaamistoimista, mikäli toimija joutuu kyberturvallisuusuhan kohteeksi sekä määrätä tai pyytää määrättäväksi hallinnolliset sanktiot riippuen kyberturvallisuushäiriöstä. Mikäli toimija ei noudattaisi valvovan viranomaisen asettamia määräyksiä, valvovilla viranomaisilla olisi mahdollisuus asettaa tietyksi ajaksi toimija ja johtoportaassa toimiva henkilö toimintakieltoon.

Lisäksi ehdotus esittää hallinnollisia sanktioita toimijan velvoitteiden laiminlyönnistä, joiden taso määräytyisi toimijan kategorian ja häiriön tai kriisin laajuuden ja aiheutetun vahingon mukaan. Komission mukaan määrättävät sakot voisivat olla 31 artiklan mukaan enimmillään vähintään 10 000 000 euroa tai jopa 2% toimijan vuosittaisesta liikevaihdosta sen mukaan kumpi olisi toimijalle korkeampi sanktio. Ehdotuksen 31 artiklan 6 kohdan mukaan sanktioiden kohdistaminen julkishallinnon toimijoihin jäisi jäsenvaltioiden kansalliseen harkintaan. Lisäksi 33 artiklan 1 kohdan mukaan jäsenvaltioiden olisi säädettävä tämän direktiivin säännösten rikkomisen seuraamuksista ja ryhdyttävä kaikkiin tarvittaviin toimenpiteisiin niiden soveltamisen varmistamiseksi.

3.10 Yhteistyön kehittäminen ja tietojenvaihto kansallisesti ja EU:ssa

Ehdotuksen 26 artiklan mukaan toimijoiden tulisi vaihtaa tietoja keskenään yhteistyön tiivistämiseksi. Lisäksi ehdotuksen 11 artiklan mukaan ehdotuksen tavoitteiden saavuttamiseksi yhteistyötä tulisi tehdä kansallisen yhteyspisteen, CSIRT –toimijan ja valvovien viranomaisten kesken. Yhteistyötä tulisi tehdä myös muiden sektorikohtaisten sääntelyiden mukaisten valvovien viranomaisten kanssa, erityisesti finanssialan digitaalisesta häiriönsietokyvystä annetun asetusehdotuksen sekä fyysisen kriittisen infrastruktuurin suojaamiseksi annetun direktiiviehdotuksen mukaisten valvovien viranomaisten kanssa.

Ehdotus jatkaa lisäksi NIS-direktiivin pohjalta aiemmin asetettuja yhteistyömekanismeja ja tarkentaa yhteistyötehtäviä ja tavoitteita. NIS-yhteistyöryhmän tehtävinä on 12 artiklan mukaan kartoittaa kansallisia kokemuksia ja ratkaisuja sekä keskustella täytäntöönpanon kokemuksista ja mahdollisista haasteista sekä laatia suosituksia säännösten implementointia varten.

Ehdotus jatkaa lisäksi NIS-direktiivin asettamia CSIRT-toimijan tehtäviä ja CSIRT-verkoston toimintaa ja yhteistyötä.

Ehdotus perustaisi EU:n jäsenvaltioista koostuvan CyCLONe (Cyber Crises Liaison Organisation Network) –verkoston 14 artiklan mukaisesti laajamittaisten kyberturvallisuuskriisien varalle. Tämän verkoston tehtävänä on tukea operationaalisen tason koordinaatio- ja johtotehtäviä kyberturvallisuushäiriöiden ja -kriisien edessä. Komissio ehdottaa myös uutena elementtinä komission järjestämän vertaisarvioinnin 18 kuukauden kuluessa päivitetyn direktiivin voimaan saattamisesta yhteistyössä ENISAn kanssa 16 artiklan mukaisesti.

3.11 Sertifiointi ja standardisointi

Ehdotuksen 21 artiklan mukaan jäsenvaltiot voivat vaatia toimijoita sertifioimaan tietyt ICT-tuotteet, -palvelut ja –prosessit perustuen Euroopan kyberturvallisuussertifiointijärjestelmiin kyberturvallisuusasetuksen (2019/881) 49 artiklan nojalla. Komissio voisi myös pyytää ENISAa valmistelemaan vaihtoehtoisen sertifiointijärjestelmän, mikäli tähän tarkoitukseen ei löytyisi sopivaa sertifiointijärjestelmää.

Kuten ensimmäisessä NIS-direktiivissä, myös tämän ehdotuksen mukaan tulisi kannustaa jäsenvaltioita hyödyntämään EU:ssa ja kansainvälisesti hyväksyttyjä verkko- ja tietojärjestelmästandardeja.

3.12 Delegoitut säädökset ja täytäntöönpanosäädökset

Ehdotuksen mukaan komissiolle siirrettäisiin valtaa antaa delegoituja säädöksiä 36 artiklan mukaisesti liittyen esityksen riskienhallintatoimiin. Komissiolle siirrettäisiin lisäksi valtaa antaa delegoituja säädöksiä, joilla tarkennettaisiin miltä keskeisiltä toimijoilta edellytettäisiin sertifiointia ja minkä kyberturvallisuussertifiointijärjestelmän perusteella. Komissio voisi ehdotuksen mukaan antaa täytäntöönpanosäädöksiä liittyen teknisiin ja metodologisiin tarkennuksiin riskienhallintatoimien osalta sekä häiriöraportoinnin osalta tiedon toimittamismuodosta ja menettelystä. Komissiota avustaisi asetuksessa (EU) (182/2011) tarkoitettu, jäsenvaltioiden edustajista koostuva komitea.

4 Ehdotuksen oikeusperusta ja suhde suhteellisuus- ja toissijaisuusperiaatteisiin

Ehdotuksen oikeusperustana on Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 114 artikla. Artikla koskee sisämarkkinoiden toteuttamiseen ja toimintaan liittyviä toimenpiteitä ja sen tavoitteena on lähentää jäsenvaltioiden lainsäädäntöjä.

Komission arvion mukaan ehdotus poistaisi esteitä ja vahvistaisi sisämarkkinoiden toimivuutta ehdotuksessa tarkoitetuille keskeisille ja tärkeille toimijoille yhdenmukaistamalla yhteisiä velvoitteita riskienhallinnan ja raportointivelvollisuuksien osalta. Nykytilanteen fragmentoituneisuus sekä lainsäädännön että valvonnasta vastaavan tason osalta EU:ssa ja kansallisesti muodostavat esteitä sisämarkkinoiden toiminnalle, sillä toimijat kohtaavat rajat ylittävässä toiminnassaan toisistaan erilaisia ja mahdollisesti päällekkäisiä vaatimuksia.

Komissio katsoo, että ehdotus on toissijaisuusperiaatteen mukainen. EU:n laajuinen resilienssi kyberturvallisuuden saralla ei komission mukaan ole mahdollista, mikäli tavoitetta lähestytään ainoastaan kansallisesti tai alueellisesti. Ensimmäinen NIS-direktiivi vastasi tähän tarpeeseen asettamalla yhteisen lainsäädäntökehyksen verkko- ja tietoturvallisuuden tason kehittämiseksi sekä EU:ssa että kansallisesti jäsenvaltioissa. EU:n talous on tänä päivänä entistä riippuvaisempi verkko- ja tietojärjestelmistä. NIS-direktiivin mukaiset sektorit ja palvelut ovat entistä kytkeytyneempiä toisiinsa. Ehdotuksen tavoitteet ovat komission mukaan perusteltuja, sillä kyberturvallisuusriskit ja -häiriöt ovat luonteeltaan rajat ylittäviä. Lisäksi komissio katsoo, että

EU:lla on potentiaalia yhteisten toimien kautta vahvistaa tehokkaita ja koordinoituja kansallisia toimia. Yhteen sovitetuilla ja yhteistoiminnallisilla toimilla on lisäksi komission mukaan myönteinen vaikutus perusoikeuksien suojaan ja erityisesti henkilötietojen ja yksityisyyden suojaan.

Komissio katsoo, että ehdotus on suhteellisuusperiaatteen mukainen. Komissio katsoo ehdotuksessaan, että tässä esitetyt säännökset ovat oikeassa suhteessa tavoitteisiin nähden. Ehdotetut kyberturvallisuus- ja raportointivelvoitteet liittyvät jäsenvaltioiden toiveisiin ja tarpeisiin kehittää nykyistä lainsäädäntökehystä toimivammaksi. Ehdotus ottaa huomioon olemassa olevat toimenpiteet ja toimintalinjaukset jäsenvaltioissa. Korkeampi kyberturvallisuuden taso, joka saavutettaisiin ehdotuksen säännöksillä, on oikeassa suhteessa kohonneisiin riskeihin, mukaan lukien rajat ylittävän luonteen omaavat riskit. Ehdotetut toimet vastaavat yleisesti toimijoiden intresseihin varmistamalla toiminnan jatkuvuus ja toimijoiden tuottamien palvelujen laatu. Komissio katsoo, että ehdotuksen myötä syntyvät kustannukset olisivat pienemmät kuin häiriötilanteissa, jotka johtaisivat merkittäviin yhteiskunnallisiin ja taloudellisiin menetyksiin. Lisäksi tulokset NIS-direktiivin julkisesta kuulemisesta osoittivat tukea direktiivin uudelleenarviointiin.

4.1 Lainsäädäntöinstrumentin valinta

Komission mukaan ehdotus yhdenmukaistaisi velvoitteita ja sääntelyä jäsenvaltioiden välillä. Samaan aikaan ehdotus tarjoaisi jäsenvaltioille joustavuutta kansallisten erojen huomioon ottamiseksi. Jäsenvaltiot voisivat kansallisen lainsäädännön mukaisesti identifioida direktiivissä esitettyjen toimijoiden lisäksi sellaiset keskeiset ja tärkeät toimijat, jotka ylittävät tämän ehdotuksen lähtötason. Tästä syystä komissio valitsi lainsäädäntöinstrumentiksi direktiivin, joka komission mukaan yhtäältä mahdollistaisi kohdennetusti parannuksia kyberturvallisuusvelvoitteiden yhdenmukaistamiseen ja toisaalta tarjoaisi kansallista joustavuutta.

Valtioneuvosto pitää ehdotuksen oikeusperustaa asianmukaisena. Ehdotusta voidaan myös pitää toissijaisuusperiaatteen ja suhteellisuusperiaatteen mukaisena. Käsittelyn edetessä tulisi varmistaa, että ehdotuksen mukaiset säännökset ovat linjassa ehdotetun oikeusperustan kanssa.

5 Ehdotuksen vaikutukset

5.1 Komission vaikutusarviointi

Vaikutustenarvioinnissa komissio tunnisti, että yritysten kyberresilienssin taso on tällä hetkellä liian heikko. Palveluntarjoajat eivät ole toteuttaneet riittävästi tietoturvaa parantavia toimenpiteitä. Lisäksi kyberturvallisuuden saralla on puutteita yhteisen tilannekuvan ja kyberturvallisuuskriisien hallinnassa. Komissio katsoo, että NIS-direktiivin soveltamisalan ulkopuolelle on voinut jäädä esimerkiksi jäsenvaltioiden suuria sairaaloita. Soveltamisalan määrittely ja keskeisten palveluntarjoajien tunnistaminen ei ole komission mukaan onnistunut aikaisemmassa sääntelyssä. Ehdotuksessa esitettyä sääntelyä uudelleenarvioitaisiin 54 kuukauden kuluttua tämän direktiivin voimaantulosta.

Ehdotus vähentäisi sisämarkkinoiden fragmentoituneisuutta ja tasaisi toimijoiden toimintaedellytyksiä. Komission mukaan ehdotettu sääntely lisäisi toimijoiden yhtenäisempää kyberturvallisuusresilienssin tasoa EU:ssa, mikä johtaisi lopulta taloudellisiin säästöihin sekä yrityksille että yhteiskunnalle. Komissio esittää, että päivitetyn sääntelyn avulla voitaisiin saavuttaa jopa 11,3 miljardin euron säästöt kustannuksissa, joita mahdolliset kyberturvallisuushäiriöt ja –hyökkäykset voisivat aiheuttaa. Yksittäisistä häiriöistä ja torjuntatoimista voi aiheutua ylimääräisiä kustannuksia esimerkiksi siinä tilanteessa, että toiminta joudutaan keskeyttämään.

Keskisuurille yrityksille kohdistuisi ehdotetun sääntelyn myötä lisääntyneitä kuluja sääntelyn ensimmäisten implementointivuosien aikana. Samanaikaisesti turvallisuusvelvoitteiden tason nostaminen näille toimijoille edistäisi näiden kyberturvallisuusvalmiuksia ja auttaisi parantamaan ICT-riskienhallintaa.

Kustannuksia voi komission arvion mukaan aiheutua kyberturvallisuushäiriöistä ja –hyökkäyksistä myös jäsenvaltioille ylimääräisinä budjettimenoina, sekä kansalaisille talouteen kohdistuvien häiriöiden aiheuttamien tulonmenetysten muodossa. Komission vaikutustenarviointi ei sisällä arvioita vaikutuksista viranomaisiin.

Komission mukaan ehdotus asettaisi ENISA:lle lisätehtäviä olemassa olevien tehtävien jatkumisen lisäksi. Näitä tehtäviä olisivat haavoittuvuusrekisterin perustaminen ja sen ylläpito, CyCLONe-verkoston sihteeristönä toimiminen, vuosittaisen raportin EU:n kyberturvallisuuden tilasta julkaiseminen, vertaisarvioinnin laadinnassa tukeminen, kyberturvallisuushäiriötietojen keräämistä kaikista jäsenvaltioista ja teknisen tuen tarjoamista sekä rekisterin luominen ja ylläpitäminen niistä toimijoista, jotka tarjoavat palveluja rajat ylittävästi. Näiden tehtävien hoitamiseksi syntyisi lisääntyneitä henkilöstöresurssitarpeita.

5.2 Vaikutukset EU:n budjettiin

Ehdotus on komission mukaan yhteensopiva nykyisen (2021-2027) monivuotisen rahoituskehyksen kanssa. Komissio aikoo kattaa ENISA:lle ehdotuksessa esitettyjen tehtävien lisääntymisen johdosta aiheutuvat lisähenkilöstökulut Digitaalinen Eurooppa –ohjelmasta.

5.3 Kansallinen vaikutusarviointi

5.3.1 Vaikutukset kansalliseen lainsäädäntöön

Ehdotus on säädöstyypiltään direktiivi, joka tulisi implementoida kansalliseen lainsäädäntöön.

Suomessa ensimmäinen NIS-direktiivi implementoitiin sektorikohtaiseen sääntelyyn lisäämällä säännökset keskeisten palveluntarjoajien velvollisuudesta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta tietoyhteiskuntakaareen (nykyisin laki sähköisen viestinnän palveluista), ilmailulakiin, rautatielakiin, alusliikennepalvelulakiin, eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annettuun lakiin, liikenteen palveluista annettuun lakiin, sähkömarkkinalakiin, maakaasumarkkinalakiin ja vesihuoltolakiin. Finanssisektorin ja terveydenhuoltosektorin kansallisiin sektorikohtaisiin lakeihin ei tehty muutoksia, koska niiden katsottiin jo täyttävän ensimmäisen NIS-direktiivin velvoitteet.

Ehdotuksessa esitetty sääntely edellyttäisi ainakin edellä mainittujen sektorikohtaisten sääntelyiden uudelleentarkastelua ja ehdotuksessa esitettyjen säännösten implementointia. Lisäksi tulisi arvioitavaksi muun relevantin sektorikohtaisen sääntelyn uudelleentarkastelu ja esitettyjen säännösten implementointi erityisesti soveltamisalan laajentamisen johdosta. Julkishallintoa koskevaa lainsäädäntöä tulisi myös tarkastella. Direktiivin implementoinnin yhteydessä tulisi tarkastella myös muilta osin jo asetettuja ja asetettavia kyberturvallisuusvelvoitteita yhdenmukaisen sääntelyn varmistamiseksi. Myös yleiseen henkilötietojen käsittelyä koskevaan lainsäädäntöön sisältyy tietoturvallisuutta koskevia vaatimuksia, joita sovelletaan kaikkiin sellaisiin tietojärjestelmiin, joissa käsitellään henkilötietoja.

Ehdotuksella olisi vaikutusta seuraamuksia koskevaan sääntelyyn. Direktiiviehdotuksen 31-33 artiklan suhde vaatii vielä kuitenkin tarkempaa arviointia. Erityisesti ehdotetun 33 artiklan so-

veltamisala vaikuttaisi osittain päällekkäiseltä hallinnollisia seuraamuksia koskevien säännösten kanssa, mutta kattaisi laajemmin direktiiviin perustuvia velvoitteita. Uusia lainsäädäntövelvoitteita seuraisi hallinnollisia seuraamuksia koskevista säännöksistä. Näiden vaikutuksia olisi arvioitava huolella neuvottelujen aikana. Vaikka direktiiviehdotus sisältää jonkin verran kansallista liikkumavaraa, hallinnollisten seuraamusten osalta olisi syytä varmistua siitä, että ne sopivat yhteen muita seuraamuksia koskevan sääntelyn kanssa.

5.3.2 Vaikutukset viranomaisten toimintaan

Suomessa ensimmäisen NIS-direktiivin implementoinnin johdosta sektorikohtaiset valvovat viranomaiset ovat vastanneet direktiivin mukaisesti asetettujen velvoitteiden valvonnasta. Suomessa nämä valvovat viranomaiset ovat Liikenne- ja viestintävirasto, Energiavirasto, Finanssivalvonta, Sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira) sekä elinkeino-, liikenne- ja ympäristökeskukset. Liikenne- ja viestintäviraston lakiin perustuvat tehtävät olivat jo ennen NIS-direktiiviä kattavat tietoturvaloukkauksiin reagoimiseksi ja loukkauksien tutkimiseksi. Tämän johdosta Liikenne- ja viestintävirasto katsottiin sopivaksi kansalliseksi yhteyspisteeksi ja CSIRT-toimijaksi.

Käsillä olevassa ehdotuksessa esitetään kansallisille valvoville viranomaisille tehtävien tarkentamista ja lisäämistä. Soveltamisalan laajentaminen lisäisi osaltaan valvovien viranomaisten tehtäviä ja todennäköisesti lisäisi valvovien viranomaisten määrää. Direktiiviehdotuksen 11 artiklassa säädettäisiin viranomaisia koskevista yhteistyövelvoitteista, joilla olisi vaikutusta kaikkien siinä tarkoitettujen viranomaisten toimintaan. Direktiiviehdotuksen 28 artikla sisältää myös viranomaisille asetettavan nimenomaisen velvoitteen tehdä yhteistyötä tietosuojaviranomaisten kanssa sellaisia tapahtumia käsiteltäessä, joista aiheutuu henkilötietojen tietoturvaloukkauksia. Tällä olisi vaikutusta tietosuojavaltuutetun toimintaan. Resurssivaikutuksia ja mahdollisia muita direktiiviehdotuksesta aiheutuvia vaikutuksia olisi arvioitava tarkemmin ehdotuksen käsittelyn aikana.

Direktiiviehdotuksen jatkokäsittelyn aikana olisi arvioitava tarkemmin, mille viranomaisille ja miltä osin direktiivistä voisi seurata uudenlaisia vaatimuksia. Direktiiviehdotuksen mukaan jäisi jäsenvaltioiden harkintaan se, voidaanko hallinnollisia seuraamuksia määrätä julkishallinnon toimijoille.

Direktiiviehdotuksen mukaan viranomaisten tulee valvoa toimijoiden tietoturvavelvoitteiden noudattamista oma-aloitteisesti etukäteen nykyisen jälkivalvonnan sijasta. Sääntelyn tehokas valvonta edellyttää merkittävää resurssien lisäämistä sektorikohtaisille valvoville viranomaisille ja tietoturvaosaamisen kasvattamista. Direktiiviehdotukseen sisältyvät myös säännökset hallinnollisista seuraamuksista sekä niihin liittyvien toimivaltuuksien käyttämisestä. Niihin liittyvästä yhteistyöstä voi seurata vähintään hallinnollista taakkaa toimivaltaisille valvontaviranomaisille ja tietosuojaviranomaisille. Ehdotetut hallinnollisia seuraamuksia koskevat säännökset voisivat merkitä myös uutta asiaryhmää hallinto-oikeuksille. Merkittävin hallinto-oikeuksiin kohdistuva vaikutus olisi kuitenkin alustavan arvion mukaan mahdollinen työmäärän kasvu. Lisäksi jonkinasteisia vaikutuksia voisi seurata myös Oikeusrekisterikeskukselle, joka vastaa rekisterinpitäjänä oikeushallinnon valtakunnallisesta tietojärjestelmästä ja hallinnollisten seuraamusmaksujen täytäntöönpanosta. Hallinnollisia seuraamuksia koskevien säännösten vaikutuksia olisi arvioitava tarkemmin direktiiviehdotuksen käsittelyn aikana.

5.3.3 Taloudelliset vaikutukset

Ehdotettu sääntely aiheuttaisi komission mukaan taloudellisia kustannuksia soveltamisalan piiriin kuuluville toimijoille. Komissio arvioi, että näiden toimijoiden ICT-kustannukset kasvaisivat 22% nykyisestä ensimmäisten implementointivuosien aikana. Kuitenkin niiden toimijoiden osalta, jotka kuuluvat jo ensimmäisen NIS-direktiivin soveltamisalaan, arvioidut kustannukset nousisivat 12%. Komission mukaan arvioidut lisäkustannukset kuitenkin johtaisivat sopusuhtaiseen kustannus-hyötysuhteeseen kyberturvallisuushäiriöiden samalla vähentyessä. Komissio arvioi häiriöiden kustannuksiksi yhteensä 118 miljardia euroa kymmenen vuoden ajalta. Lisäksi komissio katsoo, että ehdotus vähentäisi jäsenvaltioiden tasolla yksittäisistä kyberturvallisuushäiriöistä ja -kriiseistä aiheutuvaa kustannusten kasvua näiden hoitamiseksi.

Taloudellisten vaikutusten arviointiin vaikuttaa muun muassa toimijoiden yleinen kybermaturiteettitaso ja kyvykkyydet, jotka vaihtelevat tällä hetkellä niin sektoreiden kuin toimijoidenkin välillä. Taloudellisia vaikutuksia voi aiheutua myös tarpeesta huomioida samalla henkilötietojen suoja, mukaan lukien tietosuojaan liittyvä osaaminen. Siltä osin kuin direktiivin soveltamisalaan kuuluvissa järjestelmissä käsiteltäisiin henkilötietoja ja direktiivin täytäntöönpanolainsäädännön perusteella vaihdettaisiin henkilötietoja, sovellettavaksi tulisivat EU:n tietosuoja-asetuksen mukaiset vaatimukset.

Soveltamisalan laajentaminen aiheuttaisi alkuun lisäkustannuksia lisätyille sektoreille ja toimijoille, kuten julkishallinnon toimijoille valtionhallinnossa, maakunnissa ja kunnissa. Nämä lisäkustannukset voisivat siirtyä esimerkiksi asiakasmaksuihin.

Tarkempia vaikutuksia viranomaisten taloudellisiin tarpeisiin ja henkilöresurssitarpeisiin voidaan arvioida vasta ehdotetun sääntelyn täytäntöönpanon yhteydessä, mutta ne näyttäisivät kuitenkin kasvavan oleellisesti. Direktiiviehdotuksella voisi olla edellä mainittujen viranomaisvaikutusten ohella muita kustannusvaikutuksia valvontaviranomaisille ja muille viranomaisille.

5.3.4 Tietoyhteiskuntavaikutukset

Kuten ensimmäisen NIS-direktiivin kohdalla, ehdotettu sääntely lisäisi läpinäkyvyyttä kyberturvallisuushäiriöistä, niihin liittyvistä riskeistä ja riskeihin varautumisesta sekä näiden vaikutuksista yhteiskunnan eri toimijoille. Ehdotettu sääntely vahvistaisi viranomaisyhteistyötä ja tietojenvaihtoa sekä kansallisesti että jäsenvaltioiden välillä. Sääntelyn täytäntöönpano edistäisi luottamusta yhteiskunnan toiminnan jatkuvuuden kannalta keskeisiin toimijoihin. Ehdotettu sääntely parantaisi yhteiskunnan kykyä varautua ja vastata kyberturvallisuusuhkiin yhteiskunnalle merkittävien ja kriittisten toimijoiden osalta.

5.3.5 Ympäristövaikutukset

Komission arvion mukaan kyberturvallisuustason nostaminen johtaisi osaltaan ympäristöriskien ja –vahinkojen ennaltaehkäisyyn kyberhäiriön tai –kriisin edessä. Tämä olisi erityisen merkityksellistä energiasektorille, vesihuollolle ja liikennesektorille. Vahvistamalla kyberturvallisuusvalmiuksia ehdotus johtaisi viimeisimmän sukupolven ICT-infrastruktuurin ja -palvelujen parempaan hyödyntämiseen, jotka ovat ympäristön kannalta kestävämpiä. Tämä vaikuttaisi osaltaan kyberturvallisuushäiriöiden vähentämiseen ja niistä vapautuvat resurssit voisi kohdentaa kestäviin investointeihin.

6 Ehdotuksen suhde perustuslakiin sekä perus- ja ihmisoikeuksiin

Ehdotuksen mukaan EU on sitoutunut takaamaan korkean tason perusoikeuksien turvaamiselle. Kaikki vapaaehtoiset tietojenvaihtojärjestelyt toimijoiden välillä, jota tämä ehdotus tukee, tulisi

tapahtua luottamuksellisesti ja noudattaen EU:n yhteisiä tietojen käsittelyä koskevia säännöksiä, erityisesti yleistä tietosuoja-asetusta (EU) 2016/679. Tietosuoja-asetuksesta seuraa myös direktiiviehdotuksessa tarkoitetuille elinkeinonharjoittajille ja viranomaisille suoraan sovellettavia velvoitteita, jotka koskevat henkilötietojen käsittelyn tietoturvallisuutta. Osa direktiiviehdotuksen sisältämistä vaatimuksista voi samalla vahvistaa tietosuoja-asetuksen mukaista henkilötietojen suojaa.

Yksityiselämän suoja ja luottamuksellisen viestinnän suoja taataan Suomen perustuslain 10 §:ssä. Tämä perusoikeus edellyttää, että valtio pidättäytyy loukkaamasta kansalaisten yksityiselämää, mutta toisaalta sen tulee toteuttaa aktiivisia toimenpiteitä yksityiselämän suojaamiseksi toisten yksilöiden loukkauksia vastaan. Henkilötiedot kuuluvat olennaisena osana yksityisyyden suojan piiriin. Ehdotettu sääntely on merkityksellistä yksityisyyden ja viestinnän suojaamiseksi.

Ehdotettu sääntely on lisäksi merkityksellistä perustuslain 18 §:ssä turvatun elinkeinovapauden kannalta, sillä käsillä oleva ehdotus asettaisi elinkeinonharjoittajille erilaisia kyberturvallisuutta vahvistavia velvoitteita osaksi elinkeinotoiminnan harjoittamista. Ehdotus antaisi viranomaiselle toimivallan keskeyttää elinkeinonharjoittajan toiminta tapauksissa, joissa erilaisia kyberturvallisuutta koskevia velvoitteita ei ole noudatettu. Elinkeinovapauden rajoittaminen tulisi olla oikeasuhtaista tavoitteeseen nähden.

Direktiiviehdotuksen 18 artiklan säännökset, jotka velvoittaisivat elinkeinonharjoittajan tarpeen vaatiessa investoimaan sellaiseen tekniikkaan, jolla direktiivin kyberturvallisuusvaatimukset täyttyvät, puolestaan olisivat merkityksellisiä perustuslain 15 §:ssä säädetyn omaisuudensuojan kannalta. Direktiiviehdotuksen 29 artiklassa säädetään viranomaisten tarkastustoimivaltuuksista. Käsittelyn aikana tulee kiinnittää huomiota ehdotuksen 29 artiklan mahdollisiin vaikutuksiin perustuslain 10 §:n suojaamaan kotirauhaan. Lisäksi ehdotettujen hallinnollisia seuraamuksia ja muita seuraamuksia koskevien 31-33 artiklan mahdollisia vaikutuksia perustuslain 21 §:n mukaiseen oikeusturvaan olisi arvioitava.

7 Direktiiviehdotuksen suhde muuhun lainsäädäntöön ja aloitteisiin

7.1 Sektorikohtainen sääntely ja yhdenmukaisuuden varmistaminen

Ehdotuksen mukaan sektorikohtainen sääntely auttaa osaltaan varmistamaan korkean kyberturvallisuuden tason ottaen huomioon kunkin sektorin ominaispiirteet. Mikäli EU:n sektorikohtainen sääntelykehys edellyttää keskeistä tai tärkeää toimijaa asettamaan kyberturvallisuuteen liittyviä riskienhallintatoimia tai raportoimaan häiriöistä tai merkittävistä kyberturvallisuusuhkista ja nämä edellytykset vastaavat vaikutuksiltaan niitä velvollisuuksia, joista tässä ehdotuksessa säädettäisiin, tulisivat sektorikohtaiset säännökset (*lex specialis*) sovellettaviksi. Ehdotuksen mukaan komissio voisi antaa ohjeita erityissääntelyn implementointiin.

Komission mukaan ehdotus ei rajoittaisi mahdollisen lisäsääntelyn antamista sektorikohtaisesti. Lisäsääntelyllä voidaan kehittää kyberturvallisuuden riskienhallintatoimia ja häiriöilmoituksia.

Komissio katsoo, että ehdotettu sääntely on yhdenmukainen muiden annettujen säädösehdotusten kanssa, kuten finanssialan digitaalisesta häiriönsietokyvystä annetun asetusehdotuksen sekä fyysisen kriittisen infrastruktuurin suojaamiseksi annetun direktiiviehdotuksen kanssa. Lisäksi komissio katsoo, että ehdotus on yhdenmukainen yleisen tietosuoja-asetuksen, eurooppalaisen sähköisen viestinnän säännöstön sekä sähköisestä tunnistamisesta ja luottamuspalveluista annetun asetuksen kanssa.

Ehdotus on myös oleellinen osa EU:n uutta kyberturvallisuusstrategiaa ja sen tavoitteita.

8 Ahvenanmaan toimivalta

Ahvenanmaan itsehallintolain (1144/1991) 18 §:n mukaan maakunnalla on lainsäädäntövaltaa asioissa, jotka koskevat maakunnan hallitusta sekä sen alaisia viranomaisia ja laitoksia sekä eräin rajoituksin lainsäädäntövaltaa asioissa, jotka koskevat elinkeinotoimintaa. Lain 27 §:n mukaan puolestaan valtakunnalla on lainsäädäntövaltaa asioissa, jotka koskevat kauppamerenkulkua, ilmailua, standardisointia sekä valtion viranomaisten järjestysmuotoa ja toimintaa sekä teletoimintaa.

9 Ehdotuksen käsittely Euroopan unionin toimielimissä ja muiden jäsenvaltioiden kannat

Ehdotuksen käsittelystä neuvostossa vastaa horisontaalinen kybertyöryhmä. Ehdotusta käsitellään työryhmässä ensimmäisen kerran 12.1.2021. Tätä ennen ehdotusta on käsitelty osana kyberstrategian käsittelyä 17.12.2020. Ehdotusta käsitellään lisäksi horisontaalisuuden vuoksi todennäköisesti myös muissa relevanteissa työryhmissä.

Muiden jäsenvaltioiden virallisia kantoja ei ole vielä tiedossa.

10 Ehdotuksen kansallinen käsittely

Valtioneuvoston kirjelmä on valmisteltu liikenne- ja viestintäministeriössä.

Komission ehdotusta on käsitelty EU19-viestintäjaoston kokouksessa 12.1.2021.

Ehdotusta ja sitä koskevaa kirjelmäluonnosta on käsitelty kirjallisessa menettelyssä viestintäjaostossa (EU19), liikennejaostossa (EU22), oikeus- ja sisäasioiden jaostossa (EU7), kilpailukykyjaostossa (EU8), rahoituspalvelut ja pääomaliikkeet –jaostossa (EU10), energia- ja Euratom –jaostossa (EU21), terveysjaostossa (EU33), maatalous- ja elintarvikejaostossa (EU18) 15.1.2021-21.1.2021 ja ympäristöjaostossa (EU23) 20.1.-22.1.2021.

Ehdotusta on käsitelty EU-ministerivaliokunnassa 5.2.2021.

11 Valtioneuvoston kanta

Valtioneuvosto kannattaa komission ehdotuksen tavoitetta vastata paremmin muuttuneeseen kybertoimintaympäristöön ja kehittää entisestään EU:n yhteistä kyberturvallisuuden tasoa. Valtioneuvosto pitää myös tärkeinä ehdotuksen kyberturvallisuutta ja tietosuojaa vahvistavia myönteisiä vaikutuksia.

On tärkeää, että EU:lla on selkeä sääntelykehys kyberturvallisuudelle, sillä useat häiriöt ja niiden vaikutukset voivat olla jäsenvaltioiden rajat ylittäviä. Tämän seurauksena on luontevaa, että yhteiskunnan keskeisiä ja tärkeitä toimijoita koskevat kyberturvallisuusvaatimukset perustuvat yhteiseen sääntelyinstrumenttiin. Valtioneuvosto katsoo, että kyberturvallisuutta koskevan sääntelykehyksen on oltava yhdenmukainen muun sektorikohtaisen sääntelyn ja muun relevantin sääntelyn kanssa.

Valtioneuvosto pitää erityisen tärkeänä, että verkko- ja tietoturvaa koskevien uusien velvoitteiden ja vaatimusten tulee olla oikeasuhtaisia ja riskiperusteisia soveltamisalaan kuuluvien toimijoiden kokoon ja toimintaan nähden, ottaen huomioon sektorikohtaiset erityispiirteet.

Toimijoiden kategorisointia voidaan pitää kannatettavana, jos sen avulla kyetään kohdistamaan tehokkaat ja oikeasuhtaiset vaatimukset direktiivin soveltamisalaan kuuluville toimijoille. Kategorisoinnilla tulee myös välttää kohtuuttoman hallinnollisen taakan lisäämistä erityisesti pienten ja mikrotoimijoiden kohdalla.

Valtioneuvosto pitää soveltamisalan ja toimijatyyppilistauksen laajentamista lähtökohtaisesti tervetulleena, koska kyseiset toimijat ovat kriittisiä yhteiskunnan toiminnan jatkuvuuden kannalta, kuten esimerkiksi kunnat julkishallinnon sektorin osalta. Valtioneuvosto pitää hyvänä, että direktiivi ei vaikuta jäsenvaltioiden toimivaltaan, joka koskee yleisen turvallisuuden, puolustuksen ja kansallisen turvallisuuden ylläpitämistä. Valtioneuvosto pitää lisäksi hyvänä, että ehdotuksen mukaan ne julkishallinnon toimijat, jotka toimivat yleisen turvallisuuden, lainvalvonnan, puolustuksen ja kansallisen turvallisuuden aloilla eivät lukeudu soveltamisalaan.

Valtioneuvosto pitää hyvänä, että ehdotuksessa tunnistetaan kansallisten kyberturvallisuusstrategioiden tärkeys. Valtioneuvosto pitää tervetulleena toimintatapojen laatimista haavoittuvuuksien tunnistamiseksi ja laajamittaisiin kyberturvallisuushäiriöihin varautumiseksi. Valtioneuvosto pitää hyvänä turvallisuusvelvoitteiden asettamista osana riskienhallintatoimia ehdotuksessa esitetyn mukaisesti. Lisäksi valtioneuvosto tukee raportoinnin tehostamista esitetyillä raportointivelvoitteilla. Valtioneuvosto pitää kannatettavana, että direktiiviehdotuksessa tarkastellaan myös tuotantoketjujen merkitystä ja turvallisuutta.

Valtioneuvosto pitää valvontaviranomaisille esitettyjä tarkennettuja tehtäviä ja niiden lisäämistä lähtökohtaisesti perusteltuna. Neuvottelujen edetessä tulisi tarkastella näiden yhteensopivuutta perustuslain vaatimusten kanssa. Kansallisesta resursoinnista linjataan normaaliin tapaan talousarviota ja julkisen talouden suunnitelmaa koskevissa menettelyissä.

Valtioneuvosto pitää kannatettavana, että jäsenvaltiot toimivat tiiviissä yhteistyössä ja vaihtavat kyberturvallisuuteen liittyviä tietoja myös tulevaisuudessa. Yhteistyötä on hyvä tiivistää jatkossakin kansallisella tasolla sekä vapaaehtoisuuteen perustuen että ehdotuksen velvoitteiden kautta. Erityisesti nykyistä tehokkaampi vapaaehtoinen tietojen vaihto on kannatettavaa. Valtioneuvosto pitää perusteltuna, että direktiivissä esitetään lainvalvontaviranomaisten mahdollisuus saada tieto sellaisista kyberturvallisuushäiriöistä, joilla on liityntä rikolliseen toimintaan.

Valtioneuvosto pitää tärkeänä, että ehdotus säilyttää jäsenvaltioille riittävästi kansallista liikkumavaraa, jotta nämä voivat lisäksi ottaa käyttöön sellaisia kansallisia toimenpiteitä, joilla varmistetaan korkea kyberturvallisuuden taso. Viranomaisten toimivaltuuksien ja seuraamuksia koskevien säännösten osalta on tavoiteltava valmistelussa sellaista ratkaisua, jossa seuraamusjärjestelmä on kokonaisuudessaan toimiva ja yhteen sovitettavissa sekä kaikkiaan huomioi tarvittavan kansallisen liikkumavaran.

Valtioneuvosto katsoo myös, että komissiolle delegoitavien toimivaltuuksien tulisi olla tarkkarajaisia, oikeasuhtaisia, tarkoituksenmukaisia ja hyvin perusteltuja.

Valtioneuvosto katsoo, että direktiiviehdotus vastaa pääosin kansallisen ennakkovaikuttamisen sekä tietoturvan ja tietosuojan parantamista koskevan työryhmän väliraportin johtopäätöksiä.