TTU Korhonen Marieme(LVM) 20.12.2021

Asia

U-jatkokirje; Komission 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, NIS2-direktiiviehdotus)

Kokous

U/E/UTP-tunnus

U 9/2021 vp

Käsittelyvaihe ja jatkokäsittelyn aikataulu

Euroopan komissio antoi 16.12.2020 ehdotuksen (COM(2020) 823 final) Euroopan parlamentin ja neuvoston direktiiviksi kyberturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella ja direktiivin 2016/1148 (verkko- ja tietoturvadirektiivi, NIS-direktiivi) kumoamisesta.

Direktiiviehdotusta on käsitelty vuoden 2021 tammikuusta alkaen ensin EU:n neuvoston puheenjohtajamaan Portugalin johdolla EU:n neuvoston horisontaalisessa kybertyöryhmässä. Televiestintäneuvosto otti 4.6.2021 tiedoksi edistymisraportin direktiiviehdotuksen käsittelytilanteesta.

Direktiiviehdotuksen käsittely jatkui intensiivisesti seuraavan EU:n neuvoston puheenjohtajamaan Slovenian johdolla, joka pyrki yleisnäkemyksen saavuttamiseen neuvostossa vuoden 2021 loppuun mennessä. Direktiiviehdotusta käsiteltiin EU:n neuvoston horisontaalisessa kybertyöryhmässä viikoittain. Puheenjohtajamaana toimiva Slovenia antoi komission alkuperäisen direktiiviehdotuksen pohjalta ensimmäisen puheenjohtajan kompromissitekstiehdotuksen käsiteltäväksi syyskuussa 2021. Tämän jälkeen puheenjohtajamaa päivitti aktiivisesti kompromissitekstiehdotustaan jäsenvaltioiden kommenttien pohjalta. Slovenia järjesti viimeisen ad hoc –työryhmäkokouksen 22.11.2021, jolloin viimeisteltiin viimeisintä kompromissitekstiehdotusta. Yleisnäkemys hyväksyttiin kompromissitekstiehdotuksen pohjalta pienin muutoksin Coreper I –kokouksessa 24.11.2021. Yleisnäkemys vahvistettiin televiestintäneuvostossa 3.12.2021.

Yleisnäkemyksen hyväksymisen jälkeen neuvottelut jatkuvat trilogineuvotteluilla Euroopan parlamentin kanssa ensi vuoden aikana.

Suomen kanta

Suomi on vaikuttanut aktiivisesti ehdotuksen neuvotteluihin EU:n neuvoston horisontaalisessa kybertyöryhmässä U-kirjelmän U 9/2021 vp kannan mukaisesti. Tässä perusmuistiossa ei esitetä muutoksia U 9/2021 vp kantaan.

Ehdotus on edennyt kokonaisuudessaan pitkälti Suomen kannan mukaiseen suuntaan seuraavasti:

Suomi on pyrkinyt vaikuttamaan siihen, että ehdotuksen velvoitteet ovat oikeasuhtaisia ja riskiperustaisia soveltamisalaan kuuluvien toimijoiden kokoon ja toimintaan nähden, ottaen huomioon sektorikohtaiset erityispiirteet. Suomi on pyrkinyt vaikuttamaan direktiiviehdotuksen soveltamisalan selkeyteen. Suomi pitää myönteisenä, että ehdotukseen sisällytettiin muutoksia, joilla vahvistetaan velvoitteiden oikeasuhtaisuutta, riskiperustaisuutta ja kriittisyyden arviointia. Näihin muutoksiin sisältyy esimerkiksi se, että lähtökohtaisesti suuret toimijat kuuluisivat keskeisten toimijoiden kategoriaan ja keskisuuret tärkeiden toimijoiden kategoriaan, tietyt poikkeukset huomioiden. Jäsenvaltioilla on mahdollisuus kansallisesti siirtää toimijoita tärkeistä keskeisiin, mikäli katsotaan tarpeelliseksi riskiperustaisesti arvioituna. Lisäksi valvovilla viranomaisilla olisi mahdollisuus priorisoida valvontatehtäviään riskiperustaisesti.

Suomelle on ollut tärkeää, että ehdotus sisältää riittävästi liikkumavaraa direktiiviehdotuksen soveltamisalan ja seuraamusjärjestelmän osalta. Suomi pitää hyvänä, että kompromissitekstissä kansallista liikkumavaraa ei ole heikennetty alkuperäisestä ehdotuksesta. Lisäksi jäsenvaltioilla on ehdotuksen mukaan mahdollisuus ottaa käyttöön muita toimenpiteitä ja lainsäädännöllisiä muutoksia, joilla taataan direktiiviehdotuksen minimitasoa korkeampi kyberturvallisuuden taso.

Suomi on pitänyt hyvänä sitä, että direktiivi ei vaikuta jäsenvaltioiden toimivaltaan, joka koskee yleisen turvallisuuden, puolustuksen ja kansallisen turvallisuuden ylläpitämistä. Suomi on pitänyt tärkeänä, että toimijat, joilla on toimintaa yleisen turvallisuuden, kansallisen turvallisuuden, lainvalvonnan ja puolustuksen aloilla jäävät soveltamisalan ulkopuolelle. Ehdotus on tältä osin Suomen kannan mukainen, minkä lisäksi soveltamisalan ulkopuolelle jäisivät lähtökohtaisesti myös oikeuslaitokset, kansalliset parlamentit ja keskuspankit.

Soveltamisalaan tehtiin muutamia kompromissimuutoksia, joihin Suomi on voinut suhtautua joustavasti. Keskeisimpinä kompromissimuutoksina juurinimipalvelimet jäivät soveltamisalan ulkopuolelle, mutta muut digitaalisen infrastruktuurin toimijat (ml. DNS-toimijat) pysyivät soveltamisalassa. Lisäksi soveltamisalaan lisättiin Suomellekin tärkeää kansallista liikkumavaraa julkishallinnon sektorin osalta niin, että alueellisten ja paikallisten hallintotasojen osalta ei nojata aiemmin esitettyyn NUTS-luokitteluun, vaan art. 2(2a) mukaan kansalliseen arviointiin. Vaikka Suomi on pitänyt soveltamisalan laajentamista lähtökohtaisesti tervetulleena, Suomi on sääntelyn oikeasuhtaisuuden ja tarkkarajaisuuden näkökulmasta suhtautunut lähtökohtaisesti varauksella ICT-palveluntarjoajien sektorin lisäämiseen, koska kyseisen sektorin piiriin kuuluvat toimijat ja lisäyksen vaikutukset ovat olleet jossain määrin epäselviä. Neuvottelujen edetessä kyseisen sektorin toimijat rajattiin managed service providers – ja managed security service providers –toimijoihin, jotka voidaan nähdä kriittisinä toimijoina etenkin siltä osin kuin muut keskeiset toimijat ovat riippuvaisia ICT-palveluntarjoajista osana omien palveluidensa tarjontaa.

Suomi pitää muutoksia raportointivelvoitteisiin hyvinä. Raportointivelvoitteiden oikeasuhtaisuutta on pyritty vahvistamaan niin, että kyberuhkista raportointi olisi lähtökohtaisesti vapaaehtoista. Ehdotuksessa myös kannustetaan jäsenvaltioita sellaisiin kansallisiin ratkaisuihin, jotka virtaviivaistavat raportointia ja joilla vältetään päällekkäinen raportointi. On hyvä, että toimijoilla on raportointivelvoitteiden ohella mahdollisuus ilmoittaa vapaaehtoisuuteen perustuen havainnoistaan, uhkista ja häiriöistä.

Suomi on pitänyt erittäin tärkeänä, että ehdotuksen suhde muuhun EU-lainsäädäntöön on selkeä. Suomi on pyrkinyt aktiivisesti vaikuttamaan siihen, että säädösviittauksissa sekä direktiiviehdotuksen sisäisissä viittauksissa varmistetaan, että sääntelykehys on kokonaisuudessaan toimiva. Kompromissitekstissä onkin selkeytetty velvoitteiden suhdetta sektorikohtaiseen sääntelyyn. Esimerkiksi ilmailualan sääntelyä ja NIS2-direktiiviehdotuksen suhdetta koskevat selkeytykset ovat pitkälti Suomen vaikuttamistulosta. Lisäksi ehdotuksessa on selkeytetty sääntelyn suhdetta muuhun direktiiviehdotuksen soveltamisalaan kuuluvia toimijoita koskevaan lainsäädäntöön, erityisesti tietosuojalainsäädäntöön sekä muihin keskeneräisiin säädösehdotuksiin, jotka liittyvät läheisesti direktiiviehdotukseen. Kompromissitekstissä muun muassa tarkennetaan, että NIS2-direktiivi sääntelee verkkojen ja tietojärjestelmien kokonaisturvallisuutta. Suomi pitää näitä muutoksia erittäin tervetulleina.

Suomi on pitänyt tärkeänä, että komissiolle delegoitavat toimivaltuudet ovat oikeasuhtaisia, tarkkarajaisia, tarkoituksenmukaisia ja hyvin perusteltuja. Ehdotuksessa onkin esitetty, että komissio voisi antaa täytäntöönpanosäädöksiä ainoastaan liittyen teknisiin ja metodologisiin tarkennuksiin riskienhallintatoimenpiteiden ja raportoinnin osalta. Lisäksi kompromissitekstin mukaan NIS2-direktiivi tulee saattaa osaksi kansallista lainsäädäntöä 24 kuukauden kuluessa direktiivin voimaantulopäivästä. Suomi on pitänyt annettua lisäaikaa tervetulleena direktiivin laajuuden vuoksi.

Pääasiallinen sisältö

Direktiiviehdotus kumoaisi ensimmäisen verkko- ja tietoturvadirektiivin (NIS-direktiivi, 2016/1148). Ehdotuksen tavoitteena on vahvistaa sekä EU:n yhteistä että jäsenvaltioiden kansallista kyberturvallisuuden tasoa kriittisiksi katsottujen sektoreiden ja toimijoiden osalta. Ehdotus yhdenmukaistaisi kyberturvallisuus– ja raportointivelvoitteita ja laajentaisi soveltamisalaa koskettamaan uusia sektoreita ja toimijoita (liitteet I-II). Ehdotus jatkaisi olemassa olevia yhteistyömekanismeja ja tiivistäisi yhteistyötä.

Ehdotuksen mukaan kaikki suuret ja keskisuuret toimijat olisivat suoraan sääntelyn piirissä, tietyt poikkeukset huomioiden (art. 2). Pienet ja mikrotoimijat jäisivät lähtökohtaisesti ehdotetun sääntelyn ulkopuolelle. Kategorisointi keskeisiin ja tärkeisiin tehdään kompromissitekstissä 2bis artiklan mukaisesti aiemman pelkän liitteen jaottelun sijaan. Kompromissitekstissä tarkennetaan, että jäsenvaltiot voivat halutessaan hyödyntää itserekisteröintimekanismia tai muuta kansallisesti jo olemassa olevaa mekanismia, jolla soveltamisalaan kuuluvat toimijat voivat ilmoittautua toimivaltaisille viranomaisille (art. 2a).

Ehdotus sisältää haavoittuvuuksien tunnistamisen sekä varautumisen laajamittaisten kyberturvallisuushäiriöiden ja –kriisien varalle. Sekä keskeisiin että tärkeisiin toimijoihin sovellettaisiin samoja riskienhallinta– (art. 18) ja raportointivelvoitteita (art. 20). Ehdotus esittäisi keskeisille toimijoille ennakko– ja jälkivalvontaa (art. 29). Tärkeille toimijoille ehdotus esittää vain jälkivalvontaa (art. 30).

Valvoville viranomaisille muodostuisi olemassa olevien tehtävien jatkumisen lisäksi uusia valvontatehtäviä, kuten soveltamisalaan lisättyjen toimijoiden valvonta. Kompromissitekstissä esitetään tarkennuksena valvoville viranomaisille valvontatehtävien priorisointimahdollisuuksia riskiperustaisesti (art. 29-30).

Toimijoille voisi määrätä hallinnollisia seuraamuksia ja sanktioita velvoitteiden laiminlyönnin johdosta (art. 31). Hallinnollisia sanktioita on madallettu alkuperäisestä ehdotuksesta niin, että keskeisille toimijoille voisi määrätä enimmillään vähintään 4

miljoonaa euroa tai 2% maailmanlaajuisesta vuosittaisesta liikevaihdosta ja tärkeille toimijoille enimmillään vähintään 2 miljoonaa euroa tai 1 % maailmanlaajuisesta vuosittaisesta liikevaihdosta. Hallinnollisten sanktioiden määrääminen julkishallinnon sektorin toimijoille jäisi jäsenvaltioiden harkintaan.

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely

Euroopan unionin toiminnasta tehdyn sopimuksen 114 artikla; tavallinen lainsäätämisjärjestys Euroopan unionin toiminnasta tehdyn sopimuksen 294 mukaisesti.

Komissio voisi antaa täytäntöönpanosäädöksiä liittyen teknisiin ja metodologisiin tarkennuksiin riskienhallintatoimenpiteiden ja raportoinnin osalta.

Käsittely Euroopan parlamentissa

Vastuuvaliokuntana on teollisuus-, tutkimus- ja energiavaliokunta. Raportöörinä toimii Bart Groothuis (Renew, NL). Muut asiasta lausuneet valiokunnat ovat ulkoasiainvaliokunta, sisämarkkina- ja kuluttajansuojavaliokunta, liikenne- ja matkailuvaliokunta, kansalaisvapauksien ja oikeus- ja sisäasioiden valiokunta.

Vastuuvaliokunta äänesti raportistaan (A9-0313/2021) 28.10.2021.

Euroopan parlamentti (EP) kannattaa NIS-direktiivin päivittämistä NIS2-direktiiviehdotuksella. EP katsoo muun muassa, että ehdotuksessa tulisi muokata vielä soveltamisalaa digitaalisen infrastruktuurin toimijoiden osalta (DNS palveluntarjoajat tulisi jättää soveltamisalan ulkopuolelle). Lisäksi EP esittää ehdotukseen muutoksia raportointivelvoitteiden aikarajoihin ja kannattaa velvoitteiden oikeasuhtaisuuden ja riskiperustaisuuden vahvistamista.

Kansallinen valmistelu

Tämä U-jatkokirjelmä 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), ympäristöjaostossa (EU23) ja hybridiuhat –jaostossa (EU13) 3.12.-8.12.2021.

Eduskuntakäsittely

U 9/2021 vp; Eduskunta on lausunut U-kirjelmästä ja komission ehdotuksesta valiokuntalausunnossaan LiVL 8/2021 vp ja on hyväksynyt eduskunnan kannan SuVEK 15/2021 vp.

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema

Ehdotus on säädöstyypiltään direktiivi, joka tulisi implementoida kansalliseen lainsäädäntöön. Vaikutuksia kansalliseen lainsäädäntöön on kuvattu tarkemmin U-kirjelmässä U 9 / 2021 vp.

Kuten valtioneuvoston kirjelmässä U 9/2021 vp todetaan, direktiiviehdotuksella olisi vaikutusta seuraamuksia koskevaan sääntelyyn. Direktiiviehdotuksen 31 artiklan mukaan toimijoille voisi määrätä hallinnollisia sanktioita direktiivin velvoitteiden laiminlyönnistä. Artiklan 33 mukaan jäsenvaltiot voivat ottaa kansallisesti käyttöön

sellaisia seuraamusjärjestelyjä, jotka eivät ole artiklassa 31 tarkoitettuja hallinnollisia sanktioita.

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.

Vaikutukset viranomaisten toimintaan

Kuten valtioneuvoston kirjelmässä U9/2021 vp todetaan, direktiiviehdotuksella olisi vaikutuksia viranomaisten toimintaan.

Direktiiviehdotuksen vaikutuksia erityisesti valvovien viranomaisten toimintaan ja resursseihin on pyritty tarkentamaan neuvotteluiden edetessä. Direktiiviehdotuksen voidaan katsoa aiheuttavan merkittäviä muutoksia ja lisäresurssitarpeita valvovien viranomaisten toimintaan. Ehdotuksen myötä valvovien viranomaisten valvontatoimet viedään aikaisempaa laajemmalle ja yksityiskohtaisemmalle tasolle. Lisäksi uudet tehtävät edellyttävät syvällisempää ja teknisempää kyberturvallisuusosaamista. Tarvittavien lisäresurssien ja osaamistarpeen osalta tulee huomioida, että tällä hetkellä on valvovia viranomaisia, joiden toiminnassa ei ole yksinomaan tietoturvan valvontaan nimettyjä resursseja.

Myös valvottavien toimijoiden määrä tulee kasvamaan merkittävästi nykyisestä, kun soveltamisalaan tuodaan uusia sektoreita ja toimijoita. Tämän hetkisen arvion mukaan soveltamisalaan kuuluvien sektoreiden määrä on kaksinkertaistumassa verrattuna voimassaolevaan sääntelyyn.

NIS2 –direktiivin 32(1) artiklasta seuraisi lisätyötä tietosuojavaltuutetulle. Lisäksi johdanto-osan 56 kappaleessa mainittu mahdollinen keskitetty asiointikanava (*single entry point*) (NIS, GDPR ja ePrivacy) voisi lisätä tietosuojavaltuutetulle tulevien ilmoitusten määrää. Ehdotettu sääntely voisi kohentaa nykytilaa siten, että GDPR mukaisia henkilötietojen tietoturvaloukkauksia koskevat ilmoitukset voisivat ohjautua nykyistä paremmin GDPR:n mukaisesti tietosuojavaltuutetulle.

Säädösehdotuksella olisi vaikutuksia myös ainakin tuomioistuinten ja Oikeusrekisterikeskuksen toimintaan ja tietojärjestelmiin. Vaikutuksia ja niistä mahdollisesti aiheutuvia kustannuksia on mahdollista arvioida tarkemmin direktiiviehdotuksen täytäntöönpanon yhteydessä sen valossa, millä tavalla seuraamusjärjestelmää koskevat artiklat pantaisiin täytäntöön.

Alustavan arvion mukaan direktiiviehdotuksen velvoitteilla olisi merkittäviä htv-vaikutuksia jo olemassa oleviin NIS-direktiivin mukaisiin valvoviin viranomaisiin ja htv-vaikutuksia tietosuojavaltuutetulle. Nykyiset kyberturvallisuuteen ja tietoturvan valvontaan osoitetut resurssit eivät vastaa NIS2-direktiiviehdotuksessa asetettavia tehtäviä. Lisäresurssitarpeita arvioitaessa on muistettava, että valvonnan tehostamisella pyritään estämään merkittäviä taloudellisia tai muita vahinkoja, joita kyberturvallisuutta koskevat häiriöt voivat aiheuttaa NIS2-direktiiviehdotuksen soveltamisalaan kuuluville kriittisille sektoreille ja koko yhteiskunnalle.

Tarkempi lisäresurssien tarve ja määrää koskeva arvio tarkentuvat ja vahvistuvat direktiivin soveltamisalan varmistuttua ja täytäntöönpanon valmistelujen edetessä. Kansallisesta resursoinnista linjataan normaaliin tapaan talousarviota ja julkisen talouden suunnitelmaa koskevissa menettelyissä.

Taloudelliset vaikutukset

Taloudellisia vaikutuksia on kuvattu U-kirjelmässä U 9/2021 vp. Tarkempia taloudellisia vaikutuksia on mahdollista arvioida soveltamisalan varmistuttua ja täytäntöönpanon valmistelujen edetessä.

Muut asian käsittelyyn vaikuttavat tekijät

Direktiiviehdotus on tärkeä osa EU:n kyberturvallisuusstrategian tavoitteita (E 3/2021 vp).

Direktiiviehdotuksen neuvotteluissa ja kansallisessa täytäntöönpanossa huomioidaan käynnissä olevat EU-aloitteet, kuten direktiiviehdotus kriittisten toimijoiden häiriönsietokyvystä (CER-direktiiviehdotus), asetusehdotus digitaalisesta häiriönsietokyvystä rahoitusmarkkinoilla (DORA-asetusehdotus) ja asetusehdotus eurooppalaisen digitaalisen identiteetin kehyksen vahvistamisesta (eIDAS-asetusehdotus) sekä muut relevantit aloitteet selkeän sääntelykehyksen varmistamiseksi.

Asiakirjat

-

Laatijan ja muiden käsittelijöiden yhteystiedot

erityisasiantuntija Marième Korhonen, liikenne- ja viestintäministeriö, p. 0295 342 134

EUTORI-tunnus

EU/2020/0359

Liitteet LVM2021-00550

Viite

Asiasanat	tietoturva, kyber
Hoitaa	**LVM, SM, UM, VNK**
Tiedoksi	EUE, MMM, OKM, OM, PLM, RUOKA, STM, TEM, VM, VTV