U 58/2017 vp

Valtioneuvoston kirjelmä eduskunnalle ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi (”kyberturvallisuusasetus”)

Perustuslain 96 §:n 2 momentin perusteella lähetetään eduskunnalle Euroopan komission 13 päivänä syyskuuta 2017 tekemä ehdotus Euroopan parlamentin ja neuvoston asetukseksi Euroopan kyberturvallisuusvirasto ENISA:sta ja asetuksen EU 526/2013 kumoamisesta sekä tieto- ja viestintäteknologian kyberturvallisuussertifioinneista.

Helsingissä 19 päivänä lokakuuta 2017

Liikenne- ja viestintäministeri Anne Berner

Neuvotteleva virkamies Piia Nyström

LIIKENNE- JA VIESTINTÄMINISTERIÖ | MUISTIO | EU/2017/1435

2.10.2017

KOMISSION EHDOTUS EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUKSEKSI EUROOPAN KYBERTURVALLISUUSVIRASTO ENISA:STA JA ASETUKSEN EU 526/2013 KUMOAMISESTA SEKÄ TIETO- JA VIESTINTÄTEKNOLOGIAN KYBERTURVALLISUUSSERTIFIOINNEISTA (”KYBERTURVALLISUUSASETUS”)

1 Tausta ja tavoitteet

Euroopan verkko- ja tietoturvavirasto ENISA perustettiin vuonna 2004 Euroopan parlamentin ja neuvoston asetuksella viideksi vuodeksi parantamaan unionin, jäsenvaltioiden ja yritysmaailman valmiuksia ehkäistä, käsitellä ja ratkaista verkko- ja tietoturvaongelmia. Tämän jälkeen Viraston toimikautta on jatkettu kaksi kertaa. Nykyinen toimikausi päättyy vuoden 2020 kesäkuussa.

Komissio antoi 13.9.2017 ehdotuksen Euroopan parlamentin ja neuvoston asetukseksi Euroopan kyberturvallisuusvirasto ENISA:sta ja asetuksen EU 526/2013 kumoamisesta sekä tieto- ja viestintäteknologian kyberturvallisuussertifioinneista (”Kyberturvallisuusasetus”) (COM/2017/477). Ehdotuksella säädettäisiin ENISA:lle pysyvä mandaatti ja luotaisiin puitteet tieto- ja viestintäteknologiatuotteiden ja -palveluiden tietoturvasertifioinnille EU:ssa. Ehdotuksen tavoitteena on turvata sisämarkkinoiden toiminta vahvistamalla kyberturvallisuutta, sietokykyä ja luottamusta EU:ssa.

ENISA muuttuisi Euroopan verkko- ja tietoturvavirastosta Euroopan kyberturvallisuusvirastoksi ja siitä tulisi pysyvä EU-virasto.

2 Pääasiallinen sisältö

Komissio on valinnut säädösinstrumentiksi asetuksen. Asetuksella kumottaisiin ENISA:n toimintaa nykyisin sääntelevä asetus (EU 526/2013). Asetus olisi jäsenvaltioissa suoraan sellaisenaan sovellettava.

Asetusehdotus koostuu neljästä osasta. Ensimmäinen osa sisältää säädösehdotuksen tavoitteet, soveltamisalan ja määritelmät. Asetuksella säädettäisiin viraston tavoitteista, tehtävistä ja organisaatiosta. Lisäksi asetuksella luotaisiin puitteet EU:n laajuiselle tietoturvatuotteiden sertifiointijärjestelmälle.

Asetusehdotuksen toinen osa sisältä ENISA:n toimintaa ohjaavat säännökset. ENISA:n toiminnan tavoitteena olisi korkeantason tietoturvan edistäminen EU:ssa. Viraston olisi tarkoitus olla kyberturvallisuuden asiantuntijakeskus, joka avustaisi sekä jäsenvaltioita, unionin instituutioita että julkisia ja yksityisiä sidosryhmiään kyberturvallisuuden kehitystyössä ja sietokyvyn vahvistamisessa ja loisi samalla edellytyksiä jäsenvaltioiden ja muiden toimijoiden väliselle yhteistyölle. Osa viraston tehtävistä olisi sidoksissa elokuussa 2016 voimaan tulleeseen verkko- ja tietoturvadirektiiviin (EU 1148/2016) ja sen nojalla perustettuihin yhteistyömuotoihin.

Ehdotuksessa ENISA:n tehtävät on jaettu seitsemän teeman alle, joista jokaisesta on oma artiklansa. Artiklat koskevat unionin politiikan ja oikeuden kehittämistä ja täytäntöönpanoa,

valmiuksien kehittämistä, operatiivista yhteistyötä unionissa, kyberturvallisuusmarkkinoiden edistämistä, tiedon ja tietoisuuden lisäämistä, tutkimus- ja innovaatiotoimintaa sekä kansainvälistä yhteistyötä. ENISA:lla olisi lisäksi keskeinen rooli ehdotetun EU:n laajuisen tieto- ja viestintäteknologiahyödykkeiden sertifioinnin puitekehyksen mukaisten sertifiointiohjelmien valmistelussa. Virasto toimisi lisäksi kansallisista sertifiointiviranomaisista koostuvan yhteistyöryhmän sihteeristönä.

Tavoitteiden ja tehtävien lisäksi asetusehdotuksessa määritellään ENISA:n hallinnollinen rakenne. Virastoon kuuluisi johtokunta, pääjohtaja, hallitus ja pysyvä sidosryhmä. Johtokunta määrittelisi viraston toiminnan yleiset suuntaviivat ja nimittäisi pääjohtajan. Pääjohtaja vastaisi viraston päivittäisestä johtamisesta ja raportoisi johtokunnalle. Hallitus valmistelisi johtokunnan päätökset. Pysyvä sidosryhmä olisi neuvoa-antava elin, jossa olisi edustettuna yksityinen sektori, kuluttajajärjestöt ja muut keskeiset sidosryhmät. Ehdotus vastaa tältä osin pääpiirteissään viraston nykyistä toimintaa.

Asetusehdotuksen kolmas osa sisältää säännökset, joilla luotaisiin EU:n laajuinen tieto- ja viestintäteknologiahyödykkeiden sertifioinnin puitekehys. Pyrkimyksenä on säätää menettelyistä, joiden puitteissa tieto- ja viestinteknologiahyödykkeille voitaisiin myöntää EU:n laajuinen sertifikaatti osoitukseksi tuotteen tietoturvallisuudesta. Sertifikaatilla voitaisiin osoittaa, että hyödyke täyttäisi sertifioinnille asetetut vaatimukset liittyen tiedon, toiminnon tai palvelun saatavuuteen, aitouteen, eheyteen ja luottamuksellisuuteen. Keskeisenä tavoitteena on luoda vastavuoroiseen tunnustamiseen perustuva järjestelmä siten, että ehdotetun yleisen puitekehyksen nojalla laadittu sertifikaatti tunnustettaisiin kaikissa jäsenvaltioissa, eikä laitevalmistajan tai palveluntarjoajan tarvitsisi enää hankkia tuotteelleen useita erilaisia kansallisia sertifikaatteja.

Ehdotuksen mukaan ENISA valmistelisi yhteistyössä kansallisten sertifiointivalvontaviranomaisten yhteistyöryhmän ja sidosryhmien (kuten teollisuus ja standardisointielimet) kanssa ehdotuksen vaatimuksista sertifikaatin saamisen edellytykseksi (sertifiointiohjelma). Asetuksessa säädettäisiin näissä sertifiointiohjelmissa huomioitavista yleisistä tietoturvallisuuteen liittyvistä perustavoitteista (esimerkiksi suojaaminen asiattomalta pääsyltä tietoon, tiedon saatavuuden varmistaminen, ohjelmistojen päivitysten pitäminen ajan tasalla). Nämä tavoitteet olisi huomioitava sertifiointiohjelmaa laadittaessa. Lisäksi ehdotuksen mukaan sertifiointiohjelmat voitaisiin jakaa kolmelle eri luotettavuuden tasolle (basic, substantial, high) riippuen siitä kuinka luotettavasti sertifikaatti todentaisi tietoturvallisuuden tason.

Asetusehdotuksessa on määritelty ne elementit, joita puitekehyksen mukaan annetun sertifiointiohjelman tulisi sisältää. Sertifiointiohjelmasta kävisi ilmi muun muassa niiden hyödykkeiden kategoriat, joita ohjelma koskee, eritellyt turvallisuusvaatimukset (nämä voisivat perustua myös esimerkiksi EU:n laajuisiin tai kansainvälisiin olemassa oleviin standardeihin), sertifiointiohjelman luotettavuuden tason ja ehdot, joiden perusteella sertifikaatti voidaan myöntää.

Tiettyä ICT-tuotteiden tai -palveluiden joukkoa koskeva sertifiointiohjelma luotaisiin komission täytäntöönpanosäädöksellä ENISA:n ehdotuksen perusteella. Sertifiointi olisi vapaaehtoista, mutta ehdotus jättäisi mahdollisuuden myöhemmin säätää unionin tai kansallisessa lainsäädännössä pakollisesta sertifiointivaatimuksesta.

Ehdotus rajoittaisi jäsenvaltioiden mahdollisuuksia laatia omia kansallisia sertifiointiohjelmia. Sen mukaan jäsenvaltiot eivät voisi luoda uusia kansallisia tietoturvallisuuden sertifiointiohjelmia, jos ne olisivat päällekkäisiä ehdotuksen nojalla perustettujen sertifiointiohjelmien kanssa. Olemassa olevat kansalliset sertifiointijärjestelyt pysyisivät voimassa seuraavaan ko-

mission täytäntöönpanosäädöksessä säädettyyn määräpäivään saakka. Järjestelyiden puitteissa myönnetyt sertifikaatit pysyisivät voimassa niiden vanhentumiseen saakka.

Kun komissio olisi hyväksynyt sertifiointiohjelman, hyödykkeiden valmistajat ja palveluntarjoajat hakisivat sertifiointia asetusehdotuksen mukaiselta vaatimustenmukaisuuden arviointielimeltä. Tällaisia elimiä voisi olla useita ja hakijat voisivat valita haluamansa. Arviointielimen tulisi täyttää asetusehdotuksessa ja sen liitteessä määritellyt vaatimukset. Ehdotuksen mukaan arviointielin voisi olla yksityinen yritys, jos sen voidaan katsoa olevan riippumaton eikä sen toiminnassa synny eturistiriitoja. Arviointielimen hyväksyisi EU:n asetuksen (EY) N:o 765/2008 (tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja neuvoston asetuksen (ETY) N:o 339/93 kumoamisesta) mukainen kansallinen akkreditointielin (Suomessa FINAS-akkreditointipalvelu). Sertifioinnin valvontaviranomainen ilmoittaisi komissiolle jäsenvaltiossa akkreditoidut vaatimustenmukaisuuden arviointielimet.

Ehdotuksen mukaan jäsenvaltion tulisi nimittää kansallinen sertifiointivalvontaviranomainen. Kyseessä olisi itsenäinen valvontaviranomainen, jolle jäsenvaltion tulisi osoittaa riittävät resurssit suorittaa tehokkaasti sille säädettyjä tehtäviä. Viranomaisen tehtävänä olisi muun muassa seurata ja valvoa vaatimustenmukaisuuden arviointielimiä sekä sertifioinnin viitekehystä ja sertifiointiohjelmia koskevan sääntelyn toteutumista kansallisella tasolla. Valvontaviranomainen myös käsittelisi sen alueella toimivia arviointielimiä koskevia valituksia ja tekisi yhteistyötä muiden sertifiointiviranomaisten kanssa. Yksi tällaisen yhteistyön muoto olisi ehdotettu sertifiointivalvontaviranomaisten yhteistyöryhmä, jonka pääasiallisena tehtävänä olisi neuvoa komissiota sertifiointiin liittyvissä kysymyksissä ja olla ENISA:n tukena sertifiointiohjelmien valmistelussa. Ryhmä voisi myös ehdottaa sertifiointiohjelman laatimista komissiolle.

Asetusehdotuksen neljäs osa sisältää loppusäännökset muun muassa voimaantulosta ja kumottavista säännöksistä. Viraston toiminnan arviointi ja uudelleen tarkastelu tulisi ehdotuksen mukaan tehdä viiden vuoden sisällä asetuksen voimaantulosta. Uuden asetuksen tullessa voimaan silloinen pääjohtaja ja johtokunta jatkaisivat toimikautensa loppuun. Myös tehdyt päätökset säilyisivät voimassa edellyttäen, etteivät ne olisi ristiriidassa uuden asetuksen kanssa.

3 Ehdotuksen oikeusperusta ja suhde toissijaisuus- ja suhteellisuusperiaatteeseen

Komissio ehdottaa asetuksen oikeusperustaksi Euroopan unionin toiminnasta annetun sopimuksen (SEUT) 26 ja 114 artiklaa. Ehdotus käsiteltäisiin SEUT 294 artiklan mukaisessa tavanomaisessa lainsäädäntöjärjestyksessä.

SEUT 26 artiklan mukaan unioni hyväksyy toimenpiteitä, joiden tarkoituksena on toteuttaa sisämarkkinat tai varmistaa niiden toiminta noudattaen asiaa koskevia perussopimusten määräyksiä. SEUT 114 artiklan mukaan unioni voi toteuttaa sisämarkkinoiden toteuttamista ja toimintaa koskevia toimenpiteitä jäsenvaltioiden lakien, asetusten ja hallinnollisten määräysten lähentämiseksi.

Komissio tuo esille, että ehdotettu oikeusperusta on sama kuin ENISA:n toimintaa nykyisin sääntelevällä asetuksella (EU 526/2013) ja Euroopan unionin tuomioistuin on katsonut sen hyväksyttäväksi (C-2017/04 United Kingdom vs. European Parliament and Council). Lisäksi komissio katsoo, että ehdotuksella lisätään jäsenvaltioiden välistä yhteistyötä erityisesti siltä osin kuin kyse on ENISA:n roolista verkko- ja tietoturvadirektiivin mukaisten velvoitteiden täytäntöönpanossa.

Sertifiointeja koskevan sääntelyn osalta komissio katsoo, että yhteisen sääntelykehyksen puuttuminen on luonut sisämarkkinoille hajaannusta, mikä on haitannut eurooppalaisen ICT-markkinan kehitystä ja kilpailukykyä. Ehdotetulla sääntelyllä olisi tarkoitus puuttua tähän ongelmaan.

Komissio katsoo, ettei EU:n laajuista kybersietokykyä saada riittävästi lisättyä yksittäisten jäsenvaltioiden toimin, eikä hajaantunutta lähestymistapaa kyberturvallisuuteen voida pitää riittävänä. Komission mukaan ehdotetut toimenpiteet eivät mene yli sen mikä on tarpeellista asetettujen tavoitteiden saavuttamiseksi eivätkä estä myöskään jäsenvaltioiden toimia kansallisen turvallisuuden varmistamiseksi.

4 Ehdotuksen suhde perus- ja ihmisoikeusvelvoitteisiin ja perustuslakiin

Komission mukaan kyberturvallisuudella on olennainen tehtävä Euroopan perusoikeuskirjan 7 artiklassa säädetyn yksityiselämän suojan ja 8 artiklassa säädetyn henkilötietojen suojan toteutumisessa. Lisäksi kyberturvallisuudella on keskeinen tehtävä, kun pyritään suojaamaan sähköisen viestinnän luottamuksellisuutta tai toteuttamaan esimerkiksi ilmaisun, ajatuksen, omantunnon ja uskonnon vapautta.

Yksityiselämän suoja ja luottamuksellisen viestin salaisuus turvataan Suomen perustuslain 10 §:ssä. Perustuslain 10 §:n 1 momentin mukaan henkilötietojen suojasta säädetään tarkemmin lailla. Perustuslaissa säädetään myös muun muassa uskonnon ja omantunnon vapaudesta (11 §), sananvapaudesta (12 §) ja kokoontumis- ja yhdistymisvapaudesta (13 §).

5 Ehdotuksen vaikutukset

Vaikutukset EU:n budjettiin

ENISA:n budjetista päätettäisiin normaalisti monivuotisten rahoituskehyksien ja EU:n vuotuisten budjettien yhteydessä.

Vaikutukset talousarvioon

Ehdotus edellyttää, että jäsenvaltiot nimeävät kansallisen sertifiointiviranomaisen. Tämä voi edellyttää muutoksia kansallisten viranomaisten tehtäviin ja viranomaisten toimintaan liittyvien määrärahojen uudelleenarviointia.

Vaikutukset kansalliseen lainsäädäntöön

Komission ehdotus kansallisesta sertifiointiviranomaisesta voi edellyttää muutoksia viranomaisten tehtäviä ja toimivaltaa koskeviin säännöksiin. Suomessa on tällä hetkellä voimassa laki tietoturvallisuuden arviointilaitoksista (1405/2011), jossa säädetään menettelystä, jonka avulla yritykset voivat osoittaa luotettavasti ulkopuolisille, että niiden toiminnassa on toteutettu määrätty tietoturvallisuuden taso. Lain mukaan Viestintävirasto hyväksyy arviointilaitokset sekä ohjaa ja valvoo niiden toimintaa.

6 Ahvenanmaan toimivalta

Ahvenanmaan itsehallintolain (1144/1991) 27 §:n mukaan valtakunnalla on lainsäädäntövaltaa asioissa, jotka koskevat kauppamerenkulkua, ilmailua, standardisointia sekä valtion viranomaisten järjestysmuotoa ja toimintaa.

7 Ehdotuksen kansallinen käsittely ja käsittely Euroopan unionissa

Suomi on viimeksi muodostanut kantansa ENISA:n mandaatin uudistamiseen digitaalisten sisämarkkinoiden strategian täytäntöönpanon väliarvioinnin yhteydessä kesällä 2017 (E 21/2015 vp, EJ 21/2017 vp). Suomi on ottanut asiaan kantaa myös komission Euroopan kyberresilienssijärjestelmän vahvistamista koskevan tiedonannon yhteydessä (E 81/2016 vp).

Ehdotusta ja sitä koskevaa U-kirjelmää on käsitelty kansallisesti EU-valmistelujaostoissa (viestintäjaosto, liikennejaosto, sisämarkkinajaosto) 25.–28. syyskuuta 2017. Lausuntopalaute U-kirjelmästä oli myönteistä. Valtiovarainministeriön budjettiosasto esitti Suomen kantaan lisäyksiä, jotka huomioitiin. Valmisteluun on osallistunut ministeriöiden ja keskusvirastojen lisäksi myös etujärjestöjä ja sidosryhmien edustajia.

Ehdotusta on tarkoitus käsitellä neuvoston kybertyöryhmän ja teletyöryhmän yhteiskokouksissa. Käsittelyn on tarkoitus alkaa syksyn 2017 aikana. Puheenjohtajan tavoitteena on laatia edistymisraportti joulukuun liikenne-, televiestintä- ja energianeuvostoon.

Euroopan parlamentissa vastuuvaliokuntana on teollisuus-, tutkimus- ja energiavaliokunta.

8 Valtioneuvoston kanta

Valtioneuvosto pitää tärkeänä, että ehdotuksella pyritään vahvistamaan tietoturvallisuutta koko EU:n alueella, parantamaan tietoturvallisten tuotteiden ja palveluiden saatavuutta sisämarkkinoilla ja edistämään innovaatioita. Pääministeri Juha Sipilän hallitusohjelman kärkihankkeena on, että Suomeen rakennetaan digitaalisen liiketoiminnan kasvuympäristö. Asetusehdotuksen tavoitteiden voidaan katsoa olevan linjassa hallitusohjelman, sen toimeenpanosuunnitelman nojalla laaditun kansallisen tietoturvastrategian ja edellisen hallituksen hyväksymän kyberturvallisuusstrategian kanssa.

Valtioneuvosto katsoo, että ENISA:n mandaatin muuttuminen pysyväksi parantaisi viraston toimintaedellytyksiä. Se takaisi viraston toiminnan jatkuvuuden ja loisi uusia mahdollisuuksia rekrytoida virastoon korkean tason asiantuntemusta. ENISA:n toimintaa ja tavoitteita tulisi arvioida säännöllisesti, jotta se pystyisi parhaalla tavalla palvelemaan nopealla syklillä muuttuvia ja kehittyviä digitaalisia sisämarkkinoita. Tavoitteena tulee olla määrärahojen tuloksellinen, kustannustehokas ja moitteettoman varainhoidon periaatteiden mukainen käyttö.

Valtioneuvoston näkemyksen mukaan ENISA:n toimintaa tulisi kehittää vahvistamaan sisämarkkinoita erityisesti niillä alueilla, joilla käyttäjien tarpeiden mukaisten sisäänrakennetusti tietoturvallisten tuotteiden ja palveluiden saatavuus ei vastaa käyttäjien kysyntää. Yksi tällaisista alueista on niin sanottu esineiden internet (Internet of Things, IoT), jolla tarkoitetaan tietoverkkoon liitettyjen laitteiden, ohjelmistojen ja muiden hyödykkeiden muodostamaa kokonaisuutta. Komissio arvioi ehdotuksessaan, että seuraavan vuosikymmenen aikana EU:ssa otetaan käyttöön miljoonia tai jopa miljardeja tietoverkkoon kytkettyjä digitaalisia laitteita. Valtioneuvosto yhtyy komission näkemykseen siitä, että esineiden internet ja muut digitaalisten sisämarkkinoiden keskeiset voimavarat, kuten datatalous ja automatisoituva liikenne, voivat kukoistaa vain, jos ne nauttivat yleistä luottamusta ja niiden tietoturvallisuus on riittävän korkealla tasolla. Lisäksi valtioneuvosto pitää tärkeänä, että käyttäjillä on mahdollisuus suojata luottamuksellinen viestintänsä ja digitaaliset tietonsa asiakastarpeiden mukaan kehittyvillä salaus- ja suojausohjelmistoilla sekä muilla teknologisilla ratkaisuilla.

Ehdotetun tieto- ja viestintäteknologiahyödykkeiden sertifioinnin puitekehyksen tavoitteita voidaan pitää kannatettava siltä osin kuin sääntelyllä pyrittäisiin lisäämään luottamusta digi-

taalisille sisämarkkinoille ja vähentämään yrityksille sertifioinnista aiheutuvia kuluja. Ehdotettujen keinojen ja menettelyiden tehokkuutta suhteessa tavoiteltavaan päämäärään tulee kuitenkin vielä arvioida huolellisesti.

Valtioneuvosto katsoo, että ENISA:n ja komission tulisi edistää erityisesti sellaisten standardien ja sertifiointien kehittymistä, joiden avulla eri toimialoilla tietotekniikkaa ja esineiden internetiä toiminnassaan hyödyntävät käyttäjät voisivat paremmin vakuuttua EU:n sisämarkkinoilla tarjottavien esineiden internetiin liittyvien laitteiden ja ohjelmistojen sisäänrakennetusta tietoturvallisuudesta. Tässä työssä komission ja ENISA:n tulisi ottaa huomioon myös tietoturvallisuuden ja digitaalisen palvelutuotannon parantamiseksi toimialoilla jo käynnissä oleva standardointi- ja sertifiointityö ja välttää päällekkäisyyksiä sen kanssa. Valtioneuvosto pitää myös tärkeänä, että asetusehdotuksella luotavat sertifiointipuitteet tukevat turvallisen automaattisen liikenteen kehittymistä.

Valtioneuvosto haluaa kiinnittää huomiota siihen, että puitekehys ja sen nojalla laadittavat sertifiointiohjelmat saattaisivat potentiaalisesti vaikuttaa varsin suureen joukkoon erilaisia toimijoita, sillä puitekehyksen alaan kuuluvat tuotteet ja palvelut on asetusehdotuksessa määritelty laajasti. Täsmällisempi määrittely tehtäisiin komission täytäntöönpanosäädöksellä annettavissa sertifiointiohjelmissa, joissa määriteltäisiin niiden hyödykkeiden kategoriat, joita ohjelma koskisi. Asetusehdotuksen ja sen nojalla annettavan alemmanasteisen sääntelyn soveltamisalan vaikutuksia, laajuutta ja tarkoituksenmukaisuutta tulee arvioida jatkovalmistelussa, jotta voidaan varmistua siitä, että sertifioinneilla olisi aidosti positiivisia vaikutuksia ja markkinoille saataisiin nykyistä tietoturvallisempia tuotteita ja palveluita, jotka myös vastaavat käyttäjien tarpeita.

Valtioneuvosto pitää tärkeänä, että tietoturvallisten tuotteiden standardointi- ja sertifiointitoiminta hyödyttää suomalaisia yrityksiä, muttei aiheuta niille ylimääräistä, kilpailukykyä haittaavaa hallinnollista taakkaa. EU-sääntelystä johtuvat velvoitteet tietoturvariskien hallitsemiseksi tulee voida jatkossakin sovittaa osaksi muiden liiketoiminnan riskien hallintaa. Tähän on kiinnitettävä huomiota erityisesti ehdotukseen liittyvän viranomaistoiminnan jatkovalmistelussa. Ehdotetulla sääntelyllä tulisi kokonaisuudessaankin pyrkiä siihen, ettei sillä tai sen mukaisilla menettelyillä aiheuteta yksityiselle sektorille tai viranomaisille ylimääräistä hallinnollista taakkaa eikä aseteta toimijoita keskenään eriarvoiseen asemaan.

Valtioneuvosto katsoo, että ENISA:n tulisi toiminnassaan välttää päällekkäisyyksiä kansallisten viranomaisten toiminnan kanssa. Operatiivista yhteistyötä tulisi kehittää ensisijaisesti verkko- ja tietoturvadirektiivissä säädettyjen uusien yhteistyörakenteiden puitteissa, jotta niiden vaikuttavuudesta saataisiin kokemuksia. ENISA:n tehtävien ja asetusehdotuksesta jäsenmaille syntyvien velvoitteiden tulisi olla linjassa verkko- ja tietoturvadirektiivin kanssa.

Lisäksi valtioneuvosto pitää yleisesti tärkeänä seurata jatkossakin tarkasti EU-instituutioiden ja virastojen hallintomenojen ja henkilöstömäärän kehitystä. Näiden menojen taso olisi kokonaisuutena pyrittävä pitämään maltillisena.

9 Laatijan yhteystiedot

Piia Nyström Liikenne- ja viestintäministeriö p. 029 534 2969