U 83/2022 vp

Valtioneuvoston kirjelmä eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi horisontaalisista kyberturvallisuusvaatimuksista tuotteille, joissa on digitaalinen elementti (kyberkestävyyssäädös)

Perustuslain 96 §:n 2 momentin perusteella lähetetään eduskunnalle komission 15 päivänä syyskuuta 2022 antama ehdotus Euroopan parlamentin ja neuvoston asetukseksi horisontaalisista kyberturvallisuusvaatimuksista tuotteille, joissa on digitaalinen elementti ja asetuksen (EU) 2019/1020 muuttamisesta sekä siitä laadittu muistio.

Helsingissä 10.11.2022

Liikenne- ja viestintäministeri Timo Harakka

Erityisasiantuntija Outi Slant

LIIKENNE- JA VIESTINTÄMINISTERIÖ | MUISTIO | EU/2022/1203

10.11.2022

KOMISSION EHDOTUS EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUKSEKSI HORISONTAALISISTA KYBERTURVALLISUUSVAATIMUKSISTA TUOTTEILLE, JOISSA ON DIGITAALINEN ELEMENTTI JA ASETUKSEN (EU) 2019/1020 MUUTTAMISESTA

1 Tausta

Euroopan komissio antoi 15.9.2022 ehdotuksen Euroopan parlamentin ja neuvoston asetukseksi horisontaalisista kyberturvallisuusvaatimuksista tuotteille, joissa on digitaalinen elementti ja asetuksen (EU) 2019/1020 muuttamisesta (KOM (2022) 454 lopullinen) eli kyberkestävyyssäädökseksi.

Ehdotuksen taustalla on kyberturvallisuuteen liittyvä kehitys, jossa laitteet ja ohjelmistot joutuvat enenevässä määrin kyberhyökkäysten kohteeksi ja aiheuttavat merkittäviä kustannuksia hyökkäyksen kohteeksi joutuneelle sekä muita haittoja, kuten henkilötietojen vaarantumista. Näiden tuotteiden yhteisenä tekijänä on matala tietoturvallisuuden taso, joka ilmenee laajoina haavoittuvuuksina ja päivitysten puutteina sekä käyttäjien riittämätön ymmärrys turvallisuusominaisuuksista ja rajoitettu pääsy käyttämiensä tuotteiden tietoturvaominaisuuksia koskevaan tietoon. Tämä tekee tuotteiden ja niiden turvallisuusominaisuuksien vertailusta kuluttajille haastavaa.

Tuotteiden markkinoille saattamisella on vahva rajat ylittävä merkitys ja toisaalta myös tuotteisiin liittyvillä tietoturvaloukkauksilla voi olla laajasti rajat ylittävää vaikutusta, minkä vuoksi aiheesta on katsottu tarpeelliseksi säätää unionin tasolla. Yhteiset toimet EU:n tasolla on katsottu välttämättömiksi, jotta voidaan lisätä tuotteisiin kohdistuvaa luottamusta ja EU-vaatimukset täyttävien tuotteiden houkuttelevuutta.

2 Ehdotuksen tavoite

Ehdotuksen yleisenä tavoitteena on luoda olosuhteet turvallisten digitaalisen elementin sisältävien tuotteiden kehittämiselle ja varmistaa, että laitteissa ja ohjelmistoissa on vähemmän haavoittuvuuksia ja valmistajat ottavat turvallisuusnäkökohdat vakavasti tuotteen elinkaaren ajan. Toisena tavoitteena on luoda olosuhteet, joissa kuluttajat voivat ottaa kyberturvallisuusnäkökohdat huomioon valitessaan digitaalisen elementin sisältäviä tuotteita.

Ehdotuksen erityisinä tavoitteina on varmistaa tuotteiden turvallisuus niiden elinkaaren ajan, taata yhtenäinen kehys turvallisuusvaatimuksille, edistää turvallisuusominaisuuksien läpinäkyvyyttä ja mahdollistaa tuotteiden turvallinen käyttö.

3 Ehdotuksen pääasiallinen sisältö

Ehdotuksessa asetetaan yleiset turvallisuusvaatimukset tuotteille, joissa on digitaalinen elementti. Ehdotus sisältää velvoitteet valmistajalle, maahantuojalle ja jakelijalle. Lisäksi ehdotus sisältää säännökset vaatimustenmukaisuuden arvioinnista, vaatimustenmukaisuuden arviointilaitoksista, markkinavalvonnasta ja täytäntöönpanosta sekä seuraamusmaksuista.

3.1 Yleiset säännökset

Komission ehdotuksen mukaan säädöksellä luodaan säännöt markkinoille saatettavien digitaalisen elementin sisältävien tuotteiden kyberturvallisuudesta. Säädös sisältää keskeiset laatuvaatimukset tuotteiden suunnittelulle, kehitykselle ja tuotannolle sekä asettaa velvoitteet näiden tuotteiden kaupallisille toimijoille. Ehdotuksessa on mukana keskeiset haavoittuvuuksien hallinnan prosessit siten, että ne kattaisivat koko tuotteen elinkaaren. Lisäksi ehdotuksessa luodaan säännöt markkinavalvonnalle ja säännösten täytäntöönpanolle.

Asetusta sovellettaisiin tuotteisiin, joihin kuuluu digitaalinen elementti ja jotka ovat liitettävissä toiseen laitteeseen tai suoraan verkkoon. Liittäminen voitaisiin tehdä joko suoraan esimerkiksi fyysisillä kaapeleilla tai langattomasti. Lähtökohtaisesti kaikki tällaiset tuotteet kuuluisivat asetuksen soveltamisalaan, ellei poikkeuksesta olisi erikseen säädetty. Asetuksen soveltamisalasta on rajattu pois tietyt tuotteet, joiden kyberturvallisuusvaatimuksista on säädelty kattavasti hiljattain voimaan tulleessa EU-sääntelyssä. Niitä ovat lääkinnälliset laitteet, joista säädetään asetuksessa (EU) 2017/745 ja in vitro-diagnostiikkaan tarkoitetut lääkinnälliset laitteet, joista säädetään asetuksessa (EU) 2017/746. Lisäksi soveltamisalasta on rajattu pois ajoneuvojen turvallisuusasetuksen (EU) 2019/2144 alaan kuuluvat ajoneuvot ja perävaunut. Sääntelyä ei lisäksi sovellettaisi siviili-ilmailun yhteisistä säännöistä annetun asetuksen (ns. EASA-asetus (EU) 2018/1198) nojalla standardoinnin alaisiin tuotteisiin, joissa on digitaalinen elementti, eli esimerkiksi valtaosaan siviili-ilma-aluksista. Asetusta ei lisäksi sovellettaisi tuotteisiin, jotka on yksinomaan tehty kansallisen turvallisuuden tai maanpuolustuksen käyttöön tai jos tuote on nimenomaan suunniteltu prosessoimaan salassa pidettävää aineistoa. Asetusta ei sovellettaisi muuhun kuin tuotteiden saattamiseen markkinoille osana kaupallista toimintaa.

Ehdotuksen turvallisuusvaatimusten soveltamista voidaan joissain tilanteissa rajoittaa tai jättää soveltamatta. Näin on silloin, jos unionin sääntelyn piiriin kuuluvan tuotteen sääntelyssä huomioidaan vastaavia vaatimuksia siten, että ne täyttyisivät ehdotuksen vaatimusten kanssa osittain tai kokonaan. Rajaaminen on mahdollista, jos sääntelykehikko muodostuu yhtenäiseksi ja kyberturvallisuuden vaatimustaso on muualla lainsäädännössä yhdenmukainen ehdotuksen kanssa. Rajaukset ja poissulkeminen tapahtuisivat komission delegoidulla säädöksellä.

Ehdotuksen mukaan digitaalisen elementin sisältävällä tuotteella tarkoitettaisiin mitä tahansa ohjelmistoa tai laitetta sekä siihen liittyvää tietojen etäkäsittelyä sisältäen ohjelmiston tai laitteen komponentit, jotka asetetaan markkinoille erikseen. Talouden toimijalla tarkoitetaan valmistajaa, valtuutettua edustajaa, maahantuojaa, jakelijaa tai ketä tahansa luonnollista tai oikeushenkilöä, jota asetuksen vaatimukset koskevat. Valmistajalla tarkoitetaan ketä tahansa luonnollista tai oikeushenkilöä, joka kehittää tai tuottaa digitaalisen elementin sisältäviä tuotteita tai jonka nimen tai tavaramerkin alla tuotetaan digitaalisen elementin sisältäviä tuotteita joko maksua vastaan tai ilmaiseksi.

Jäsenvaltiot eivät saisi estää markkinoille tuloa, jos tuote täyttää asetuksen vaatimukset. Markkinoille saisi tuoda asetuksessa tarkoitettuja tuotteita vain, jos ne ja niihin liittyvät prosessit täyttävät asetuksen liitteen I vaatimukset. Vaatimusten täyttymisestä voidaan poiketa muun muassa näyttely- ja demonstraatiotarkoituksissa tai keskeneräisen ohjelmiston rajoitetussa testauksessa, kunhan tällöin käy selvästi ilmi, että se ei täytä asetuksen vaatimuksia.

Asetusehdotuksen liitteessä III on määritelty kriittiset digitaalisen elementin sisältävät tuotteet. Nämä tuotteet on jaettu edelleen kahteen luokkaan niihin liittyvän riskin perusteella. Luokkaan yksi kuuluu muun muassa erilaisia ohjelmistojen ja henkilöllisyyden suojaamisen hallintaan liittyviä ohjelmistoja ja laitteita. Lisäksi siellä on verkon hallintaan liittyviä tuotteita sekä päi-

vitysten hallintajärjestelmiä. Luokkaan yksi kuuluvat esimerkiksi reitittimet, modeemit ja mikroprosessorit sekä teollisuusautomaation järjestelmät, elleivät ne erityisistä syistä kuulu luokkaan kaksi. Luokassa kaksi ovat korkeariskisimmät tuotteet, joita ovat muun muassa palvelinten, ja mobiililaitteiden hallinnointijärjestelmät, erilaiset mikroprosessorit, julkinen avaininfrastruktuuri, älykortit sekä verkko- ja tietoturvadirektiivin (NIS2-direktiivi, COM (2020) 823 final) alaan kuuluvien toimijoiden teolliset automaatiojärjestelmät tai verkkoon kytketyt laitteet. Kummallekin tuotekategorialle on määritelty omat vaatimustenmukaisuuden arviointiprosessinsa. Komissio voisi antaa delegoituja säädöksiä liitteen III muuttamiseksi. Liitteen muuttamisessa huomioidaan kyberturvariskin taso tietyn kategorian tuotteille. Asetuksessa olisi määritelty kriteeristö riskitason arvioinnille, johon kuuluu muun muassa tuotteen mahdollinen käyttö NIS2-direktiivissä tarkoitettujen keskeisten toimijoiden toiminnoissa tai se on olennainen toimitusketjujen kannalta.

Asetusehdotuksen 7 – 9 artikloissa selvennettäisiin sen suhdetta eräisiin muihin tuotteita koskeviin säädöksiin, kuten yleiseen tuoteturvallisuusasetukseen (COM (2021) 346 final), ehdotettuun tekoälyasetukseen (COM (2021) 206 final) ja koneista annettuun asetusehdotukseen (COM (2021) 202 final. Ehdotetun 7 artiklan nojalla digitaalisia elementtejä sisältäviin tuotteisiin sovellettaisiin pääosin yleisessä tuoteturvallisuusasetuksessa säädettyjä vaatimuksia ja näiden kuluttajatuotteiden tietoturvallisuusvaatimukset voitaisiin osoittaa kyberkestävyyssäännöksen mukaisilla menettelyillä. Ehdotetun 8 artiklan nojalla eräiden tekoälyjärjestelmien, jotka täyttäisivät kyberkestävyysasetuksen vaatimukset, olisi katsottava täyttävän myös tekoälyasetuksella asetettavat kyberturvallisuusvaatimukset. Näihin tuotteisiin sovellettaisiin kuitenkin joko tekoälyasetuksen tai kyberkestävyyssäädöksen mukaista vaatimustenmukaisuusarviointia riippuen siitä, millaista riskiä tuotteeseen liittyy. Ehdotetun 9 artiklan nojalla koneasetusehdotuksen soveltamisalaan kuuluvien tuotteiden, jotka kuuluisivat kyberkestävyysasetuksen soveltamisalaan ja joille tulisi laatia asetuksen perusteella EU-vaatimustenmukaisuusvakuutus, jolloin sen katsotaan täyttävän olevan koneasetuksen tietyt tietoturvavaatimukset. Kyseessä olevat koneasetusehdotuksen vaatimukset kohdat käsittelevät koneasetuksen soveltamisalaan kuuluvien tuotteiden suojaamista korruptiolta sekä koneiden turvallisuuteen liittyvän ohjausjärjestelmän luotettavuutta.

3.2 Taloudellisille toimijoille asetettavat vaatimukset

Soveltamisalaan kuuluvan tuotteen valmistajan olisi ennen tuotteen asettamista markkinoille varmistuttava, että tuote täyttää asetuksen liitteessä 1 säädetyt vaatimukset. Näitä vaatimuksia ovat esimerkiksi se, että tuotteet on suunniteltava, kehitettävä ja tuotettava siten, että niiden turvallisuustaso suhteutetaan riskeihin. Lisäksi tuotteet eivät saa sisältää tunnistettuja haavoittuvuuksia. Liitteessä on myös yksityiskohtaisempia vaatimuksia esimerkiksi datan käsittelystä ja uhkien torjunnasta. Valmistajien on toteutettava arviointi tuotteiden kyberturvariskeistä ja huomioitava se tuotteen koko elinkaaren ajan, suunnittelusta käyttöön ja ylläpitoon, sekä minimoitava kyberturvallisuusriskit ja riskien mahdolliset vaikutukset. Asetettaessa tuotteita markkinoille valmistajan on liitettävä tekniseen dokumentaatioon kyberturvallisuusriskien arviointi. Valmistajan on varmistuttava, että kolmannen osapuolen toimittamat komponentit eivät vaaranna tuotteen turvallisuutta. Tietoon tulevat kyberturvallisuuteen vaikuttavat tekijät, kuten haavoittuvuudet on dokumentoitava. Tuotteiden haavoittuvuuksista on huolehdittava koko tuotteen elinkaaren ajan tai viiden vuoden ajan markkinoille saattamisesta sen mukaan, kumpi ajanjaksoista on lyhyempi. Turvallisuusnäkökohdat on dokumentoitava ja tuotteelle on toteutettava vaatimustenmukaisuusarviointi. Vaatimusten täyttymisestä laaditaan EU:n vaatimustenmukaisuusilmoitus ja tuotteeseen lisätään CE-merkintä.

Ehdotuksen mukaan käyttäjälle on toimitettava liitteen II mukaiset tiedot ja ohjeet, jotka sisältävät tuotteen ja valmistajan yhteystiedot sekä muun muassa tiedon siitä, miten mahdollisista

tuotteeseen liittyvistä haavoittuvuuksista saa tietoa. Jos tuotteen elinkaaren aikana huomataan sen olevan asetuksen turvallisuusvaatimusten vastainen, tulee tuote korjata vaatimusten mukaiseksi tai vetää tuote pois markkinoilta. Valmistajien tulee toimia yhteistyössä markkinavalvontaviranomaisten kanssa. Jos valmistaja lopettaa toimintansa tuotteen elinkaaren aikana, tulee tästä ilmoittaa markkinavalvontaviranomaiselle ja parhaiden mahdollisuuksien mukaan informoida myös käyttäjiä.

Valmistajien olisi ilmoitettava EU:n kyberturvallisuusvirasto ENISAlle 24 tunnin kuluessa tapahtuman tietoon tulosta, jos tuotteeseen liittyy aktiivisesti hyödynnetty haavoittuvuus tai tietoturvaloukkaus. ENISA jakaisi tiedon kansallisille CSIRT-verkoston jäsenille (Computer Security Incident Response Team) ja markkinavalvontaviranomaiselle. Valmistajan on ilmoitettava tuotteen käyttäjille ilman aiheetonta viivästystä havaituista tapahtumista ja tarvittaessa kerrottava, miten käyttäjä voi minimoida haitalliset vaikutukset. Valmistajan on ilmoitettava tuotteiden komponenttien valmistajille komponenteissa havaituista haavoittuvuuksista.

Maahantuojille asetettavana keskeisimpänä vaatimuksena ne saisivat jatkossa asettaa markkinoille vain sellaisia tuotteita, jotka täyttävät asetuksen vaatimukset turvallisuudesta. Maahantuojan olisi varmistuttava, että vaatimustenmukaisuusarviointi on tehty, tekninen dokumentointi on olemassa, tuotteessa on CE-merkintä ja tuote sisältää vaadittavat ohjeet käyttäjälle. Maahantuojien, jotka huomaavat turvallisuuteen liittyviä puutteita tuomissaan tuotteissa, on ryhdyttävä välittömästi korjaaviin toimiin ja tarvittaessa vedettävä tuote pois markkinoilta. Korjaavista toimista vastaa valmistaja. Maahantuojan on toimitettava vaadittava dokumentaatio tarvittaessa markkinavalvontaviranomaisille ja informoitava viranomaisia ja mahdollisuuksien mukaan käyttäjiä, mikäli valmistaja lopettaa toimintansa, eikä voi hoitaa velvoitteitaan. Maahantuojien velvoitteita vastaavasti ehdotetaan säädettäväksi jakelijoiden velvoitteesta toimia yhteistyössä markkinavalvontaviranomaisten kanssa ja ilmoittaa valmistajan toiminnan lopettamisesta.

Jakelijoiden velvoitteiksi on asetettu tuotteen CE-merkinnän varmistaminen ja se, että valmistaja ja maahantuoja noudattavat niille asetettuja dokumentaatioon ja ohjeistukseen liittyviä vaatimuksia. Vaatimusten vastaisia tuotteita ei voi tuoda markkinoille. Jos vaatimustenvastaisuutta on syytä epäillä, on jakelijan ryhdyttävä vastaavalla tavalla toimiin, mitä on ehdotettu maahantuojien osalta. Valmistajaa koskevia vaatimuksia sovelletaan maahantuojaan ja jakelijaan esimerkiksi tilanteessa, jossa ne tekisivät tuotteeseen merkittävän muutoksen.

Taloudellisten toimijoiden, kuten jakelijoiden, on pyynnöstä luovutettava markkinavalvontaviranomaiselle tietoja siitä taloudellisesta toimijasta, joka on toimittanut heille digitaalisen elementin sisältävän tuotteen ja sen, kenelle kyseisiä tuotteita on toimitettu.

3.3 Tuotteiden vaatimustenmukaisuus

Ehdotuksen nojalla tuotteen katsotaan täyttävän ehdotuksen vaatimukset, jos valmistaja on täyttänyt tuotteelle asetetut harmonisoidut standardit, jotka on julkaistu EU:n virallisessa lehdessä, oletetaan olevan asetuksen liitteen I vaatimusten mukaisia. Tuotteiden, jotka täyttävät asetuksessa määritellyt tekniset eritelmät, katsotaan olevan asetuksen turvallisuutta koskevien vaatimusten mukaisia. Tuotteet, jolla on EU:n vaatimustenmukaisuusilmoitus tai kyberturvallisuusasetuksen (EU) 2019/881 mukainen, ehdotetun asetuksen vaatimuksia vastaava sertifikaatti, joka vastaa asetuksen vaatimuksia, katsotaan täyttävän asetuksen turvallisuusvaatimukset. Komissio voi täytäntöönpanosäädöksillä tarkentaa kyberturvallisuusasetuksen sertifiointiskeemoja, jotta ne vastaavat asetuksessa asetettuja vaatimuksia.

Niiltä osin, kun harmonisoituja standardeja ei ole tai komissio katsoo ne riittämättömiksi tai muutoin puutteellisiksi, komissio voisi antaa täytäntöönpanosäädöksiä teknisistä eritelmistä liittyen asetuksen liitteessä määriteltyihin turvallisuusvaatimuksiin. CE-merkinnän osalta noudatetaan yleisiä periaatteita Euroopan parlamentin ja neuvoston asetuksesta tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista (EY) N: 765/2008. Ehdotus sisältää säännöt ja ehdot CE-merkinnän kiinnittämisestä.

Ehdotuksessa on tarkempia säännöksiä vaatimustenmukaisuuden arvioinnista. Ehdotuksen lähtökohta vaatimustenmukaisuuden arvioinnille olisi valmistajan itsearviointi. Valmistaja suorittaisi tuotteen vaatimustenmukaisuuden arvioinnin määrittääkseen, täyttääkö tuote liitteen I keskeiset vaatimukset- Vaatimustenmukaisuuden arviointi voidaan toteuttaa itsearvioinnin kautta tai EU:n tyyppitarkastuksella, jonka toteuttaa tietty ilmoitettu laitos. Jos tuote sisältää tavanomaista korkeampia riskejä kyberturvallisuuden kannalta, vaatimustenmukaisuus olisi osoitettava ulkopuolisen arviointilaitoksen toimesta. Lisäksi vaatimustenmukaisuus voidaan osoittaa täydellä laadunvarmistuksella, jossa arvioinnin toteuttaa myös ilmoitettu laitos. Vaatimustenmukaisuuden osoittamisesta säädettäisiin asetusehdotuksen liitteessä IV.

Korkean riskin, eli kriittisten digitaalisen elementin sisältävien tuotteiden osalta tuotteissa vaatimustenmukaisuus osoitetaan EU:n tyyppitarkastuksella, jota seuraa itsearviointiin perustuva vaatimustenmukaisuusarviointi, mikäli tuotteelle ei ole olemassa ollenkaan tai kokonaan harmonisoituja kyberturvallisuussertifiointeja. Lisäksi vaatimustenmukaisuus voidaan osoittaa täydellä laadunvarmistuksella. Erittäin kriittisten tuotteiden osalta vaatimustenmukaisuuden arviointi toteutetaan samalla tavoin aina ilmoitetun ulkopuolisen laitoksen tekemän arvioinnin perusteella. Ilmoitettujen laitosten olisi huomioitava pienten ja keskisuurien yritysten tarpeet kohtuullisuudessa, kun se asettaa maksuja vaatimustenmukaisuuden arvioinnille.

3.4 Ilmoittaminen vaatimusten mukaisuutta arvioivista laitoksista

Jäsenvaltioiden olisi ilmoitettava komissiolle ja muille jäsenvaltioille niistä arviointilaitoksista, jotka saavat tehdä asetuksen mukaista vaatimustenmukaisuuden arviointia. Jäsenvaltioiden on asetettava ilmoituksesta vastaava viranomainen, jonka vastuulla olisi huolehtia ilmoitettujen laitosten ja arviointilaitosten ilmoittamisesta ja arvioinnista. Ilmoituksesta vastaavalle viranomaiselle on asetettu vaatimuksia intressiristiriitojen välttämiseksi ja puolueettomuuden turvaamiseksi. Jäsenvaltioiden on ilmoitettava komissiolle ilmoituksesta vastaavan viranomaisen arviointi- ja ilmoitusprosessista sekä valvonnasta.

Asetuksessa asetetaan erityisiä vaatimuksia arviointilaitoksille, jotka tekevät vaatimustenmukaisuusarviointia. Laitoksella tulee olla oikeushenkilöllisyys ja sen, samoin kuin sen henkilöstön, tulee olla itsenäinen suhteessa niihin organisaatioihin, joiden tuotteita se arvioi. Laitoksilla on oltava riittävän asiantunteva henkilöstö, tarvittava laitteisto ja arviointiprosessin kuvaus, joka takaa arviointiprosessin läpinäkyvyyden. Arviointitoiminta on erotettava laitoksen mahdollisista muista toiminnoista ja se on luottamuksellista muutoin paitsi suhteessa markkinavalvontaviranomaiseen. Arviointilaitoksen katsotaan täyttävän vaatimukset, jos se täyttää vaadittavat standardit, jotka on julkaistu EU:n virallisessa lehdessä. Myös ilmoitettujen laitosten alihankkijoiden on täytettävä edellä mainitut vaatimukset ja ilmoitetut laitokset kantavat vastuun alihankkijoidensa toiminnasta.

Arviointilaitokseksi hakeudutaan hakemuksella ilmoituksesta vastaavalle viranomaiselle. Hakemuksessa kuvataan toimintaa ja niitä tuotteita, joita se tulisi arvioimaan. Ilmoituksista vastaava viranomainen laatii vaatimukset täyttävistä laitoksista ilmoituksen ja ilmoittaa sen komissiolle. Komissio pitää listaa arviointilaitoksista. Mikäli laitosten vaatimustenmukaisuuden täyttymisessä tapahtuu muutoksia, tulee näistä ilmoittaa komissiolle. Komissio voi myös arvioida

ilmoitettujen laitosten pätevyyden tai vaatimustenmukaisuuden jatkuvuuden, mikäli näistä on epäilyksiä.

Vaatimustenmukaisuuden arviointi on toteutettava suhteellisuutta noudattaen ja tarpeetonta taloudellista haittaa välttäen. Arvioinnissa on huomioitava yrityksen koko, toimintasektori, rakenne, teknologian monimutkaisuus sekä se, onko tuote tarkoitettu sarjatuotantoon. Arvioinnin perusteella voidaan esittää tuotteeseen korjaavia toimenpiteitä, jotta se täyttää asetuksessa asetetut vaatimukset. Komissio varmistaisi arviointilaitosten välisen koordinaation ja yhteistyön ja jäsenvaltion huolehtisivat arviointilaitosten osallistumisesta tähän yhteistyöhön.

3.5 Markkinavalvonta ja täytäntöönpano

Digitaalisen elementin sisältävien tuotteiden markkinavalvontaan sovellettaisiin Euroopan parlamentin ja neuvoston asetusta (EU) 2019/1020 markkinavalvonnasta ja tuotteiden vaatimustenmukaisuudesta (markkinavalvonta-asetus). Jäsenvaltiot osoittavat yhden tai useamman viranomaisen markkinavalvontaviranomaiseksi varmistamaan asetuksen tehokkaan täytäntöönpanon. Viranomainen voi olla olemassa oleva tai uusi. Markkinavalvontaviranomaiset voivat toimia yhteistyössä ja vaihtaa tietoa kyberturvallisuussertifiointiviranomaisten kanssa säännöllisesti. Yhteistyötä on tehtävä myös muiden relevanttien viranomaisten, kuten tietosuojaviranomaisten kanssa. Tietosuojaviranomaisilla on oikeus saada pääsy tämän asetuksen nojalla syntyneeseen tarpeellisen dokumentaatioon tehtävänsä hoitamiseksi.

Markkinavalvontaviranomaisille olisi turvattava riittävät taloudelliset ja henkilöstöresurssit. Viranomaisten on raportoitava komissiolle valvonnan tuloksista vuosittain. Korkeariskisten tekoälyjärjestelmien markkinavalvontaa tehtäisiin tekoälyasetuksen mukaisesti, mutta yhteistyössä ehdotuksen mukaisten markkinavalvontaviranomaisten kanssa. Markkinavalvontaviranomaisille on annettava pääsy tarvittavaan dataan, sisältäen sisäinen dokumentaatio, arvioidakseen vaatimustenmukaisuutta. Säädöksen täytäntöönpanon yhdenmukaisuuden varmistamiseksi perustetaan hallinnollinen yhteistyöryhmä, jossa ovat edustettuna markkinavalvontaviranomaiset.

Jos kansallinen markkinavalvontaviranomainen perustellusti arvioi, että markkinoilla olevaan tuotteeseen liittyy merkittävä kyberturvallisuusriski, sen tulee toteuttaa asiasta arviointi. Jos tuotteen ei katsota vastaavan asetettuja vaatimuksia, sen täytyy ilmoittaa siitä asian kannalta olennaiselle toimijalle puutteiden korjaamiseksi ja tarvittaessa tuotteen markkinoilta pois vetämiseksi. Jos puutteiden arvioidaan ulottuvan kansallista alaa laajemmalle, tulee tästä informoida komissiota ja muita jäsenvaltioita. Valmistajan on toteutettava kaikki mahdolliset korjaavat toimenpiteet tilanteen korjaamiseksi. Jos tarvittavia toimenpiteitä ei tehdä, voi markkinavalvontaviranomainen kieltää tai rajoittaa tuotteen saatavuutta markkinoilla. Prosessin käynnistymisestä ja kansallisista toimenpiteistä on informoitava komissota ja muita jäsenvaltioita. Muiden jäsenvaltioiden markkinavalvontaviranomaisten on toimitettava kyseistä tuotetta koskevaa tietoa, mikäli sellaista on. Myös erimielisyydestä olisi ilmoitettava. Mikäli vastustusta ei tule kolmen kuukauden kuluessa, kansalliset toimenpiteet astuvat voimaan.

Mikäli jäsenvaltio vastustaa toisen jäsenvaltion käynnistämiä valvontatoimenpiteitä tai komissio katsoo seurausten olevan vastoin unionin lainsäädäntöä, komissio käynnistää neuvottelut jäsenvaltioiden välillä ja taloudellisen toimijan kanssa kansallisten toimenpiteiden arvioimiseksi. Komissio toteaa tämän perusteella yhdeksän kuukauden kuluessa, oliko seuraamus oikeutettu.

Mikäli komissiolla on perusteltua syytä epäillä, että digitaalisen elementin sisältä tuote muodostaa merkittävän kyberturvallisuusriskin, se voi pyytää relevanttia markkinavalvontaviran-

omaista suorittamaan arvioinnin. Poikkeuksellisissa tilanteissa se voi pyytää myös ENISAa tekemään kyseisen arvioinnin. Arvioinnin perusteella komissio päättää tarvittavista korjaavista toimista. Tämän jälkeen komissio konsultoi jäsenvaltioita sekä relevantteja taloudellisia toimijoita. Konsultoinnin perusteella komissio voi antaa täytäntöönpanosäädöksiä.

Tilanteissa, joissa tuote täyttää asetuksen vaatimukset, mutta se silti sisältää merkittävän kyberturvallisuuden riskin, jonka lisäksi se aiheuttaa uhkan ihmisten terveydelle ja turvallisuudelle, unionin tai kansallisen lainsäädännön turvaamille perusoikeuksille, sellaisten palveluiden luottamukselle tai eheydelle, jotka kuuluvat keskeisesti NIS2-direktiivissä tarkoitettujen keskeisten toimijoiden joukkoon tai muiden yleisten intressien suojaamiselle, jäsenvaltio voi vaatia toimijaa suorittamaan tarvittavat toimenpiteet, jotta tuote ei enää sisältäisi kyseistä riskiä. Tuote voidaan myös vetää markkinoilta kohtuullisessa ajassa riskin luonne huomioiden. Päätöksestä on heti informoitava komissiota ja jäsenvaltioita, jonka jälkeen komissio aloittaa välittömästi konsultaation jäsenvaltioiden ja relevanttien taloudellisten toimijoiden kanssa. Konsultaation perusteella päätetään, oliko toimi oikeasuhtainen. Komissiolla on toimivaltuus tällaisissa tilanteissa ja menettely on samanlainen, mitä edellisessä kappaleessa on kuvattu toimenpiteistä.

Erilaisia vaatimustenvastaisuutta koskevia tilanteita ovat asetusehdotuksen mukaan seuraavat: CE-merkintä on liitetty asetuksen vaatimusten vastaisesti tai sitä ei ole ollenkaan, EU:n vaatimustenmukaisuusilmoitusta ei ole tehty tai se on tehty virheellisesti, arviointilaitoksen tietoja ei ole liitetty taikka teknillinen dokumentointi ei ole saatavilla tai se ei ole valmis. Tällaisissa tilanteissa jäsenvaltiot voivat ryhtyä tarvittaviin toimiin rajoittaakseen tai kieltääkseen tuotteen tuotannon tai vetää sen markkinoilta.

Markkinavalvontaviranomaiset voivat ryhtyä yhteistyöhön, jonka tarkoituksena on kyberturvallisuuden varmistaminen ja kuluttajien suojaaminen. Tällaista yhteistyötä voisi tehdä sellaisten tuotteiden osalta, joissa usein on havaittavissa kyberturvallisuusriskejä. Myös komissio ja ENISA voivat ehdottaa vaatimustenmukaisuuden arviointiin yhteisiä toimenpiteitä, jotka perustuvat tietoihin mahdollisista vaatimusten noudattamatta jättämisestä. Tämä ei kuitenkaan saa johtaa markkinoiden vääristymiseen. Markkinavalvontaviranomaiset voivat myös toteuttaa koordinoituja samanaikaisia kontrollitoimia (sweeps) tietyille tuotteille tai tuotekategorioille.

3.6 Delegoitu toimivalta ja komiteamenettely

Luvussa määritellään komission toimivalta antaa delegoituja säädöksiä. Komissio voisi antaa delegoituja säädöksiä seuraavista asiakokonaisuuksista: Liitteen I soveltamatta jättämisestä tai osittaisesta soveltamisesta joihinkin tuotteisiin, liitteen III kriittisten tuotteiden listan muuttamisesta, liitteen IV EU:n vaatimustenmukaisuusilmoituksen sisällöstä ja liitteen V teknisen dokumentaation sisällöstä. Parlamentti ja neuvosto voisivat peruuttaa säädösvallan siirron milloin tahansa. Komission on konsultoitava kansallisia asiantuntijoita ennen delegoitujen säädösten antamista. Ehdotuksen mukaisten täytäntöönpanosäädösten käsittelyssä komissiota avustaa komitea.

3.7 Luottamuksellisuus ja sanktiot

Kaikkien osapuolten, jotka osallistuvat asetuksen täytäntöönpanoon, on noudatettava tiedon luottamuksellisuutta erityisesti immateriaalioikeuksien ja liikesalaisuuksien suojaamiseksi, tehokkaan täytäntöönpanon takaamiseksi, kansallisen ja yleisen turvallisuuden turvaamiseksi ja hallinnollisten toimenpiteiden loukkaamattomuuden takaamiseksi. Markkinavalvontaviranomaiset voivat vaihtaa tietoa keskenään ja komission kanssa. Vaatimukset eivät kuitenkaan vaikuta velvoitteisiin rikosoikeudellisessa prosessissa. Tietoa voidaan vaihtaa myös kolmansien

maiden kanssa, mikäli näiden maiden ja EU:n tai jäsenvaltion välillä on laadittu sopimus tiedon vaihdon luottamuksellisuudesta.

Jäsenvaltioiden olisi asetettava säännöt säännösten loukkausten sanktioista. EU:n yleisten periaatteiden mukaisesti sanktioiden tulisi olla tehokkaita, suhteellisia ja varoittavia. Sanktioissa olisi kyse hallinnollisista sanktioista. Jäsenvaltioilla olisi liikkumavaraa hallinnollisten sanktioiden toteuttamisessa, mutta ehdotuksessa säädettäisiin jäsenvaltioihin kohdistuvasta sanktiointivelvoitteesta sekä sanktion enimmäismäärästä, joita sääntelyn vastaisesta toiminnasta tulisi voida määrätä. Liitteen I keskeisten tietoturvavaatimusten ja asetuksen valmistajia koskevien vaatimusten rikkomisesta tulisi voida määrätä hallinnollisia maksuja enintään 15 miljoonaa euroa tai 2,5 prosenttia vuosittaisesta liikevaihdosta sen mukaan, kumpi on korkeampi. Muiden velvoitteiden osalta sanktio voisi olla enintään 10 miljoonaa euroa tai 2 prosenttia vuosittaisesta liikevaihdosta sen mukaan, kumpi on korkeampi. Väärän, harhaanjohtava tai epätäydellisen tiedon jakamisesta arviointilaitokselle tulisi voida määrätä enintään 5 miljoonan euron tai 1 prosentin vuosittaista liikevaihtoa vastaavan hallinnollisen maksun sen mukaan, kumpi on korkeampi. Hallinnollista maksua määrättäessä huomioidaan yksittäiset tapaukset ja siihen liittyvät olosuhteet. Niitä ovat loukkauksen luonne, laajuus, kesto ja sen vaikutukset, onko muut viranomaiset määränneet jo vastaavia maksuja sekä loukkaukseen syyllistyvän toimijan koko ja markkinaosuus. Tieto sanktiosta on ilmoitettava muille markkinavalvontaviranomaisille. Jokainen jäsenvaltio määrittää sen, missä määrin hallinnollisia maksuja voidaan määrätä viranomaisille. Hallinnolliset maksut voitaisiin määrätä kansallisen järjestelmän mukaisessa viranomaisessa. Maksuja voidaan määrätä muiden korjaavien tai rajoittavien toimenpiteiden yhteydessä.

3.8 Loppusäännökset

Nykyiset EU:n tyyppitarkastuksen sertifikaatit ja hyväksynnän päätökset, jotka koskevat tuotteiden kyberturvallisuusvaatimuksia olisivat voimassa 48 kuukautta ellei niiden määräaika lopu ennen sitä tai ellei unionin lainsäädännössä muuta täsmennetä. Ennen voimaantuloa markkinoille tulleisiin tuotteisiin sovelletaan asetusta vain, jos niihin tulee merkittäviä muutoksia. Raportointivelvoitteet tuotteen haavoittuvuuksista koskevat kuitenkin myös ennen voimaantuloa markkinoille tulleisiin tuotteisiin.

Asetuksen toimivuutta arvioidaan neljän vuoden välein ja ensimmäisen kerran kolmen vuoden kuluttua sen soveltamisen aloittamisesta. Asetuksen soveltaminen alkaisi kaksi vuotta sen voimaantulosta. Kuitenkin haavoittuvuuksien raportointivelvoitteita sovellettaisiin jo vuoden kuluessa asetuksen voimaantulosta.

4 Ehdotuksen oikeusperusta ja suhde suhteellisuus- ja toissijaisuusperiaatteisiin

Ehdotuksen oikeusperusta on Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 114 artikla, jonka nojalla voidaan antaa sisämarkkinoiden toteuttamista ja toimintaa ohjaavia säännöksiä jäsenvaltioiden lakien, asetusten ja hallinnollisten määräysten lähentämiseksi. Ehdotusta käsitellään noudattaen tavallista lainsäätämisjärjestystä, jossa Euroopan parlamentti ja neuvosto hyväksyvät yhdessä asetuksen. Neuvostossa edellytetään määräenemmistöpäätöksentekoa.

Ehdotuksen tarkoituksena on harmonisoida soveltamisalaan kuuluvien tuotteiden kyberturvallisuusvaatimukset jäsenvaltioissa ja poistaa näin esteitä tavaroiden vapaalle liikkuvuudelle. Komissio on perustellut oikeusperustan valintaa muun muassa sillä, että nykyinen EU-sääntely, jota sovelletaan digitaalisia elementtejä sisältävien tuotteiden tiettyihin turvallisuusaspekteihin tai tuotevastuukysymyksiin perustuu SEUT 114 artiklaan. Komissio perustelee harmonisoinnin

tarvetta sillä, että kansallisella tasolla jäsenvaltiot ovat jo alkaneet toteuttaa toimia, joilla edellytetään kyberturvallisuusseikkojen kehittämistä digitaalisten tuotteiden myyjiltä. Samaan aikaan digitaalisten tuotteiden kyberturvallisuuteen liittyy vahva jäsenvaltioiden rajat ylittävä ulottuvuus, sillä tuotteita myydään ja käytetään sekä mahdolliset kyberhäiriöt tuotteissa heijastuvat koko sisämarkkinalla. Ehdotuksella harmonisoitaisiin ja yhdenmukaistettaisiin EU:n sisämarkkinoilla kyberturvallisuusvaatimukset tuotteille, joissa on digitaalisia elementtejä.

Komissio katsoo ehdotuksen olevan Euroopan unionista tehdyn sopimuksen (SEU) 5 artiklassa tarkoitetun toissijaisuusperiaatteen mukainen. Komission mukaan ehdotuksen tavoitteet eivät ole tehokkaasti toteutettavissa jäsenvaltioiden kansallisen lainsäädännön tasolla kyberturvallisuusuhkien kansainvälisen luonteen vuoksi. Jäsenvaltioiden eriävät kansalliset lähestymistavat voisivat luoda oikeudellista epävarmuutta ja esteitä tuotteiden liikkuvuudelle. EU:n yhteinen lähestymistapa parantaisi käyttäjien luottamusta tuotteisiin, joissa on digitaalisia elementtejä, sekä turvaisi oikeusvarmuutta ja toimijoiden tasapuolisia toimintaedellytyksiä sisämarkkinoilla.

Komissio katsoo ehdotuksen olevan SEU 5 artiklassa tarkoitetun suhteellisuusperiaatteen mukainen eikä ylitä sitä, mikä on tarpeen sen tavoitteiden saavuttamiseksi tai aiheuta suhteettomia kustannuksia. Tuotteille asetettaisiin niiden elinkaaren kattavia, riskiin suhteutettuja ja teknologianeutraaleja kohtuullisia vaatimuksia. Kyberturvallisuudelle asetettavat vaatimukset olisivat standardointien kautta riskiperusteisia. Komissio arvioi, että sääntelyn johdosta tuotteiden kyberturvallisuustason noususta saatava hyöty ylittäisi ne kustannukset, joita sääntelyn noudattamisesta yrityksille aiheutuisi.

Valtioneuvoston alustava kanta on, että komission näkemykset ehdotuksen oikeusperustasta sekä toissijaisuus- ja suhteellisuusperiaatteista ovat asianmukaisia. Asetuksen ehdotettu soveltamisala on kuitenkin laaja, mikä edellyttää oikeusperustakysymyksen tarkastelua sääntelyn jatkokäsittelyn aikana. Komissiolle delegoitavan säädösvallan ala vaikuttaa myös arviointiin.

5 Ehdotuksen vaikutukset

5.1 Komission vaikutustenarviointi

Komissio on tehnyt laajan arvioinnin toimintavaihtoehdoista ja niiden vaikutuksista ehdotuksen tavoitteiden saavuttamiseksi ja taustalla olevaan ongelmaan puuttumiseksi.

Komission vaikutustenarvioinnin nojalla esityksellä olisi merkittäviä hyötyjä. Yrityksille hyödyksi olisi, että ehdotus estäisi toisistaan eroavien kyberturvallisuusvaatimuksien syntymisen EU:n sisämarkkinalla, mikä alentaisi vaatimustenmukaisuudesta aiheutuvia kustannuksia. Ehdotus alentaisi tietoturvaloukkausten määrää, kun markkinoilla olevien tuotteiden turvallisuuden taso paranisi, mikä alentaisi tietoturvaloukkauksista ja niiden selvittämisestä aiheutuvia kustannuksia. Komissio arvioi, että ehdotus voisi alentaa koko EU:n tasolla tietoturvaloukkauksista yrityksille aiheutuvia kustannuksia jopa 180 – 290 miljardia euroa. Ehdotus lisäisi yrityksien liikevaihtoa lisäämällä soveltamisalaan kuuluvien tuotteiden kysyntää sekä parantaisi yrityksien ja niiden soveltamisalaan kuuluvien tuotteiden mainetta myös EU:n ulkopuolella. Käyttäjille ehdotus lisäisi tietoturvaominaisuuksien läpinäkyvyyttä ja auttaisi tuotteiden tietoturvallista käyttöä. Kuluttajat ja kansalaiset hyötyisivät myös ehdotuksen tuotteille aiheuttamista vaikutuksista, jotka parantaisivat yksityisyyden ja tiedon luottamuksellisuuden suojaa sekä tietosuojaa.

Komissio arvioi ehdotuksen merkittävimmiksi haitoiksi uusien vaatimuksien noudattamisesta aiheutuvat kustannukset. Ehdotus lisäisi vaatimustenmukaisuuden noudattamisesta sekä nou-

dattamisen valvonnasta aiheutuvia kustannuksia yrityksille, ilmoitetuille laitoksille ja viranomaisille. Ehdotus lisäisi suoraan akkreditointien tarvetta ja markkinavalvontaan osoitettavan viranomaisen työmäärää. Soveltamisalaan kuuluvien ohjelmistojen kehittäjille ja tuotteiden valmistajille ehdotus lisäisi suoraan kustannuksia, jotka aiheutuvat uusien turvallisuusvaatimuksien noudattamisesta, vaatimustenmukaisuuksien arvioinnista, dokumentaatiosta ja raportoinnista. Komissio arvioi näiden kustannuksen suuruusluokaksi koko EU:n tasolla noin 29 miljardia euroa, kun soveltamisalaan kuuluvan markkinan koko olisi noin 1 485 miljardia euroa. Ehdotus voisi nostaa soveltamisalaan kuuluvien tuotteiden hintoja, mikä aiheuttaisi haittaa käyttäjille, kuluttajille ja muille ohjelmistojen ja tuottajien ostajille.

5.2 Kansalliset vaikutukset

Ehdotuksen kansallisia vaikutuksia Suomeen ja suomalaisiin toimijoihin arvioidaan tarkemmin käsittelyn edetessä.

5.2.1 Vaikutukset tuotteiden käyttäjiin

Ehdotuksella tulee olemaan vaikutuksia kuluttajille ja muille soveltamisalaan kuuluvien tuotteiden tilaajille ja käyttäjille, kuten yrityksille. Markkinoille saatettavat tuotteet olisivat nykyistä korkeammalla tasolla niiden kyberturvallisuusominaisuuksien kannalta ja kuluttajilla olisi parempi pääsy tietoon tuotteiden kyberturvallisuusominaisuuksista, millä olisi merkittäviä hyödyllisiä vaikutuksia tuotteiden käyttäjille. Kyberturvallisuusvaatimusten parantuessa tuotteiden tilaajat ja käyttäjät voivat luottaa kyberturvallisuuden perustasoon kaikissa tuotteissa. Ehdotus parantaisi yksityisyyden suojan ja viestinnän luottamuksellisuuden toteutumista sekä sähköisen viestinnän tietosuojaa. Kuitenkin voidaan arvioida, että kyberturvallisuusvaatimuksien täyttäminen aiheuttaa uusia kustannuksia, mistä johtuen on ennakoitavissa, että tuotteiden hinta voi nousta tai tuotteista voidaan karsia ominaisuuksia, jotka vaarantaisivat kyberturvallisuuden tasoa tai vaikuttaisivat vaatimuksien soveltamiseen tuotetta markkinoille asetettaessa.

5.2.2 Vaikutukset valmistajiin, maahantuojiin ja jakelijoihin

Ehdotuksella olisi vaikutuksia sen soveltamisalaan kuuluvien tuotteiden valmistajille, jakelijoille ja maahantuojille Suomessa. Erityisesti valmistajille tulisi vaatimustenmukaisuuden noudattamisesta uusia kustannuksia. Ehdotus kasvattaisi digitaalisia elementtejä sisältävien tuotteiden valmistamisesta, jakelemisesta ja maahantuonnista aiheutuvia kustannuksia lisääntyvien kyberturvallisuusvaatimuksien myötä. Toisaalta on huomattava, että osa yrityksistä noudattaa jo nykyisellään ehdotuksen kaltaisia turvallisuustoimenpiteitä, joten vaikutukset eivät siten jakaudu yhtäläisesti kaikkiin valmistajiin. Ehdotus parantaisi yleisesti markkinoilla olevien tuotteiden turvallisuustasoa kyberympäristössä, josta olisi välillisesti merkittäviä hyötyjä. Lisäksi digitaalisia elementtejä sisältävä tuote täyttäisi kerralla koko EU:n tasolla yhteisesti harmonisoidut kyberturvallisuusvaatimukset, mikä helpottaisi suomalaisten valmistajien ja jakelijoiden vientiä sisämarkkinoille, ja vahvistaisi niiden asemaa ja mahdollisuuksia myös globaaleilla markkinoilla. On huomattava, että kriittisyyden arviointi ja sen kautta arviointivaatimukset perustuvat asetusehdotuksessa osittain tuotteen loppukäytön perusteella, mutta valmistajalla ei aina ole näkymää siihen, missä kaikkialla tuotetta tullaan lopulta käyttämään. Lisäksi kaikilla taloudellisilla toimijoilla ei välttämättä ole resursseja vaatimusten täyttämiseksi, mikä voi vaikuttaa liiketoimintaan.

5.2.3 Vaikutukset arviointilaitostoimintaan

Tuotteiden vaatimustenmukaisuuden arvioinnin lisääntyessä tarvitaan myös laajemmin arviointilaitoksia ja sitä kautta myös arviointia tekeviä asiantuntijoita. Kansallisesti ehdotuksen siirtymäkaudella haasteeksi voisi muodostua tuotteiden ulkopuolisten vaatimustenmukaisuusarviointien toteuttaminen, koska Suomessa toimii rajallinen määrä vaatimustenmukaisuusarviointeja toteuttavia ilmoitettuja laitoksia. Lisäksi jo nykyisellään on tunnistettu haasteeksi se, että tietoturva-alan ammattilaisia on saatavilla rajoitetusti ja työvoimasta käydään kovaa kilpailua. Myös koulutustarve on ilmeinen sekä käyttäjissä, valmistajissa, maahantuonnissa, arviointilaitoksissa sekä viranomaisissa. Alustavissa keskusteluissa sidosryhmien kanssa on tunnistettu, että tiettyjen tuotekategorioiden arviointi edellyttää lisäksi kyseisen toimialan erityispiirteiden tunnistamista, mikä rajaa entisestään asiantuntevan tietoturva-arviointia tekevän henkilöstön joukkoa. Tällaisten henkilöiden tarve on kuitenkin ilmeinen, jotta arviointitoiminnalla saataviin hyötyihin voidaan päästä. Toisaalta arviointitoiminnan laajentaminen luo myös liiketoimintamahdollisuuksia niin kansallisesti kuin EU:n tasollakin.

5.2.4 Viranomaisvaikutukset

Ehdotuksen täytäntöönpanolla olisi olennaisia vaikutuksia viranomaisten toimintaan. Digitaalisia elementtejä sisältävien tuotteiden markkinavalvontaan liittyvät viranomaistehtävät olisivat uusia, ja ne edellyttäisivät uusia resursseja kansallisesti. Asetusehdotus sisältäisi nimenomaisen velvoitteen jäsenvaltioille huolehtia markkinavalvontaviranomaisten resursseista. Ehdotuksen täytäntöönpanolla olisi siten budjettivaikutuksia, joiden määrää arvioidaan neuvotteluiden edetessä. Budjettivaikutuksen voidaan ennakoida olevan vähäistä suurempia ottaen huomioon sääntelyn soveltamisalaan kuuluvien tuotteiden laajan määrän ja siten markkinavalvontatoiminnan edellyttämän resursoinnin. Toinen viranomaisten toimintaan vaikuttava seikka olisi ilmoitettujen laitosten hakemuksien käsittelystä ja valvonnasta vastaavan viranomaisen tehtävä. On todennäköistä, että ehdotus aiheuttaa kasvavan tarpeen arviointilaitoksille, jolloin se edellyttää myös vastaavalla tavalla viranomaisresurssien vahvistamista niin määrällisesti kuin osaamisen osalta.

Tietosuojavaltuutetulle aiheutuisi lisätyövaikutuksia asetusehdotuksen 41 artiklan nimenomaisesta markkinoiden valvontaviranomaisten ja tietosuojaviranomaisten yhteistyötä koskevasta säännöksestä. Tarkat resurssivaikutukset riippuisivat siitä, missä määrin lopullinen artikla velvoittaisi yhteistyöhän ja tarkoittaisiko ehdotettu säännös uutta tehtävää.

Ehdotus tulee todennäköisesti edellyttämään myös täydentävää kansallista sääntelyä koskien esimerkiksi tiedonvaihtovelvoitteita erityisesti markkinavalvontaviranomaisten, tietosuojavaltuutetun sekä kyberturvallisuusasetuksen mukaisten valvontaviranomaisten välillä, jotta viranomaiset kykenevät suorittamaan niille säädettävät tehtävät.

6 Ehdotuksen suhde perustuslakiin sekä perus- ja ihmisoikeuksiin

Ehdotettu sääntely on merkityksellistä perustuslain 10 §:n 1 momentissa turvatun yksityiselämän ja henkilötietojen suojan, 10 §:n 2 momentissa turvatun luottamuksellisen viestinnän suojan kannalta ja jotka on turvattu myös EU:n perusoikeuskirjan 7 ja 8 artiklassa. Ehdotus on merkityksellinen myös perustuslain 18 §:n 1 momentissa turvatun elinkeinovapauden kannalta, josta on säädetty myös perusoikeuskirjan 15 artiklassa. Lisäksi ehdotuksella on merkitystä perustuslain 21 §:ssä turvatun oikeusturvan kannalta, joka on turvattu perusoikeuskirjan 47 artiklassa. Arviointia on tarpeen tehdä myös rikosoikeudellisen laillisuusperiaatteen suhteen ja ehdotuksessa on lisäksi ehdotuksia säädöksiksi, joissa julkista hallintotehtävää siirretään muulle kuin viranomaisille. Tällä on merkitystä perustuslain 124 §:n kannalta.

6.1 Yksityiselämän suoja

Digitaalisia elementtejä sisältäville tuotteille asetettavat kyberturvallisuusvaatimukset toisaalta edistäisivät yksityiselämän suojan ja luottamuksellisen viestinnän suojan toteutumista näiden tuotteiden käytössä. Asia on siten merkityksellinen perustuslain 10 §:ssä turvatun yksityiselämän ja luottamuksellisen viestin suojan kannalta. Ehdotuksen arvioidaan edistävän näiden perusoikeuksien toteutumista erityisesti siksi, että tuotteiden tietoturvaominaisuuksien parantuminen vaikuttaa suoraan viestinnän luottamuksellisuuden säilymiseen ja sitä kautta yksityiselämän suojaan. Ehdotuksella on tästä syystä merkitystä myös henkilötietojen suojalle. Horisontaalisilla kyberturvallisuusvaatimuksilla komission mukaan vaikutetaan erityisesti henkilökohtaisen datan, kuten henkilötietojen turvallisuuteen suojaamalla luottamuksellisuutta, eheyttä ja saatavuutta. Asetusehdotuksen johdanto-osan 17 kappaleen mukaan asetuksen ei tulisi rajoittaa yleisen tietosuoja-asetuksen (EU) 2016/679 kanssa.

6.2 Elinkeinovapaus ja oikeus työhön

Ehdotuksen vaatimuksilla olisi elinkeinonvapautta rajoittava ulottuvuus, koska niiden vastaiset tuotteet eivät olisi sallittuja sisämarkkinoilla. Ehdotus on siten merkityksellinen perustuslain 18 §:ssä suojatun elinkeinovapauden kanssa, jonka mukaan jokaisella on oikeus lain mukaan hankkia toimeentulonsa valitsemallaan työllä, ammatilla tai elinkeinolla. Elinkeinovapauden rajoituksella on kuitenkin tarkoitus parantaa markkinoille tulevien tuotteiden tietoturvaominaisuuksia ja sen kautta edistää muiden oikeushyvien toteutumista, minkä vuoksi rajoitukset voidaan nähdä perusteltuina.

Vastaavasti ehdotuksella on merkitystä elinkeinonvapauteen myös siitä näkökulmasta, että arviointilaitosten toiminta perustuisi luvanvaraisuuteen. Vaatimus viranomaisen myöntämästä luvasta työn, ammatin tai elinkeinon harjoittamiseen merkitsee rajoitusta perustuslain 18 §:n 1 momentissa turvattuun elinkeinovapauteen. Säännökset elinkeinonvapauden rajoittamiselle tulee olla täsmällisiä ja tarkkarajaisia ja lisäksi rajoittamisen laajuuden ja edellytysten tulee ilmetä laista. Perustuslakivaliokunta on pitänyt tärkeänä, että säännökset luvan edellytyksistä ja pysyvyydestä antavat riittävän ennustettavuuden viranomaistoiminnasta.

6.3 Oikeusturva

Perustuslain 21 §:n 1 momentin mukaan jokaisella on oikeus saada asiansa käsitellyksi asianmukaisesti ja ilman aiheetonta viivytystä lain mukaan toimivaltaisessa tuomioistuimessa tai muussa viranomaisessa sekä oikeus saada oikeuksiaan ja velvollisuuksiaan koskeva päätös tuomioistuimen tai muun riippumattoman lainkäyttöelimen käsiteltäväksi. Ehdotuksessa on markkinavalvontatoimenpiteitä ja täytäntöönpanoa koskevia säännöksiä siitä, millaisiin toimenpiteisiin markkinavalvontatoimenpitein voidaan ryhtyä ja millä edellytyksillä. Viranomaisten toimivallasta ja toimivaltuuksista tulee perustuslain 2 §:n 3 momentin nojalla säätää lailla. Asetuksen suorasta sovellettavuudesta huolimatta eräistä esimerkiksi viranomaisten toimivaltuuksia koskevista asioista saattaa olla tarpeen säätää kansallisessa laissa.

Ehdotukseen sovellettaisiin yleistä markkinavalvonta-asetusta (EU) 2019/1020, jonka 18 artiklassa on säädetty talouden toimijan menettelyllisistä oikeuksista, mikä tarkoittaa erityisesti oikeutta tulla kuulluksi. Markkinavalvonta-asetusta kansallisesti täydentää horisontaalinen laki eräiden tuotteiden markkinavalvonnasta (1137/2016), jossa on säädetty tarkemmin viranomaisten valvontatoimenpiteistä ja muun muassa muutoksenhakumenettelystä. Oletettavaa on, että lakia sovellettaisiin myös jatkossa ehdotetun asetuksen markkinavalvontaan.

Ehdotuksen mukaan markkinavalvontatoimenpiteiden yhtenäisyyttä EU:n alueella varmistettaisiin erityisin 44 artiklassa säädetyin toimenpitein, joiden mukaan komissio voi aloittaa jäsenmaiden ja taloudellisen toimijan välisen konsultaation, mikäli markkinavalvontatoimenpidettä

vastustetaan jäsenvaltion toimesta. Komissio päättäisi tämän konsultaation perusteella, onko toimenpide oikeasuhtainen.

6.4 Rikosoikeudellinen laillisuusperiaate

Ehdotuksen 53 artiklassa on säännökset hallinnollisista maksuista, joita voitaisiin säätää turvallisuusvaatimuksien rikkomisesta, muiden asetuksen vaatimusten rikkomisesta sekä harhaanjohtavan tai väärän tiedon antamisesta valvontaviranomaiselle. Perustuslakivaliokunnan vakiintuneen tulkinnan mukaan tällaiset maksut eivät ole perustuslain 81 §:n mielessä veroja tai maksuja vaan lainvastaisesta teosta määrättäviä sanktioluonteisia hallinnollisia seuraamuksia, jonka se on rinnastanut rikosoikeudelliseen seuraamukseen (PeVL 14/2013 vp, PeVL 17/2012 vp, PeVL 9/2012 vp, s. 2/I, PeVL 55/2005 vp, s. 2/I ja PeVL 32/2005 vp, s. 2/II). Perustuslakivaliokunta on katsonut, että vaikka hallinnolliseen seuraamukseen ei sellaisenaan voida soveltaa rikosoikeudellisen laillisuusperiaatteen täsmällisyysvaatimusta, ei tarkkuuden vaatimusta voida tällaisen sääntelyn yhteydessä sivuuttaa. Säännösten tulee täyttää myös sanktioiden oikeasuhtaisuuteen liittyvät vaatimukset (PeVL 37/2021 vp, kohta 32).

Perustuslakivaliokunta on arvioinut vastaavan kaltaista säännösehdotusta tekoälyasetuksen yhteydessä. Se on kiinnittänyt huomiota siihen, että tekoälyasetuksessa oli ehdotettu vastaavasti, mitä käsillä olevassa ehdotuksen 53 (4) artiklassa siitä, että hallinnollinen seuraamus voidaan määrätä silloin, jos muita kun turvallisuutta koskevia velvoitteita ei noudateta, joka vaikuttaisi merkitsevän sitä, että sanktioitavien tekojen tai laiminlyöntien piiriin lukeutuu kaikenlainen asetuksen rikkominen. Perustuslakivaliokunta ei sinällään ole pitänyt tätä perustuslain kannalta kiellettynä sääntelytekniikkana, mutta on kiinnittänyt huomiota siihen, että silloin kun asetuksen seuraamussääntely voi merkitä, että mikä tahansa osittainenkin laiminlyönti voi muodostua virhemaksulla sanktioitavaksi, se ei täyttäisi hallinnolliselle seuraamusmaksulle asetettuja täsmällisyyden ja tarkkarajaisuuden vaatimuksia, eikä näin avoimena ja ennakoimattomuutta luovana vaikuta myöskään oikeasuhtaiselta elinkeinovapauden rajoitukselta (PeVL 37/2021 vp, kohdat 35-36). Ehdotus siitä, että seuraamusmaksujen määräämisestä viranomaiselle, jäisi kansallisen harkinnan varaan, olisi linjassa perustuslakivaliokunnan näkemyksen kanssa. Se on painottanut, että sanktioiden määräämiseen tulisi liittyä riittävä kansallinen liikkumavara erityisesti sen huomioimiseksi, että Suomessa ei voida määrätä hallinnollisia seuraamusmaksuja viranomaisille, sillä viranomaisille voidaan määrätä ainoastaan rikosoikeudellisia seuraamuksia. (PeVL 37/2021 vp, kohta 40)

6.5 Hallintotehtävän antaminen muulle kuin viranomaiselle

Ilmoitetun laitoksen toiminnan kohdalla kyse julkisen hallintotehtävän siirtämisestä muulle kuin viranomaiselle, josta on säädetty perustuslain 124 §:ssä. Sen mukaan julkinen hallintotehtävä voidaan antaa muulle kuin viranomaiselle vain lailla tai lain nojalla ja vain, jos se on tarpeen tehtävän tarkoituksenmukaiseksi hoitamiseksi eikä vaaranna perusoikeuksia. Merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan kuitenkin antaa vain viranomaiselle ja vain, jos se on tarpeen tehtävän tarkoituksenmukaiseksi hoitamiseksi. Asetusehdotuksessa ilmoitetuille laitoksille annettaisiin viranomaiselle kuuluvia tehtäviä, koska laitokset vahvistaisivat digitaalisen elementin sisältävien tuotteiden vaatimustenmukaisuuden. Tällaista toimintaa ei ole pidetty merkittävänä julkisen vallan käyttönä ja toisaalta viranomaisten mahdollisuudet hoitaa tämän tyyppistä tehtävää ovat rajalliset, jolloin toiminnan tehokkuus voisi kärsiä ja markkinoille tulo viivästyä.

Alihankinnan osalta ehdotuksessa on annettu mahdollisuus käyttää myös alihankintaa arviointitoiminnassa. Tällaisessa tilanteessa ilmoitetun laitoksen olisi varmistuttava siitä, että alihank-

kija täyttää ilmoitettuja laitoksia koskevat vaatimukset ja ilmoittaa tästä ilmoituksista vastaavalle viranomaiselle. Tällaiseen edelleen siirtämiseen perustuslakivaliokunta on suhtautunut lähtökohtaisesti kielteisesti (PeVL 26/2017 vp), mutta ehdotonta kieltoa tällaiselle siirtämiselle ei kuitenkaan ole ollut tilanteessa, jossa kyse olisi teknisluonteisesta tehtävästä ja jossa alihankkijana kohdistuu samat laatuvaatimukset ja vastaava valvonta kuin alkuperäiseen palveluntuottajaan (PeVL 6/2013 vp. s. 4).

6.6 Toimivallan siirto

Ehdotuksessa on ehdotettu siirrettäväksi komissiolle toimivaltaa asetuksen liitteiden osalta. Liitteen 1 osalta komissio voisi antaa delegoituja säädöksiä liitteen vaatimusten soveltamatta jättämisestä joko kokonaan tai osittain. Liitteen III osalta komissio voisi antaa delegoituja kriittisiä tuotteita koskevan listauksen sisällöstä. Tekoälyasetuksen osalta perustuslakivaliokunta on katsonut hyvin vastaavan kaltaisten säädösehdotusten kohdalla kyseessä olevan sääntelyn soveltamisalan mahdollisesta laajentamisesta ja se on katsonut niiden antavan komissiolle liian lavean vallan muuttaa asetusta. Euroopan unionista tehdyn sopimuksen 290 artiklan mukaan lainsäätämisjärjestyksessä hyväksyttävässä säädöksessä voidaan siirtää komissiolle valta antaa muita kuin lainsäätämisjärjestyksessä hyväksyttäviä, soveltamisalaltaan yleisiä säädöksiä, joilla täydennetään tai muutetaan lainsäätämisjärjestyksessä hyväksyttyjä tiettyjä säännöksiä muilta kuin sen keskeisiltä osin. Perustuslakivaliokunta on tässä yhteydessä pitänyt tarpeellisena täsmentää sääntelyä, sillä asetuksen soveltamisalan täsmällisuus ja tarkkarajaisuus on merkityksellistä myös elinkeinovapauden kannalta. (PeVL 37/2021 vp, kohdat 41-42)

7 Ahvenanmaan toimivalta

Ahvenanmaan itsehallintolain (1144/1991) 27 §:n 10 kohdan mukaan valtakunnalla on lainsäädäntövalta muun muassa sopimatonta menettelyä elinkeinotoiminnassa, kilpailun edistämistä ja kuluttajansuojaa koskevissa asioissa. Ehdotuksen horisontaalisuudesta johtuen se sivuaa kuitenkin sellaisia asioita, jotka kuuluvat myös maakunnan lainsäädäntövaltaan johtuen siitä, että esimerkiksi tietojärjestelmiä käytetään osana kyseisiä toimintoja ja ehdotuksen turvallisuutta koskevat vaatimukset koskevat siten myös näitä järjestelmiä. Ehdotus on merkityksellinen siten itsehallintolain 18 §:n 12–14 ja 20–24 kohtien perusteella.

8 Ehdotuksen käsittely Euroopan unionin toimielimissä ja muiden jäsenvaltioiden kannat

Komissio antoi asetusehdotuksen 15.9.2022.

Ehdotuksen käsittely on alkanut neuvoston horisontaalisessa kybertyöryhmässä 23.9.2022. Ehdotukseen on suhtauduttu lähtökohtaisesti positiivisesti.

Ehdotuksen käsittely Euroopan parlamentissa ei ole vielä alkanut.

9 Ehdotuksen kansallinen käsittely

U-kirjelmä on valmisteltu liikenne- ja viestintäministeriössä yhteistyössä muiden ministeriöiden ja virastojen kanssa.

Luonnos U-kirjelmäksi on käsitelty viestintäjaostossa (EU-19) 7.10.2022–12.10.2022 ja kilpailukykyjaostossa (EU-8) 7.10.2022–12.10.2022. Lisäksi ehdotuksesta järjestettiin kuulemistilaisuus 23.9.2022.

10 Valtioneuvoston kanta

Valtioneuvosto kannattaa asetusehdotuksen tavoitetta saattaa markkinoille kyberympäristössä turvallisempia tuotteita, joiden turvallisuusominaisuuksilta vaaditaan hyvätasoisuutta sekä turvallisuusominaisuudet ja -vaatimukset ovat läpinäkyvämpiä niitä käyttäville kuluttajille ja yrityksille. Ehdotuksella on mahdollisuus horisontaalisena säädöksenä konkreettisesti parantaa kaikkien yhteiskunnan toimijoiden tietoturvaa. Valtioneuvosto pitää verkkoon kytkettyjen laitteiden ja ohjelmistojen turvallisuuden parantamista merkittävänä kehityskohteena kyberturvallisuussektorilla. Valtioneuvosto pitää kannatettavana, että vastuuta tuotteiden turvallisuudesta kyberympäristössä kohdistetaan nykyistä enemmän käyttäjältä valmistajalle riippumatta siitä, missä sisämarkkinoille asetettavat tuotteet valmistetaan. Verkkoon kytkettyjen laitteiden ja ohjelmistojen määrän kasvaessa ja niiden merkityksen korostuessa kasvaa myös tarve varmistua niiden turvallisuudesta ja mahdollisiin haavoittuvuuksiin reagoimisesta tuotteen elinkaaren aikana.

Valtioneuvosto kannattaa asetusehdotuksen laajaa soveltamisalaa, jotta digitaalisen elementin sisältävien tuotteiden turvallisuusvaatimukset soveltuisivat mahdollisimman laajasti markkinoilla. Pilvipalveluita hyödyntävien tuotteiden osalta tulisi pyrkiä varmistumaan siitä, että ehdotus muodostaa selkeät rajat vastuiden ja velvoitteiden osalta ja on selkeä suhteessa muihin pilvipalveluihin liittyviin säädöksiin kuitenkaan heikentämättä ehdotuksen tavoitteita tai rajaamatta pilviteknologiaa hyödyntäviä tuotteita soveltamisalan ulkopuolelle. Valtioneuvosto katsoo, että neuvottelujen kuluessa asetuksen soveltamisalasta tulee pyrkiä saamaan mahdollisimman selkeä. Valtioneuvosto pitää tärkeänä, että nykyinen ja valmisteilla oleva EU-lainsäädäntö muodostaisi selkeän ja eheän kokonaisuuden siten, että eri toimijoille asetettavat vaatimukset ovat selkeitä ja oikeasuhtaisia, eivätkä muodosta ristiriitaa sovellettavien EU-oikeudesta johtuvien oikeudellisten vaatimusten kanssa. Päällekkäistä sääntelyä on vältettävä ja sääntelystä aiheutuvan taakan vähentämiseksi säädösten keskinäisten suhteiden on oltava selviä. Myös suhdetta esimerkiksi datasäädösehdotukseen, yleisen tietosuoja-asetuksen, NIS2-direktiiviin sekä CER-direktiiviin (Critical Entities Resilience Directive) sekä juuri annettuihin komission ehdotuksiin tuotevastuusta (COM (2022) 495 final) sekä tekoälyyn liittyvästä vastuusta (COM (2022) 496 final) on tarpeen arvioida neuvottelujen kuluessa tarkemmin siten, että säädökset muodostaisivat soveltamiseltaan mahdollisimman eheän kokonaisuuden.

Valtioneuvosto pitää riskiperusteista lähestymistapaa vaatimuksien ja velvoitteiden asettamisessa lähtökohtaisesti kannatettavana. Valtioneuvosto katsoo, että yleisesti digitaalisen elementin sisältävistä tuotteista on hyvä riskiperusteisesti erottaa kriittisemmät tuotteet, joiden turvallisuusvaatimusten täyttymistä valvottaisiin vahvemmin ulkopuolisen ilmoitetun laitoksen toimesta. Valtioneuvosto kuitenkin pitää tärkeänä, että asetuksessa huomioidaan tuotteiden pääasiallinen käyttötarkoitus.

Asetusehdotuksen liitteessä kuvatut vaatimukset ovat lähtökohtaisesti sellaisia, joiden huomioimista digitaalisen elementin sisältävissä tuotteissa voidaan pitää valtioneuvoston näkemyksen mukaan tärkeänä. Vaatimuksien kattavuutta ja asianmukaisuutta on arvioitava neuvotteluiden edetessä. Valtioneuvosto pitää kannatettavana myös ehdotettua vaatimusta hyväksikäytettyjen haavoittuvuuksien ilmoittamisesta, jotta tarvittaviin suojaaviin toimenpiteisiin voidaan ryhtyä tuotteen käyttäjien parissa ja tieto näiden toimien tarpeesta saatetaan tehokkaasti tarvittaville toimijoille. Valtioneuvosto pitää tarpeellisena vaatimuksia maahantuojille ja jakelijoille, joiden merkitys korostuu erityisesti silloin, kun tuotteita tuodaan EU:n ulkopuolelta sisämarkkinoille tai tuotteen valmistajan toiminta päättyy tuotteen elinkaaren aikana. Valtioneuvosto pitää kannatettavana lähtökohtaa, jossa vaatimukset asetetaan ensisijaisesti valmistajalle ja toissijaisesti jakelijalle tai maahantuojalle. Lisäksi jatkovalmistelussa on tarpeen arvioida etämyynnin sekä

verkkomarkkinapaikkojen erityisvelvoitteita sekä ehdotuksen suhdetta kolmansissa valtioissa sijaitseviin valmistajiin.

Valtioneuvosto pitää vaatimustenmukaisuuden arviointia olennaisena osana turvallisuusvaatimusten täyttymisen varmistamista. Valtioneuvosto kuitenkin katsoo, että vaatimustenmukaisuuden arvioinnissa tulee kiinnittää erityistä huomiota siihen, ettei eri säädösten mukaisista prosesseista, kuten sertifioinneista, synny keskenään päällekkäisiä ja olemassa olevia järjestelmiä hyödynnettäisiin mahdollisimman pitkälle. Valtioneuvosto katsoo, että vaatimustenmukaisuuden täyttymisen arvioinnissa on tarpeen hyödyntää mahdollisimman pitkälle hyväksi havaittuja, jo olemassa olevia menettelyjä ja asettaa uusia yhteisiä vaatimuksia vain silloin, kun niitä ei ole olemassa. Vaatimustenmukaisuuden arviointiprosessissa tulee pyrkiä läpinäkyvyyteen ja ennustettavuuteen, eikä siitä saa aiheutua tarpeetonta haittaa uusien teknologioiden markkinoille saattamiselle ja EU-alueen kilpailukyvylle.

Vaatimustenmukaisuuden arviointivelvoitteiden osalta valtioneuvosto pitää tärkeänä, että ulkopuolista arviointia vaadittaisiin riskiperusteisesti vain sellaisilta tuotteilta, joilla on erityistä merkitystä kyberturvallisuuden kannalta ja lähtökohtaisesti muiden tuotteiden osalta riittäisi valmistajan itsearviointi. Ulkopuolisen arvioinnin tarpeen merkittävällä lisäämisellä voidaan pahimmillaan merkittävästi hidastaa tuotteiden markkinoille pääsyä, mikäli asiantuntevia arviointilaitoksia ei ole riittävästi tarjolla. Valtioneuvosto katsoo, että vaatimustenmukaisuuden arviointi tulee toteuttaa tavalla, jolla on tosiasiallista vaikutusta ja arviointia tuotteen turvallisuusominaisuuksien kannalta. Valtioneuvosto pitää myös kyberturvallisuutta koskevien vaatimusten osalta ehdotusta CE-merkinnästä yhtenä hyvänä tapana ilmaista vaatimustenmukaisuuden täyttyminen. Olennaista on, että tuotteiden kyberturvallisuuden vaatimustenmukaisuus kävisi tuotteesta selkeästi ilmi.

Ilmoitettujen laitosten vaatimusten osalta valtioneuvosto pitää tärkeänä, että laitosten henkilöstön osaaminen ja tekniset valmiudet ovat korkealla tasolla, jotta arvioinnilla saatavat hyödyt voidaan saavuttaa. Valtioneuvosto pitää arviointitoiminnan luottamuksellisuutta tärkeänä niin liiketoiminnan kuin yleisestikin turvallisuuden kannalta. Valtioneuvosto pitää asianmukaisena, että ilmoitetut laitokset vastaisivat myös mahdollisesti käyttämiensä alihankkijoiden toiminnasta. Valtioneuvosto katsoo tärkeäksi, että arviointi toteutetaan tehokkaasti ja suhteellisuusperiaatetta noudattaen. Valtioneuvosto pitää tärkeänä kiinnittää neuvotteluissa huomioita siihen, että arvioinnista aiheutuvat kustannukset eivät muodostuisi korkeiksi tavalla, joka muodostaisi merkittäviä haasteita uusien tuotteiden tuomiseksi markkinoille erityisesti pienten ja keskisuurten yrityksien osalta. Valtioneuvosto pitää tärkeänä, että esityksen valmistelussa ja täytäntöönpanossa kiinnitetään huomiota pienille ja keskisuurille yrityksille aiheutuvaan sääntelytaakkaan ja kustannuksiin sekä neuvontaan vaatimuksien soveltamisessa. Kansallisesti on tarve kiinnittää huomiota arviointilaitosten riittävään määrään siten, että arviointimenettely ei tarpeettomasti viivästytä tuotteiden markkinoille saattamista.

Markkinavalvonnan osalta valtioneuvosto kannattaa markkinavalvonta-asetuksen (EU) 2019/1020 soveltamista huomioiden, että jäsenvaltioille jätetään tarpeeksi liikkumavaraa kansallisten toimivaltaisten viranomaisten nimeämisessä ja markkinavalvonnan järjestämisessä käytännössä. Valtioneuvosto pitää tärkeänä, että valvontatoimenpiteisiin liittyy riittävät oikeussuojakeinot ja mahdollisista vaatimustenvastaisuuksista turvallisuuspuutteista aiheutuvat sanktiot ovat yhdenmukaisia ja oikeasuhtaisia unionin alueella. On myös tärkeää, että tietosuojaviranomaisille ehdotettuja tehtäviä ja toimivaltuuksia arvioidaan neuvottelujen aikana tarkemmin suhteessa niihin tehtäviin ja toimivaltuuksiin, joista säädetään EU:n yleisessä tietosuoja-asetuksessa.

Komissiolle ehdotetun delegoidun säädösvallan osalta valtioneuvosto pitää tarpeellisena, että neuvottelujen edetessä arvioidaan delegoidun säädösvallan tarvetta ja laajuutta. Valtioneuvosto pitää välttämättömänä, että komissiolle delegoitavat toimivaltuudet ovat selkeitä, tarkkarajaisia, oikeasuhtaisia, tarkoituksenmukaisia ja hyvin perusteltuja. Ehdotuksella delegoidusta lainsäädäntövallasta olisi merkitystä erityisesti ulkopuoliseen arviointiin liittyvien vaatimusten suhteen, minkä vuoksi on tarpeellista kiinnittää huomiota siihen, kuinka delegoiduilla säädöksillä voitaisiin laajentaa ulkopuolista arviointia vaativien tuotteiden alaa.

Valtioneuvosto pitää tarpeellisena asetuksessa ehdotettuja hallinnollisia sanktioita ottaen huomioon taloudellisen hyödyn, joka vilpillisestä tai vaatimusten vastaisesta toiminnasta voisi valmistajalle, jakelijalle tai maahantuojalle syntyä. Valtioneuvosto pitää tarpeellisena, että neuvotteluissa arvioidaan sanktioiden oikeasuhtaisuutta ja kohtuullisuutta, sekä jätetään jäsenvaltioille riittävä liikkumavara säätää sanktioiden kansallisesta täytäntöönpanosta kunkin jäsenvaltion oikeusjärjestelmän edellyttämällä tavalla.