ITS Finland ry
Mikonkatu 9
00100 HELSINKI
www.its-finland.fi

LAUSUNTO

17.11.2022

Eduskunta
Liikenne- ja viestintävaliokunta

Asia: U 83/2022 vp Valtioneuvoston kirjelmä eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi horisontaalisista kyberturvallisuusvaatimuksista tuotteille, joissa on digitaalinen elementti (kyberkestävyyssäädös)

Älykkään liikenteen verkosto ITS Finlandin lausunto valtioneuvoston kirjelmään U 83/2022 vp eduskunnalle.

ITS Finland ry on älykkään liikenteen verkosto, jonka vuoksi lausuntomme koskee ensisijaisesti älykkään liikenteen toimialaan, suoraan tai välillisesti, liittyviä näkökulmia. Viime vuosina verkostossamme ovat korostuneet älyliikennepainotusten rinnalla liikennejärjestelmän kestävyys ja erityisesti digitalisaation mahdollisuudet yhteiskunnallisten tavoitteiden saavuttamisessa.

ITS Finland toimii digitaalisen liikenteen ja kuljetuksen kehittämisen yhteistyöfoorumina kooten hallinnon, tutkimuksen ja elinkeinoelämän toimijat yhteen. ITS Finland on voittoa tavoittelematon asiantuntijaverkosto, johon kuuluu yli 100 jäsenorganisaatiota, joissa työskentelee yli 30 000 työntekijää. Yhdistyksen tavoitteena on edistää liikenteen digitalisaation ja uusien palvelujen toteuttamisen yleisiä edellytyksiä sekä tehdä tunnetuksi tieto- ja viestintätekniikan yhteiskunnallista vaikuttavuutta.

Älykkään liikenteen verkosto - ITS Finland ry kiittää lausuntopyynnöstä ja toteaa lausuntonaan seuraavaa.

Lausunto

EU:n kyberkestävyyssäädös täydentää EU:n kyberturvallisuusstrategiaa (2020) ja EU:n kyberturvallisuusasetusta (2019) sekä asetuksen osana luotua EU:n laajuista kyberturvallisuuden sertifiointijärjestelmää.

ITS Finland pitää kannatettavana komission aitoa pyrkimystä nostaa eurooppalaisen kyberturvallisuuden tasoa ja lisätä tietoisuutta kyberturvallisuuden merkityksestä. Kannatamme myös ajatusta siirtää vastuuta kyberturvallisuuden varmistamisesta kuluttajilta digitaalisten ohjelmistojen ja niihin liittyvien laitteistojen valmistajille ja jälleenmyyjille. Kyberturvallisuudesta huolehtiminen on aivan liian tärkeää, ja myös liian vaikeaa, jätettäväksi digitaalisten laitteiden ja palvelujen loppukäyttäjien vastuulle.

Yhä nopeammin digitalisoituvassa maailmassa käyttäjien tulee voida tuntea olonsa turvalliseksi digitaalisten laitteiden ja ohjelmistojen kanssa. Kyberkestävyyssäädöksen tarkoituksena on varmistaa, että kaikki ohjelmistot tai tietoverkkoihin liitetyt laitteet, jotka on sertifioitava ja varustettava CE-

merkinnällä säädöksen mukaisesti, varmistavat kuluttajille ja yrityksille kyberturvallisen toimintaympäristön. Kyberturvallisuussäädös nostaa kyberturvallisuuden varmistamisen kaikkien digitaalisia laitteita ja ohjelmistoja tuottavien toimijoiden yhteiseksi asiaksi, eikä kyberturvallisuutta voi enää ulkoistaa vain siihen erikoistuneille tahoille. Kyseessä on hieman vastaavanlainen uudistus kuin GDPR, joka sai toimijat panostamaan kuluttajien yksityisyyden suojelemiseen ja heidän digitaalisten yksityisyytensä vahvistamiseen.

Kyberkestävyyssäädös pyrkii luomaan olosuhteet, joissa käyttäjät voivat ottaa kyberturvallisuuden huomioon valitessaan ja käyttäessään digitaalisia elementtejä sisältäviä tuotteita. Kyberkestävyyssäädös täydentää Data Act:n myötä omaksuttua ”data access by design” -ajattelutapaa lisäämällä verkkoon kytkettäville laitteille ja ohjelmistoille ”cybersecure by design” -periaatteen.

Erityistä huomiota on kiinnitettävä kyberkestävyyssäädöksen myötä perustettavalla arviointilaitostoiminnalla. Arviointilaitostoiminnan osalta on tärkeää miettiä avoimesti eri vaihtoehtoja, ja hyödyntää yksityisen sektorin osaamista kulloisenkin tarpeen mukaan. Arviointitoiminnasta ei saa muodostua aikataulullista tai kustannuksellista pullonkaulaa uusien digitaalisten ratkaisujen kehittämiselle.

Suomen kannassa on hyvin tunnistettu kyberkestävyyssäädöksen uhat ja mahdollisuudet. ITS Finland pitää oikein hyvänä valtioneuvoston näkemystä siitä, *että ”ulkopuolista arviointia vaadittaisiin riskiperusteisesti vain sellaisilta tuotteilta, joilla on erityistä merkitystä kyberturvallisuuden kannalta ja lähtökohtaisesti muiden tuotteiden osalta riittäisi valmistajan itsearviointi”.*

Valtioneuvoston kannassa esitetty huoli siitä, että *”ulkopuolisen arvioinnin tarpeen merkittävällä lisäämisellä voidaan pahimmillaan merkittävästi hidastaa tuotteiden markkinoille pääsyä, mikäli asiantuntevia arviointilaitoksia ei ole riittävästi tarjolla”,* on erittäin merkittävä. Lähtökohtana tulee olla, että arviointilaitoksia tulee olla riittävästi, ja arvioinnin kestolle ja kustannuksille tulee asettaa tiukat raamit. Pelkkä ajatuskin siitä, että arviointilaitoksista voisi tulla samanlainen hidaste kuin joistakin lupaviranomaisista on tullut, tuntuu mahdottomalta hyväksyä.

”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”. ITS Finland on tuosta samaa mieltä, mutta huomauttaa kustannusten olevan tärkeitä myös suurille yrityksille.

Datasääntelyn velvoitteet ja niiden rikkomisesta seuraavat sanktiot ovat varsin ankarat, ja voivat olla kohtalokkaan suuret pienille ja keskisuurille yrityksille. Säädösten rikkomisesta voi seurata hallinnollinen sakko, jonka suuruus on enintään 20 miljoonaa euroa tai 4 % yrityksen globaalista liikevaihdosta sen mukaan, kumpi on suurempi. Käytännössä tämä voi vähentää pienten ja keskisuurien yritysten kiinnostusta toimia digitaalisten tuotteiden parissa.

ITS Finland ry
Mikonkatu 9
00100 HELSINKI
www.its-finland.fi

LAUSUNTO

17.11.2022

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. Valtioneuvoston kanta sanktioiden oikeasuhtaisuuden ja kohtuullisuuden arvioinnista on luonnollisesti hyvä lähtökohta, mutta saavutetun taloudellisen hyödyn lisäksi tulisi tarkastella myös mahdollisesti aiheutettuja haittoja kyseisen tuotteen hyödyntäjille ja loppukäyttäjille. Myös ajatus siitä, että sanktiot voisivat vaihdella eri jäsenvaltioissa huomattavastikin, tuntuu vaikeasti hyväksyttävältä tilanteessa, jossa ollaan rakentamassa digitaalisia yhteismarkkinoita.

Lopuksi

Kyberkestävyyssäädös on tiettävästi myös maailman mittakaavassa toistaiseksi ainutlaatuinen lainsäädäntöaloite ja sitä voi kutsua ensimmäiseksi IoT -lainsäädännöksi. Parhaimmillaan se nostaa eurooppalaiset digitaaliset ratkaisut kuluttajien ja yritysasiakkaiden suosioon ja lisää ratkaisujen kysyntää maailmalla, samalla kuin erilaiset haavoittuvuuksien aiheuttamat vahingot ja kustannukset vähenevät. Pahimmillaan säädös hidastaa uusien palvelujen kehittämistä ja markkinoille pääsyä, ja aiheuttaa rehellisille yrityksille tarpeettomia kustannuksia mahdollisten arviointiprosessien puutteiden vuoksi.

Suomi on yksi Euroopan edelläkävijämaita älykkäiden laitteiden ja ohjelmistojen kehittämisessä. Suomessa on myös erinomaista osaamista kyberturvallisuudessa sekä yrityksissä että viranomaistahoilla. Suomalaisilla on tässä keskimääräistä enemmän hävittävää, mutta myös voitettavaa. Rakennettaessa Suomen kansallisia ratkaisuja kyberkestävyyssäädöksen antamissa raameissa tulisi käydä aktiivista vuoropuhelua yritysten ja julkisten toimijoiden kesken samanlaisessa yhteistyön ja luottamuksen hengessä, kuin huoltovarmuusasioissa, jossa eri osapuolet työskentelevät tiiviisti yhteisen asian hyväksi.

Kunnioittavasti,

Marko Forsblom
Toiminnanjohtaja
ITS Finland ry