

erityisasiantuntija Klemola, pääsihteeri Karanko

Eduskunta
Liikenne- ja viestintävaliokunta

Viite: HE 179/2025 vp

**PUOLUSTUS- JA ILMAILUTEOLLISUUS PIA RY:N LAUSUNTO ASIAAN HE 179/2025 VP:
HALLITUKSEN ESITYS EDUSKUNNALLE KYBERKESTÄVYYSASETUKSEN TOIMEENPANOJA
KOSKEVAKSI LAINSÄÄDÄNNÖKSI**

1. YLEISTÄ

Hallituksen esitys kyberkestävyysasetuksen toimeenpanosta on lähtökohtaisesti kannatettava, sillä Euroopan unionin alueella käytössä olevien ja käyttöön tulevien digitaalisen elementin omaavien tuotteiden kyberturvallisuuteen pitää kyetä luottamaan. Erityisen tyytyväisiä olemme siitä, että kyberkestävyysasetuksella tavoitellaan entistä turvallisempia ja vähemmän haavoittuvia tuotteita samalla, kun niiden käyttäjille luodaan näkyvyyttä niiden tietoturvaominaisuuksiin.

Vaikka maanpuolustukseen, yksinomaan kansalliseen turvallisuuteen tai salassa pidettävän tiedon käsittelyyn liittyvät tuotteet ovatkin rajattu lain soveltamisalan ulkopuolelle, esitämme kuitenkin huolestamme lain soveltamisesta teollisuudelle koituvien kustannusten nousun osalta. Huolestamme kattaa näin ollen myös kaksikäyttötuotteiden suunnittelun, valmistuksen ja myynnin unionin alueella. Vaikka turvallisuusasenteen ja turvallisuuteen liittyvien toimenpiteiden selkeä parantaminen on erittäin hyvä tavoite, pitää samalla kuitenkin huolehtia maamme teollisuuden kilpailukyvyistä sekä Euroopassa että muualla maailmassa. Turvallisuustason parantamisella ei saa rakentaa kaupan ja kilpailukyvyn kasvun esteitä.

Esitämme seuraavassa mielestämme tarkempaa tarkastelua vaativia näkökohtia ennen kaikkea teollisuuden kilpailukyvyn kannalta.

2. ARVIOMME KYBERKESTÄVYYSASETUKSESTA

Lain perustelun kohdassa 2.1.6 ”Markkinavalvonta ja täytäntöönpano” todetaan asetuksen 52 artiklan kohdan 8 mukaan jäsenvaltioiden veloitteesta varmistaa markkinavalvontaviranomaisille riittävät taloudelliset ja tekniset resurssit, mukaan lukien henkilöstöresurssit. Olemme tyytyväisiä siitä, että eri viranomaistahot ovat arvioineet asetuksen toimeenpanon vaatimat taloudelliset ja henkilöstövaikutukset melko kokonaisvaltaisella tavalla. Kannamme kuitenkin huolta siitä, tullaanko nämä tunnistetut resurssitarpeet toteuttamaan. **Viranomaisten resurssipula ei saa olla teollisuuden kilpailukyvyn edistämisen esteenä.**

Kohdassa 2.1.8 käsitellään asetuksen voimaantuloa ja siirtymäsäännöksiä. Huolestamme mukaan asetuksen voimaantulo saattaa ainakin aluksi nostaa kotimaisten ja eurooppalaisten tuotevalmistajien kynnystä tuoda digitaalisia elementtejä sisältäviä tuotteita markkinoille samalla, kun niiden innovaatiokyky hidastuu monisyisen ja epäselvän regulaation ja lainsäädännön takia. **On keskeistä, että laissa määritellyt vaatimustenmukaisuuden arviointilaitokset ja**

erityisasiantuntija Klemola, pääsihteeri Karanko

kyberkestävyyden sääntelyn testiympäristöt laativat suomalaiselle teollisuudelle yleisesti saatavilla olevat, riittävän selkeät ja yksinkertaiset ohjeet lain soveltamiseksi.

Kohdassa 2.1.10 käsitellään jäsenvaltioiden kansallista liikkumavaraa vaatimustenmukaisuuden arviointilaitosten nimeämisessä. **Kannatamme näiden laitosten toiminnan järjestämistä kaupalliselta pohjalta viranomaisten resurssien suuntaamiseksi ydintehtäviin.**

Kantamme mukaan viranomaisten on myös huolehdittava siitä, että Suomessa on riittävä määrä näitä laitoksia niin, että teollisuutemme kilpailukyky ei kärsi pitkien arviointijonojen vuoksi.

Edelliseen liittyen tulee huolehtia myös eturistiriitojen ehkäisystä, jotta arviointilaitosstatuksen saanut yritys ei päätyisi valvomaan itseään muun liiketoimintansa osalta.

Kohdan 2.1.10 mukaan jäsenvaltiot voivat perustaa kyberkestävyyden sääntelyn testiympäristöjä. Asetus ei kuitenkaan velvoita testiympäristöjen perustamiseen. **Tuemme vahvasti sitä, että testiympäristöjä perustettaisiin kaupalliselta pohjalta riittävä määrä. Testiympäristöjen puute ei saa estää suomalaisten yritysten kehitystyötä ja liiketoimintaa.**

Kohdan 2.2.2 mukaan kyberturvallisuussertifiointi on vapaaehtoista, jollei jäsenvaltioiden lainsäädännössä toisin säädetä. Samassa yhteydessä todetaan kuitenkin, että eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän käytön voidaan olettaa lisääntyvän asetuksen myötä. **Suomessa tulee huolehtia siitä, että yrityksiltä ei tulla vaatimaan kaksinkertaista ja päällekkäistä sertifiointia esimerkiksi suhteessa Kansallisen turvallisuusauditointikriteeristöön (KATAKRI) tai Pilviturvallisuuskriteeristöön (PITUKRI).**

Kohdassa 4.2.1 arvioidaan kyberkestävyydsasetuksen yritysvaikutuksia. Yritysten tuotekehityskustannusten arvioidaan nousevan asetuksen takia jopa 19-42 %. **Näkemyksemme mukaan tuotteiden hintojen nousu saataisiin parhaiten minimoitua asetustenmukaisuuteen liittyvällä selkeällä ohjeistuksella ja huolehtimalla huokeiden testausympäristöjen riittävästä määrästä. Tämä on tärkeää suomalaisen teollisuuden tuotteiden kilpailukyvyn varmistamiseksi myös Euroopan ulkopuolella.**

Kohdan 7.1 luvussa 1 käsitellään vaatimustenmukaisuuden arviointilaitoksen määritelmää. **On keskeisen tärkeää, että Suomeen perustettavat laitokset toimivat täsmälleen samoilla säännöillä (vrt. ajoneuvojen katsastus).**

Kohdan 7.1 luvussa 3 käsitellään ilmoitetuksi laitokseksi nimeämistä. **Korostamme, että laissa ja siitä annetuissa viranomaistulkinnoissa tulee selkeästi ja yksikäsitteisesti ilmoittaa pätevyysalueittain kriteeristöt, jotka ilmoitetuksi laitokseksi hakevalta taholta edellytetään.**

Kohdan 7.1 luvussa 3 käsitellään ilmoittavan viranomaisen oikeutta luovuttaa arviointilaitoksia koskevia salassa pidettäviä tietoja komissiolle ja muille jäsenvaltioille. **Huomautamme, että salassa pidettävän tiedon vastaanottajan tulee osoittaa kykenevänsä hallinnoimaan salassa pidettävää tietoa niin henkilöstön, tiedonsiirron, tiedonkäsittely-ympäristön kuin tilojenkin osalta. Tämä vaatimus on ulotettava koskemaan myös komissiota ja niitä jäsenvaltioita, jolle tieto luovutetaan. Viranomaisella ja arviointilaitoksella on**

erityisasiantuntija Klemola, pääsihteeri Karanko

oltava velvollisuus olla ilmoittamatta haluttuja tietoja, mikäli edellä kuvatut asiat eivät ole kunnossa.

Jos edellisen kohdan perusteella arvioitava tuote, esim. kaksoiskäyttötuote, liittyy sisäiseen tai ulkoiseen turvallisuuteen, tulee sitä koskeva luovutettava tieto arvioida ensin ao. viranomaisen toimesta (esim. Puolustusvoimat tai Poliisi).

Kohdan 7.1 luvun 5 mukaan kyberturvallisuussertifikaatin myöntäminen voidaan delegoida myös vaatimuksenmukaisuuden arviointilaitokselle. **Tämä on kannatettavaa tilanteissa, joissa viranomaisen henkilöresurssit eivät riitä virkatehtävien hoitamiseen. Olemme kuitenkin huolissamme yrityksille mahdollisesti koituvista korkeista kustannuksista.** Tilanteessa, joissa lähinnä muutama kaupallinen toimija myöntää tällaisia sertifikaatteja, on suuri vaara ylihinnoittelulle. Tämä aiheuttaa haasteita erityisesti PK-yrityksille, joilla se voi olla sertifikaatin hankkimisen este.

Kohdan 7.1 luvussa 6 käsitellään seuraamusmaksuja. **Seuraamusmaksut tulee laittaa täytäntöön vasta, kun on selkeää näyttöä tuottamuksellisuudesta ja lain noudattamatta jättämisestä. Epäilyn kohteena olevalle taholle tulee antaa kohtuullinen seuranta-aika tuotteiden saattamiseksi asianmukaiselle tasolle. Ennen kaikkea viranomaisen ja sen seurannassa olevien laitosten tulee kyetä tuottamaan valmistajille riittävän yksinkertainen ja kattava tarkastuslista tuotteiden lainmukaisuuden toteutukseksi.**

Pidämme hyvänä sitä, että lain perustelukohdissa 11 ja 12 on tarkasteltu asetuksen suhdetta muihin esityksiin ja perustuslakiin. **Huomautamme vielä kohdan 12.6 osalta tarvetta peilata esitystä sotilastiedustelulakiin etenkin viranomaisten tiedonsaantioikeuksien varmistamiseksi.**

3. YHTEENVETO

Kannatamme hallituksen esitystä kyberkestävyysasetukseksi. Oikealla tavalla toteutettuna esityksellä parannetaan EU:n alueen kyberturvallisuutta merkittävästi. Vaikka maanpuolustukseen, yksinomaan kansalliseen turvallisuuteen tai salassa pidettävän tiedon käsittelyyn liittyvät tuotteet ovatkin rajattu lain soveltamisalan ulkopuolelle (pois lukien kaksikäyttötuotteet), esitämme kuitenkin huolestua lain soveltamisesta teollisuudelle koituvien kustannusten nousun osalta. Kannamme tämän vuoksi huolta suomalaisen teollisuuden tuotteiden kilpailukyvystä Euroopan lisäksi myös sen ulkopuolella, sillä asetuksen toimeenpanolla näyttää arvioiden mukaan olevan merkittäviä vaikutuksia tuotteiden hintoihin.

Arviomme perusteella esitämme seuraavia näkökohtia kyberkestävyysasetukseen:

1. Asetuksen toimeenpanosta koituvat viranomaisten resurssien lisäystarpeet tulee toteuttaa täysimääräisesti, sillä viranomaisten resurssipula ei saa olla teollisuuden kilpailukyvyn edistämisen esteenä.
2. Viranomaisten, arviointilaitosten ja testausympäristöjen tulee laatia teollisuudelle yleisesti saatavilla olevat, riittävän selkeät ja yksinkertaiset ohjeet lain soveltamiseksi.
3. Kannatamme vaatimustenmukaisuuden arviointilaitosten toiminnan järjestämistä kaupalliselta pohjalta.
4. Kantamme mukaan viranomaisten on myös huolehdittava siitä, että Suomessa on riittävä määrä arviointilaitoksia teollisuutemme kilpailukyvyn varmistamiseksi.

erityisasiantuntija Klemola, pääsihteeri Karanko

5. Viranomaistoiminnalla on varmistettava, ettei arviointilaitosstatuksen saanut yritys päätyisi valvomaan itseään muun liiketoimintansa osalta.
6. Esitämme vahvan tukemme sille, että myös kyberkestävyyden sääntelyn testiympäristöjä perustettaisiin kaupalliselta pohjalta riittävä määrä suomalaisten tuotteiden nopean markkinoille pääsyn varmistamiseksi.
7. Kyberturvallisuussertifiointien yhteydessä yrityksiltä ei tule vaatia päällekkäistä sertifiointia esimerkiksi suhteessa Kansallisen turvallisuusauditointikriteeristöön (KATAKRI) tai Pilviturvallisuuskriteeristöön (PITUKRI).
8. Suomalaisen teollisuuden tuotteiden kilpailukyvyn varmistamista myös Euroopan ulkopuolella tukisi asetustenmukaisuuteen liittyvä selkeä ohjeistus yhdistettynä huokeiden testausympäristöjen ja arviointilaitosten riittävään määrään.
9. On keskeisen tärkeää, että Suomeen perustettavat vaatimustenmukaisuuden arviointilaitokset toimivat täsmälleen samoilla säännöillä (vrt. ajoneuvojen katsastus).
10. Laissa ja siitä annetuissa viranomaistulkinnossa tulee selkeästi ja yksikäsitteisesti ilmoittaa pätevyysalueittain kriteeristöt, jotka ilmoitetuksi laitokseksi hakevalta taholta edellytetään.
11. Salassa pidettävän tiedon vastaanottajan (komissio, muu jäsenvaltio tai ulkomainen arviointilaitos) tulee osoittaa kykenevänsä hallinnoimaan salassa pidettävää tietoa niin henkilöstön, tiedonsiirron, tiedonkäsittely-ympäristön kuin tilojenkin osalta. Viranomaisella ja arviointilaitoksella on oltava velvollisuus olla ilmoittamatta haluttuja tietoja, mikäli edellä kuvatut asiat eivät ole kunnossa.
12. Jos luovutettavaksi harkittava salassa pidettävä tieto liittyy sisäiseen tai ulkoiseen turvallisuuteen, tulee luovutettava tieto arvioida ensin ao. viranomaisen toimesta (esim. Puolustusvoimat tai Poliisi).
13. Kannatamme kyberturvallisuussertifikaatin myöntämisoikeuden delegoimista vaatimuksenmukaisuuden arviointilaitoksille etenkin tilanteissa, joissa viranomaisen henkilöresurssit eivät riitä virkatehtävien hoitamiseen. Olemme kuitenkin huolissamme yrityksille mahdollisesti koituvista korkeista kustannuksista tilanteessa, jossa alan harvalukuiset toimijat ylihinnottelevat palvelunsa.
14. Seuraamusmaksut tulee laittaa täytäntöön vasta, kun on selkeää näyttöä tuottamuksellisuudesta ja lain noudattamatta jättämisestä. Epäilyn kohteena olevalle taholle tulee antaa kohtuullinen seuranta-aika tuotteiden saattamiseksi asianmukaiselle tasolle.
15. Peräänkuulutamme vielä tarvetta peilata kyberturvallisuusasetusta sotilastiedustelulakiin etenkin viranomaisten tiedonsaantioikeuksien varmistamiseksi.