Euroopan talous- ja sosiaalikomitean lausunto aiheesta ”Ehdotus Euroopan parlamentin ja neuvoston asetukseksi digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetuksen (EU) 2019 1020 muuttamisesta”

(COM(2022) 454 final – 2022/0272 (COD))

(2023/C 100/15)

Esittelijä: **Maurizio MENSI**

Yhteisesittelijä: **Marinel Dănuț MUREȘAN**

Lausuntopyyntö	Euroopan parlamentti, 9.11.2022
	Euroopan unionin neuvosto, 28.10.2022
Oikeusperusta	Euroopan unionin toiminnasta tehdyn sopimuksen 114 artikla
Vastaava jaosto	sisämarkkinat, tuotanto ja kulutus
Hyväksyminen jaostossa	10.11.2022
Hyväksyminen täysistunnossa	14.12.2022
Täysistunnon numero	574
Äänestystulos	
(puolesta / vastaan / pidättyi äänestämästä)	177/0/0

1. **Päätelmät ja suositukset**

1.1 Euroopan talous- ja sosiaalikomitea (ETSK) suhtautuu myönteisesti komission ehdottamaan kyberresilienssisäädökseen, jonka tavoitteena on asettaa tiukemmat kyberturvallisuusstandardit, jotta voidaan luoda luotettava järjestelmä talouden toimijoille ja varmistaa EU:n kansalaisille mahdollisuus käyttää markkinoilla olevia tuotteita turvallisesti. Tämä aloite on osa EU:n datastrategiaa, jolla vahvistetaan tietoturvaa, myös henkilötietojen turvaa, ja perusoikeuksia, jotka ovat digitaalisen yhteiskunnan olennaisia edellytyksiä.

1.2 ETSK pitää olennaisen tärkeänä, että vahvistetaan yhteistä reagointia kyberhyökkäyksiin ja edistetään kansallisella tasolla kyberturvallisuuden alan yhdenmukaistamista toimintasääntöjen ja -välineiden osalta, jotta voidaan välttää se, että erilliset kansalliset lähestymistavat loisivat oikeudellista epävarmuutta ja oikeudellisia esteitä.

1.3 ETSK suhtautuu myönteisesti komission aloitteeseen, joka paitsi auttaa vähentämään kyberhyökkäyksistä yrityksille aiheutuvia merkittäviä kustannuksia myös antaa kansalaisille ja kuluttajille perusoikeuksien, kuten yksityisyyden, paremman suojan. Komissio näyttää ottavan erikseen huomioon pk-yritysten erityiset tarpeet sertifiointiviranomaisten tarjoamissa palveluissa. ETSK korostaa, että sovellettavia kriteerejä on kuitenkin aiheellista selventää.

1.4 ETSK pitää tärkeänä painottaa, että vaikka on myönteistä, että kyberresilienssisäädös kattaa lähes kaikki digitaaliset tuotteet, sen käytännön soveltaminen saattaa osoittautua ongelmalliseksi, sillä se tuo mukanaan paljon monimutkaista todentamista ja valvontaa. Tästä syystä on tarpeen vahvistaa seuranta- ja todentamisvälineitä.

1.5 ETSK katsoo, että kyberresilienssisäädöksen aineellista soveltamisalaa on tarkennettava erityisesti digitaalisia elementtejä sisältävien tuotteiden ja ohjelmistojen osalta.

1.6 ETSK toteaa, että valmistajilla on velvollisuus kertoa tuotteiden haavoittuvuuksista sekä mahdollisista tietoturvapoikkeamista ja ilmoittaa asiasta Euroopan unionin kyberturvallisuusvirastolle (ENISA). Onkin tärkeää, että virastolle annetaan tarvittavat resurssit, jotta se voi hoitaa tehokkaasti ja täsmällisesti sille osoitetut tärkeät ja vaativat tehtävät.

1.7 Tulkintaepäselvyyksien välttämiseksi ETSK ehdottaa, että komissio laatisi suuntaviivat, jotka antaisivat valmistajille ja kuluttajille ohjeita sovellettavista säännöistä ja menettelyistä, sillä useisiin ehdotuksen soveltamisalaan kuuluviin tuotteisiin näytetään sovellettavan myös muita kyberturvallisuussäännöksiä. Tässä yhteydessä olisi myös tärkeää, että erityisesti mikro- ja pk-yritykset voivat saada pätevää asiantuntija-apua ja erityisiä asiantuntijapalveluja.

1.8 ETSK toteaa, että suhde kyberresilienssisäädöksessä tarkoitettujen sertifiointiviranomaisten ja muiden säännösten nojalla kyberturvallisuussertifikaatteja myöntävien muiden elinten välillä ei ole täysin selvä. Sama operatiivinen koordinointiongelma saattaa syntyä myös ehdotuksessa tarkoitettujen valvontaviranomaisten ja muiden samoihin tuotteisiin sovellettavan lainsäädännön nojalla jo toimivien valvontaviranomaisten välillä.

1.9 ETSK katsoo, että ehdotuksessa osoitetaan huomattava määrä toimia ja tehtäviä sertifiointiviranomaisille, joiden käytännön toimintavalmiudet on varmistettava, jotta voidaan välttää myös se, että kyberresilienssisäädös johtaisi byrokratian lisääntymiseen ja rankaisisi valmistajia, joiden on noudatettava useita muita sertifiointivaatimuksia voidakseen jatkaa toimintaansa markkinoilla.

2. **Analyysi ehdotuksesta**

2.1 Kyberresilienssisäädöksellä komission on tarkoitus järkeistää nykyistä kyberturvallisuuslainsäädäntöä, muotoilla sitä uudelleen yhtenäisesti ja horisontaalisesti ja samalla päivittää sitä uusien teknologisten innovaatioiden pohjalta.

2.2 Kyberresilienssisäädöksellä on neljä päätavoitetta: varmistetaan, että valmistajat parantavat digitaalisia elementtejä sisältävien tuotteiden tietoturvaa suunnittelu- ja kehitysvaiheessa ja koko elinkaaren ajan; luodaan johdonmukaiset kyberturvapuitteet, joissa laite- ja ohjelmistovalmistajien on helpompi noudattaa vaatimuksia; lisätään läpinäkyvyyttä digitaalisia elementtejä sisältävien tuotteiden tietoturvaominaisuuksien suhteen; luodaan yrityksille ja kuluttajille edellytyksiä käyttää digitaalisia elementtejä sisältäviä tuotteita tietoturvallisesti. Ehdotuksessa esitetään CE-kyberturvallisuusmerkinnän käyttöön ottamista ja edellytetään, että merkintä lisätään kaikkiin kyberresilienssisäädöksen soveltamisalaan kuuluviin tuotteisiin.

2.3 Kyseessä on horisontaalinen toimenpide, jolla komissio aikoo säännellä aihetta jäsennellysti, sillä se kattaa lähes kaikki tuotteet, joissa on digitaalisia elementtejä. Soveltamisalan ulkopuolelle jäävät ainoastaan lääkinnälliset laitteet sekä siviili-ilmailu-, ajoneuvo- ja sotilasalan tuotteet. Ehdotus ei koske myöskään ohjelmistopalveluja (pilvipalveluja), paitsi jos niitä käytetään digitaalisia elementtejä sisältävien tuotteiden kehittämiseen.

2.4 ”Digitaalisia elementtejä sisältävien tuotteiden” määritelmä on hyvin laaja, ja se kattaa kaikki ohjelmisto- ja laitteistotuotteet sekä ohjelmistot ja laitteistot, joita ei ole sisällytetty tuotteeseen, vaan jotka on saatettu markkinoille erillisinä.

2.5 Säädöksessä vahvistetaan pakolliset kyberturvallisuusvaatimukset digitaalisia elementtejä sisältäville tuotteille koko niiden elinkaaren ajaksi, mutta se ei korvaa jo käytössä olevia vaatimuksia. Näin ollen tuotteet, jotka on jo sertifioitu aiempien EU:n vaatimusten mukaisesti, katsotaan myös uuden asetuksen vaatimusten mukaisiksi.

2.6 Yleisenä perusperiaatteena on, että Euroopassa saatetaan markkinoille ainoastaan turvallisia tuotteita, joiden valmistajat varmistavat, että tuotteet ovat turvallisia koko niiden elinkaaren ajan.

2.7 Tuote on turvallinen silloin, kun se on suunniteltu ja valmistettu niin, että sen turvallisuustaso on asianmukainen sen käyttöön liittyviin kyberriskeihin nähden, sillä ei ole tiedossa olevia haavoittuvuuksia myyntihetkellä, siinä on oletusarvoisesti tietoturvalliset asetukset, se on suojattu laittomilta yhteyksiltä, sen keräämät tiedot on suojattu ja tietojen keruu rajoittuu yksinomaan sen toiminnan kannalta tarpeellisiin tietoihin.

2.8 Valmistajan katsotaan voivan saattaa tuotteensa markkinoille, kunhan se asettaa saataville tuotteidensa eri ohjelmistokomponenttien luettelon, korjaa viipymättä ja maksutta uudet haavoittuvuudet, julkistaa ja erittelee havaitsemansa ja ratkaisemansa haavoittuvuudet ja varmentaa säännöllisesti markkinoille saattamiensa tuotteiden häiriönsietokyvyn. Näiden ja muiden kyberresilienssisäädökseen sisältyvien toimien on katettava tuotteen koko elinkaari tai vähintään viisi vuotta sen markkinoille saattamisesta. Valmistajan on varmistettava, että haavoittuvuudet poistetaan säännöllisillä ohjelmistopäivityksillä.

2.9 Eri aloihin sovellettavan yleisen periaatteen mukaan velvoitteet koskevat myös maahantuojia ja jakelijoita.

2.10 Kyberresilienssisäädöksessä säädetään niin sanottujen normaalien tuotteiden ja ohjelmistojen makroluokasta, jonka kohdalla riittää valmistajan tekemä itsearviointi. Näin tehdään jo muuntyyppisten CE-merkintöjen sertifioinnin kohdalla. Komission mukaan 90 prosenttia markkinoilla olevista tuotteista kuuluu tähän luokkaan.

2.11 Valmistaja voi saattaa kyseiset tuotteet markkinoille sen jälkeen, kun niiden kyberturvallisuutta koskeva itsearviointi on tehty ja kun valmistaja on toimittanut säädöksessä annettujen ohjeiden mukaiset asiakirjat. Valmistajan on toistettava arviointi, jos tuotetta muutetaan.

2.12 Loput 10 prosenttia tuotteista on jaettu kahteen luokkaan (luokka I, vaarattomammat tuotteet, ja luokka II, vaarallisemmat tuotteet), jotka vaativat enemmän huomiota, kun tuotteet saatetaan markkinoille. Nämä ovat digitaalisia elementtejä sisältäviä kriittisiä tuotteita, joissa olevat viat voivat johtaa vaarallisempiin ja laajempiin tietoturvaloukkauksiin.

2.13 Näihin kahteen luokkaan kuuluvien tuotteiden kohdalla voidaan hyväksyä itsearviointiin perustuvat sertifikaatit vain, jos valmistaja osoittaa noudattaneensa erityisiä markkinavaatimuksia ja EU:n jo edellyttämiä turvallisuuseritelmiä tai kyberturvallisuussertifiointeja. Muussa tapauksessa valmistaja voi saada tuotteelleen sertifikaatin akkreditoidulta sertifiointielimeltä, jonka todistus on pakollinen luokan II tuotteille.

2.14 Järjestelmä tuotteiden riskiluokittelusta sisältyy myös ehdotettuun tekoälyasetukseen. Jotta vältytään epäselvyyksiltä sovellettavista säännöksistä, kyberresilienssisäädös kattaa digitaalisia elementtejä sisältävät tuotteet, jotka on samaan aikaan luokiteltu tekoälyehdotuksessa suuririskisiksi tekoälyjärjestelmiksi. Tällaisten tuotteiden on yleensä noudatettava tekoälyasetuksessa säädettyä vaatimustenmukaisuuden arviointimenettelyä. Tämä ei koske digitaalisia elementtejä sisältäviä kriittisiä tuotteita, joihin sovelletaan kyberresilienssisäädöksen olennaisten vaatimusten lisäksi kyberresilienssisäädöksen vaatimustenmukaisuuden arviointisääntöjä.

2.15 Kyberresilienssisäädöksen noudattamisen varmistamiseksi kunkin jäsenvaltion on nimettävä kansallinen viranomainen suorittamaan markkinavalvontaa. Muiden tuoteturvallisuussääntöjen tapaan kansallisen viranomaisen todetessa, ettei tuotteella ole enää kyberturvallisuusominaisuuksia, sen markkinoille saattaminen voidaan keskeyttää kyseessä olevassa valtiossa. ENISAlla on toimivalta arvioida yksityiskohtaisesti ilmoitettu tuote, ja jos se toteaa, ettei tuote ole turvallinen, kyseisen tuotteen kaupan pitäminen EU:ssa voidaan keskeyttää.

2.16 Kyberresilienssisäädökseen sisältyy seuraamusjärjestelmä, jossa seuraamukset ovat suhteessa rikkomuksen vakavuuteen. Jos tuotteiden olennaisia kyberturvallisuusvaatimuksia ei noudateta, seuraamus voi olla enimmillään jopa 15 miljoonaa euroa tai 2,5 prosenttia edeltävän tilikauden liikevaihdosta.

3. **Huomioita**

3.1 ETSK suhtautuu myönteisesti komission aloitteeseen, jonka tarkoituksena on lisätä kyberturvallisuuden laajempaan säädöskokonaisuuteen uusi keskeinen osa koordinoidusti verkko- ja tietoturvadirektiiviä ([1]) täydentäen ja kyberturvallisuusasetuksen ([2]) lisäksi. Tiukoilla kyberturvallisuusstandardeilla on keskeinen asema luotaessa EU:n vankkaa kyberturvallisuusjärjestelmää kaikille talouden toimijoille pyrkien varmistamaan kaikkien markkinoilla olevien tuotteiden turvallinen käyttö EU:n kansalaisille ja vahvistamaan heidän luottamustaan digitaaliseen maailmaan.

3.2 Asetuksessa tarkastellaan tätä varten kahta kysymystä: monien tuotteiden alhaista kyberturvallisuustasoa ja ennen kaikkea sitä, että monet valmistajat eivät tarjoa tietoturvapäivityksiä haavoittuvuuksien poistamiseksi. Vaikka digitaalisia elementtejä sisältävien tuotteiden valmistajille aiheutuu toisinaan mainehaittoja, jos niiden tuotteet eivät ole turvallisia, haavoittuvuuksien kustannuksista vastaavat pääasiassa ammattikäyttäjät ja kuluttajat. Tämä ei kannusta valmistajia investoimaan turvallisten tuotteiden suunnitteluun ja kehittämiseen ja tarjoamaan tietoturvapäivityksiä. Lisäksi yrityksillä ja kuluttajilla ei useinkaan ole riittävää ja tarkkaa tietoa turvallisten tuotteiden valinnasta eivätkä ne useinkaan tiedä, miten

([1]) Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa (EUVL L 194, 19.7.2016, s. 1).

([2]) Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus) (EUVL L 151, 7.6.2019, s. 15).

varmistua siitä, että niiden ostamissa tuotteissa on tietoturvalliset asetukset. Uusissa säännöissä puututaan näihin kahteen seikkaan käsittelemällä päivityksiä ja ajantasaisten tietojen antamista asiakkaille. ETSK katsoo, että ehdotetusta asetuksesta voisi tulla tässä suhteessa oikein sovellettuna kyberturvallisuuden kansainvälinen vertailukohta ja malli.

3.3 ETSK suhtautuu myönteisesti ehdotukseen ottaa käyttöön tietoturvavaatimuksia digitaalisia elementtejä sisältäville tuotteille. On kuitenkin tärkeää välttää päällekkäisyyksiä muun asiaa koskevan voimassa olevan lainsäädännön kanssa, kuten uuden verkko- ja tietoturvadirektiivin ([3]) ja tekoälysäädöksen kanssa.

3.4 ETSK pitää tärkeänä korostaa, että vaikka on myönteistä, että kyberresilienssisäädös kattaa lähes kaikki digitaaliset tuotteet, sen käytännön soveltaminen saattaa osoittautua ongelmalliseksi, sillä se tuo mukanaan paljon todentamista ja valvontaa.

3.5 Kyberresilienssisäädöksen aineellinen soveltamisala on laaja ja kattaa kaikki digitaalisia elementtejä sisältävät tuotteet. Ehdotetun määritelmän mukaan se kattaa kaikki ohjelmistot ja laitteistot ja niihin liittyvät tietojenkäsittelytoimet. ETSK ehdottaa, että komissio selventäisi, kuuluvatko kaikki ohjelmistot asetusehdotuksen soveltamisalaan.

3.6 Valmistajilla on velvollisuus kertoa aktiivisesti hyödynnetyistä haavoittuvuuksista sekä turvallisuushäiriöistä. Niiden on ilmoitettava ENISAlle kaikista tuotteisiinsa sisältyvistä aktiivisesti hyödynnetyistä haavoittuvuuksista ja (erikseen) kaikista häiriöistä, joilla on vaikutusta tuotteen turvallisuuteen, 24 tunnin kuluessa siitä, kun ne ovat tulleet tietoisiksi näistä. ETSK toteaa tässä yhteydessä, että ENISAlla on oltava sekä määrällisesti että ammatillisesti riittävät resurssit, jotta se voi hoitaa tehokkaasti asetuksessa sille annetut tärkeät ja arkaluonteiset tehtävät.

3.7 Se, että useisiin ehdotuksen soveltamisalaan kuuluviin tuotteisiin sovelletaan myös muita kyberturvallisuussäännöksiä, voi aiheuttaa epävarmuutta sovellettavasta lainsäädännöstä. Vaikka kyberresilienssisäädöksen on tarkoitus olla yhdenmukainen EU:n nykyisen tuotelainsäädäntökehyksen ja muiden parhaillaan EU:n digitaalistrategian yhteydessä valmisteilla olevien ehdotusten kanssa, esimerkiksi suuririskisiä tekoälytuotteita koskevat säännökset sivuavat henkilötietojen käsittelyä koskevan asetuksen säännöksiä. ETSK ehdottaakin, että komissio laatisi valmistajia ja kuluttajia varten ohjeet oikeasta soveltamisesta.

3.8 ETSK toteaa, että suhde kyberresilienssisäädöksessä tarkoitettujen sertifiointiviranomaisten ja muiden sovellettavien säännösten nojalla kyberturvallisuussertifikaatteja mahdollisesti myöntävien muiden elinten välillä ei ole täysin selvä.

3.9 Näillä sertifiointiviranomaisilla on myös huomattava työtaakka ja suuri vastuu. On tarkistettava ja varmistettava, että ne ovat käytännössä toimintakykyisiä, jotta kyberresilienssisäädös ei lisäisi entisestään byrokratiaa, jota markkinoilla toimiminen aiheuttaa valmistajille. Tässä yhteydessä olisi myös tärkeää, että erityisesti mikro- ja pk-yritykset voivat saada pätevää asiantuntija-apua ja erityisiä asiantuntijapalveluja.

3.10 Kyberresilienssisäädöksen mukaan sertifiointiviranomaisten on otettava palveluissaan huomioon pk-yritysten erityiset tarpeet. ETSK korostaa, että sovellettavia kriteerejä on kuitenkin aiheellista selventää.

3.11 Saattaa myös syntyä koordinointiongelma tarkasteltavana olevassa asetuksessa tarkoitettujen valvontaviranomaisten ja samoihin tuotteisiin sovellettavan muun lainsäädännön nojalla jo toimivien valvontaviranomaisten välillä. ETSK ehdottaakin, että komissio kehottaa jäsenvaltioita seuraamaan tilannetta ja ryhtymään tarvittaessa toimiin tämän mahdollisuuden välttämiseksi.

Bryssel 14. joulukuuta 2022.

Euroopan talous- ja sosiaalikomitean
puheenjohtaja
Christa SCHWENG

([3]) Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi) (EUVL L 333, 27.12.2022, s. 80).