Teknologiateollisuus

29.9.2026

Eduskunta
Talousvaliokunta

Viite: U 54/2026 vp

Lausunto: Valtioneuvoston kirjelmä eduskunnalle ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi kehyksen perustamiseksi Euroopan pilvipalvelu- ja tekoälyekosysteemin vahvistamiseksi (pilvipalveluiden ja tekoälyn kehittämisen säädös, Cloud and AI Development Act, CADA), COM(2026) 502 final

Teknologiateollisuus ry edustaa yrityksiä, jotka vastaavat puolesta Suomen viennistä, tutkimus- ja kehitysinvestoinneista ja työllistävät suoraan ja välillisesti neljäsosan suomalaisista. Lausunto on laadittu yhdessä toimialayhdistyksemme Kyberala ry:n kanssa, joka edustaa Suomessa toimivaa kyberturvallisuusalaa. Painopiste on asetusehdotuksen IV luvussa (autonomia): suvereniteettikehyksessä, varmuustasoissa ja julkisen sektorin velvoitteissa.

Tiivistelmä

Kannatamme asetusehdotuksen tavoitteita ja yhdymme pääosin valtioneuvoston kantaan, erityisesti siihen, että suvereniteettivaatimukset asetetaan yhteisesti EU-tasolla, henkilöstön luotettavuutta ei arvioida kansalaisuuden perusteella ja tunnustamispäätöksiin voi hakea muutosta. Poikkeamme valtioneuvoston kannasta kahdessa kohdassa. Ensinnäkin kannatamme komission toimivaltaa puuttua jäsenvaltion riskiarvioon (29 art. 5 kohta), koska se suojaa sisämarkkinoita varmuustasojen mielivaltaiselta nostamiselta tai laskemiselta kotimaisten toimittajien hyväksi. Se olisi Suomen kaltaiselle pienelle ja avoimelle jäsenvaltiolle erityisen haitallista. Toiseksi valtioneuvosto katsoo, ettei sääntelyn tulisi olla kansallisen turvallisuuden osalta velvoittavaa. Esitämme sen sijaan, että kansallisessa turvallisuudessa, puolustuksessa ja turvallisuusluokitellun tiedon käsittelyssä varmuustasoja sovelletaan ”sovella tai selitä” -periaatteella: jäsenvaltio soveltaa niitä lähtökohtaisesti ja voi poiketa niistä perustellusti. Näin jäsenvaltion harkintavalta säilyy, mutta korkeimpien tasojen keskeinen kysyntä ei jää yhteisen kehyksen ulkopuolelle.

Korkeimpien varmuustasojen (3 ja 4) osalta esitämme tasapainoista ratkaisua. Kansallinen turvallisuus kuuluu jäsenvaltioiden yksinomaiseen vastuuseen (SEU 4 art. 2 kohta), ja jäsenvaltioilla on oltava liikkumavara korkeimman suojan toteuttamisessa. Suvereniteettikehyksen oikeusperusta on kuitenkin sisämarkkinoiden toimivuus (SEUT 114 art.), ja juuri korkeimmilla tasoilla aidoille sisämarkkinoille on vahva peruste: kysyntä on kapeaa, eikä pienen jäsenvaltion markkina riitä ylläpitämään kilpailukykyistä eurooppalaista tarjontaa. Keskeiset esityksemme ovat:

- Kannatetaan 29 ja 30 artiklaa, mutta säilytetään niissä kaksi vyöhykettä: kansallisen turvallisuuden, puolustuksen ja turvallisuusluokitellun tiedon peruste ei kytkeydy NIS2-direktiivin sektoreihin, ja niissä varmuustasoja sovelletaan ”sovella tai selitä” -periaatteella; NIS2-sektoreiden yleisen järjestyksen kannalta merkittävissä julkisen

Teknologiateollisuus ry
Kyberala ry

Eteläranta 10, PL 10, 00131 Helsinki
Puhelin 09 192 31
www.teknologiateollisuus.fi
Y-tunnus: 0215289-2

Teknologiateollisuus

28.9.2026

sektorin toiminnoissa riskiarviointi tehdään yhdenmukaisesti ja sen mukaista tasoa sovelletaan.
- Kannatetaan komission toimivaltaa määrittää varmuustaso (29 art. 5 kohta) selkein edellytyksin ja menettelytakein; sen ulottamista kansalliseen turvallisuuteen, puolustukseen ja turvallisuusluokiteltuun tietoon harkitaan tarkasti sisämarkkinoiden ja yhteentoimivuuden kannalta.
- Tasojen 3 ja 4 tunnustus kelpaa kaikissa jäsenvaltioissa, ja kansalliset lisävaatimukset sallitaan vain kansallisen turvallisuuden ja turvallisuusluokitellun tiedon suojaamiseksi, perusteltuina ja julkisina.
- EU-kansalaisuusvaatimus korvataan objektiivisella henkilöstöturvallisuusmenettelyllä (turvallisuusselvitys), ja vähintään ETA-kansalaiset rinnastetaan unionin kansalaisiin.
- Tason 4 ohjelmistotoimitusketjuvaatimus muotoillaan todennettavaksi ja saavutettavaksi, jotta taso ei jää käytännössä tyhjäksi.
- Tasojen 2–4 velvoitteet kytketään EUCS-sertifiointijärjestelmän valmistumiseen, KriPa tunnustetaan siirtymäkaudella ja näyttöjä hyödynnetään ristiin (”ilmoita kerran, hyödynnä monesti”).
- Tunnustamismenettelylle säädetään sitova kokonaismääräaika ja muutoksenhakuoikeus, tunnustamisen periytyvyys pilvipinon kerrosten välillä (IaaS, PaaS, SaaS) turvataan ja valvonta keskitetään Suomessa Traficomille.
- Migraation siirtymäaika pidennetään 24–36 kuukauteen, velvoitteita ei sovelleta taannehtivasti kesken sopimuskausien ja 31 artiklan 3 kohdan delegointivaltuus poistetaan.

1. Yleistä

Kannatamme asetusehdotuksen tavoitteita. Peruslinjamme on, että suvereniteettia rakennetaan ensisijaisesti kilpailukykyisen eurooppalaisen tarjonnan kautta ja sääntelyvaatimuksin vain perustelluissa tapauksissa. Ehdotuksen kriteeri-, läpinäkyvyys- ja tunnustamispohjainen kehys on tämän linjan mukainen: se avaa suomalaisille pilvi- ja kyberturvallisuusyrityksille uutta kysyntää ja auttaa julkista sektoria hallitsemaan riippuvuuksiaan.

Yhdymme valtioneuvoston näkemykseen siitä, että EU-tasoiset suvereniteettivaatimukset tuovat lisäarvoa sisämarkkinoille ja että sertifiointijärjestelmät tulee rajata teknisiin kysymyksiin, sekä sen huoleen delegoidun vallan laajuudesta, uusista viranomaistehtävistä ja siirtymäajoista. Korjauksia vaativat erityisesti hankintavelvoitteiden laajuus ja ajoitus, päällekkäisyys muun kybersääntelyn kanssa sekä tunnustamis- ja auditointijärjestelmän hallinnollinen taakka.

2. Korkeimmat varmuustasot 3 ja 4: toimivalta, liikkumavara ja sisämarkkinat

Komission ehdotuksen mukaan tasoilla 3 ja 4 palveluntarjoaja ja sen alihankkijat eivät saa olla kolmannen maan määräysvallassa, henkilöstön on oltava unionin kansalaisia, tuki- ja ylläpitotoimintojen on tapahduttava unionissa ja tasolla 4 on hallittava myös ohjelmistokomponenttien kehitystä (liite II, 3.1 ja 4.1 kohdat). Komission vaikutusarvioinnin mukaan tasot kattaisivat noin kymmenen prosenttia julkisen sektorin tarpeista (U 54/2026 vp, s. 18).

Teknologiateollisuus

28.9.2026

Arvioinnin lähtökohta on IV luvun oikeusperusta. Ehdotus perustuu SEUT 114 artiklaan (sisämarkkinoiden lainsäädännön lähentäminen) ja 173 artiklan 3 kohtaan (teollisuuden kilpailukyky), joita valtioneuvosto pitää alustavasti asianmukaisina (U 54/2026 vp, luku 4). Suvereniteettikehys ja hankintavelvoitteet nojaavat käytännössä 114 artiklaan: niillä poistetaan kansallisista eroista johtuvia sisämarkkinaesteitä. SEU 4 artiklan 2 kohta rajaa unionin toimia, mutta ei poista unionin toimivaltaa säännellä sisämarkkinoilla tarjottavia palveluja silloinkaan, kun ostaja on turvallisuusviranomainen. EU-tuomioistuimen mukaan kansalliseen turvallisuuteen vetoaminen ei sellaisenaan sulje unionin oikeutta pois, kun sääntely koskee palveluntarjoajien velvoitteita (ks. esim. yhdistetyt asiat C-511/18, C-512/18 ja C-520/18 La Quadrature du Net ym. sekä C-623/17 Privacy International), ja myös SEUT 346 artiklaa tulkitaan suppeasti. Kansallisen turvallisuuden varauma koskee siis jäsenvaltion harkintaa suojattavista toiminnoista ja tiedoista, ei sitä, onko palvelumarkkinoilla yhteiset säännöt.

Jäsenvaltioilla on silti oltava liikkumavaraa: turvallisuusluokitusjärjestelmät ja varautumisen rakenteet poikkeavat toisistaan, ja Suomen vaatimukset ovat osin EU-tasoa tiukempia (esimerkiksi turvallisuusluokitellun tiedon sijainti ja henkilöstöturvallisuus). Samalla korkeimmilla tasoilla yhteiselle markkinalle on erityisen vahva tarve. Kysyntä on kapeaa, investoinnit raskaita ja sertifiointi kallista. Jos jokainen jäsenvaltio ylläpitää omia kriteerejään, eurooppalaiset toimittajat eivät saavuta mittakaavaa, ja markkinaa hallitsevat suurten jäsenvaltioiden kansallisten järjestelmien (kuten SecNumCloud) mukaiset toimijat. Suomelle yhteinen, unionin laajuisesti tunnustettava taso on sekä huoltovarmuuden että elinkeinopolitiikan kannalta parempi kuin kansallinen erillisratkaisu.

Tavoitteiden yhteensovittaminen edellyttää selkeää työnjakoa: EU määrittää yhteiset kriteerit ja tunnustamisen, jäsenvaltio tekee riskiarvioinnin yhteisellä menetelmällä ja voi kansallisessa turvallisuudessa perustellusti poiketa EU-tasoista, ja komissio valvoo, ettei tasomäärityksiä käytetä kotimaisen tarjonnan suosimiseen.

2.1 Riskiarviointien harmonisointi ja kaksi vyöhykettä (29 ja 30 art.)

Kannatamme 29 ja 30 artiklaa. Artiklassa 29 on kyse jäsenvaltioiden ja unionin toimielinten riskiarvioinneista ja niiden suorittamisen harmonisoinnista: arvioinneissa tunnistetaan yleisen järjestyksen kannalta merkittävät julkisen sektorin toiminnot ja määritetään niille soveltuva varmuustaso yhteisen menetelmän mukaisesti (29 art. 1–3 kohta). Artikla 30 kytkee hankintavelvoitteet arvioinnin tulokseen. Yhdenmukaiset riskiarvioinnit ovat edellytys sille, että varmuustasot tarkoittavat samaa kaikissa jäsenvaltioissa ja tunnustettu palvelu kelpaa koko unionissa.

Artiklat käsittelevät kuitenkin samassa yhteydessä kahta perusteiltaan erilaista kokonaisuutta, ja tämä vyöhykkeistö on säilytettävä. Ensimmäisen muodostavat kansallinen turvallisuus, puolustus ja turvallisuusluokitellun tiedon käsittely. Niissä peruste varmuustason määrittämiselle on valtion turvallisuus, eikä se kytkeydy sinänsä yhteiskunnan kannalta keskeisiin elinkeinoelämän sektoreihin (NIS2-direktiivin liitteet I ja II). Toisen muodostavat NIS2-sektoreilla toimivat julkisen sektorin toiminnot, kuten terveydenhuollon, energian ja liikenteen järjestelmät, joissa yleisen järjestyksen kannalta merkittävä peruste johdetaan sektorin kriittisyydestä. Ensimmäisessä vyöhykkeessä SEU 4 artiklan 2 kohta edellyttää jäsenvaltiolle harkintavaltaa, mutta täysi vapaaehtoisuus jättäisi korkeimpien tasojen

Teknologiateollisuus

28.9.2026

keskeisen kysynnän yhteisen kehyksen ulkopuolelle. Tasapainoinen ratkaisu on ”sovella tai selitä”: jäsenvaltio soveltaa lähtökohtaisesti EU-varmuustasoja ja voi poiketa niistä perustellusti, esimerkiksi kansallisten turvallisuusvaatimusten tai turvallisuusviranomaisten paikallisten, hybridi- ja varajärjestelyjen vuoksi. Ehdotuksen 29 artiklan 4 kohdan ilmoitusvelvollisuus poikkeamista on tälle hyvä pohja. Toisessa vyöhykkeessä riskiarviointi tehdään yhteisellä menetelmällä ja sen mukaista varmuustasoa sovelletaan 30 artiklan poikkeusperustein.

Kannanotto: Suomen tulee kannattaa 29 ja 30 artiklaa ja ajaa niiden jäsentämistä kahteen vyöhykkeeseen. Kansallisessa turvallisuudessa, puolustuksessa ja turvallisuusluokitellun tiedon käsittelyssä varmuustasojen käyttö perustuu ”sovella tai selitä” -periaatteeseen, eikä peruste kytkeydy NIS2-direktiivin sektoreihin. NIS2-sektoreiden yleisen järjestyksen kannalta merkittävissä julkisen sektorin toiminnoissa riskiarviointi tehdään yhteisellä menetelmällä ja sen mukaista tasoa sovelletaan. Lisäksi ”yleisen järjestyksen” (public order) käsite on selvennettävä, koska se määrittää korkeiden tasojen velvoitteiden ulottuvuuden.

2.2 Komission toimivalta riskiarvioinnissa on sisämarkkinoiden tae

Ehdotuksen 29 artiklan 5 kohdan nojalla komissio voisi täytäntöönpanosäädöksellä määrittää toiminnolle vaadittavan varmuustason, jos jäsenvaltion riskiarvion taso ei ole asianmukainen. Valtioneuvosto suhtautuu tähän varauksellisesti. Poikkeamme tästä ja kannatamme toimivaltaa, koska se on Suomen etujen mukainen.

Kehyksen suurin riski ei ole komission liian laaja valta vaan se, että jäsenvaltiot käyttävät riskiarviota teollisuuspolitiikan välineenä. Tasoa voidaan nostaa perusteettomasti, jotta vain kotimaiset tai kansallisen järjestelmän mukaan jo arvioidut toimittajat täyttävät vaatimukset, tai laskea, jotta vaatimukset alittava kotimainen toimittaja voi jatkaa sopimuksiaan. Kummassakin tapauksessa markkina jakautuu uudelleen kansallisiin lohkoihin.

Tämä on erityisen haitallista Suomen kaltaiselle pienelle ja avoimelle jäsenvaltiolle. Suomalaiset yritykset tarvitsevat muiden jäsenvaltioiden julkisia markkinoita, koska kotimarkkina ei riitä korkeimpien tasojen investointeihin. Suurilla jäsenvaltioilla on kotimaista tarjontaa ja markkinavoimaa suosia sitä, eikä pienellä jäsenvaltiolla ole keinoja puuttua toisen maan perusteettomiin tasomäärityksiin. Tasojen perusteeton laskeminen heikentäisi myös Suomen turvallisuutta, koska julkiset järjestelmät ovat yhä useammin kytköksissä rajojen yli. Pelkkä vertaispaine tai sitomaton suositus ei riitä estämään kansallista suosimista.

Toimivalta on sovitettava yhteen SEU 4 artiklan 2 kohdan kanssa, ja sen ulottumista kansalliseen turvallisuuteen, puolustukseen ja turvallisuusluokiteltuun tietoon on jatkovalmistelussa harkittava tarkasti. Jäsenvaltiolla on oltava harkintavaltaa kansallisen turvallisuutensa suojaamisen tasosta. Toisaalta tasojen 3 ja 4 kysyntä painottuu juuri näihin toimintoihin: jos ne jäävät kokonaan valvonnan ulkopuolelle, suosimisriski osuu siihen markkinaan, jossa eurooppalaisen tarjonnan mittakaava on kriittisin, ja vaarantuu turvallisuusviranomaisten, puolustushallinnon ja EU-toimielinten järjestelmien yhteentoimivuus. Valtioneuvosto on perustellusti todennut, ettei ehdotuksesta käy ilmi, millä perusteilla komissio voisi pitää jäsenvaltion arviota riittämättömänä.

Teknologiateollisuus

28.9.2026

Kannanotto: Suomen tulee kannattaa komission 29 artiklan 5 kohdan mukaista toimivaltaa ja edellyttää, että 1) toimivallan ulottumisen kansalliseen turvallisuuteen, puolustukseen ja turvallisuusluokiteltuun tietoon (SEU 4 art. 2 kohta) vaikutukset sisämarkkinoiden toimintaan ja yhteentoimivuuteen tasoilla 3 ja 4 harkitaan jatkovalmistelussa tarkasti; 2) käytön perusteet, kuten ilmeinen poikkeama yhteisestä menetelmästä tai syrjivä vaikutus muiden jäsenvaltioiden toimittajiin, kirjataan asetukseen; 3) jäsenvaltiota kuullaan ja päätös perustellaan; 4) päätökset tehdään tarkastelumenettelyssä; ja 5) tason muutokselle varataan riittävä siirtymäaika. Riskiarviointimenetelmän keskeisistä elementeistä säädetään asetuksessa.

2.3 Yhteinen kriteeristö – kansalliset lisävaatimukset vain perustellusti

Tasojen 3 ja 4 lisäarvo syntyy siitä, että kertaalleen tunnustettu palvelu kelpaa kaikissa jäsenvaltioissa. Samaa tarkoitusta palvelevat kansalliset suvereniteettijärjestelmät on siksi rajattava siirtymäkauteen. Jäsenvaltion on kuitenkin voitava edellyttää kansallisen turvallisuuden ja turvallisuusluokitellun tiedon suojaamiseksi tiukempia ehtoja, esimerkiksi tiedon sijainnista tai kansallisesta turvallisuusselvityksestä. Johdanto-osan 62 kappaleen toteamus, että tiedon arkaluonteisuuden määrittäminen kuuluu jäsenvaltioille, on kirjattava artiklatekstiin. Tunnustuksen tulee kelvata osanäyttönä myös kansallisessa tietoturvallisuusarvioinnissa (ks. HE 85/2026 vp) ja KriPassa.

Kannanotto: Tasojen 3 ja 4 tunnustus on voimassa kaikissa jäsenvaltioissa. Kansallisia lisävaatimuksia saa asettaa vain kansallisen turvallisuuden ja turvallisuusluokitellun tiedon suojaamiseksi, ne on perusteltava ja julkaistava, eivätkä ne saa olla piilotettua kansallisen alkuperän suosimista. Kansalliset suvereniteettiskeemat korvautuvat EU-tasoilla määräajassa.

2.4 Henkilöstö: turvallisuusselvitys kansalaisuuden sijaan

Tasot 3 ja 4 edellyttävät henkilöstöltä unionin kansalaisuutta (liite II, 3.1 d ja 4.1 d). Suomessa luotettavuus varmistetaan turvallisuusselvityksellä, ja yhdymme valtioneuvoston varaukseen. Kansalaisuus on karkea mittari: se sulkee pois esimerkiksi Norjan ja Islannin kansalaiset, vaikka ehdotus on ETA-merkityksellinen, mutta ei yksin takaa luotettavuutta. Vaatimus kaventaisi myös kyberturvallisuusalan jo ennestään niukkaa osaajapohjaa.

Turvallisuusluokitellun tiedon käsittelyssä henkilöstövaatimukset ovat perusteltuja ja kuuluvat jäsenvaltioiden ja EU:n turvallisuussääntöjen piiriin. Suomessa tämä edellyttää, että turvallisuusselvitysmenettely toimii myös yksityisen sektorin henkilöstön osalta ennakoitavin käsittelyajoin.

Kannanotto: Tasojen 3 ja 4 EU-kansalaisuusvaatimus korvataan vaatimuksella jäsenvaltion myöntämästä turvallisuusselvityksestä tai vastaavasta objektiivisesta henkilöstöturvallisuusmenettelystä. ETA-valtioiden kansalaiset rinnastetaan vähintään unionin kansalaisiin. Jäsenvaltio voi edellyttää kansalaisuutta tai kansallista turvallisuusselvitystä turvallisuusluokitellun tiedon käsittelyssä.

Teknologiateollisuus

28.9.2026

2.5 Tason 4 toimitusketjuvaatimus saavutettavaksi

Tasolla 4 on osoitettava, ettei kolmannella maalla ole tosiasiallista määräysvaltaa ohjelmistokomponenttien suunnitteluun, kehitykseen ja ylläpitoon (liite II, 4.1 kohdan i alakohta). Tavoite on kriittisimmissä toiminnoissa perusteltu, mutta vaatimus koskee kaikkia komponentteja, ja vaikutusarvioinnin mukaan sen täyttäviä ratkaisuja on vasta kehitteillä. Jos taso 4 jää käytännössä tyhjäksi, jäsenvaltiot turvautuvat kansallisiin erillisratkaisuihin ja markkina pirstoutuu. Myös tasojen 2 ja 3 lähdekoodiauditointivaatimus on suljetun lähdekoodin tuotteissa osin mahdoton toteuttaa.

Kannanotto: Tason 4 vaatimus kohdistetaan riskiperusteisesti turvallisuuskriittisiin komponentteihin ja muotoillaan todennettaviksi kyvykkyyksiksi: kyky ylläpitää, korjata ja jatkaa palvelua itsenäisesti (esimerkiksi lähdekoodin talletus, mahdollisuus jatkaa avoimen lähdekoodin komponentin kehitystä itsenäisesti (haarautettavuus), oma käännös- ja päivitysketju ja dokumentoitu migraatiosuunnitelma). Toimitusketjuvaatimukset ja SBOM-velvoitteet yhdenmukaistetaan kyberkestävyyssäädöksen (CRA) käsitteiden ja prosessien kanssa.

2.6 Kolmannen maan määräysvalta ja kumppanimaat (18 art.)

Pidämme omistukseen ja määräysvaltaan perustuvaa rajausta tasoilla 3 ja 4 hyväksyttävänä, koska se vastaa niiden tarkoitusta suojata toimintoja kolmansien maiden oikeudelliselta ulottuvuudelta ja keskeytysriskiltä. 18 artiklan kumppanimaamekanismi tuo tarpeellista joustoa ja tukee valtioneuvoston tavoitetta vastavuoroisesta tunnustamisesta luotettujen kumppanien kanssa. Päätösten peruuttamiselle on säädettävä siirtymäajat, ja telemetriavaatimukset on rajattava niin, etteivät ne estä kyberuhkatiedon jakamista. Teknisenä korjauksena liitteen II 3.1 kohdan g alakohdan viittaus 19 artiklaan tulee korjata viittaukseksi 18 artiklaan.

3. Sertifiointi, tunnustaminen ja valvonta (16–28 art.)

Tasot 2–4 edellyttävät EUCS-sertifikaattia, mutta järjestelmää ei ole vielä hyväksytty, ja sen aikataulu on valtioneuvoston mukaan avoin. Kansallisiin järjestelmiin nojaava siirtymäratkaisu sirpaloi sisämarkkinaa. Velvoitteet on siksi kytkettävä EUCS:n valmistumiseen ja Suomen kansalliset arviointikäytännöt tunnustettava siirtymäkaudella. Sertifikaattien ja auditointien on kelvattava näyttönä myös NIS2- ja CRA-vaatimuksista.

Tunnustamismenettely (17 art.) voi venyä, koska komission lopulliselle päätökselle ei ole määräaikaa. Menettelylle on säädettävä sitova kokonaismääräaika ja valtioneuvoston tavoin muutoksenhakuoikeus. Auditointikapasiteetista uhkaa tulla pullonkaula, jota 10 vuoden rotaatio ja 12 kuukauden karenssi (20 art. 4 kohta) pahentavat; riittävä määrä päteviä auditointiorganisaatioita on varmistettava ennakoivasti.

Velvoitteiden jakautuminen pilvipinon kerrosten (IaaS, PaaS, SaaS) kesken on epäselvä. Sovelluspalvelua tarjoava pk-yritys vastaisi myös alustatoimittajansa omistus-, lähdekoodi- ja migraationäytöistä ilman neuvotteluasemaa saada niitä. Ilman tunnustamisen periytyvyyttä koko pino auditoidaan jokaisen palvelun kohdalla, ja korkeiden tasojen markkina kapenee suurille integroituneille toimijoille.

Teknologiateollisuus

28.9.2026

Suomessa toimivaltaiseksi viranomaiseksi on luontevinta nimetä Traficom (Kyberturvallisuuskeskus) synergiasyistä NIS2- ja CRA-valvonnan kanssa.

Kannanotto: Tasojen 2–4 velvoitteet sidotaan EUCS:n hyväksymiseen, KriPa tunnustetaan siirtymäkaudella ja näyttöjä hyödynnetään ristiin. Tunnustamiselle säädetään sitova kokonaismääräaika, muutoksenhakuoikeus ja periytyvyys – tunnustetun palvelun päälle rakennettu kerros auditoidaan vain omalta osaltaan – sekä alustatoimittajan velvollisuus antaa tarvittava näyttö kohtuullisin ja syrjimättömin ehdoin. Valvonta keskitetään Traficomille.

4. Julkisten hankintojen velvoitteet (29–33 art.)

Riskiperusteinen tason määräytyminen toiminnon kriittisyyden mukaan on oikea, ja multi-cloud-strategioiden huomiointi (29 art. 9 kohta) on myönteistä. Enintään 12 kuukauden migraatioaika (29 art. 6 kohta) on suurissa järjestelmissä epärealistinen ja itsessään jatkuvuusriski. Yhdymme valtioneuvoston varaukseen velvoitteiden soveltamisesta olemassa oleviin järjestelmiin kesken sopimuskauden.

Tason 1 vähimmäisvaatimus kaikissa julkisissa pilvihankinnoissa (30 art. 2 kohta) on merkittävä markkinainterventio, jonka oikeasuhtaisuus on arvioitava uudelleen ja poikkeusperusteet (30 art. 4 kohta) täsmennettävä. Tunnustettuja palveluja on oltava rekisterissä saatavilla ennen soveltamista.

Yksityisen sektorin vapaaehtoiset vaikutusarvioinnit (31 art.) ovat hyväksyttäviä, mutta 31 artiklan 3 kohdan valtuus velvoittaa NIS2-toimialojen yrityksiä delegoidulla säädöksellä on poistettava: yksityistä sektoria velvoittavista vaatimuksista säätäminen tulisi harkita tarkkaan joko ehdotetun tai tavallisen lainsäätämisjärjestyksen mukaisesti.

Unionin lisäarvon kriteerit (32 art.) on pidettävä liitännäisinä, esimerkiksi enimmäispainoarvolla rajattuina. Ne eivät saa syrjiä globaaleissa arvoketjuissa toimivia vientiyrityksiä, ja niiden tulisi olla sopusoinnussa WTO:n GPA-sopimuksen kanssa. Pk-yritysten 25 prosentin hankintatavoite (33 art.) on myönteinen, kunhan raportointi pysyy kevyenä.

Kannanotto: Migraatioaika pidennetään 24–36 kuukauteen ja sidotaan palvelun elinkaareen ja sopimuskauteen, 30 artiklan poikkeukset täsmennetään, tason 1 yleisvelvoite arvioidaan uudelleen ja 31 artiklan 3 kohdan delegointivaltuus harkitaan tarkasta jatkovalmistelussa.

5. Komissiolle siirrettävä säädösvalta (16 art.)

Markkinoillepääsyn kannalta ratkaisevia liitteitä II ja III komissio voisi muuttaa delegoiduilla säädöksillä ja tarkistaisi ne 18 kuukauden välein (16 art. 2 ja 3 kohta). Vaatimustenmukaisuusinvestoinnit ovat monivuotisia, joten liikkuva kriteeristö heikentää ennakoitavuutta – erityisesti korkeimmilla tasoilla.

Kannanotto: Varmuustasojen keskeiset kriteerit kirjataan asetuksen artikloihin, delegoitu valta rajataan teknisiin päivityksiin, pakollista tarkistussykliä

Teknologiateollisuus

28.9.2026

pidennetään ja kriteerimuutoksille säädetään siirtymäajat, jotta jo myönnetyt tunnustamiset eivät raukea takautuvasti.

6. Muut huomiot

EuroCloud-federaation (34–36 art.) kustannusperusteinen palvelujen jakaminen ilman kilpailutusta on rajattava aitoon ylikapasiteettiin, ja jaettaviin palveluihin on sovellettava samoja vaatimuksia kuin hankittaviin. Viranomaisten ei tule tuottaa palveluja, joita markkinat tarjoavat.

Avoimen lähdekoodin osalta yhdymme valtioneuvostoon: suvereniteetti ei riipu lisensointimallista, ja hankintojen on säilyttävä teknologianeutraaleina.

Tekoälyn kokemus- ja kiihdytyskeskusten (5 art.) rinnalla tulee tunnistaa yritysvetoiset tekoälyverkostot, kuten AI Finland, päällekkäisten julkisvetoisten rakenteiden välttämiseksi. Datakeskusten nopean kehittämisen alueiden nimeämisen on oltava vapaaehtoista, hankkeiden on oltava mahdollisia myös alueiden ulkopuolella ja kuntien kaavoitusautonomia on turvattava.

Lisätietoja:

Peter Sund, toimitusjohtaja, Kyberala ry, peter.sund@teknologiateollisuus.fi, 050-5650621

Ville Peltola, päällikkö, Teknologiateollisuus ry, ville.peltola@teknologiateollisuus.fi, 040-553 9941