U 54/2026 vp
Google Finland Oy
Kirjallinen asiantuntijalausunto
TaV 6.10.2026

Valtioneuvoston kirjelmä eduskunnalle ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi kehyksen perustamiseksi Euroopan pilvipalvelu- ja tekoälyekosysteemin vahvistamiseksi (pilvipalveluiden ja tekoälyn kehittämisen säädös)

Google kiittää mahdollisuudesta lausua asiasta talousvaliokunnalle.

1. Tiivistelmä

Google jakaa Suomen näkemyksen kilpailukykyisestä, innovatiivisesta, häiriönsietokykyisestä, avoimesta ja teknologisesti suvereenista eurooppalaisesta digitaalisesta taloudesta. Katsomme, että Euroopan digitaalisen johtoaseman tulisi perustua **markkinaehtoisiin ratkaisuihin, sääntelyn yksinkertaistamiseen, teknologianeutraaliuteen, avoimeen kilpailuun ja luotettaviin kansainvälisiin kumppanuuksiin**.

Näiden tavoitteiden osalta näkemyksemme on pitkälti yhtenevä Suomen kannan kanssa keskeisillä politiikan aloilla. Kannatamme jäsenvaltioiden harkintavaltaa kansalliseen turvallisuuteen liittyvissä kysymyksissä, suhtaudumme pidättyvästi julkista sektoria koskevien riskiarviointien laajentamiseen yksityisiin NIS2-toimijoihin, vastustamme maantieteelliseen alkuperään perustuvaa protektionismia, emme kannata avoimen lähdekoodin kategorista asettamista suljettujen ohjelmistojen edelle ja pidämme toimivaa auditointikehystä tarpeellisena.

Suomen turvallisia kansainvälisiä tietovirtoja koskevan kannan pohjalta suosittelemme, että CADA-asetusehdotuksen telemetriaa ja metatietoja koskevan, Eurooppaan rajattuun lokalisointiin perustuvan lähestymistavan aiheuttamiin kyberturvallisuusriskeihin kiinnitettäisiin vahvemmin huomiota. Näkemyksemme mukaan Suomen kannassa olisi tärkeää erottaa nimenomaisesti toisistaan asiakassisältö sekä uhkatiedusteluun liittyvät telemetriatiedot ja metatiedot.

Telemetriatietojen maailmanlaajuinen käsittely on teknisesti välttämätöntä tehokkaalle kyberpuolustukselle ja uhkien ennaltaehkäisylle. Se mahdollistaa hyökkäysvektorien tunnistamisen, varhaisen tiedon Eurooppaan kohdistuvista maailmanlaajuisista kyberuhkista sekä reaaliaikaisen puolustuksen, jolla uhkia voidaan torjua ennen kuin ne kohdistuvat EU:ssa sijaitseviin kohteisiin.

2. Yleisesti: kilpailukyky, yksinkertaistaminen ja markkinaehtoinen kasvu

2.1 Tuki Suomen näkemykselle sääntelyn yksinkertaistamisesta ja oikeasuhteisuudesta

Google pitää myönteisenä valtioneuvoston painotusta siitä, että CADA-asetuksella on edistettävä sääntelyn yksinkertaistamista, teknologianeutraaliutta ja oikeasuhteisuutta. Suomi korostaa nimenomaisesti, että viranomaisille asetettavat uudet tehtävät on rajattava soveltamisen kannalta

aidosti välttämättömiin tehtäviin, EU:n toimielinten hallinnolliset menot ja henkilöstöresurssit on pidettävä kohtuullisina ja olemassa olevia rakenteita on hyödynnettävä mahdollisimman laajasti.

Google tukee vahvasti Suomen yksinkertaistamista koskevaa painotusta. Jotta tavoite toteutuisi täysimääräisesti, Suomi voisi edistää sitä, että uudella lainsäädännöllä vältetään data-asetuksen, NIS2-direktiivin, yleisen tietosuoja-asetuksen ja kyberturvallisuussäädöksen mukaisten velvoitteiden päällekkäisyys. Vastaavasti olisi vältettävä ristiriitaisia velvoitteita uusien EU-säädösten, kuten CSA2:n, CADA-asetuksen ja EU:n julkisia hankintoja koskevan sääntelyn, välillä. Tämä tukisi Euroopan kilpailukykyä ja tekoälyn käyttöönottoa.

2.2 Pilvi-infrastruktuurin markkinaehtoinen kehittäminen

Pilvi-infrastruktuuria ja laskentakapasiteettia olisi kehitettävä mahdollisimman pitkälle markkinaehtoisesti. Julkisessa rahoituksessa, kuten tutkimus-, kehittämis- ja innovaatiorahoituksessa, kasvurahoituksessa ja innovatiivisissa hankinnoissa, olisi keskityttävä skaalautuvuuden ja avoimen kilpailun edistämiseen.

Pidämme Suomen markkinaehtoista lähestymistapaa kannatettavana. Kaupalliset investoinnit, joita ohjaavat avoimet energia- ja sähköverkkokehykset sekä asiakkaiden kysyntä, tarjoavat tehokkaimman keinon kasvattaa Euroopan häiriönsietokykyistä laskentakapasiteettia.

3. Pilari I: tutkimus, kehitys, innovaatiot, käyttöönoton vauhdittaminen ja osaaminen (3–9 artikla)

3.1 Tekoälykokemus- ja kiihdytyskeskukset (5 artikla)

Suomi tukee tekoälykokemus- ja kiihdytyskeskusten perustamista olemassa olevien eurooppalaisten digitaali-innovointikeskittymien (EDIH) pohjalta, mutta korostaa, että päällekkäisiä julkisvetoisia rakenteita on vältettävä ja keskusten on vastattava todellisiin liiketoimintatarpeisiin.

Google yhtyy näkemykseen olemassa olevien keskittymärakenteiden hyödyntämisestä. Keskusten tulisi kuitenkin säilyä ketterinä, markkinoiden tarpeisiin vastaavina ja suoraan yksityisen sektorin innovoijien sekä pk-yritysten saavutettavissa olevina. Keskuksia ei tulisi nimetä maantieteellisten kiintiöiden perusteella, vaan laskentakysynnän, kuituyhteyksien tiheyden ja käytettävissä olevan sähköverkkokapasiteetin perusteella.

3.2 Prioriteettihankkeet ja laskentaresurssien kohdentaminen (8–9 artikla)

Pidämme myönteisenä Suomen painotusta markkinaehtoisiin hankintoihin sekä yhteistyöhön luotettavien kaupallisten pilvipalveluntarjoajien kanssa. Näin voidaan varmistaa uusimman teknologian saatavuus ilman julkisten laskentamonopolien syntymistä.

Tällainen lähestymistapa turvaa riittävät tekoälylaskentaresurssit prioriteettihankkeille ja mahdollistaa parhaan saatavilla olevan innovaation hyödyntämisen.

3.3 Kansalliset pilvi- ja tekoälystrategiat (7 artikla)

Ymmärrämme Suomen kyseenalaistavan, tuottaako velvollisuus laatia kansallisia pilvi- ja tekoälystrategioita tosiasiallista lisäarvoa, sekä korostavan, että velvoitteen on pysyttävä tiukasti oikeasuhteisena.

Tämän mukaisesti ehdotamme, että hallinnollisten velvoitteiden sijasta painotetaan konkreettisia puitteita, jotka mahdollistavat teknologioiden käyttöönoton.

4. Pilari II: datakeskukset, luvitus ja nopean kehittämisen alueet (10–15 artikla)

4.1 Nopean kehittämisen alueiden vapaaehtoinen osoittaminen (10 artikla)

Pidämme myönteisenä, että Suomi kiinnittää huomiota datakeskusten nopean kehittämisen alueisiin. Sähköverkkokapasiteetin kohdentamisen tulisi perustua tiukasti sähkömarkkinoiden sääntöihin. Kohdentaminen ei saa perusteettomasti syrjäyttää muita investointeja eikä mahdollistaa spekulatiivisia kapasiteettivarauksia.

Alueiden tulisi toimia investointeja helpottavana vaihtoehtona eikä investointien edellytyksenä. Kehittämisen nimettyjen alueiden ulkopuolella on säilyttävä joustavana, syrjimättömänä ja tarpeettomista rasitteista vapaana. Alueen ulkopuolelle jääminen ei saa hidastaa hankkeita eikä johtaa uusiin sääntelyesteisiin.

Jos alueita osoitetaan, niiden valinnan tulisi perustua laskentakysyntään, yhteyksiin ja käytettävissä olevaan sähköverkkokapasiteettiin eikä maantieteellisiin kiintiöihin. Kestävyysvaatimusten tulisi perustua EU:n luokitusjärjestelmään, mutta niiden soveltamisessa olisi oltava joustavuutta paikallisten ympäristö-, ilmasto-, vesi- ja lämpöverkko-olosuhteiden osalta.

Google kannustaa Suomea hyödyntämään kaavoitusta ennakoivasti datakeskuskampusten ympärille muodostuvien taloudellisten ekosysteemien rakentamisessa. Datakeskusten viereisten, ennakolta kaavoitettujen teollisuusalueiden varaaminen mahdollistaa esimerkiksi kasvihuoneiden, vertikaaliviljelyn, vesiviljelyn ja kaukolämpöverkkojen kytkemisen suoraan datakeskusten hukkalämpöön. Näin kaavoitus muuttuu lupamenettelyn esteestä alueellisen kasvun välineeksi. Kokemuksemme mukaan tämä on tehokkain tapa varmistaa laajamittaisten investointien pysyvä paikallinen hyväksyttävyys.

Google ehdottaa joustavaa lähestymistapaa, jossa nopean kehittämisen alueiden osoittaminen sovitetaan yhteen käytettävissä olevan puhtaan energian ja sähköverkkoinfrastruktuurin kanssa sen sijaan, että alueet määriteltäisiin ylhäältä ohjatuin maantieteellisin perustein. Samalla nimettyjen alueiden ulkopuolella oleville kypsille sähköverkkoliityntähakemuksille on säilytettävä sitovat käsittelyajat. Sovittua kapasiteettia ei saa viivästyttää, jäädyttää tai kohdentaa uudelleen sillä perusteella, ettei hanke sijaitse nopean kehittämisen alueella.

Sääntelyn pirstaloitumisen välttämiseksi kaikki datakeskusten kestävyysvaatimukset olisi sidottava EU:n luokitusjärjestelmään. Järjestelmän on samalla mahdollistettava joustavuus paikallisten ympäristö-, ilmasto-, vesi- ja lämpöverkko-olosuhteiden huomioon ottamiseksi.

4.2 Pakollisen hiljaisen hyväksynnän ja peruslupien vastustaminen (13 artikla)

Ymmärrämme Suomen vastustavan pakollista hallinnollista hiljaista hyväksyntää perustuslain 21 §:ssä turvattujen oikeusturvatakeiden vuoksi. Yhteen koottujen peruslupien edistämistä pidetään ongelmallisena kunnallisen kaavoitusautonomian kannalta, joka perustuu perustuslain 121 §:ään.

Google kunnioittaa Suomen valtiosääntöoikeudellisia näkökohtia. Tehokkaat lupamenettelyjen määräajat, esimerkiksi tavoitteellinen 12 kuukauden käsittelyaika, voidaan saavuttaa hallinnollisia menettelyjä sujuvoittamalla siten, että jäsenvaltioiden oikeusturvatakeet säilyvät täysimääräisesti.

5. Pilari III: pilvisuvereniteetti, varmuustasot ja sertifiointi (16–28 artikla)

5.1 Henkilöstön kansalaisuusvaatimusten vastustaminen (16 ja 29 artikla sekä liite II)

Pidämme myönteisenä Suomen esittämiä varaumia vaatimuksiin, joissa henkilöstön luotettavuutta arvioitaisiin kansalaisuuden tai muiden ei-objektiivisten perusteiden nojalla. Kansallinen luotettavuus on arvioitava objektiivisten taustaselvitysten, ei kansalaisuuden, perusteella.

Tuemme Suomen kantaa, jonka mukaan varmuustasoihin 3 ja 4 ei tule sisällyttää henkilöstön kansalaisuuteen perustuvia rajoituksia. Henkilöstön rajaaminen kansalaisuuden perusteella vaikeuttaa maailmanlaajuisen teknisen asiantuntemuksen hyödyntämistä ja heikentää turvallisuuden vaikuttavuutta lisäämättä luottamusta.

CADA-asetuksen liitteessä II oleva rajoittamaton viittaus kaikkiin pilvipalvelujen tarjoamiseen osallistuviin alihankkijoiden työntekijöihin, joiden olisi oltava EU:n kansalaisia, merkitsisi, etteivät alihankkijoiden työntekijät voisi osallistua pilvipalvelujen tuottamiseen, vaikka he sijaitsisivat EU:ssa ja heillä olisi oikeus tehdä työtä EU:ssa.

Pilvipalveluntarjoajat ja niiden alihankkijat hyödyntävät usein maailmanlaajuista osaajapoolia myös Euroopassa toteutettavassa toiminnassaan. Vaatimus vaikeuttaisi merkittävästi pilvipalveluntarjoajien mahdollisuuksia tarjota palvelujaan varmuustasoilla 3 ja 4. Se voi myös kasvattaa kustannuksia ja heikentää Euroopan kilpailukykyä, jos pätevä henkilöstö ei voi osallistua pilvipalvelujen tarjoamiseen.

5.2 Muutoksenhakuoikeus ja menettelylliset oikeudet (17 artikla)

CADA-asetuksen mukainen varmuustasojen tunnustaminen edellyttää tarjoajien oikeusvarmuutta, jotta ne voivat palvella EU:n julkisen sektorin markkinoita tehokkaasti ja johdonmukaisesti. Suomi edellyttää nimenomaisesti, että CADA-asetuksessa säädetään selkeästä muutoksenhakuoikeudesta pilvipalvelujen varmuustasojen tunnustamista tai peruuttamista sekä strategisten hankkeiden nimeämistä koskeviin päätöksiin.

Yhdymme näkemykseen, jonka mukaan 17 artiklan mukainen pilvipalveluntarjoajien tunnustamismenettely edellyttää muutoksia riittävän oikeusvarmuuden turvaamiseksi. Suomen

vaatimus vahvoista menettelyllisistä oikeuksista korostaa, että nimenomaiset oikeussuojakeinot ovat välttämättömiä oikeusvarmuuden ja tasapuolisen markkinakilpailun kannalta.

5.3 Auditointi, sertifiointi ja toimiva vaatimustenmukaisuus (19–21 artikla)

Pidämme myönteisenä Suomen periaatteellista tukea riippumattomille kolmannen osapuolen auditoinneille. Samalla on tärkeää huomioida, että vaatimukset pysyvät oikeasuhteisina, vältetään olemassa olevien sertifiointien, kuten EUCS:n, päällekkäisyyttä ja ehkäistään kohtuuttomien markkinoille pääsyn esteiden muodostuminen.

Tarkastusten ja auditointien tulisi tarkoituksenmukaisen yhdenmukaistamisen varmistamiseksi perustua vakiintuneisiin kansainvälisiin standardeihin, kuten ISO/IEC 27001- ja SOC 2 -standardeihin.

5.3.1 Auditointiraporttien saatavuuden pullonkaulojen estäminen

CADA-asetuksen 20 artiklan 4 kohdan a alakohdassa pyritään määrittelemään eturistiriitoja ja asetetaan perusteita, joiden nojalla tarkastusyhteisö ei voisi tarjota palveluja tarkastettavalle pilvipalveluntarjoajalle. Alakohdan a alakohdassa ii otetaan käyttöön kymmenen vuoden estoaika yhteistyölle kyseisen tarkastusyhteisön kanssa.

Näissä olosuhteissa pätevät tarkastusyhteisöt sulkeutuisivat automaattisesti pois kymmeneksi vuodeksi ensimmäisen toimeksiannon jälkeen. Lisäksi alakohdassa a alakohdassa i säädetään hyvin laajasta kiellosta tarjota muita kuin auditointipalveluja. Suuret tarkastusyhteisöt tarjoavat maailmanlaajuisesti laajan valikoiman vero-, konsultointi- ja paikallisia vaatimustenmukaisuuspalveluja. Koska rajoitus ulottuu kaikkiin yhteenliittyneisiin oikeushenkilöihin, jo vähäinen toimeksianto palveluntarjoajan konserniyhtiölle missä tahansa maailmassa voisi estää koko maailmanlaajuisen tarkastusverkoston osallistumisen auditointipalvelun tarjoamista koskevaan kilpailutukseen.

Kymmenen vuoden takautuva tilintarkastajan vaihtovaatimus voisi käytännössä edellyttää uuden tarkastusyhteisön käyttämistä joka vuosi. Tällaisella tulkinnalla Google Cloudin kaltaiset palveluntarjoajat tarvitsisivat CADA-auditointien ollessa vuosittaisia kymmenen täysin erillisen, erittäin pätevän tarkastusyhteisön joukon, jota kierrätettäisiin liukuvalla kymmenen vuoden jaksolla. Tälle jäähtymisajalle ei ole esitetty perusteltua sääntelypoliittista syytä.

Samalla CADA-asetuksen 20 artiklan 4 kohdassa omaksutaan muusta EU-sääntelystä poikkeava lähestymistapa, mikä lisää sääntelyn pirstaloitumista. Digipalvelusäädöksessä (DSA) kielletään tarkastusyhteisön käyttäminen vasta silloin, kun sitä on käytetty yli kymmenen peräkkäisen vuoden ajan. Sama tarkastusyhteisö voidaan siis käyttää vuodesta toiseen tähän rajaan asti.

Nykyisillä auditointimarkkinoilla kymmenen erillisen, pätevän sekä laajoihin hyperscale-pilviympäristöihin soveltuvan tarkastusyhteisön löytäminen on käytännössä lähes mahdotonta. Yhdessä muiden rajoitusten, kuten muiden kuin auditointipalvelujen rajoitusten, kanssa käytettävissä olevien toimijoiden joukko supistuu tosiasiallisesti olemattomaksi. Tällaiset yksityiskohtaiset ja käytännössä toteuttamiskelvottomat kelpoisuussäännöt sulkisivat markkinoilta lähes kaikki pätevät tarkastajat. Pilvipalveluntarjoajat eivät tällöin voisi sertifioida palvelujaan, mikä muodostaisi keinotekoisen pullonkaulan ja pysäyttäisi EU:n julkisen sektorin pilvipalvelujen käyttöönottoa.

5.3.2 Alihankintaa koskevien vaatimusten mukauttaminen markkinarealiteetteihin ja oikeusvarmuuden varmistaminen

Suomi korostaa tarvetta välttää tarpeettomia vaatimustenmukaisuuskustannuksia ja hallinnollista taakkaa pilvipalveluntarjoajille sekä niiden toimitusketjuille. CADA-asetuksen liite II aiheuttaa huolestuttavaa oikeudellista epävarmuutta alihankintaa koskevassa lähestymistavassaan.

Alihankinnan soveltamisala. CADA-asetuksessa ei määritellä, mitä alihankkijalla tarkoitetaan. Tässä lausunnossa lähtökohtana on siten, että asetuksen alihankintavaatimuksia sovelletaan kaikkiin toimeksisaajiin, joita pilvipalveluntarjoaja (CSP) ohjeistaa suoraan tai välillisesti suorittamaan ja toimittamaan osan tarjottavista pilvipalveluista.

Tämä merkitsee, että alihankintavelvoitteiden soveltamisala ei ole selkeä, oikeasuhteinen eikä riskiperusteinen. Velvoitteet voisivat ulottua kaikkiin alihankkijoihin riippumatta niiden tosiasiallisesta roolista pilvipalvelujen tuottamisessa.

Maantieteellinen sijainti. Kaikilla varmuustasoilla edellytetään, että pilvipalvelujen tarjoamiseen osallistuvien alihankkijoiden infrastruktuuri ja omaisuus sijaitsevat EU:ssa. Varmuustasolla 1 julkisen sektorin toimija voi poiketa tästä vaatimuksesta. Varmuustasoilla 2, 3 ja 4 maantieteellinen vaatimus ulotetaan myös alihankkijoiden henkilöstöön.

Hyperscale-pilvipalveluntarjoajien ja niiden alihankkijoiden infrastruktuuri, omaisuus ja henkilöstö ovat usein maailmanlaajuisesti hajautettuja. Käytännössä vaatimus todennäköisesti estäisi monia pilvipalveluntarjoajia, myös sellaisia EU:hun sijoittautuneita toimijoita, jotka hyödyntävät maailmanlaajuisia alihankkijoita, tarjoamasta palvelujaan varmuustasoilla 2, 3 ja 4. Lisäksi olisi huomattavaa epävarmuutta siitä, milloin palveluntarjoaja voisi tarjota palveluja varmuustasolla 1.

Varmuustasoihin 2, 3 ja 4 sisältyy lisäksi erillinen vaatimus, jonka mukaan tekninen ja operatiivinen tuki tai avustaminen, myös edelleen alihankitut järjestelyt, on aloitettava ja toteutettava yksinomaan unionin alueella. Pilvipalveluntarjoajien tuki on tavallisesti maailmanlaajuisesti järjestettyä, erityisesti ympärivuorokautisten 24/7/365-tukipalvelujen tarjoamiseksi. Tuen rajaaminen yksinomaan EU:ssa sijaitsevaan henkilöstöön voi kasvattaa kustannuksia ja heikentää palvelun laatua, koska tukipyyntöjä ei voida ratkaista tehokkaimmin sen henkilöstön toimesta, jolla on parhaat edellytykset ja osaaminen ratkaista tekniset ongelmat.

Sijoittautuminen EU:hun. Varmuustasot 2, 3 ja 4 edellyttävät, että alihankkijat ovat sijoittautuneet EU:hun. Jos alihankkijan käsitettä tulkitaan laajasti, vaatimus muodostuu erittäin ongelmalliseksi. Pilvipalveluntarjoajat käyttävät erilaisia alihankkijoita, joista monet sijaitsevat EU:n ulkopuolella. Joissakin tapauksissa alihankkijat tarjoavat tiettyjä tuotteita maailmanlaajuisesti yhden palveluntarjoajien kanssa tehdyn puitesopimuksen perusteella. Tällaisia voivat olla esimerkiksi alkuperäiset laitevalmistajat, joiden tuotteet on usein integroitu pilvipalveluntarjoajien palveluihin maailmanlaajuisesti.

Vaatimus erottaa maailmanlaajuiset käytännöt ja alihankkijat EU:ssa toteutettavista toiminnoista asettaisi Euroopan kilpailullisesti epäedulliseen asemaan. Se johtaisi myös käytännön esteisiin, joiden vuoksi keskeisiä palveluja ei ehkä olisi saatavilla varmuustasoilla 2, 3 ja 4. Lähestymistapa estäisi myös asiakkaita hankkimasta pilvipalveluja EU:hun sijoittautuneelta tarjoajalta, joka hankkii kriittisiä palveluja

tai teknologioita EU:n ulkopuolisilta alihankkijoilta, vaikka niitä ei muutoin olisi saatavilla EU:ssa tai samalla teknisellä tasolla.

EU-kansalaisuus. Varmuustasoilla 3 ja 4 kaikkien pilvipalvelujen tarjoamiseen osallistuvien alihankkijoiden työntekijöiden olisi oltava EU:n kansalaisia. Tämä estäisi alihankkijoiden henkilöstöä osallistumasta pilvipalvelujen tuottamiseen, vaikka henkilöstö sijaitsisi EU:ssa ja sillä olisi oikeus työskennellä unionin alueella.

Alihankintaketjut. Liitteen II kohtien 1.2 ja 2.2 mukaan alihankkijoilla on oltava suora sopimussuhde pilvipalveluntarjoajaan. Jos tätä luetaan kirjaimellisesti, alihankintaketjuja ei sallittaisi, esimerkiksi alihankkijan alihankintaa. Tämä ei vastaa pilvipalvelujen käytännön toteutustapaa, jossa hyödynnetään usein useita alihankintatasoja.

Monitasoinen alihankintaketju hyödyttää loppuasiakasta, koska se mahdollistaa erikoistuneen osaamisen, skaalautuvien resurssien ja ketterän palvelutuotannon hyödyntämisen, samalla kun vastuullinen päätoimittaja säilyttää kokonaisvastuun. Liitteen II sanamuoto ei ole riittävän selkeä siitä, sovelletaanko CADA-asetuksen alihankintavaatimuksia vain alihankkijoihin, joilla on suora sopimussuhde pilvipalveluntarjoajaan, ilman että alihankintaketjuja kuitenkaan kielletään. Kohtia 1.2 ja 2.2 on täsmennettävä, jotta vältetään suhteeton vaikutus alihankintaketjuihin.

Kokonaisuutena CADA-asetuksen alihankintavaatimusten laajuus todennäköisesti estäisi tai vaikeuttaisi merkittävästi pilvipalveluntarjoajien palvelutarjontaa kaikilla varmuustasoilla ja erityisesti varmuustasoilla 2, 3 ja 4. Monissa tapauksissa vaatimusten täyttäminen ei olisi käytännössä mahdollista. Muissa tapauksissa vaatimusten noudattaminen kasvattaisi kustannuksia ja voisi rajoittaa Euroopassa saatavilla olevia parhaita palveluja ja tukitoimintoja.

5.3.3 Kolmannen maan määräysvalta

Liitteen II 3.1 kohdan g alakohdassa ja 4.1 kohdan g alakohdassa kielletään se, että pilvipalveluntarjoaja tai sen alihankkija on kolmannen maan tai kolmanteen maahan sijoittautuneen oikeushenkilön määräysvallassa. Varmuustasolla 3 poikkeuksena ovat kolmannet maat, jotka sisältyvät vielä vahvistamatta olevaan hyväksyttyjen maiden luetteloon.

Jo varmuustasolla 2 palveluntarjoajien ja alihankkijoiden olisi kuitenkin voitava osoittaa täyttävänsä useita kolmansiin maihin liittyvää riippumattomuutta koskevia vaatimuksia. Lähestymistapa aiheuttaa haitallista oikeudellista epävarmuutta ja vaaran siitä, että EU:n ulkopuoliset toimijat suljetaan pois riippumatta luotettavasta kumppanuussuhteesta tai siitä, että niiden palvelut tarjoavat eurooppalaisille asiakkaille korkeatasoista hallintaa.

Alihankkijat voisivat jäädä varmuustasolla 2 pilvipalvelujen tukitoimintojen ulkopuolelle. Tämä merkitsisi myös sitä, ettei EU:hun sijoittautunut palveluntarjoaja voisi käyttää EU:n ulkopuolella sijaitsevaa tytäryhtiötään alihankkijana. Tämän vuoksi hyperscale-pilvipalveluntarjoajat eivät ehkä voisi tukea pilvipalveluja varmuustasolla 2.

5.3.4 Kolmansien maiden tunnustaminen

Suomi tukee nimenomaisesti teknologisia kumppanuuksia, jotka perustuvat EU:n kahdenvälisiin sopimuksiin ja vastavuoroista tunnustamista koskeviin järjestelyihin luotettavien kansainvälisten kumppaneiden kanssa.

Ehdotetun 18 artiklan kumulatiiviset hyväksymiskriteerit voivat johtaa Euroopan markkinoiden vakavaan eristäytymiseen. Suomen luotettavaa kansainvälistä yhteistyötä ja turvallisia tietovirtoja koskevan tavoitteen toteuttamiseksi **suosittelemme 18 artiklan mekanismin kääntämistä siten, että kolmannen maan liittäminen järjestelmään olisi lähtökohtaisesti sallittua**. Samalla olisi säädettävä selkeästi rajatuista varavaltuuksista rajoitusten asettamiseksi vain määritellyille korkean riskin toimijoille tai lainkäyttöalueille poikkeustilanteissa, kuten silloin, kun kyseessä on todennettu uhka kansalliselle turvallisuudelle.

Oletusarvoisesti avoin lähestymistapa varmistaa, että Euroopan julkisella sektorilla säilyy pääsy maailmanlaajuiseen kyberturvallisuus-, pilvipalvelu- ja tekoälyinnovaatioiden kirjoon. Se mahdollistaa joustavat käyttöönottomallit julkisista pilviratkaisuista eriytettyihin suvereeneihin infrastruktuureihin vaarantamatta häiriönsietokykyä tai turvallisuutta.

Ymmärrämme Euroopan tavoitteen arvioida tietosuojan tason riittävyyden ja viranomaistoimenpiteiden vaikutusta EU:n julkisen sektorin käyttämien pilvipalvelujen häiriönsietokykyyn ja toiminnan jatkuvuuteen. Kehotamme kuitenkin välttämään syrjivää lähestymistapaa, joka rajoittaisi Euroopan mahdollisuuksia hyödyntää kyberturvallisuutta ja innovaatioita.

Alkuperämaan huomioon ottaminen edellyttää huolellista tasapainoa julkisen sektorin etujen ja mahdollisten riskien välillä. CADA-asetuksen 18 artiklan 1 kohdan sallittujen maiden luetteloon perustuva lähestymistapa ei tätä tasapainoa EU:n eduksi toteuta. Laajalla kumulatiivisten kriteerien luettelolla ehdotus ei ota riittävästi huomioon kansainvälisen kaupan ja turvallisuuden puitteissa jo olemassa olevia maailmanlaajuisia suhteita, yhteisiä arvoja, pitkäaikaisia sopimuksia, WTO-sitoumuksia ja kumppanuuksia.

Transatlanttinen suhde on edelleen yksi maailman merkittävimmistä taloudellisista ja geopoliittisista kumppanuuksista. Se perustuu sitoutumiseen avoimiin markkinoihin, demokraattisiin arvoihin ja sääntöpohjaiseen kauppaan. Vaikka kauppayhteistyöhön liittyy ajoittain jännitteitä ja merkittäviä neuvotteluja, osapuolet tukeutuvat edelleen miljardien dollarien arvoiseen integroituneeseen taloussuhteeseen. Samalla yhteistyö ja sääntelyllinen yhteensovittaminen digitaalisella alalla ovat nousseet keskeisiksi nykyaikaisen digitaalisen talouden hallinnassa.

Katsomme, että CADA-asetuksen 18 artiklan olisi heijastettava tätä suhdetta vahvemmin. Kolmansien maiden tunnustamista koskevan menettelyn tulisi perustua tavoitteelliseen ja näyttöön perustuvaan nimeämiskehykseen, joka vastaa vakiintuneita kansainvälisiä järjestelyjä, kuten vapaakauppasopimuksia, tulliliittoja tai WTO:n julkisia hankintoja koskevaa sopimusta (GPA). Näin yrityksille ja kansainvälisille kumppaneille muodostuisi selkeä oikeusvaltioperiaatteeseen perustuva kehys.

Sen sijaan CADA-asetuksen 18 artiklassa asetetaan oikeudellisesti epävarmoja kynnysarvoja jäykkien ja paikallisesti rajattujen tasojen kautta. Käytännössä lähes minkään teknologiaa tuottavan valtion ei

olisi realistista täyttää niitä. Lähestymistapa on voimakkaan poissulkeva, altis vakavalle markkinoiden pirstaloitumiselle eikä jätä toimivaa väylää luotettavalle kansainväliselle yhteistyölle.

6. Keskeinen tarkastelualue: turvallisuustelemetrian ja metatietojen lokalisointi

Tuemme eurooppalaista intressiä tarkastella tietojen säilytyspaikkaa osana pilvipalvelujen turvallista hallintaa ja toimijuutta.

Haluamme kuitenkin nostaa esiin CADA-asetuksen liitteen II kohtien 1.1 c, 2.1 c, 3.1 c ja 4.1 c aiheuttaman tahattoman kyberturvallisuusriskin Euroopan julkiselle sektorille. Kyseiset kohdat edellyttävät **telemetria- ja metatietojen pakollista lokalisointia Eurooppaan**, mistä voi aiheutua merkittävää haittaa.

Kun telemetria ja metatiedot on pakko lokalisoida erilliseen eurooppalaiseen kokonaisuuteen, CADA-asetus estää pääsyn maailmanlaajuisen pilvi-infrastruktuurin tarjoamaan suojaan. Nykyaikainen pilvi-infrastruktuuri on suunniteltu toimimaan saumattomana, yhtenäisenä kokonaisuutena eikä erillisten alueellisten käyttöönottomallien joukkona. Tällaisen arkkitehtuurin ytimessä ovat erittäin käytettävissä olevat, pysyvät, maailmanlaajuisesti replikoidut ja automaattisesti skaalautuvat telemetria- ja metatiedot.

Maailmanlaajuisten ja rajat ylittävien metatietojen ja telemetriatietojen, myös tietoturvakokoonpanojen, analysointi on välttämätöntä haitallisen infrastruktuurin kartoittamiseksi, uhkien tunnistamiseksi, puolustustoimien automatisoimiseksi ja laajalle levinneiden virheellisten määritysten nopeaksi korjaamiseksi. Yhtenäinen näkyvyys on ratkaisevan tärkeää, jotta EU:n julkisen sektorin toimijoita ja kriittisiä työkuormia voidaan ennakoivasti suojata kehittyneiltä ja maailmanlaajuisesti hajautetuilta kybervakoilukampanjoilta.

Telemetrian ja metatietojen käsittely tiukasti paikallisena tai maantieteellisesti rajoitettuna hajottaa maailmanlaajuisen näkyvyyden ja synnyttää vaarallisia katvealueita. Ilman rajat ylittävää näkyvyyttä uhkatutkijat eivät voi verrata paikallisia EU:ssa havaittavia hyökkäysmalleja maailmanlaajuiseen toimintaan ja muodostaa uhkatiedustelusta nopeasti kokonaiskuvaa.

Telemetrian rajaaminen tietyille alueille estää sellaisten kyvykkäiden uhkatoimijoiden pysäyttämiseksi tarvittavan nopean seurannan, attribuution ja torjunnan. Ilman rajat ylittävää näkyvyyttä paikalliset viranomaisjärjestelmät menettävät maailmanlaajuisen puolustusverkon tarjoaman suojan, mikä antaa hyökkääjille tahattomasti etulyöntiaseman.

Kun uhkatiedustelu on eriytetty alueellisiin siiloihin, ratkaisevia telemetriatietoja ei voida jakaa maailmanlaajuisesti kiireellisten kyberturvallisuusriskien torjumiseksi. Tehokkain tapa puolustautua laajamittaista hyökkäystä, kuten hajautettua palvelunestohyökkäystä (DDoS) tai nollapäivähaavoittuvuuden hyväksikäyttöä, vastaan on tunnistaa uhan tunnusmerkit maailmanlaajuisesti ja estää haitallinen liikenne mahdollisimman lähellä hyökkäyksen lähdettä.

Jos hyökkäys käynnistyy Aasiassa ja kohdistuu eurooppalaiseen infrastruktuuriin, maailmanlaajuisesti integroitu telemetriaverkko mahdollistaa uhan estämisen Aasiassa sijaitsevissa reunasolmuissa. Jos eurooppalainen telemetria erotetaan muusta verkosta, järjestelmä ei voi yhdistää Euroopan

liikennemalleja muualla havaittaviin poikkeamiin. Haitallisen liikenteen on tällöin saavutettava Euroopan rajat ennen kuin sitä voidaan analysoida ja torjua tehokkaasti, mikä kasvattaa infrastruktuurin ylikuormittumisen riskiä.

Esimerkkejä

COLDRIVER-tapaus (Venäjään kytkeytyvä toimija ja EU:n jäsenvaltioiden suojaaminen). COLDRIVER on erittäin aktiivinen kybervakoilutoimija, joka kohdistaa toimintaansa usein Euroopan jäsenvaltioihin. Kesä- ja heinäkuussa 2026 maailmanlaajuinen telemetria mahdollisti Googlelle EU:n ulkopuolisiin organisaatioihin kohdistuneiden COLDRIVER-operaatioiden havaitsemisen varhaisessa vaiheessa. Koska Google pystyi analysoimaan näitä varhaisia varoitussignaaleja maailmanlaajuisesti, haitallinen infrastruktuuri voitiin lisätä ennakoivasti maailmanlaajuiselle estolistalle. Tämä maailmanlaajuinen näkyvyys suojasi suoraan EU:n jäsenvaltioita ja julkisen sektorin toimijoita, jotka olisivat voineet joutua seuraaviksi kohteiksi, ja uhka oli mahdollista neutraloida ennen sen leviämistä eurooppalaisiin verkkoihin.

APT43-tapaus (Pohjois-Koreaan kytkeytyvä toimija ja EU-alueiden suojaaminen). Tammikuussa 2026 Google hyödynsi maailmanlaajuista sisäistä telemetriaa, kuten MX-reititystietoja, seurantapikseleitä ja Password Protection -palvelua, tunnistaakseen APT43-toimijan spear phishing -kampanjan, joka kohdistui aluksi Yhdysvalloissa sijaitseviin kohteisiin. Maailmanlaajuinen näkyvyys mahdollisti ennakoivat tilien sulkemiset ja kehittyneiden suojaustoimien käyttöönoton. Infrastruktuuri oli mahdollista neutraloida varhaisessa vaiheessa ennen kuin vakoilukampanja ehti kohdistaa toimintaansa Euroopan julkiseen sektoriin ja kriittiseen infrastruktuuriin.

Ottaen huomioon Suomen vahvan sitoutumisen kyberturvallisuuteen ja tietovirtoihin, pidämme tervetulleena Suomen panosta neuvoston keskusteluun Euroopan julkiseen sektoriin kohdistuvien kyberturvallisuusriskien käsittelemiseksi. Google Cloud on jo sitoutunut asiakastietojen asianmukaiseen lokalisointiin. Näin ollen katsomme, että eurooppalaisten tietojen luottamuksellisuus ja hallinta voidaan turvata ilman telemetriaa ja metatietoja koskevaa lisälokalisointivaatimusta.

Todellinen suvereniteetti voidaan määritellä todennettavana, päästä päähän ulottuvana operatiivisena ja kryptografisena hallintana eikä rajoittavina maantieteellisinä tietojen lokalisointivaatimuksina. Tämä kattaa levossa olevien ja siirrettävien tietojen salauksen sekä luottamuksellisen laskennan ja/tai asiakkaan hallinnoimien salausavainten käytön.

Pidämme myönteisenä Suomen harkintaa ja panosta neuvoston kannan muodostamisessa tämän Eurooppaa koskevan riskin esiin nostamiseksi. Katsomme, että liitteen II kohtiin 1.1 c, 2.1 c, 3.1 c ja 4.1 c sisältyvien viittausten poistaminen vahvistaisi Euroopan kyberresilienssiä vaarantamatta tietosuvereniteettia.

7. Pilari IV: kysyntäpuolen toimet, julkiset hankinnat ja soveltamisala (29–40 artikla)

7.1 Rajoittavien ohjelmistolisenssien ja monipilviympäristöjen esteiden käsitteleminen

Euroopan julkisen sektorin toimijoiden ja viranomaisten digitaalista suvereniteettia ei voida saavuttaa yhden toimittajan riippuvuuden tai suljettujen perintöjärjestelmämonopolien kautta. Yhteentoimiva monipilvilähestymistapa vahvistaa suoraan Euroopan avointa strategista autonomiaa, koska se varmistaa, että julkiset toimijat säilyttävät täyden hallinnan arkaluonteisiin tietoihinsa, salausavaimiinsa ja digitaaliseen infrastruktuuriinsa ilman toimittajalukkiutumisen riskiä.

Lisensointiin liittyvien esteiden poistaminen ja toimittajajoustavuuden varmistaminen mahdollistavat sen, että eurooppalaiset viranomaiset voivat hyödyntää parhaita maailmanlaajuisia tekoäly- ja pilvipalvelukyvykkyyksiä sekä samalla edistää eurooppalaisten ohjelmistotoimittajien, järjestelmäintegraattoreiden ja suvereenien pilvipalvelukumppaneiden muodostamaa paikallista teknologiaekosysteemiä. Näin julkiset palvelut säilyvät häiriönsietokykyisinä, kustannustehokkaina ja täysimääräisesti vastuullisina Euroopan kansalaisille.

Todellinen teknologinen kehitys ja digitaalisten markkinoiden tasapuolisuus edellyttävät avointa monipilviekosysteemiä, joka perustuu avoimiin standardeihin, tietojen siirrettävyyteen ja vahvaan yhteentoimivuuteen. Kilpailua rajoittavat ohjelmistolisensointikäytännöt, kuten keinotekoiset hinnankorotukset, rankaisevat sopimusehdot ja tekniset esteet, jotka haittaavat ohjelmistojen käyttöä kilpailevissa pilvipalveluissa, vääristävät kilpailua ja ylläpitävät keinotekoista toimittajalukkiutumista.

Kun tällaiset epäoikeudenmukaiset lisensointirajoitukset poistetaan ja pilvi- ja tekoälyarkkitehtuurien avoin yhteentoimivuus varmistetaan, organisaatiot voivat siirtää työkuormia saumattomasti, välttää suljettuja toimittajaekosysteemejä ja valita pilvi-infrastruktuurinsa turvallisuuden, suorituskyvyn, kustannusten ja innovatiivisuuden perusteella.

Avoin lähdekoodi ehkäisee osana aidosti yhteentoimivaa pilvilähestymistapaa keinotekoista toimittajalukkiutumista ja turvaa hallintaan perustuvaa teknologista suvereniteettia. Kun pilviarkkitehtuurit perustuvat avoimiin standardeihin, yhteisiin koodipohjiin ja yhteisiin ohjelmointirajapintoihin, yritykset ja julkisen sektorin toimijat voivat rakentaa, ottaa käyttöön ja siirtää työkuormia saumattomasti omissa konesaleissa, reunaympäristöissä sekä monipilviympäristöissä.

Neutraalit, yhteisöjen hallinnoimat konttiteknologian, tietojenhallinnan ja orkestroinnin protokollat vähentävät suljettujen ratkaisujen aiheuttamaa kitkaa, lisäävät hinta- ja palvelukilpailua sekä edistävät organisaatioiden pysyvää hallintaa digitaaliseen infrastruktuuriinsa ja tieto-omaisuuteensa.

CADA-asetuksen 29 artiklan kehittäminen. Pidämme myönteisenä komission avointa lähdekoodia koskevaa painotusta, joka ilmenee muun muassa erillisessä avoimen lähdekoodin strategiassa. Katsomme kuitenkin, että CADA-asetuksen 29 artiklan 1 kohdassa olisi mahdollisuus vahvistaa sitoutumista avoimeen lähdekoodiin ja sisällyttää julkisen sektorin hankintalähestymistapaan nimenomaisia monipilviratkaisuja koskevia näkökohtia.

Jotta julkisen sektorin asiakkaille voidaan turvata todellinen autonomia ja siirrettävyys, yhteentoimivuutta haittaavia perintöjärjestelmäesteitä on käsiteltävä. Epäoikeudenmukaiset ohjelmistolisensointikäytännöt muodostavat tällä hetkellä keskeisen esteen julkisen sektorin mahdollisuudelle hyödyntää parhaiten soveltuvia ja teknisesti parhaimpia pilvipalveluja. Niitä olisi käsiteltävä CADA-asetuksessa.

Tällaiset käytännöt aiheuttavat eurooppalaisille yrityksille ja viranomaisille huomattavia keinotekoisia kustannuksia ja kilpailua rajoittavaa lukkiutumista. Ne perustuvat määräävän aseman hyödyntämiseen perinteisissä omiin konesaleihin asennettavissa tuottavuus- ja käyttöjärjestelmäohjelmistoissa pilvilaskentamarkkinoiden vääristämiseksi.

Riippumattoman taloudellisen tutkimuksen mukaan esimerkiksi professori Frédéric Jennyn CISPE:lle laatima selvitys epäoikeudenmukaisten ohjelmistolisenssien kustannuksista osoitti, että syrjivät ehdot, kuten rajoittavat omien lisenssien käyttöä koskevat säännöt (BYOL) ja 300–400 prosentin suuruiset hinnankorotukset perintöohjelmistojen käyttämisestä kilpailevilla pilvialustoilla, aiheuttavat Euroopan taloudelle yli miljardin euron vuotuisen kustannuksen SQL Server -käyttöönottojen osalta. Lisäksi tuottavuusohjelmistopakettien kustannus on 560 miljoonaa euroa vuodessa eli 28 prosenttia korkeampi.

Rahoitukselliset seuraamukset vääristävät vakavasti hankintoja ja pilvipalvelujen käyttöönottoa. Savantan eurooppalaisen kyselytutkimuksen ja Yhdistyneen kuningaskunnan kilpailuviranomaisen CMA:n pilvimarkkinatutkimuksen mukaan yli 50 prosenttia pilvipalveluntarjoajan vaihtamista harkinneista eurooppalaisista IT-päättäjistä oli luopunut vaihtamisesta olemassa olevien rajoittavien lisenssiehtojen ja pakettialennusten menettämisen pelon vuoksi.

Asiakkaiden keinotekoinen lukitseminen yhden toimittajan ekosysteemiin kasvattaa IT-budjetteja ja kuluttaa verovaroja. Social Market Foundation on arvioinut, että ylimääräiset kustannukset Yhdistyneen kuningaskunnan julkiselle sektorille ovat yksinään 300 miljoonaa puntaa. Käytännöt myös heikentävät Euroopan digitaalista suvereniteettia, monipilviympäristöjen resilienssiä ja organisaatioiden mahdollisuuksia valita ansioiden perusteella parhaat, turvalliset tekoäly- ja pilvi-infrastruktuurit.

Tämän vuoksi 29 artiklan 2 ja 9 kohtaan olisi monitoimittaja- tai monipilvistrategiaa koskevan näkökohdan lisäksi lisättävä viittaus ohjelmistolisenssien ehtoihin ja käytäntöihin. **Jäsenvaltioiden riskiarvioinneissa olisi nimenomaisesti arvioitava niiden riskiä synnyttää rajoittavaa toimittajalukkiutumista esimerkiksi asettamalla epäoikeudenmukaisia taloudellisia tai teknisiä seuraamuksia tai rajoittamalla siirrettävyyttä pilvipalveluntarjoajien välillä**.

7.2 Yksityisen sektorin NIS2-toimijoiden rajaaminen soveltamisalan ulkopuolelle (31 artikla)

Tuemme vahvasti Suomen varaumaa, joka koskee komission toimivaltuuttamista laajentaa pakollisia riskiarviointeja yksityisiin NIS2-toimijoihin. Kannatamme Suomen vaatimusta arvioida huolellisesti ehdotuksen tarkoituksenmukaisuutta ja oikeasuhteisuutta. EU-lainsäätäjän olisi varmistettava CADA-asetuksen soveltamisalan oikeusvarmuus välttämällä 31 artiklan mukaisia pyrkimyksiä laajentaa sääntelyä yksityiselle sektorille. Artikla olisi poistettava.

Julkisia hankintoja koskevien suvereniteettirajoitusten laajentaminen yksityisille kaupallisille markkinoille aiheuttaisi merkittäviä taloudellisia vääristymiä Euroopan keskeisillä toimialoilla. Vaikka CADA-asetus on ensisijaisesti kehystetty julkisen sektorin hankintoja koskevaksi, 31 artiklassa luodaan suora mekanismi, jossa aluksi vapaaehtoisina ehdotuksina 31 artiklan 1 kohdan nojalla ja myöhemmin komission delegoiduilla säädöksillä 31 artiklan 3 kohdan nojalla voidaan tehdä suvereniteettivaikutusten arvioinneista ja toiminnallisista riskinhallintatoimista pakollisia NIS2-direktiivin liitteessä I tarkoitetuilla kriittisillä aloilla toimiville yksityisille yrityksille. Tällaisia aloja ovat esimerkiksi pankkitoiminta, energia, liikenne, terveys ja digitaalinen infrastruktuuri.

Jos yksityiset eurooppalaiset yritykset velvoitetaan soveltamaan kaupallisissa yritysten välisissä hankinnoissa jäykkiä maantieteellisiä ja kansalaisuuteen perustuvia suodattimia, niiden mahdollisuudet hyödyntää maailmanlaajuisesti parhaita ohjelmisto- ja tekoälyratkaisuja rajoittuvat. Tämä kasvattaa toimintakustannuksia ja asettaa eurooppalaiset yritykset huomattavasti epäedullisempaan kilpailuasemaan suhteessa maailmanlaajuisiin kilpailijoihin.

Laajentaminen yksityiselle sektorille synnyttäisi myös vaarallisia sääntelyristiriitoja ja päällekkäisyyksiä jo vakiintuneiden, riskiperusteisten eurooppalaisten kehysten kanssa. Kriittisiin yksityisiin toimialoihin sovelletaan jo kattavaa ja perusteellisesti neuvoteltua lainsäädäntöä, joka on suunniteltu erityisesti toiminnallista häiriönsietokykyä varten. Näistä keskeisiä ovat rahoituspalvelujen digitaalista häiriönsietokykyä koskeva asetus (DORA) sekä kriittistä infrastruktuuria koskeva NIS2-direktiivi.

Nämä sektorikohtaiset järjestelmät perustuvat objektiiviseen toiminnalliseen luotettavuuteen, monipilvihajautukseen ja osoitettavissa oleviin teknisiin turvatoimiin eivätkä protektionistisiin käsityksiin toimittajan alkuperästä. Epämääräisten suvereniteettivelvoitteiden ja mielivaltaisten toimittajarajoitusten asettaminen DORA-asetuksen ja NIS2-direktiivin päälle synnyttäisi huomattavaa oikeudellista epävarmuutta, toimivaltaristiriitoja rahoitus- ja energia-alan sääntelyviranomaisten sekä digiviranomaisten välillä sekä ohjaisi yritysten resursseja aidosta kyberresilienssistä hallinnolliseen velvoitteiden täyttämiseen.

Lisäksi toimivallan siirtäminen komissiolle suvereniteettivelvoitteiden laajentamiseksi yksityisille markkinoille toimeenpanovallan kautta kiertäisi välttämättömän demokraattisen valvonnan ja vaikutustenarvioinnin. Komissiolle 31 artiklan 3 kohdassa annettava yksipuolinen toimivalta muuttaa vapaaehtoiset suuntaviivat sitoviksi kaupallisiksi rajoituksiksi ohittaisi tavallisen lainsäätämisjärjestyksen sekä kaventaisi Euroopan parlamentin ja jäsenvaltioiden täysimääräistä yhteispäätösvaltaa.

Koko yksityisten toimialojen hankintasääntöjen perusteellinen uudistaminen edellyttää yksityiskohtaisia toimialakohtaisia taloudellisia vaikutustenarviointeja ja avointa parlamentaarista keskustelua eikä toissijaisen sääntelyn nojalla annettavia säädöksiä. Euroopan teknologista suvereniteettia olisi edistettävä kannustamalla avoimeen innovointiin, kilpailukykyiseen pilvipalvelujen käyttöönottoon ja monipilviresilienssiin, ei asettamalla pakottavia markkinaesteitä Euroopan yksityiselle sektorille.

7.3 Voimassa olevien hankintasopimusten suojaaminen takautuvalta soveltamiselta (29–30 artikla)

Pidämme myönteisenä Suomen tarkkaa huomiota siihen, että uusien varmuustasokriteerien soveltaminen takautuvasti käynnissä oleviin julkisiin sopimuksiin voi aiheuttaa merkittäviä ongelmia.

Pakotettu palveluntarjoajan tai ratkaisun vaihtaminen sopimuskauden aikana aiheuttaisi tarpeettomia taloudellisia rasitteita.

Jos viranomaiset velvoitettaisiin korvaamaan, uudelleenrakentamaan tai päättämään olemassa olevia pilvipalvelusopimuksia kesken sopimuskauden, seurauksena voisi olla huomattavia ja ennakoimattomia kustannuksia. Viranomaisille voisi aiheutua sopimussakkoja, ennenaikaisesta siirtymisestä johtuvia kustannuksia ja päällekkäisiä kustannuksia vanhoista sekä korvaavista järjestelmistä.

Tuemme Suomen vastustusta takautuvia velvoitteita kohtaan. Uusia varmuustasoja olisi sovellettava yksinomaan uusiin hankintoihin, ja käyttöön olisi otettava kohtuulliset siirtymäajat.

7.4 Kansallisen turvallisuuden poikkeuksen vahvistaminen (SEU 4 artiklan 2 kohta)

Google kunnioittaa täysimääräisesti jäsenvaltioiden toimivaltaa kansallisen turvallisuuden alalla. Tuemme Suomen vaatimusta joustavista hybridi- ja omiin konesaleihin perustuvista käyttöönottomalleista puolustus- ja turvallisuustehtävissä.

Euroopan unionista tehdyn sopimuksen 4 artiklan 2 kohdan mukaan kansallinen turvallisuus kuuluu yksinomaan jäsenvaltioiden toimivaltaan. Nykyaikaiset puolustusoperaatiot ovat ohjelmistomääriteltyjä ja edellyttävät reaaliaikaista maailmanlaajuista uhkatiedustelua sekä saumatonta tietojenvaihtoa liittolaisten verkostojen välillä.

EU:n perussopimuksissa rajataan tämä toimivaltajako selkeästi. Vaikka komissio voi toimia teollisen koordinoinnin, yhteishankintojen ja tutkimusrahoituksen edistäjänä esimerkiksi Euroopan puolustusrahaston ja puolustusalan omnibus-sääntelyn kautta, sillä ei ole oikeudellista toimivaltaa määrätä sotilasdoktriinista, operatiivisista arkkitehtuureista tai kansallisista puolustushankinnoista.

Koska asevoimat ovat suoraan vastuussa kansallisille parlamenteille ja kansalaisille, jäsenvaltioiden on säilytettävä rajoittamaton toimivalta valita käyttöönsä mahdollisimman kyvykkäitä, häiriönsietokykyisiä ja tehtäväkriittisiä teknologioita. Näin varmistetaan, etteivät rauhanajan sisämarkkinasäännöt vaaranna toiminnallista valmiutta kriisitilanteissa.

7.5 Pilvipalveluja hyödyntävä puolustusinnovaatio Euroopan suojaamiseksi

Tekoälyn ja jatkuvien valtiollisesti tuettujen kyberuhkien aikakaudella kaupallinen hyperscale-pilvi-infrastruktuuri muodostaa välttämättömän digitaalisen perustan kansalliselle turvallisuudelle, demokraattisille instituutioille ja kriittiselle infrastruktuurille. Hajautuneet, vanhentuneet omiin konesaleihin perustuvat järjestelmät eivät enää pysty tarjoamaan kehittyneitä vastustajia vastaan tarvittavaa laskentamittakaavaa, fyysistä redundanssia tai jatkuvia ohjelmistopäivityksiä.

Kaupalliset pilviympäristöt tarjoavat syvällistä sisäänrakennettua häiriönsietokykyä, johon kuuluvat maailmanlaajuisesti redundantit maa- ja merenalaiset kuituverkot. Ne tarjoavat puolustusorganisaatioille myös automatisoituja, tekoälyä hyödyntäviä kyberturvallisuusominaisuuksia, joiden avulla puolustus siirtyy reaktiivisesta kehäpuolustuksesta reaaliaikaiseen uhkien havaitsemiseen ja haavoittuvuuksien automatisoituun korjaamiseen.

Pääsy nykyaikaiseen pilviarkkitehtuuriin on yhtä lailla edellytys liittolaisten yhteentoimivuudelle, operatiiviselle nopeudelle ja teknologiselle ylivoimalle. Kun liittolaisten asevoimat ja julkisen sektorin toimijat ottavat käyttöön avoimiin standardeihin perustuvia monipilvialustoja, ne voivat purkaa jäykkiä tietosiiloja, jakaa eri toimintaympäristöjä koskevaa tiedustelutietoa saumattomasti ja ottaa käyttöön kehittyneitä tekoälymalleja kaupallisen innovoinnin tahdissa monivuotisten hankintasyklien sijasta.

Kehittyneet suvereniteettia tukevat hallintakeinot, kuten ilmarakoistetut infrastruktuurit ja asiakkaan hallinnoima salaus, varmistavat lisäksi, että viranomaiset voivat säilyttää täyden toiminnallisen autonomian, sääntelyn noudattamisen ja tietosuvereniteetin ilman, että pääsyä uusimpaan teknologiaan rajoitetaan.
Yhdysvaltalaisten hyperscale-pilvipalveluntarjoajien sulkeminen pois puolustuskäytöstä varmuustasolla 4 estäisi näiden olennaisten hyötyjen toteutumisen Euroopan puolustuksen ja turvallisuuden kannalta.

7.6 CADA-asetus ei saa estää EU:n tiivistä integroitumista Naton puolustuskyvykkyyksiin

Pilvi- ja tekoälyohjelmistojen kehittämisen tai toiminnan rajaaminen yksinomaan EU:n alueelle heikentäisi ohjelmistomääriteltyä puolustusta, vaikeuttaisi kriittisiä tietoturvapäivityksiä ja synnyttäisi Natoon vaarallisen kaksitasoisen digitaalisen ekosysteemin. Se eristäisi EU:n joukot teknisesti yhteisissä johtamisrakenteissa käytettävistä EU:n ulkopuolisista liittolaisista, kuten Yhdysvalloista ja Yhdistyneestä kuningaskunnasta.

Puolustuksen suvereniteetti on siksi saavutettava vahvoilla teknisillä, kryptografisilla ja operatiivisilla hallintakeinoilla eikä protektionistisella maantieteellisellä eristäytymisellä.

Ankaran huippukokouksen julistuksessa heinäkuussa 2026 Naton valtioiden ja hallitusten johtajat sitoutuivat nimenomaisesti kehittämään yhteentoimivan transatlanttisen sodankäynnin pilven ja ottamaan käyttöön tehokkaita tekoälymalleja yhteisen pidäkkeen vahvistamiseksi nykyaikaisia hybridi- ja valtiollisesti tuettuja uhkia vastaan. Pääsy kehittyneisiin yhdysvaltalaisiin ja muiden liittolaisten pilvialustoihin on Euroopan puolustukselle olennaista, koska nykyaikainen liittoumapuolustus tarvitsee yhteisen ohjelmistomääritellyn digitaalisen perustan. Sen on kyettävä käsittelemään useita toimintaympäristöjä koskevaa tiedustelutietoa sekä toteuttamaan koneen nopeudella toimivaa kyberpuolustusta reaaliaikaisesti.

Jäykät alkuperään perustuvat suvereniteettivaatimukset, jotka irrottavat eurooppalaiset asevoimat transatlanttisista hyperscale-arkkitehtuureista, uhkaavat luoda vaarallisen kaksitasoisen liittokunnan. Eurooppalaiset asevoimat voivat tällöin jäädä eriytyneisiin IT-siiloihin ja menettää pääsyn maailmanlaajuiseen uhkatelematriaan.

Poistamalla varmuustason 4 CADA-asetus voisi varmistaa, että pääsy luotettaviin maailmanlaajuisiin kumppaneihin säilyy yhdenmukaisena Nato-liittokunnassa. Tämä mahdollistaisi yhteistyön palveluntarjoajien kanssa Atlantin molemmin puolin ja jo nykyisin saatavilla olevien, operatiivisesti kehittyneiden suvereenien arkkitehtuurien hyödyntämisen.

Google Cloudin ilmarakoistetut käyttöönottomallit ja asiakaspuolen salaukseen perustuvat mallit mahdollistavat sen, että Euroopan puolustusministeriöt voivat saavuttaa kansallisen

tietosuvereniteetin ja toiminnallisen autonomian säilyttäen samalla täyden yhteentoimivuuden Naton tasolla kehitettävän yhteisen sodankäynnin pilven kanssa. CADA-asetus ei saa muodostaa estettä tälle Euroopan sotilaallisen puolustuksen kannalta keskeiselle yhteistyölle.

7.7 Sääntelyn liiallisen laajentamisen välttäminen 29 artiklan 5 kohdassa

Suomi korostaa nimenomaisesti, että 29 artiklan 5 kohta voi puuttua kansalliseen päätöksentekoon ja jäsenvaltioiden harkintavaltaan yleisen järjestyksen ja kriittisten toimintojen osalta. SEU 4 artiklan 2 kohdan mukaisesti kansallinen turvallisuus ja yleinen järjestys kuuluvat jäsenvaltioiden yksinomaiseen toimivaltaan.

Komissiolle annettava rajoittamaton varatoimivalta aiheuttaisi merkittävää oikeudellista epävarmuutta jäsenvaltioiden riskiarviointien lopullisuudesta. Pilvipalvelujen mukauttaminen julkisen sektorin tarpeisiin on teknisesti monimutkaista, ja kansallisten hankintojen operatiiviset vaatimukset ovat huomattavia. Jos näihin perustaviin arviointeihin liittyy epävarmuutta, se vaikeuttaa merkittävästi teknologian tehokasta käyttöönottoa Euroopassa.

Keskittäminen vaikuttaa myös kansalliseen turvallisuuteen ja suvereniteettiin, jotka kuuluvat SEU 4 artiklan 2 kohdan nojalla yksittäisten jäsenvaltioiden yksinomaiseen toimivaltaan. Unionin laajuinen yhdenmukaistaminen ja digitaalisten sisämarkkinoiden eheys voidaan turvata soveltamalla yhdenmukaisia, riskiperusteisia kriteerejä ja menetelmiä. Kehotamme välttämään ylhäältä ohjattua veto-oikeutta.

Katosmme, että 29 artiklan 5 kohdassa olisi vähintäänkin säädettävä konkreettisista menettelyistä ja takeista, joiden avulla jäsenvaltiot voivat perustella alkuperäisen riskiarviointinsa. Jotta Euroopan julkinen sektori pääsisi oikea-aikaisesti hyödyntämään innovatiivista teknologiaa, hallinnollista ohitusmenettelyä olisi harkittava vain korkean riskin tilanteissa, jotka koskevat yleisen järjestyksen kannalta arkaluonteisia työkuormia. Oikeasuhteisuuden varmistamiseksi ohitusvaltaa olisi voitava käyttää vasta, kun lievemmät toimenpiteet on käytetty loppuun.

8. Pilari V: avoin lähdekoodi, teknologianeutraalius ja lisensointi (41–45 artikla)

8.1 Teknologianeutraalius julkisissa hankinnoissa

Suomi korostaa vahvasti, ettei digitaalinen suvereniteetti riipu siitä, perustuuko ohjelmisto avoimeen vai suljettuun lähdekoodiin. Julkisten hankintojen tulisi säilyä teknologianeutraaleina, ja ratkaisujen arvioinnissa olisi otettava huomioon toiminnallisuus, turvallisuus, kustannustehokkuus ja elinkaarivaikutukset.

Google pitää Suomen kantaa kannatettavana. Sekä avoimen lähdekoodin että kaupallisilla ehdoilla tarjottavilla ohjelmistoilla on keskenään täydentävä ja merkittävä rooli eurooppalaisen innovoinnin sekä valinnanvapauden edistämisessä.

Miksi avoin lähdekoodi on Googlelle tärkeää:

Google Cloud toteuttaa yhteentoimivuutta arkkitehtuurisena periaatteena eikä jälkikäteen lisättävänä ominaisuutena. Google Cloud oli ensimmäinen merkittävä hyperscale-pilvipalveluntarjoaja, joka poisti tiedonsiirtomaksut asiakkailta, jotka siirtävät työkuormiaan toiselle palveluntarjoajalle tai takaisin omiin konesaleihin. Näin poistettiin merkittävä kaupallinen este monipilviympäristöjen ketteryydeltä.

Google mahdollistaa hybridi- ja monipilviympäristöjen vapauden myös Google Distributed Cloudin ja BigQuery Omnin kaltaisilla tuotteilla. Niiden avulla organisaatiot voivat toteuttaa analytiikkaa ja ottaa sovelluksia käyttöön useilla pilvialustoilla yhtenäisen hallintakerroksen avulla.
Google vahvistaa avointa lähestymistapaansa Euroopassa myös strategisilla suvereenin pilven kumppanuuksilla. Tällaisia ovat esimerkiksi Ranskassa Thalesin kanssa toteutettava S3NS, Saksassa T-Systems ja Espanjassa Telefónica. Kumppanuuksien avulla eurooppalaiset viranomaiset voivat säilyttää täyden toiminnallisen autonomian ja tietojen hallinnan luopumatta järjestelmien välisestä yhteentoimivuudesta.

Avoin lähdekoodi on olennainen osa Googlen toimintaa. Googlella on useiden vuosikymmenten historia sellaisten perustavanlaatuisten teknologioiden kehittämisessä ja avaamisessa, jotka ovat muuttaneet maailmanlaajuista digitaalista taloutta. Google kehitti ja avasi Kubernetesin lähdekoodin. Kubernetesista muodostui nykyaikaisen pilvipohjaisen konttien orkestroinnin yleinen standardi, ja se lahjoitettiin Cloud Native Computing Foundationille (CNCF). Lisäksi Google on kehittänyt avoimia alustoja, kuten Androidin ja Chromiumin, osallistunut Linux-ytimen kehittämiseen sekä edistänyt avoimesti saatavilla olevia tekoälykehyksiä ja avoimilla painoilla julkaistuja malleja, kuten TensorFlow'ta, JAX:ia ja Gemmaa.

Google jatkaa turvallisen, läpinäkyvän ja yhteistyöhön perustuvan teknologian kehittämisen tukemista Open Source Security Foundationissa (OpenSSF), avoimen tieteen hankkeissa, kuten AlphaFoldissa, sekä muilla aloitteilla. Näiden toimien tarkoituksena on demokratisoida innovointia organisaatioille maailmanlaajuisesti.