MICROSOFT CORPORATIONIN KANNANOTTO

Pilvipalveluiden ja tekoälyn kehittämisen säädös (CADA)

Euroopan laskentakapasiteetti käyttöön ja
toiminnallinen pilvisuvereniteetti tekoälyn tulevaisuutta varten

Lokakuu 2026

Tiivistelmä

Microsoft pitää pilvipalveluiden ja tekoälyn kehittämisen säädöksen (CADA) julkaisemista tervetulleena ja tärkeänä askeleena, joka luo edellytyksiä Euroopan tekoälytavoitteiden tukemiseen tarvittavalle infrastruktuurille. Tuemme EU:n pyrkimystä vahvistaa taloudellista turvallisuutta, häiriönsietokykyä ja strategista autonomiaa. Katsomme, että nämä tavoitteet saavutetaan parhaiten digitaalista suvereniteettia koskevalla toiminnallisella ja riskiperusteisella lähestymistavalla, jossa painopiste on tehokkaissa oikeudellisissa, operatiivisissa ja teknisissä suojatoimissa eikä kansallisuuteen perustuvissa kriteereissä. CADA tarjoaa tilaisuuden laajentaa Euroopan tekoäly- ja pilvi-infrastruktuuria, houkutella investointeja, vahvistaa häiriönsietokykyä ja säilyttää pääsyn uusimpiin teknologioihin. Euroopan digitaalinen tulevaisuus on vahvimmillaan, kun siinä yhdistyvät aiempaa suurempi oma kapasiteetti sekä avoimuus, innovointi ja luotettavat kumppanuudet.

Tasapainoisella lähestymistavalla voidaan vahvistaa Euroopan autonomiaa ja samalla laajentaa infrastruktuuria ja innovaatiotoimintaa, joita tekoälyn aikakausi edellyttää. Euroopan strategisten tavoitteiden tukemiseksi Microsoft suosittelee, että säädökseen sisällytetään seuraavat periaatteet:

1. Mahdollistetaan pilvi-infrastruktuurin nopeampi rakentaminen

Euroopan kilpailukyky tekoälyn alalla riippuu digitaalisen infrastruktuurin nopeasta laajentamisesta. Microsoft tukee tavoitetta kasvattaa merkittävästi EU:n datakeskus- ja pilvikapasiteettia ja on valmis investoimaan Eurooppaan auttaakseen sitä toteuttamaan tekoälytavoitteensa. Onnistuakseen Eurooppa tarvitsee kehyksen, joka nopeuttaa lupamenettelyjä, parantaa energian saatavuutta ja pääsyä sähköverkkoinfrastruktuuriin sekä tarjoaa ennakoitavat ja yhdenmukaistetut säännöt, jotka houkuttelevat pitkäjänteisiä investointeja. Johtavien eurooppalaisten ja maailmanlaajuisesti toimivien teknologiayritysten väliset avoimet kumppanuudet ovat välttämättömiä sen varmistamiseksi, että Euroopalla on se laskentakapasiteetti, jota se tarvitsee noustakseen johtavaksi tekoälymantereeksi.

2. Mitataan suvereniteettia määräysvallan ja häiriönsietokyvyn eikä kansallisuuden perusteella

Euroopan digitaalista suvereniteettia koskevat tavoitteet ovat oikeutettuja ja tärkeitä. Suvereniteetti tulisi kuitenkin saavuttaa osoitettavissa olevilla teknisillä, operatiivisilla ja oikeudellisilla

suojatoimilla eikä kansallisuuteen perustuvilla rajoituksilla. Asiakkaille on olennaista, kenellä on määräysvalta heidän dataansa, kuka pääsee käsiksi järjestelmiin, miten palvelut pysyvät toiminnassa kriisien aikana ja täyttävätkö palveluntarjoajat tiukat turvallisuus- ja sääntelyvaatimukset. Nykyaikaisilla suojatoimilla, kuten salauksella, asiakkaan hallinnoimilla salausavaimilla, operatiivisella autonomialla, tarkastettavuudella ja sopimuksellisilla sitoumuksilla, voidaan saavuttaa tehokas suvereniteetti riippumatta siitä, missä palveluntarjoajan pääkonttori sijaitsee. Riskiperusteinen lähestymistapa vahvistaa häiriönsietokykyä ja turvaa samalla innovoinnin, kilpailun ja asiakkaiden valinnanvapauden.

3. Luodaan tasapainoinen kehys, jossa yhdistyvät kilpailukyky, turvallisuus ja valinnanvapaus

CADA:n onnistuminen riippuu avoimen, kilpailullisen ja innovaatiomyönteisen digitaalisen ekosysteemin säilyttämisestä. Eurooppalaisilla asiakkailla ja viranomaisilla tulisi jatkossakin olla pääsy parhaisiin saatavilla oleviin teknologioihin, samalla kun suvereniteettivaatimuksia sovelletaan oikeasuhtaisesti niihin työkuormiin, jotka ovat aidosti kriittisiä. Liian yksityiskohtaiset tai protektionistiset toimenpiteet uhkaavat nostaa kustannuksia, vähentää innovointia, rajoittaa asiakkaiden valinnanvapautta ja hidastaa tekoälyn käyttöönottoa. Objektiivisiin ja riskiperusteisiin kriteereihin perustuva yhdenmukaistettu EU-kehys voi samanaikaisesti vahvistaa turvallisuutta, tukea eurooppalaista kilpailukykyä, houkutella pitkäjänteisiä investointeja ja vauhdittaa digitaalista muutosta koko Euroopan unionissa.

Tässä kannanotossa keskitytään asetusehdotuksen pilvilaskennan suvereniteettikehykseen ja unionin varmuustasoihin sekä sen datakeskuskapasiteettia ja luvitusta koskeviin säännöksiin, ja siinä esitetään Microsoftin suositukset siitä, miten nämä säännökset voivat paremmin tukea pilvipalvelujen turvallista, kilpailulle avointa ja riskiperusteista käyttöönottoa julkisella sektorilla sekä lisätä investointeja pilvi- ja tekoälyinfrastruktuuriin ja sen rakentamista kaikkialla EU:ssa. Suositusten tarkoituksena on auttaa EU:n päättäjiä, jäsenvaltioita ja julkisia hankkijoita tekemään tietoon perustuvia, investointimyönteisiä ja suvereniteettinäkökohdat huomioon ottavia pilvipalveluvalintoja.

Johdanto

Pilvilaskennasta on tullut Euroopan digitaalitalouden perusinfrastruktuuria, joka tukee julkishallintoa, teollisuuden uudistumista, tieteellistä tutkimusta ja tekoälyn nopeaa käyttöönottoa. Geopoliittisten jännitteiden ja teknologisen kilpailun kiristyessä päättäjät tarkastelevat pilvipalveluja yhä useammin digitaalisen suvereniteetin näkökulmasta.

Viranomaiset käyttävät julkisiin hankintoihin vuosittain noin 2,5 biljoonaa euroa, ja siksi on arvioitu, että jo 1 %:n tehokkuusparannuksella EU voisi säästää jopa 20 miljardia euroa vuodessa.[1] Tehokkaat julkisia hankintoja koskevat säännöt voisivat siten edistää myös monipuolisemman pilviekosysteemin kehittymistä EU:ssa, jotta teknologiat voisivat kilpailla maailmanlaajuisesti. Ehdotettu CADA tarjoaa ratkaisevan tärkeän tilaisuuden muotoilla tasapainoinen toimintalinja, joka turvaa Euroopan autonomian ja säilyttää samalla pääsyn maailman johtaviin teknologioihin.

Ehdotus tulee ratkaisevaan aikaan, kun Euroopan unioni pyrkii vahvistamaan kilpailukykyään, edistämään innovatiivista ja kestävää laskentakapasiteettia, vauhdittamaan investointeja sekä varmistamaan pilvipalvelujen toiminnan jatkuvuuden ja häiriönsietokyvyn erityisesti julkisella

[1] Why public procurement is important – Euroopan komissio (linkki)

sektorilla. EU:n Digitaalinen vuosikymmen 2030 -toimintaohjelmassa esitetään kunnianhimoinen visio julkisten palvelujen ja laajemmin koko talouden digitaalisesta muutoksesta, ja siinä asetetaan tavoitteet sen varmistamiseksi, että keskeiset julkiset palvelut ovat kokonaan saatavilla verkossa, että julkishallinto ottaa käyttöön kehittyneitä digitaalisia ratkaisuja ja että Eurooppa vahvistaa teknologista ja teollista johtoasemaansa vuoteen 2030 mennessä. Näiden tavoitteiden saavuttaminen riippuu siitä, onko viranomaisilla pääsy turvallisiin, skaalautuviin ja uusimpiin teknologioihin, jotka voivat tukea innovointia, tehokkuutta ja häiriönsietokykyä eri aloilla. Julkisilla hankinnoilla on siksi ratkaiseva rooli Euroopan talouden digitalisaation mahdollistamisessa: niillä varmistetaan, että hankintayksiköt voivat valita alkuperästä riippumatta luokkansa parhaat digitaaliset ratkaisut, jotka täyttävät korkeat suorituskyky-, turvallisuus- ja kestävyysvaatimukset, ja samalla edistetään kilpailua ja innovointia koko digitaalisessa ekosysteemissä. Tavoitteiden toteuttaminen edellyttää sääntelykehystä, joka yhdistää nopeamman käyttöönoton ja oikeusvarmuuden, on sopusoinnussa sellaisten avointen ja kilpailullisten sisämarkkinoiden kanssa, jotka arvostavat ja houkuttelevat pitkäjänteisiä investointeja eurooppalaiseen digitaaliseen infrastruktuuriin, ja edistää yhteistyötä kaikkien niiden palveluntarjoajien kanssa, jotka osoittavat todennettavasti täyttävänsä turvallisuutta, toiminnan jatkuvuutta ja kestävyyttä koskevat tekniset vaatimukset.

Microsoft tukee siksi CADA:n toimenpiteitä, joilla pyritään edistämään tavoitetta vähintään kolminkertaistaa EU:n datakeskuskapasiteetti seuraavien 5–7 vuoden aikana yksinkertaistamalla luvitusta, parantamalla välttämättömien resurssien saatavuutta ja vahvistamalla Euroopan pilvi- ja tekoälyekosysteemiä. Jotta tämä kunnianhimoinen tavoite saataisiin muutettua käyttöön otettavaksi kapasiteetiksi, CADA:n tulisi vahvistaa selkeät ja yhdenmukaistetut säännöt, varmistaa, että ehdotettua nopeutettua luvitusta täydennetään lisätoimilla, joilla turvataan oikea-aikainen ja ennakoitava pääsy sähköverkkoinfrastruktuuriin, sovittaa kestävyysehdot yhteen EU:n datakeskusten kestävyysluokitusjärjestelmän kanssa sekä soveltaa vaatimuksia oikeasuhtaisesti, riskiperusteisesti ja syrjimättömästi.

Samaan aikaan näiden investointeihin kannustavien toimenpiteiden vaikuttavuus uhkaa heikentyä merkittävästi, koska CADA:n suvereniteettikehykseen tuodaan epäselviä tai rajoittavia vaatimuksia sekä ennakoimattomia ja raskaita menettelyjä, jotka luovat epävarmuutta tulevasta markkinoille pääsystä ja toimintaedellytyksistä. Tällainen epävarmuus uhkaa viivästyttää ja jopa karkottaa niitä mittavia yksityisen sektorin investointeja, joita Euroopan datakeskuskapasiteettia koskevien kunnianhimoisten tavoitteiden saavuttaminen edellyttää.

Tässä yhteydessä keskeinen huolenaihe nykymuotoisessa ehdotuksessa on se, että siinä suvereniteetti rinnastetaan yrityksen kansallisuuteen sen sijaan, että suvereniteetti sidottaisiin todennettavissa oleviin teknisiin ja operatiivisiin hallintakeinoihin. Näin ehdotus rajoittaa eurooppalaisten julkisen sektorin asiakkaiden valinnanvapautta ja heidän pääsyään lukuisiin ratkaisuihin, joita he tarvitsevat turvallisuutensa ja kilpailukykynsä varmistamiseksi sekä tavoitteidensa ja päämääriensä tehokkaaksi saavuttamiseksi. Tärkeimpinä kriteereinä tulisi olla organisaation kyky hallita dataansa, pitää kriittiset operatiiviset järjestelmänsä toiminnassa paineen alla, siirtää työkuormia ja yhdistää eri palveluntarjoajien palveluja eikä yrityksen kansallisuus, sillä kansallisuuteen nojaava arviointi aliarvostaa rakenteellisia kriteerejä, kuten teknistä suunnittelua, palveluvalikoiman laajuutta ja riippumattomasti tarkastettuja hallintakeinoja.

Pilvilaskennan suvereniteettikehys, johon kuuluu neljä unionin varmuustasoa (UAL), on tasolta toiselle yhä rajoittavampi paitsi sen suhteen, mitä palveluntarjoajien on osoitettava, myös sen suhteen, keitä niiden on oltava. Tämä ajatus huipentuu varmuustasoon 4, jossa asetetaan vaatimus täysin EU:n hallinnassa olevasta ohjelmistojen toimitusketjusta. Tätä vaatimusta ei tällä

hetkellä pysty täyttämään yksikään pilvipalveluntarjoaja, eurooppalaiset palveluntarjoajat mukaan lukien. Tämä rakenne paljastaa siihen sisältyvän paradoksin: julkisen sektorin kriittisimmät työkuormat (sektorit, kuten puolustus, kansallinen turvallisuus ja kriittinen infrastruktuuri) ovat juuri niitä, jotka tarvitsevat kipeimmin kehittyneen tekoälyn (frontier AI) kyvykkyyksiä, edistyksellisiä kyberturvallisuustyökaluja ja maailmanlaajuista uhkatiedustelua, joita tällä hetkellä pystyvät tarjoamaan vain maailmanlaajuisesti toimivat palveluntarjoajat.

Mittakaava vahvistaa turvallisuutta: maailmanlaajuisesti toimivat palveluntarjoajat investoivat vuosittain miljardeja uhkatiedusteluun, valmiuksiin reagoida poikkeamiin, haavoittuvuustutkimukseen ja suojausinfrastruktuuriin tasolla, johon yksikään kansallinen tai alueellinen palveluntarjoaja ei tällä hetkellä pysty yltämään. Sellainen kehyksen rakenne, jonka seurauksena nämä kyvykkyydet suljetaan pois niitä eniten tarvitsevista järjestelmistä, ei vahvista suvereniteettia vaan heikentää juuri niiden instituutioiden turvallisuustasoa, joita kehyksellä pyritään suojaamaan.

Jos keskeiset poliittiset huolenaiheet liittyvät toiminnan jatkuvuuteen epäsuotuisissa poliittisissa skenaarioissa, oikeasuhtaisen ja tehokkaimman vastauksen tulisi perustua häiriönsietokykyyn eikä poissulkemiseen. Häiriönsietokykyä tulisi vahvistaa lisäämällä toimitusketjujen monipuolisuutta ja säilyttämällä EU:n asiakkaiden valinnanvapauden eikä rajoittamalla sitä. Ukrainan ja Lähi-idän digitaaliseen infrastruktuuriin kohdistuneet hyökkäykset ovat osoittaneet tämän selvästi: kun todellinen geopoliittinen kriisi puhkeaa ja jopa paikallisia datakeskuksia tuhoutuu, julkishallinnon palvelut turvaa nimenomaan maailmanlaajuisesti hajautettu pilvi-infrastruktuuri. Vahvempi häiriönsietokyky saavutetaan parhaiten monipuolistamalla toimittajia tai varmistamalla vaihtoehtoisen kapasiteetin, jonka avulla asiakkaat voivat ylläpitää toiminnan jatkuvuutta, jos jokin palvelu ei ole enää käytettävissä, eikä rajoittamalla EU:n asiakkaiden valinnanvapautta ja katkaisemalla heiltä pääsyn markkinoiden johtaviin ratkaisuihin.

Todennettavissa olevan määräysvallan kriteerien kautta ymmärretty suvereniteetti – suvereenit pilvialueet, asiakkaan hallinnoimiin avaimiin perustuva salaus, arkkitehtuurit, joissa palveluntarjoajalla ei ole pääsyä asiakkaan dataan (operator zero access), sopimukselliset suojatoimet ja riippumaton tarkastus – on vahvempi, paremmin todennettavissa ja häiriönkestävämpi kuin kansallisuuden kautta ymmärretty suvereniteetti. Tämä lähestymistapa säilyttää kilpailun periaatteet, ylläpitää investointikannustimia, kunnioittaa kansainvälisiä kauppasitoumuksia ja varmistaa, että eurooppalaisilla instituutioilla ja kansalaisilla on suojakseen käytettävissä suorituskykyisimmät teknologiat.

Lisäksi kehyksen rakenne voi tahattomasti rajoittaa kilpailua ja innovointia asettamalla epäedulliseen asemaan palveluntarjoajat, jotka tukeutuvat maailmanlaajuisesti integroituihin toimitusketjuihin – todellisuus, joka koskee sekä kansainvälisiä että eurooppalaisia pilvipalveluntarjoajia. Olennaista on, että tämä kaventaa myös niiden asiakkaiden valinnanvapautta, jotka tukeutuvat tällaisiin palveluntarjoajiin.

Tulevaisuutta ajatellen Euroopalla on ainutlaatuinen tilaisuus osoittaa, että digitaalinen suvereniteetti ja avoimuus eivät ole keskenään kilpailevia vaan toisiaan vahvistavia tavoitteita. Suvereniteettikehys, joka perustuu todennettavissa oleviin teknisiin hallintakeinoihin, operatiiviseen häiriönsietokykyyn, yhteentoimivuuteen ja asiakkaiden valinnanvapauteen, vahvistaisi Euroopan strategista autonomiaa ja säilyttäisi samalla pääsyn maailmanluokan teknologioihin, joita tarvitaan innovoinnin, turvallisuuden ja talouskasvun vauhdittamiseen. Edistämällä ennakoitavaa investointiympäristöä, kannustamalla kilpailuun ja mahdollistamalla yhteistyön koko monimuo-

toisessa pilviekosysteemissä CADA voi auttaa houkuttelemaan investointeja siinä mittakaavassa, jota Euroopan digitaalisten tavoitteiden saavuttaminen edellyttää. Oikein mitoitettuna kehys voi tehdä Euroopan unionista paitsi häiriönkestävän ja luotettavan digitaalisen infrastruktuurin edelläkävijän myös maailmanlaajuisen esikuvan siitä, miten suvereniteettia, kilpailukykyä ja teknologista huippuosaamista voidaan edistää rinnakkain.

Keskeiset suositukset tiivistettynä

I. Toimiva pilvilaskennan suvereniteettikehys

Pilvilaskennan suvereniteettikehys

1. **16 artikla – Soveltamisala:** Kaikki varmuustasojen vaatimuksiin, tarkastuskriteereihin tai todisteita koskeviin velvoitteisiin myöhemmin tehtävät muutokset on toteutettava täytäntöönpanosäädöksillä eikä delegoiduilla säädöksillä
2. **17 artikla – Pilvipalveluntarjoajien tunnustaminen:** On estettävä jäsenvaltioita kyseenalaistamasta tunnustamista toistuvasti, jotta vältetään tunnustamisen tarpeeton viivästyminen sekä arkaluonteisten turvallisuutta ja toimintaa koskevien tietojen tarpeeton luovuttaminen
3. **18 artikla – Assosioituneet kolmannet maat:** On varmistettava, että kolmansien maiden tunnustamismekanismi on toimiva ja syrjimätön
4. **19 artikla – Itsearviointi:** Mahdollisuus osoittaa vaatimustenmukaisuus itsearvioinnilla on laajennettava koskemaan varmuustasoa 2

Kysyntätoimet:

5. **29 artikla – Riskinarvioinnit:** Käsite ”yleinen järjestys” on määriteltävä täsmällisesti, on yksilöitävä selkeästi toiminnot, joissa korkeammat varmuustasot voivat olla perusteltuja, ja siirtymäaika on pidennettävä 24 kuukauteen
6. **31 artikla – Yksityistä sektoria koskevat vaikutustenarvioinnit:** Kehyksen suhteeton ulottaminen yksityiseen sektoriin on estettävä
7. **32 artikla – Unionin lisäarvo:** Unionissa suunnitellun, kehitetyn, valmistetun tai käyttöön otetun kestävän infrastruktuurin tuoma panos on otettava nimenomaisesti huomioon

Liitteen II kriteerit unionin varmuustasoille:

8. **Unionin varmuustasojen kriteerit:** On omaksuttava aidosti riskiperusteinen lähestymistapa – ei kaikkiin tilanteisiin samaa suvereniteettivelvoitetta
9. **Kolmansien maiden pääsyä ja määräysvaltaa torjuvien toimenpiteiden kriteerit:** Tekniset ja operatiiviset suojatoimet on tunnustettava päteviksi suvereniteetin välineiksi kolmansien maiden pääsyä ja määräysvaltaa vastaan
10. **Alihankkijoita, henkilöstöä ja asiakastukea koskevat kriteerit:** Alihankkijoiden, henkilöstön ja asiantuntijatuen kohtelua on selkeytettävä, jotta kehittyneiden pilvipalvelujen toimittamista eurooppalaisille asiakkaille ei rajoiteta
11. **Asiakasdataa, metatietoja ja telemetriatietoja koskevat kriteerit:** Tekniset telemetria- ja metatiedot on erotettava asiakasdatasta, ja metatietojen ja telemetriatietojen rajat ylittävä käsittely on sallittava silloin, kun niitä käytetään tietoturvaan, häiriönsietokykyyn ja operatiiviseen toimintaan liittyviin oikeutettuihin tarkoituksiin
12. **Ohjelmistohaavoittuvuuksista raportointi:** On selkeytettävä, ettei osallistuminen oikeutettuihin ja koordinoituihin haavoittuvuuksien julkistamisjärjestelyihin, joissa haavoittuvuuksista ilmoitetaan ennen korjauspäivityksen julkaisua, sellaisenaan estä palveluntarjoajaa täyttämästä suvereniteettivaatimuksia
13. **Kyberturvallisuutta ja ohjelmistojen toimitusketjua koskevien toimenpiteiden kriteerit:** CADA on sovitettava yhteen EU:n voimassa olevan kyberturvallisuuskehyksen kanssa, ja on vältettävä luomasta rinnakkaista ja ristiriitaista velvoitekokonaisuutta
14. **Tekoälyjärjestelmien koulutusta ja hienosäätöä koskevien rajoitusten kriteerit:** Tekoälyyn liittyvät suvereniteettivaatimukset on pidettävä oikeasuhtaisina ja selkeästi rajattuina

II. Kestävien datakeskusten lupamenettelyjen sujuvoittaminen

1. **11 artikla – Nopean kehittämisen alueiden kytkeminen EU:n datakeskusten luokitusjärjestelmään:** Pääsy nopean kehittämisen alueille on sidottava EU:n datakeskusten luokitusjärjestelmän kestävyysindikaattoreihin
2. **11 artikla – Nopean kehittämisen alueiden kytkeminen sähköverkkoon pääsyyn:** Nopean kehittämisen alueet on kytkettävä sähköverkkoon pääsyyn valmiusjärjestysperiaatteen (first-ready, first-served) mukaisesti
3. **13 artikla – Hallinto- ja lupamenettelyjen helpottaminen:** Lupamenettelyn digitalisointi
4. **13 artikla – Hallinto- ja lupamenettelyjen helpottaminen:** Perusluvan soveltamisalan ja toiminnan selkeyttäminen
5. **14 artikla – Strategisten datakeskushankkeiden nimeäminen:** Selkeytettävä, että hankkeen nimeäminen strategiseksi oikeuttaa samoihin lupamenettelyetuihin
6. **14 artikla – Strategisten datakeskushankkeiden nimeäminen:** Ympäristöomnibusin kunnianhimon säilyttäminen

I. Toimiva EU:n pilvilaskennan suvereniteettikehys

Microsoft tukee EU:n pyrkimystä vahvistaa taloudellista turvallisuuttaan, häiriönsietokykyään ja strategista autonomiaansa. Katsomme, että nämä tavoitteet saavutetaan parhaiten **toiminnallisella, riskiperusteisella digitaalisen suvereniteetin mallilla**, joka nojaa osoitettavissa oleviin teknisiin, operatiivisiin ja oikeudellisiin suojatoimiin, sen sijaan että turvauduttaisiin poissulkeviin, kansallisuuteen perustuviin kriteereihin.

Tässä mallissa suvereniteetti saavutetaan yhdistämällä seuraavat keinot:

- **Tekniset hallintakeinot:** Kehittyneiden tietoturvateknologioiden avulla asiakkaat voivat säilyttää datansa hallinnan riippumatta siitä, kuka infrastruktuurin omistaa. Näihin teknologioihin kuuluvat asiakaspuolen salaus, asiakkaan hallinnoimat salausavaimet, luottamuksellisen laskennan (confidential computing) ympäristöt, työkuormien eristäminen sekä identiteetin- ja pääsynhallinta. Tällaiset mekanismit varmistavat, että data pysyy vain valtuutettujen osapuolten käytettävissä silloinkin, kun infrastruktuuria ylläpitävät ulkopuoliset palveluntarjoajat.
- **Operatiiviset suojatoimet:** Pilvipalveluntarjoajat voivat ottaa käyttöön hallintorakenteita, jotka varmistavat operatiivisen autonomian EU:ssa. Niihin kuuluvat muun muassa EU:hun sijoittautuneet toimintayksiköt, rajoitettu ylläpitäjäpääsy, turvallisuusselvitetty henkilöstö ja tarkastettavissa olevat toimintamenettelyt.
- **Sopimukselliset suojakeinot:** Vahvoilla sopimuksellisilla sitoumuksilla ja takeilla voidaan suojata asiakasdataa luvattomalta pääsyltä ja varmistaa EU:n lainsäädännön noudattaminen.

Digitaalista suvereniteettia ei tulisi rinnastaa poissulkeviin tai keinotekoisiin lokalisointikriteereihin. Edellä kuvattu toiminnallinen lähestymistapa voi tarjota tosiasiallisen hallinnan rajoittamatta tarpeettomasti asiakkaiden mahdollisuuksia valita ja yhdistellä tarpeisiinsa parhaiten soveltuvia teknologioita ja ratkaisuja sekä siirtyä niiden välillä. Rajoittavat lähestymistavat uhkaavat aiheuttaa merkittäviä taloudellisia kustannuksia, ja ne voivat viime kädessä heikentää turvallisuutta ja innovaatiokykyä.

Microsoft on investoinut merkittävästi vastatakseen suvereniteettia koskeviin huolenaiheisiin Euroopassa: se on antanut eurooppalaiset digitaaliset sitoumuksensa (European Digital Commitments), tuonut tarjolle suvereeneja pilvipalveluja ja laajentanut alueellista infrastruktuuriaan. Näiden aloitteiden ansiosta eurooppalaiset asiakkaamme voivat säilyttää datansa, toimintojensa ja vaatimustenmukaisuusvelvoitteidensa hallinnan ja hyötyä samalla maailmanlaajuisista innovaatioista ja häiriönkestävästä, laajamittaisesta pilvi-infrastruktuurista.

Seuraavat suositukset keskittyvät CADA:n autonomiapilariin, unionin varmuustasojen kriteereihin ja muihin asiaan liittyviin säännöksiin. Kussakin suosituksessa esitetään keskeinen perustelu, lyhyt selvitys ja suositeltu etenemistapa.

1. 16 artikla – Soveltamisala

Keskeinen perustelu: ***Ehdotuksen 16 artikla valtuuttaa komission muuttamaan delegoiduilla säädöksillä unionin varmuustasoja (UAL) ja niihin liittyviä tarkastustodisteita koskevia vaatimuksia. Koska varmuustasojen vaatimukset määrittävät suoraan pilvipalveluntarjoajien markkinoille pääsyn edellytykset ja vaatimustenmukaisuusvelvoitteet, kehyksen***

soveltamisala ja siitä aiheutuva taakka voisivat tulevien muutosten myötä muuttua olennaisesti ilman riittävää jäsenvaltioiden valvontaa tai sidosryhmien tarkastelua.

Ehdotettu pilvisuvereniteettikehys tuo mukanaan merkittäviä vaatimustenmukaisuusvelvoitteita, joilla on laaja-alaisia kaupallisia ja operatiivisia vaikutuksia. Varmuustasojen vaatimuksia muutettaessa olisi siksi varmistettava suurempi avoimuus ja ennakoitavuus sekä jäsenvaltioiden tiiviimpi osallistuminen. Täytäntöönpanosäädösten käyttäminen lisäisi oikeusvarmuutta, vähentäisi riskiä siitä, että muuttuvat vaatimukset kasvattavat ajan mittaan vähitellen vaatimusten noudattamisesta aiheutuvaa taakkaa, ja loisi vakaamman sääntely-ympäristön pitkän aikavälin investoinneille pilvi- ja tekoälyinfrastruktuuriin Euroopassa.

Suositus

On muutettava 16 artiklan 2 kohtaa siten, että kaikki varmuustasojen vaatimuksiin, tarkastuskriteereihin tai todisteita koskeviin velvoitteisiin myöhemmin tehtävät muutokset toteutetaan täytäntöönpanosäädöksillä eikä delegoiduilla säädöksillä.

2. 17 artikla – Pilvipalveluntarjoajien tunnustaminen

Keskeinen perustelu: ***Ehdotuksen 17 artiklan mukaisen tunnustamiskehyksen tulisi olla riskiperusteinen ja teknologianeutraali, ja se olisi pantava täytäntöön yhdenmukaisesti kaikkialla EU:n sisämarkkinoilla. Kehyksen tulisi välttää päällekkäisiä arviointeja, mahdollistaa toisiinsa liittyvien palvelujen tehokas tunnustaminen ja tarjota ennakoitava väylä kelpoisuuteen julkisiin hankintoihin siten, että turvallisuutta ja suvereniteettia koskeva varmuustaso säilyy samalla korkeana. Tunnustamiskehyksessä tulisi välttää arkaluonteisten turvallisuus- ja toimintatietojen tarpeetonta luovuttamista.***

Tunnustamismenettelystä tulee ratkaisevan tärkeä portti kelpoisuuteen julkisiin hankintoihin, ja siksi sen rakenteella on suuri merkitys. Menettelyn tulisi olla tehokas ja kaikissa jäsenvaltioissa ennakoitava, ja sen tulisi soveltua erilaisiin palvelumalleihin.

Tunnustamismenettelyjen tulisi perustua jo tehtyihin arviointeihin. Jos palveluntarjoaja on jo osoittanut tunnustetun infrastruktuurin tai palvelun vaatimustenmukaisuuden, siihen liittyvät palvelut ja kokoonpanot, jotka nojaavat samoihin tai vahvempiin hallintakeinoihin, olisi arvioitava ainoastaan lisäriskien osalta. Uudelleenarviointi olisi rajattava olennaisiin muutoksiin, jotka vaikuttavat suvereniteettiriskiprofiiliin, kuten muutoksiin datan sijainnissa, etuoikeutetussa pääsyssä, salauksen hallinnassa, alihankkijoiden pääsyssä tai altistumisessa kolmannen maan oikeudellisille velvoitteille.

Tietyllä varmuustasolla tunnustettu palvelu olisi hyväksyttävä kaikkialla EU:ssa ilman kansallisia lisävaatimuksia, paitsi jos lisävaatimukset ovat perusteltuja erityisten kansalliseen turvallisuuteen liittyvien huolenaiheiden vuoksi. Yhdenmukainen täytäntöönpano on välttämätöntä, jotta voidaan estää markkinoiden pirstoutuminen, tukea rajat ylittävää toimintaa ja luoda varmuutta sekä asiakkaille että palveluntarjoajille. Myös vastalausemenettelyn tulisi tukea vastavuoroista tunnustamista eikä heikentää sitä. Tunnustamispäätöksen kyseenalaistamisen tulisi aina nojata objektiivisiin, näyttöön perustuviin ja täytäntöönpanokelpoisiin kriteereihin, jotka koskevat yksinomaan sovellettavan varmuustason vaatimusten täyttymistä. Tunnustamismenettelyjä ei tulisi käyttää kansallisuuteen perustuvien tai protektionististen tavoitteiden ajamiseen.

Lisäksi 17 artiklan 4 ja 5 kohdassa edellytetään, että tunnustamista hakevat palveluntarjoajat toimittavat riippumattoman tarkastuskertomuksen lisäksi myös koko sen todisteaineiston, joka on aiemmin annettu kolmannen osapuolen tarkastajille. Liitteen III laajojen tarkastusvaatimusten vuoksi tämä voisi johtaa siihen, että suuria määriä erittäin arkaluonteisia teknisiä, operatiivisia ja turvallisuuteen liittyviä tietoja kiertäisi useiden toimivaltaisten viranomaisten välillä.

Riippumattomien kolmannen osapuolen tarkastusten tarkoituksena on antaa toimivaltaisille viranomaisille varmuus siitä, että vaatimustenmukaisuus on arvioitu riippumattomasti suhteessa säädettyihin kriteereihin. Vaatimus, jonka mukaan palveluntarjoajien on rutiininomaisesti luovutettava koko tarkastustodisteaineisto, heikentää tätä lähestymistapaa ja aiheuttaa huomattavia luottamuksellisuuteen, liikesalaisuuksiin ja kyberturvallisuuteen liittyviä riskejä. Kehyksen tulisi ensisijaisesti nojata akkreditoituihin tarkastajiin, ja lisätietopyynnöt olisi varattava poikkeuksellisiin tilanteisiin, joissa tarkastuskertomus ei sellaisenaan anna riittävää varmuutta.

Suositus

On estettävä jäsenvaltioita kyseenalaistamasta tunnustamista toistuvasti, jotta tunnustamispäätökset eivät viivästy tarpeettomasti:

- Viranomaisten on voitava tukeutua aiemmin arvioituihin todisteisiin ja soveltaa tunnustamisessa kerroksittaista lähestymistapaa toisiinsa liittyviin palveluihin, infrastruktuureihin ja käyttöönottomalleihin.
- Uudelleenarvioinnit on rajattava olennaisiin muutoksiin, jotka vaikuttavat suvereniteettiriskiin.
- On varmistettava, että palvelujen tunnustaminen tietyllä varmuustasolla on voimassa koko EU:ssa, ja on estettävä tarpeeton kansallinen lisäsääntely (ns. gold plating).
- On perustettava avoin EU-tason tunnustettujen palvelujen ja vireillä olevien hakemusten rekisteri.
- Vastalauseiden on perustuttava näyttöön ja oltava kohdennettuja, ja niihin on sovellettava selkeitä menettelyllisiä määräaikoja.
- On vahvistettava täytäntöönpanosäädöksillä yhdenmukaistettu EU-tason riskinarviointimenetelmä ja varmistettava kaikkien palveluntarjoajien yhdenvertainen kohtelu.
- On muutettava 17 artiklan 4 ja 5 kohtaa siten, että riippumaton tarkastuskertomus ja myönteinen tarkastuslausunto ovat tunnustamispäätösten ensisijainen peruste.
- On poistettava vaatimus, jonka mukaan pilvipalveluntarjoajien on rutiininomaisesti toimitettava kaikki kolmannen osapuolen tarkastajille annetut tarkastustodisteet.
- On muutettava 17 artiklan 5 kohdan b alakohtaa siten, että lisätietoja voidaan pyytää vain, jos palveluntarjoajan toimittama tarkastuskertomus ja myönteinen tarkastuslausunto ovat riittämättömiä, eikä silloin, kun itse todisteita pidetään riittämättöminä.

3. 18 artikla – Assosioituneet kolmannet maat

Keskeinen perustelu: ***Luotettavien kolmansien maiden palveluntarjoajien väylä varmuustasolle 3 on sovitettava paremmin yhteen EU:n riittävyyspäätöskehyksiä koskevien GDPR:n periaatteiden kanssa.***

Ehdotetussa muodossaan CADA-kehys sulkee unionin varmuustason 3 kolmannen maan määräysvallassa olevilta palveluntarjoajilta, ellei Euroopan komissio tee myönteistä päätöstä siitä,

että kyseinen kolmas maa tarjoaa ”riittävät suojatoimet”. Tämä 18 artiklan mukainen assosioituneita maita koskeva mekanismi edellyttää kumulatiivisesti muun muassa seuraavien ehtojen täyttymistä: kyseisestä maasta on oltava tehty GDPR:n mukainen tietosuojan riittävyyspäätös, maassa ei saa olla toimenpiteitä, jotka mahdollistavat ristiriitaisen määräysvallan tai lainvastaisen pääsyn dataan, maan markkinoille pääsyn on oltava avointa ja EU:n määräysvallassa olevilla pilvipalveluilla on oltava vastavuoroinen pääsy maan julkisiin hankintoihin. Ehdotuksen 18 artiklassa säädetyn poikkeuksen perusteet jäävät epäselviksi, koska liitteen II datan lokalisointivaatimusten soveltaminen kolmansiin maihin, joista on tehty riittävyyspäätös, herättää jo sellaisenaan kysymyksiä GDPR-kehyksen kannalta. Lisäksi on hyviä perusteita kyseenalaistaa viimeksi mainittujen, riittävyyspäätöskehyksen kriteerin ylittävien vaatimusten pätevyys. Tämä koskee erityisesti vaatimusta, jonka mukaan maassa ei saa olla voimassa täytäntöönpanokelpoisia pakotejärjestelmiä, mikä olisi tiukempi ehto kuin se, mitä EU soveltaa itseensä.[2]

Suositus

On varmistettava, että kolmansien maiden tunnustamismekanismi on toimiva ja syrjimätön. GDPR:n mukaisesti 18 artiklassa säädetty menettely olisi sovitettava tiiviimmin yhteen EU:n nykyisen riittävyyspäätöskehyksen sekä datasäädöksen mukaisen kehyksen kanssa. Menettely olisi käynnistettävä viipymättä ja objektiivisesti silloin, kun edellytykset täyttyvät, eikä sitä tulisi voida käyttää poliittisena painostusvälineenä. Ennakoitava tunnustamisväylä lähettäisi EU:n ulkopuolisille pilvipalveluntarjoajille vahvan viestin siitä, että laajamittaiset investoinnit eurooppalaiseen infrastruktuuriin johtavat vakaaseen ja luotettavaan pääsyyn markkinoille. Tämä kannustaisi juuri siihen datakeskus- ja tekoälykapasiteetin laajentamiseen, jota CADA itse pyrkii vauhdittamaan.

4. 19 artikla – Vaatimustenmukaisuuden itsearviointi

Keskeinen perustelu: ***Koska unionin varmuustaso 2 (UAL 2) on tarkoitettu vähemmän arkaluonteisiin julkisen sektorin käyttötapauksiin kuin varmuustasot 3 ja 4, pakollinen kolmannen osapuolen suorittama vaatimustenmukaisuuden arviointi tällä tasolla uhkaa aiheuttaa tarpeetonta hallinnollista taakkaa, lisätä vaatimusten noudattamisen kustannuksia ja hidastaa julkisen sektorin digitalisaatiota tuottamatta vastaavassa määrin turvallisuus- tai suvereniteettihyötyjä. Itsearvioinnin laajentaminen varmuustasolle 2 olisi sopusoinnussa sen kanssa, että EU on sitoutunut sääntelyn yksinkertaistamiseen, oikeasuhtaisuuteen ja riskiperusteiseen sääntelyyn.***

Palveluntarjoajien mahdollisuus osoittaa itsearvioinnilla ja vaatimustenmukaisuusvakuutuksella täyttävänsä unionin varmuustason 1 (UAL 1) vaatimukset on tervetullut askel kohti käytännönläheisempää ja toimivampaa kehystä.

CADA-kehys nojaa riskiperusteiseen lähestymistapaan, jossa varmuusvaatimukset tiukkenevat asteittain sitä mukaa kuin työkuorman arkaluonteisuus suvereniteetin kannalta kasvaa. Varmuustaso 2 sijoittuu varmuustason 1 perusvaatimusten ja varmuustasoille 3 ja 4 kaavailtujen erittäin rajoittavien hallintakeinojen välille. Siksi varmuustason 2 tulisi pysyä saavutettavana ja käytännössä toimivana tasona monenlaisille tavanomaisille julkisen sektorin työkuormille, jotka eivät liity kaikkein arkaluonteisimpiin kansallisen turvallisuuden tai yleisen järjestyksen toimintoihin.

[2] When European Governments Pull the Plug – Lawfare, syyskuu 2025 (linkki)

Lisäksi itsearvioinnin laajentaminen varmuustasolle 2 tukisi paremmin kilpailua ja palveluntarjoajien osallistumista. Samalla vastuuvelvollisuus säilyisi vaatimustenmukaisuusvakuutusten, jälkikäteisten valvontamekanismien sekä mahdollisen viranomaisvalvonnan avulla, jos huolenaiheita ilmenee. Tämä auttaisi varmistamaan, että suvereniteettitavoitteet saavutetaan rajoittamatta tarpeettomasti asiakkaiden valinnanvapautta tai supistamatta vähemmän arkaluonteisia työkuormia varten käytettävissä olevien palveluntarjoajien joukkoa. Tällainen lähestymistapa olisi myös sopusoinnussa laajemman tavoitteen kanssa pitää suvereniteettivaatimukset oikeassa suhteessa kunkin käyttötapauksen tosiasialliseen riskiin, sen sijaan että kaikilla varmuustasoilla asetettaisiin sama hallinnollinen taakka.

Suositus

Ehdotuksen 19 artiklaa olisi muutettava siten, että varmuustason 2 tunnustamista hakevat palveluntarjoajat voivat osoittaa täyttävänsä vaatimukset vaatimustenmukaisuusvakuutuksella ja itsearvioinnilla samalla tavoin kuin varmuustason 1 osalta on ehdotettu. Pakollinen kolmannen osapuolen suorittama vaatimustenmukaisuuden arviointi olisi varattava varmuustasoille 3 ja 4, joilla työkuormien arkaluonteisuus ja tavoiteltu suvereniteettivarmuuden taso oikeuttavat lisätarkastelun.

Tämä muutos säilyttäisi vastuuvelvollisuuden ja varmistaisi samalla, että vaatimustenmukaisuusvelvoitteet pysyvät oikeassa suhteessa riskiin, vähentäisi tarpeetonta sääntelytaakkaa, nopeuttaisi pilvipalvelujen käyttöönottoa julkisella sektorilla ja tukisi EU:n ilmoittamaa tavoitetta yksinkertaistaa digitaalista sääntelyä ja vahvistaa Euroopan digitaalista kilpailukykyä.

5. 29 artikla – Riskinarvioinnit

Keskeinen perustelu: ***Määrittelemättömään käsitteeseen ”yleinen järjestys” liittyy keskeinen riski siitä, että sääntelytoimet ulottuvat aiottua soveltamisalaansa laajemmalle; käsite on määriteltävä suppeasti ja täsmällisesti. Ehdotuksen 29 artiklan 6 kohdassa edellytetään, että asiakkaat siirtyvät pois tunnustetusta pilvipalvelusta 12 kuukauden kuluessa, jos palveluntarjoajan tunnustaminen peruutetaan. Monimutkaisten pilviympäristöjen siirtäminen on monille organisaatioille, erityisesti julkisen sektorin toimijoille ja kriittisten palvelujen tuottajille, paljon resursseja sitova ja teknisesti vaativa prosessi, joka kestää usein yli vuoden.***

Käsite ”yleisen järjestyksen ylläpitämisen edistäminen” – josta seuraa velvoite käyttää korkeamman varmuustason pilvipalveluja (unionin varmuustasoa 1 korkeampia) – jää CADA:n tekstissä määrittelemättä, sille ei ole yhtenäistä EU-oikeudellista määritelmää, ja siksi sitä tulkitaan eri jäsenvaltioissa eri tavoin. Tästä aiheutuu merkittävä riski laajentavista tulkinnoista, joiden seurauksena monenlaiset tavanomaiset julkishallinnon toiminnot joutuisivat korkeamman varmuustason vaatimusten piiriin. CADA:ssa otetaan lisäksi käyttöön suvereniteettiriskien arviointi eli mekanismi, jolla määritetään, mitä pilvipalveluja viranomaiset saavat käyttää. Keskeinen huolenaihe on, että nämä arvioinnit lisäävät vähitellen korkeampia suvereniteettitasoja edellyttävien työkuormien määrää, mikä rajoittaa kilpailua ja kaventaa markkinoille pääsyä sellaisilta palveluntarjoajilta, jotka eivät pysty täyttämään näiden tasojen vaatimuksia.

Lisäksi 12 kuukauden pituinen siirtymisen määräaika ei ota riittävästi huomioon laajamittaisiin pilvisiirtoihin liittyvää teknistä monimutkaisuutta, operatiivisia riskejä ja sopimuksellisia realiteetteja. Asiakkaat tukeutuvat pilvipalveluihin usein liiketoimintakriittisissä työkuormissa, jotka

edellyttävät laajaa suunnittelua, testausta, tietoturvan todentamista ja toiminnan jatkuvuutta turvaavia toimenpiteitä, ennen kuin siirto voidaan viedä turvallisesti päätökseen.

Siirtymäajan pidentäminen 24 kuukauteen antaisi asiakkaille riittävästi aikaa toteuttaa hallittu siirtyminen ja vähentäisi palvelukatkosten riskiä, ja sen ansiosta vältettäisiin tarpeettomien operatiivisten ja kyberturvallisuusriskien syntyminen. Pidempi siirtymäaika parantaisi myös pilvipalvelujen asiakkaiden oikeusvarmuutta ja varmistaisi samalla, että kehyksen vaatimustenmukaisuutta koskevat tavoitteet saavutetaan oikeasuhtaisella ja käytännönläheisellä tavalla.

Suositus

- Käsite ”yleinen järjestys” on määriteltävä täsmällisesti, ja on yksilöitävä selkeästi ne toiminnot, joissa korkeampi varmuustaso voi olla perusteltu. CADA:ssa olisi vahvistettava selkeät ja sitovat kriteerit, jotka rajaavat korkeampia tasoja edellyttävien ”yleiseen järjestykseen” liittyvien toimintojen piirin ja säilyttävät aidon joustavuuden julkisen sektorin pilvipalvelujen käytön valtaosassa. Kannustamme ottamaan käyttöön joko tarkasti määritellyn luettelon julkisen sektorin toiminnoista, joissa edellytetään korkeampia tasoja, tai komission yhteisen menetelmän, joka asettaa aidosti korkean kynnyksen sille, että toiminnan katsotaan liittyvän ”yleiseen järjestykseen” – rajattuna kaikkein kriittisimpiin käyttötapauksiin puolustuksessa, lainvalvonnassa, rajaturvallisuudessa ja vastaavilla aloilla. Määrittelemätön mittapuu avaa tien sisämarkkinoiden pirstoutumiselle, ja siitä uhkaa tulla se väline, jonka kautta kehys ulottuu paljon ilmoitettua tarkoitustaan laajemmalle.
- On muutettava 29 artiklan 6 kohtaa siten, että siirtymäaika pidennetään 12 kuukaudesta 24 kuukauteen.

6. 31 artikla – Yksityistä sektoria koskevat vaikutustenarvioinnit

Keskeinen perustelu: ***CADA:n suvereniteettikehyksen on pysyttävä tiukasti julkiseen sektoriin keskittyvänä, eikä se saa ulottua NIS2-direktiivin piiriin kuuluviin yksityisen sektorin toimijoihin*****.**

Vaikka CADA:n mukaiset velvoitteet kohdistuvat julkiseen sektoriin, NIS2-direktiivin liitteen I toimialojen yksityisiä toimijoita kannustetaan tekemään vastaavia vaikutustenarviointeja. Ehdotus menee kuitenkin kannustamista pidemmälle, sillä se antaa komissiolle mahdollisuuden velvoittaa erittäin kriittiset toimijat delegoiduilla säädöksillä tekemään tällaisia arviointeja. Tämä laajentaa ehdotuksen soveltamisalaa merkittävästi, vaikka delegoituja säädöksiä tulisi käyttää vain muiden kuin keskeisten osien osalta. Lisäksi säännöksessä ei ole minkäänlaisia selkeitä perusteluja eikä objektiivisia kriteerejä sisältävää kehystä, jonka nojalla tällainen laajentaminen olisi oikeutettua. Näin säännös laajentaa CADA:n suvereniteettikehyksen soveltamisalaa jo luonteeltaan suhteettomasti.

Suositus

Jotta estetään kehyksen suhteeton ulottaminen yksityiseen sektoriin, minkäänlainen laajentaminen julkisen sektorin ulkopuolelle ei saisi olla mahdollista delegoiduilla säädöksillä, vaan siitä olisi päätettävä tavallisessa lainsäätämisjärjestyksessä sellaisen uudelleentarkastelulausekkeen perusteella, joka on sidottu selkeisiin kriteereihin ja perusteelliseen vaikutustenarviointiin. Lainsäätäjien tulisi siksi harkita 31 artiklan 3 kohdan poistamista.

7. 32 artikla – Unionin lisäarvo

Keskeinen perustelu: ***Ehdotuksen 32 artiklassa pyritään määrittelemään strategisista hankkeista syntyvä unionin lisäarvo. Nykyisessä muotoilussa ei kuitenkaan oteta riittävästi huomioon niitä laajempia ekosysteemihyötyjä, joita kestävät infrastruktuuri-investoinnit tuottavat.***

Euroopan kyky kasvattaa pilvi- ja tekoälykapasiteettiaan edellyttää myös sellaisen **kestävän infrastruktuurin** käyttöönottoa, joka tukee pitkän aikavälin kasvua, energiatehokkuutta ja häiriönsietokykyä. Laajemmassa unionin lisäarvon määritelmässä olisi siksi otettava nimenomaisesti huomioon investoinnit kestävään infrastruktuuriin, joka on suunniteltu, kehitetty, valmistettu tai otettu käyttöön unionissa. Tällainen lähestymistapa kuvastaisi paremmin näiden investointien panosta Euroopan digitaalisten tavoitteiden ja kestävyystavoitteiden saavuttamiseen ja loisi samalla vahvempia kannustimia laajentaa infrastruktuuripohjaa, jota Euroopan pilvi- ja tekoälypyrkimysten tukeminen edellyttää.

Suositus

On laajennettava 32 artiklan 3 kohdan a alakohtaa siten, että siinä otetaan nimenomaisesti huomioon unionissa suunnitellun, kehitetyn, valmistetun tai käyttöön otetun **kestävän infrastruktuurin** tuoma panos.

8. Liite II – Unionin varmuustasojen kriteerit

Keskeinen perustelu: ***Suvereniteettivaatimusten tulisi olla oikeassa suhteessa sekä kunkin työkuorman arkaluonteisuuteen että kunkin yksittäisen suvereniteettiulottuvuuden edellyttämään varmuustasoon, eikä niitä tulisi asettaa yhtenäisesti koko organisaation tasolla tai niputtaa yhdeksi ainoaksi tasoksi.***

CADA asettaa unionin varmuustason 1 kaikkia julkisia hankintoja koskevaksi vähimmäistasoksi, mikä velvoittaa kaikki julkisen sektorin elimet hankkimaan pilvipalveluja, jotka täyttävät vähintään perustason suvereniteettikriteerit. Korkeammat tasot (2, 3 ja 4) tulevat sovellettaviksi, jos suvereniteettiriskien arvioinnissa todetaan, että julkisen sektorin toiminta ”edistää yleisen järjestyksen ylläpitämistä”. Esimerkiksi unionin varmuustaso 4 edellyttää kokonaan EU:ssa sijaitsevaa infrastruktuuria ja tiukkoja ohjelmistojen toimitusketjua koskevia toimenpiteitä, ja se on puolustukselle ja kriittisimmille toiminnoille tarkoitettu taso. Nykyinen rakenne, jossa kaikkiin tilanteisiin sovelletaan samaa mallia, aiheuttaa kaksi erillistä ongelmaa. Ensinnäkin riski vaihtelee työkuormasta toiseen, joten varmuustasoa koskevat vaatimukset tulisi arvioida työkuormakohtaisesti eikä asettaa koko organisaatiota koskeviksi. Korkeampi varmuustaso voi olla perusteltu kriittisissä julkisen sektorin sovelluksissa, kun taas rutiininomaisissa tai vähemmän arkaluonteisissa työkuormissa tulisi säilyttää joustavuus. Toiseksi saman asiakkaan tai työkuorman edellyttämä varmuustaso voi vaihdella suvereniteetin eri ulottuvuuksien välillä. Asiakas voi esimerkiksi tarvita kyberturvallisuuden osalta erittäin korkean varmuustason mutta datan lokalisoinnin osalta matalamman. Vaatimus, jonka mukaan asiakkaiden on valittava yksi ainoa unionin varmuustaso – 1, 2, 3 tai 4 – kaikille osa-alueille, estää tämän välttämättömän hienosäädön. Siksi on olennaista, että erittäin kriittiset julkisen sektorin käyttötapaukset määritellään suppeasti ja rajataan tiukasti ja että kehys samalla sallii varmuustason eriyttämisen kriteereittäin. Näin voidaan estää perusteeton syrjintä ja varmistaa, että EU noudattaa WTO:n julkisia hankintoja koskevan sopimuksen (GPA) mukaisia sitoumuksiaan.

Suositus

On omaksuttava aidosti riskiperusteinen lähestymistapa – ei kaikkiin tilanteisiin samaa suvereniteettivelvoitetta. Jäykkä vaatimus valita yksi varmuustaso kaikille suvereniteettikriteereille olisi korvattava modulaarisella lähestymistavalla, jossa asiakkaat voivat soveltaa eri kriteereihin – kuten kyberturvallisuuteen, operatiiviseen hallintaan, datan sijaintiin ja datan lokalisointiin – eri varmuustasoja kunkin työkuorman erityisen riskiprofiilin mukaisesti. Ilman tällaista hienosäätöä julkishallinnon rutiininomaiset työkuormat (esim. henkilöstöhallinnon järjestelmät, julkisen viestinnän alustat ja muu kuin arkaluonteinen analytiikka) ovat vaarassa joutua liian laajalle ulotetun riskinarvioinnin vuoksi korkeammille varmuustasoille, mikä kaventaisi käytettävissä olevien palveluntarjoajien joukkoa, nostaisi kustannuksia ja hidastaisi julkisten palvelujen digitalisointia.

9. Liite II – Kolmansien maiden pääsyä ja määräysvaltaa torjuvien toimenpiteiden kriteerit

Keskeinen perustelu: ***CADA:ssa palveluntarjoajia tulisi arvioida sen perusteella, kuinka tehokkaita ovat ne oikeudelliset, tekniset ja organisatoriset suojatoimet, joita ne toteuttavat estääkseen kolmansien maiden luvattoman pääsyn dataan ja varmistaakseen palvelun jatkuvuuden, eikä omistusrakenteiden, kansallisuuteen perustuvien kriteerien tai kolmannen maan lainsäädännölle altistumisen teoreettisen mahdollisuuden perusteella. Altistumisen EU:n ulkopuoliselle lainsäädännölle – myös viranomaisten pääsylle dataan oikeutettuja yleiseen turvallisuuteen liittyviä tarkoituksia varten – ei tulisi olla automaattinen este tietyn varmuustason saavuttamiselle, jos palveluntarjoaja pystyy osoittamaan, että sillä on käytössään vankat ja todennettavat toimenpiteet, jotka lieventävät tähän liittyviä riskejä tehokkaasti.***

Jos palveluntarjoajia vaadittaisiin osoittamaan, että ne ovat täysin kolmannen maan lainsäädännön ulottumattomissa tai yhtiörakenteeltaan kokonaan erillään EU:n ulkopuolisista yhteisöistä, luotaisiin vaatimustaso, joka olisi maailmanlaajuisesti verkottuneessa digitaalitaloudessa oikeudellisesti epävarma ja käytännössä saavuttamaton. Tällainen lähestymistapa uhkaa sulkea pois palveluntarjoajia, jotka ovat toteuttaneet vankat ja tehokkaat suojatoimet, samalla kun se painottaa suhteettomasti muodollista yhtiörakennetta eikä tosiasiallista riskien lieventämistä. Vaatimustenmukaisuutta tulisi sen sijaan arvioida osoitettavissa olevien oikeudellisten, teknisten ja operatiivisten suojatoimien perusteella. Näitä ovat muun muassa EU:ssa toimiva riippumaton hallintorakenne, tekninen eristäminen, tiukka pääsynvalvonta, salaus ja avaintenhallinta, sopimukseen perustuvat suojakeinot, avoimuussitoumukset sekä menettelyt, joilla viranomaisten dataan pääsyä koskevia pyyntöjä tarkastellaan, riitautetaan ja rajataan mahdollisimman suppeiksi.

Kolmannen maan määräysvaltaa koskevissa säännöksissä tulisi myös selventää, että palveluntarjoajien nykyiset sitoumukset – mukaan lukien sitoumus riitauttaa sellaiset viranomaisten dataan pääsyä koskevat määräykset tai pakotteet, jotka vaarantaisivat palvelun tuottamisen – riittävät niiden riskien hallintaan, joihin nämä säännökset kohdistuvat. Vastaavaa kohtelua tulisi soveltaa myös palveluntarjoajiin, joiden päätoimipaikka on EU:ssa ja joilla on merkittävää toimintaa kolmansissa maissa. Lisäksi ”palvelun epäämistä” sekä ”pakotteita ja kauppasaartoa” koskevia kriteerejä tulisi käsitellä yhtenä johdonmukaisena arviointiperusteena eikä päällekkäisinä vaatimuksina, ja keskeiset käsitteet, kuten ”kolmannen maan määräysvalta”, tulisi määritellä selkeästi, erityisesti sen osalta, tarkoitetaanko määräysvallalla lainkäyttövaltaa, omistusta vai molempia.

Tällainen suojatoimiin perustuva lähestymistapa vastaisi uskottavammin palvelun keskeytymistä koskeviin huoliin. Olennaista ei tulisi olla se, onko palveluntarjoajalla mitään yhteyttä kolmanteen maahan, vaan se, onko se ottanut käyttöön tehokkaat järjestelyt, joiden avulla välttämättömät palvelut voivat jatkua, jos pääsy tiettyihin teknologioihin, infrastruktuuriin, henkilöstöön tai konsernin tukeen häiriintyy. Tästä syystä merkityksellisiksi todisteiksi tulisi tunnustaa teknisten jatkuvuusjärjestelyjen ja operatiivisten varautumissuunnitelmien ohella palveluntarjoajien nykyiset sitoumukset riitauttaa viranomaisten määräykset, pakotteet tai muut toimenpiteet, jotka vaarantaisivat palvelun tuottamisen lainvastaisesti tai suhteettomasti.

Laajemmin tarkasteltuna häiriönsietokykyä tulisi vahvistaa lisäämällä toimitusketjujen monipuolisuutta ja säilyttämällä eurooppalaisten asiakkaiden valinnanvapaus eikä kaventamalla niiden käytettävissä olevien palvelujen valikoimaa. Tehokkaampi häiriönsietokykystrategia kannustaisi siksi asiakkaita monipuolistamaan toimittajiaan ja ylläpitämään vaihtoehtoista kapasiteettia, myös toimivaa varajärjestelyä, jonka avulla kriittiset toiminnot voidaan pitää käynnissä, jos ensisijainen palvelu ei ole enää käytettävissä. Näin jatkuvuusriskiin puututaan suoraan sulkematta pois markkinoiden johtavia palveluja tai korvaamatta yhtä riippuvuutta keskittyneemmällä ja mahdollisesti vähemmän häiriönkestävällä toimitusketjulla.

CADA:ssa tulisi soveltaa samaa riskiperusteista logiikkaa viranomaisten pääsyyn dataan. Mahdollisuus hankkia sähköisiä todisteita rajat ylittävin vaikutuksin on vakiintunut osaksi lainvalvonnan tavanomaista käytäntöä. Useissa oikeusjärjestyksissä on otettu käyttöön mekanismeja, joiden nojalla viranomaiset voivat pyytää dataa lainkäyttövaltansa alaisilta palveluntarjoajilta myös silloin, kun data on tallennettu ulkomaille. Esimerkkejä tästä ovat EU:n sähköisiä todisteita koskeva asetus (e-Evidence-asetus) ja lukuisten EU:n jäsenvaltioiden omat lait. Tämä on tunnustettu myös OECD:n kehyksissä, kuten julistuksessa viranomaisten pääsystä yksityisen sektorin hallussa oleviin henkilötietoihin.

Lisäksi pelkkä päätoimipaikka EU:ssa ei suojaa palveluntarjoajaa kolmannen maan lainkäyttövallalta. EU-palveluntarjoajatkin voivat ulkomaisesta läsnäolostaan tai toiminnastaan riippuen kuulua muiden valtioiden dataan pääsyä koskevien lakien soveltamisalaan[3]. Esimerkiksi OVHcloud, jonka päätoimipaikka on Ranskassa, myöntää verkkosivustollaan[4], että sen yhdysvaltalainen konserniyhtiö noudattaa Yhdysvaltain viranomaisten lainmukaisia pyyntöjä. Hiljattain ontariolainen tuomioistuin määräsi OVHcloudin luovuttamaan Kanadan ulkopuolelle tallennettua dataa todettuaan, että yhtiö kuului Kanadassa harjoittamansa toiminnan vuoksi Kanadan lainkäyttövallan piiriin. Nämä esimerkit havainnollistavat, miksi CADA:ssa tulisi arvioida palveluntarjoajien tosiasiallista altistumista kolmansien maiden lainkäyttövallalle ja niiden kykyä lieventää sitä sen sijaan, että arviointi perustuisi ensisijaisesti omistukseen tai kansallisuuteen.

Lopuksi todettakoon, että kun Euroopan komissio on tehnyt GDPR:n mukaisen tietosuojan riittävyyspäätöksen, se on arvioinut perusteellisesti kolmannen maan oikeudellisen kehyksen, mukaan lukien viranomaisten pääsyä dataan koskevat suojatoimet. CADA:ssa nämä päätelmät tulisi ottaa täysimääräisesti huomioon. Erillinen arviointi, jossa olennaisesti samasta kehyksestä päädyttäisiin eri johtopäätökseen, ei olisi sopusoinnussa GDPR:n 49 artiklan 5 kohdan kanssa, ja se aiheuttaisi oikeudellista epävarmuutta, koska se merkitsisi tarpeetonta päällekkäisyyttä ja toisistaan poikkeavia arvioita.

[3] CLOUD Act -lain osalta asiaa selvitettiin alankomaalaisen Greenberg Traurig -asianajotoimiston vuonna 2022 antamassa oikeudellisessa lausunnossa (linkki)
[4] Cloud Act - Clarifying Lawful Overseas Use of Data - OVHCloud (linkki)

Suositus

Tekniset ja operatiiviset suojatoimet on tunnustettava päteviksi suvereniteetin välineiksi kolmansien maiden pääsyä ja määräysvaltaa vastaan. CADA:ssa kansallisuuteen ja omistukseen keskittyvät arvioinnit tulisi korvata riskiperusteisella arvioinnilla niistä suojatoimista, joita palveluntarjoajat toteuttavat estääkseen luvattoman pääsyn ja varmistaakseen operatiivisen autonomian.

Liitteissä II ja III tulisi erityisesti:

- selventää, että altistuminen kolmannen maan lainsäädännölle ei automaattisesti sulje pois vaatimusten täyttymistä, jos käytössä on tehokkaita riskejä lieventäviä suojatoimia;
- arvioida määräysvaltaa osoitettavissa olevan oikeudellisen, teknisen ja organisatorisen autonomian perusteella eikä yksittäisten yhtiötason indikaattorien irrallisen tarkastelun perusteella;
- tunnustaa hallintorakenteet, tekninen eristäminen, pääsynhallintakeinot, sopimukseen perustuvat suojatoimet, avoimuustoimenpiteet ja oikeudelliset riitauttamiskeinot päteviksi todisteiksi vaatimustenmukaisuudesta;
- yhdenmukaistaa lainmukaista dataan pääsyä koskevat arvioinnit soveltuvin osin niiden voimassa olevien riittävyyspäätösten kanssa, jotka Euroopan komissio on tehnyt GDPR:n nojalla;
- tunnustaa nimenomaisesti asiakkaan hallinnoimat salausmekanismit tärkeiksi suvereniteetin suojatoimiksi, kun arvioidaan dataan pääsyä ja kolmannen maan määräysvaltaa koskevien vaatimusten noudattamista.

Tällainen lähestymistapa kuvastaisi paremmin tosiasiallisesti saavutettavaa turvallisuutta ja suvereniteettia, tarjoaisi objektiivisemman ja näyttöön perustuvan arviointikehyksen ja varmistaisi, että CADA pysyy oikeasuhtaisena, teknologianeutraalina ja operatiivisesti toimivana sen suvereniteettitavoitteista tinkimättä.

10. Liite II – Alihankkijoita, henkilöstöä ja asiakastukea koskevat kriteerit

Keskeinen perustelu: ***Alihankkijoiden, henkilöstön ja asiantuntijatuen kohteluun on sovellettava oikeasuhtaisia sääntöjä. Vaatimukset, joiden mukaan henkilöstön, alihankkijoiden tai asiakastuen on sijaittava yksinomaan EU:ssa, sulkevat pois ne maailmanlaajuiset palvelutuotantomallit, joista kilpailukykyiset, innovatiiviset ja häiriönkestävät pilvipalvelut ovat riippuvaisia.***

Käsitteen ”alihankkija” määritelmä tulisi rajata toimijoihin, jotka osallistuvat aktiivisesti pilvipalvelun tuottamiseen ja joilla on palvelun kannalta merkitykselliset toiminnot operatiivisessa hallinnassaan. Sen ei tulisi ulottua palvelun perustana olevan infrastruktuurin, tietoliikenneyhteyksien, laitteistojen tai muiden toimitusketjun osien tarjoajiin, joilla ei ole pääsyä asiakasdataan ja jotka eivät itse operoi palvelua. Tämä erottelu on erityisen tärkeä korkeammilla varmuustasoilla, joilla laajat alihankkijamääritelmät voisivat käytännössä ulottaa suvereniteettivaatimukset koko teknologian toimitusketjuun.

Samoin sijoittautumis- ja henkilöstövaatimusten tulisi olla riskiperusteisia, ja niitä tulisi soveltaa vain henkilöstöön, jolla on pääsy asiakasdataan tai infrastruktuuriin, jossa asiakasdataa säilytetään. Palveluntarjoajat voivat vastata suvereniteettia koskeviin huolenaiheisiin tehokkaasti

EU:ssa toimivien asiakasrajapinnan, tietoturvan ja operoinnin tiimien avulla asettamatta rajoituksia työntekijöille, joilla ei ole pääsyä asiakasdataan. Liian laajat vaatimukset voisivat tarpeettomasti rajoittaa maailmanlaajuisesti toimivien pilvipalveluntarjoajien mahdollisuuksia tarjota turvallisia ja innovatiivisia palveluja eurooppalaisille julkisen sektorin asiakkaille.

Lopuksi kehyksessä tulisi säilyttää käytännössä toimiva mahdollisuus eskaloida tapauksia erikoistuneille teknisille asiantuntijoille. EU:n ulkopuolisten asiantuntijoiden rajattua, valvottua ja tarkastettavissa olevaa pääsyä poikkeamiin reagointia tai palvelun jatkuvuuden turvaamista varten ei tulisi automaattisesti pitää alihankkija- tai sijoittautumisvaatimusten vastaisena, jos käytössä on asianmukaiset tekniset, operatiiviset ja sopimukseen perustuvat suojatoimet.

Suositus

Käsitettä ”alihankkija” tulisi soveltaa suppeasti kaikilla varmuustasoilla. Sen tulisi kattaa vain sellaiset kolmannet osapuolet, jotka osallistuvat aktiivisesti kyseisen pilvipalvelun tuottamiseen. On tärkeää, että varmuustason 2 alihankkijoita koskevat vaatimukset yhdenmukaistetaan varmuustason 1 vastaavien vaatimusten kanssa, jotta vaatimukset olisivat oikeassa suhteessa palvelun tasoon eivätkä sulkisi pois niitä maailmanlaajuisia palvelutuotantomalleja, joista kilpailukykyiset, innovatiiviset ja häiriönkestävät pilvipalvelut ovat riippuvaisia.

Kehyksessä tulisi erottaa selvästi pilvipalvelujen tuottaminen laajemmasta teknologian toimitusketjusta ja mahdollistaa tarvittaessa erikoistuneen asiantuntemuksen valvottu hyödyntäminen edellyttäen, että käytössä on asianmukaiset tekniset, operatiiviset ja sopimukseen perustuvat suojatoimet. Mahdolliset jäljelle jäävät velvoitteet, jotka koskevat unionin kansalaisuutta tai yksinomaan EU:sta käsin annettavaa asiakastukea, tulisi kirjata selkeästi lainsäädäntöön ja rajata koskemaan vain suppeaa ja tarkasti määriteltyä joukkoa tehtäviä. Tämä vahvistaa turvallisuutta ja häiriönsietokykyä koskevien tavoitteiden toteutumista rajoittamatta tarpeettomasti kehittyneiden pilvipalvelujen tarjoamista eurooppalaisille asiakkaille.

11. Liite II – Asiakasdataa, metatietoja ja telemetriatietoja koskevat kriteerit

Keskeinen perustelu: ***Tekniset telemetria- ja metatiedot on erotettava asiakasdatasta, ja metatietojen ja telemetriatietojen rajat ylittävä käsittely on sallittava silloin, kun niitä käytetään tietoturvaan, häiriönsietokykyyn ja operatiiviseen toimintaan liittyviin oikeutettuihin tarkoituksiin.***

Unionin varmuustason 1 kriteeri 1.1 c (ja samansisältöiset kriteerit kaikilla muilla varmuustasoilla) edellyttää, että tarkastuksen kohteena olevan palveluntarjoajan ja palvelun tarjoamiseen osallistuvien alihankkijoiden käsittelemä, tallentama ja siirtämä asiakasdata, mukaan lukien metatiedot ja telemetriatiedot, pysyy yksinomaan unionin alueella. Vaatimus on monien työkuormien kannalta suhteeton, ja se voisi pikemminkin heikentää kuin vahvistaa kyberturvallisuutta. Pilvipalvelujen tietoturva nojaa nykyään maailmanlaajuisesti hajautettuun toimintaan ja kykyyn korreloida eri ympäristöjen uhkasignaaleja keskenään. Tekniset artefaktit, kuten uhkaindikaattorit, haittaohjelmatunnisteet, tietoturvalokit ja aggregoidut telemetriatiedot, ovat usein välttämättömiä uhkien havaitsemisessa ja niihin reagoimisessa, mutta ne eivät aiheuta samoja suvereniteettiriskejä kuin asiakasdata. Rajat ylittävä pääsy voi myös olla tarpeen, jotta haittaohjelmiin, forensiikkaan tai poikkeamiin reagointiin erikoistuneet tiimit voivat vastata nopeasti EU-asiakkaisiin kohdistuviin uhkiin.

On tärkeää huomata, että CADA:n liitteessä II asetettuja datan lokalisointivaatimuksia on vaikea sovittaa yhteen GDPR:n kansainvälisiä tiedonsiirtoja koskevan sääntelykehyksen kanssa.

GDPR:n V luvun nojalla henkilötietoja voidaan siirtää kolmansiin maihin, kun GDPR:n 45, 46 tai 49 artiklan sovellettavat edellytykset täyttyvät.

CADA:ssa asetetaan kuitenkin eriasteisia datan lokalisointivaatimuksia julkisen sektorin elimille sekä näitä elimiä palveleville pilvipalveluntarjoajille. Kuten Euroopan tietosuojavaltuutetun (EDPS) lausunnossa 14/2026 on tuotu esiin, nämä vaatimukset voivat siksi käytännössä rajoittaa tiedonsiirtoja, jotka olisivat muutoin sallittuja GDPR:n V luvun nojalla.

CADA:ssa ei ole täsmennetty riittävästi näiden kahden sääntelykehyksen välistä suhdetta. Erityisesti on edelleen epäselvää, miten liitteen II lokalisointivaatimuksia tulisi soveltaa silloin, kun siirto on GDPR:n nojalla lainmukainen. Kuten Euroopan tietosuojavaltuutettu on painottanut, tämä aiheuttaa oikeudellista epävarmuutta, johon lainsäätäjien tulisi puuttua. Suosittelemme varmistamaan, että CADA:n tulkinta ja soveltaminen ovat yhdenmukaisia GDPR:n kansainvälisiä tiedonsiirtoja koskevan sääntelykehyksen kanssa.

Tässä yhteydessä olisi otettava erityisesti huomioon myös GDPR:n 49 artiklan 5 kohta. Säännöksen nojalla unionin oikeudessa tai jäsenvaltion lainsäädännössä voidaan yleistä etua koskevien tärkeiden syiden vuoksi asettaa rajoituksia tiettyjen henkilötietoryhmien siirroille kolmanteen maahan, mutta ainoastaan silloin, kun tietosuojan riittävyyspäätöstä ei ole tehty:

- Yleistä etua koskevan edellytyksen osalta kyseenalaistamme, onko laaja velvoite sijoittaa kaikki asiakasdata, metatiedot ja telemetriatiedot EU:hun välttämätön ja oikeasuhtainen, yleistä etua koskevilla tärkeillä syillä perusteltu rajoitus, kun siihen ei sisälly asianmukaisia poikkeuksia, jotka koskisivat oikeutettuja ja tärkeitä käsittelytarkoituksia, kuten kyberturvallisuutta ja maailmanlaajuista asiakastukea. Samankaltaisia oikeasuhtaisuuteen liittyviä huolenaiheita herättävät vaatimukset, jotka koskevat kaikkien alihankkijoiden käsittelemää dataa.
- Toiseksi GDPR:n 49 artiklan 5 kohdan nimenomainen viittaus riittävyyspäätöksen puuttumiseen herättää perustavanlaatuisen kysymyksen siitä, mikä oikeuttaisi asettamaan datan lokalisointia koskevia lisärajoituksia tilanteissa, joissa komissio on virallisesti todennut, että kolmas maa varmistaa riittävän tietosuojan tason.

Suositus

- CADA:n tulisi sallia ainakin metatietojen ja telemetriatietojen rajat ylittävä käsittely silloin, kun niitä käytetään tietoturvaan, häiriönsietokykyyn ja operatiiviseen toimintaan liittyviin oikeutettuihin tarkoituksiin, edellyttäen että käytössä on asianmukaiset suojatoimet, kuten tietojen minimointi, salaus, pääsynvalvonta ja tarkastettavuus. Tämän tulisi koskea sekä tarkastuksen kohteena olevaa palveluntarjoajaa että palvelun tarjoamiseen osallistuvia alihankkijoita.
- Datan lokalisointivaatimusten tulisi olla yhdenmukaisia GDPR:n kanssa ja keskittyä asiakasdataan, ja niitä tulisi kaikissa tilanteissa soveltaa oikeasuhtaisesti eri palvelumalleissa ottaen huomioon, että monien PaaS- ja SaaS-palvelujen osalta salaus, sopimukselliset sitoumukset ja tekniset hallintakeinot vastaavat jo tehokkaasti suvereniteettiriskeihin.
- CADA:ssa tulisi selventää yksityiskohtaisemmin, miten se oikeudellisesti suhteutuu GDPR:ään, ja varmistaa, että GDPR:n mukaista tietovirtojen sääntelykehystä kunnioitetaan. Suosittelemme siksi, että liitteen II datan lokalisointivaatimuksista säädetään selkeä poikkeus, joka koskee siirtoja sellaisiin kolmansiin maihin, joista on tehty GDPR:n 45 artiklan mukainen tietosuojan riittävyyspäätös. Tämä lisäisi oikeusvarmuutta ja varmistaisi CADA:n ja GDPR:n keskinäisen johdonmukaisuuden.

12. Liite II – Ohjelmistohaavoittuvuuksista raportointi

Keskeinen perustelu: ***CADA:n ei tulisi rajoittaa osallistumista oikeutettuihin ja koordinoituihin haavoittuvuuksien julkistamisjärjestelyihin. Vaatimuksissa, jotka liittyvät haavoittuvuuksista raportointia edellyttäviin kolmansien maiden lakeihin, tulisi erottaa toisistaan haitalliset ilmoituskäytännöt ja vastuulliset mekanismit, joissa haavoittuvuuksista ilmoitetaan ennen korjauspäivityksen julkaisua ja jotka edistävät maailmanlaajuista kyberturvallisuutta.***

Esimerkiksi unionin varmuustason 1 kriteeri 1.1 g koskee kolmansien maiden voimassa olevia lakeja ja käytäntöjä, jotka edellyttävät ohjelmistohaavoittuvuuksista raportointia. Kriteerin mukaan kolmannen maan määräysvallassa olevien palveluntarjoajien on taattava, ettei mikään kyseisen kolmannen maan laki tai käytäntö velvoita niitä raportoimaan ohjelmistohaavoittuvuuksista viranomaisille, ennen kuin tiedetään, että kyseisiä haavoittuvuuksia on hyödynnetty. Koska kriteerissä ei oteta huomioon oikeutettuja, ennen korjauspäivityksen julkaisua tapahtuvia ilmoituksia valtion viranomaisille eikä koordinoituja haavoittuvuuksien julkistamisjärjestelyjä, yritykset tarvitsevat lisää ohjeistusta siitä, miten ne voivat osallistua näihin aloitteisiin joutumatta varmuustason 1 ulkopuolelle.

Koordinoidun haavoittuvuuksien julkistamisen (CVD) toimintamallien avulla ohjelmistotoimittajat, tietoturvatutkijat ja viranomaiset voivat puuttua haavoittuvuuksiin, ennen kuin niitä voidaan hyödyntää. Joillakin lainkäyttöalueilla rajattu, ennen korjauspäivityksen julkaisua tapahtuva ilmoittaminen nimetyille valtion viranomaisille on osa vakiintuneita kyberturvallisuusprosesseja ja tukee laajempia toimia uhkien torjumiseksi. Tällaisiin järjestelyihin osallistumista koskeva yleinen rajoitus voisi vähentää halukkuutta noudattaa vastuullisia julkistamiskäytäntöjä, aiheuttaa palveluntarjoajille oikeudellista epävarmuutta ja viime kädessä heikentää tietoturvan tasoa.

Suositus

Varmuustason 1 kriteeri 1.1 g – samoin kuin vastaavat kriteerit varmuustasoilla 2, 3 ja 4 – koskee kolmansien maiden voimassa olevia lakeja ja käytäntöjä, jotka edellyttävät ohjelmistohaavoittuvuuksista raportointia. Näiden kriteerien osalta CADA:ssa tulisi selventää, että osallistuminen oikeutettuihin ja koordinoituihin haavoittuvuuksien julkistamisjärjestelyihin, joissa haavoittuvuuksista ilmoitetaan ennen korjauspäivityksen julkaisua, ei sellaisenaan estä palveluntarjoajaa täyttämästä suvereniteettivaatimuksia. Kehyksen tulisi omaksua riskiperusteinen lähestymistapa, jossa vastuullinen haavoittuvuuksien hallinta erotetaan sellaisista ilmoituksista, jotka aiheuttavat olennaisia riskejä asiakasdatalle, palvelun eheydelle tai operatiiviselle tietoturvalle.

13. Liite II – Kyberturvallisuutta ja ohjelmistojen toimitusketjua koskevien toimenpiteiden kriteerit

Keskeinen perustelu: ***CADA:n kyberturvallisuutta ja ohjelmistojen toimitusketjua koskevat kriteerit tulisi toteuttaa EU:n jo olemassa olevan kyberturvallisuuskehyksen – kyberresilienssisäädöksen (CRA), NIS2-direktiivin ja kyberturvallisuuden sertifiointijärjestelmien – kautta ja yhdenmukaistaa sen kanssa, sen sijaan että luotaisiin rinnakkainen ja ristiriitainen velvoitekokonaisuus.***

Asiaankuuluvat eurooppalaiset kyberturvallisuussertifioinnit (EUCC ja tulevaisuudessa EUCS) eivät ole vielä pilvipalveluntarjoajien saatavilla, ja samalla ohjelmistojen toimitusketjua, haavoittuvuuksista raportointia ja avointa lähdekoodia koskevat kriteerit vastaavat läheisesti vaatimuksia, joista on jo säädetty CRA:ssa ja siihen liittyvissä säädöksissä. Jos sääntelyn noudattamista koskevia vaatimuksia otetaan käyttöön ennen näiden sertifiointijärjestelmien täyttä toimintavalmiutta tai CRA:sta poikkeavasti muotoiltuina, seurauksena on päällekkäisyyttä, oikeudellista epävarmuutta ja kansallisten vaatimusten pirstaloitumista – esimerkiksi jäsenvaltioiden toisistaan poikkeavia odotuksia, kuten Saksan liittovaltion tietoturvaviraston BSI:n odotuksia ohjelmiston materiaaliluettelon (SBOM) sisällöstä.

Suositus

Kehyksen tulisi nopeuttaa sitä, että eurooppalaiset kyberturvallisuussertifioinnit tulevat saataville, ja edellyttää, että ne yhdenmukaistetaan NIS2-direktiivin, CRA:n ja CADA:n kesken; jos sertifiointeja ei vielä ole saatavilla, kehyksen tulisi nimetä sovellettavat, pilvipalvelujen kannalta merkitykselliset sertifiointijärjestelmät ja hyväksyä sisällöltään samankaltaiset vaihtoehdot – kuten CRA:n mukainen vaatimustenmukaisuuden arviointi – samanarvoisiksi; ohjelmiston materiaaliluetteloa (SBOM), kolmansien osapuolten komponentteja, haavoittuvuuksista raportointia ja avointa lähdekoodia koskevat kriteerit tulisi yhdenmukaistaa vastaavien CRA:n mukaisten vaatimustenmukaisuuden osoittamistapojen kanssa, mukaan lukien tapa, jolla niissä käsitellään ohjelmistoihin sisällytettyjä kolmansien osapuolten ja avoimen lähdekoodin komponentteja; lisäksi ilmauksen ”kolmanteen maahan sijoittautuneen oikeushenkilön omistamat tai lisensoimat ohjelmistokomponentit” soveltamisalaa tulisi kaventaa niin, että se kattaa vain sen, mikä on tarpeen tavoitellun tietoturvavaikutuksen saavuttamiseksi.

14. Liite II – Tekoälyjärjestelmien koulutusta ja hienosäätöä koskevien rajoitusten kriteerit

Keskeinen perustelu: ***Tekoälyyn liittyvien suvereniteettivaatimusten tulisi olla kohdennettuja ja oikeasuhtaisia, ja niiden tulisi keskittyä asiakkaan sisällön suojaamiseen. Niiden ei tulisi tahattomasti rajoittaa sellaisten tekoälyominaisuuksien käyttöä, jotka ovat välttämättömiä pilvipalvelujen suojaamisen, tukemisen ja ylläpitämisen kannalta.***

Varmuustason 2 kriteeri 2.1 f ja varmuustason 3 kriteeri 3.1 f jättävät tällä hetkellä määrittelemättä keskeisiä käsitteitä, muun muassa ”tarkastuksen kohteena olevan palvelun käytöstä syntyvä data” ja ”tekoälyjärjestelmä”. Ilman selkeämpää rajausta näitä säännöksiä voitaisiin tulkita niin laajasti, että ne kattaisivat rutiininomaiset palvelutoiminnot, kuten etädiagnostiikan, kyberturvallisuuden valvonnan, poikkeamiin reagoinnin ja tukipalvelujen automatisoinnin, jotka nojaavat tekoälytyökaluihin.

Kehyksen tulisi rakentua pilvipalveluntarjoajien jo antamien vakiintuneiden sitoumusten varaan. Esimerkiksi Microsoftin tuoteehdoissa (Product Terms) sitoudutaan siihen, ettei asiakasdataa käytetä generatiivisen tekoälyn palvelujen perusmallien kouluttamiseen muutoin kuin asiakkaan dokumentoitujen ohjeiden mukaisesti. Suvereniteettikehyksen tulisi vahvistaa näitä suojatoimia ja samalla välttää rajoittamasta tahattomasti tekoälyä hyödyntäviä ominaisuuksia, jotka parantavat palvelujen tietoturvaa, luotettavuutta ja häiriönsietokykyä.

Suositus

Tekoälyyn liittyvät suvereniteettivaatimukset on pidettävä oikeasuhtaisina ja selkeästi rajattuina. Kehyksen tulisi turvata tekoälyn käyttö tietoturvaan, operatiiviseen häiriönsietokykyyn, tukeen ja palvelunhallintaan liittyvissä toiminnoissa ottaen huomioon, että nämä toiminnot pikemminkin vahvistavat kuin heikentävät suvereniteettitavoitteiden toteutumista.

II. Kestävien datakeskusten lupamenettelyjen sujuvoittaminen

Pidämme tervetulleina CADA:n datakeskuskapasiteettipilarin ehdotettuja toimenpiteitä, jotka ovat tärkeä askel kohti Euroopan tekoälytavoitteiden edellyttämän infrastruktuurin mahdollistamista. Katsomme, että pilaria voitaisiin vahvistaa edelleen, jotta se lisäisi oikeudellista selkeyttä koko unionissa ja tukisi kestäviä datakeskusinvestointeja koskevia vankkoja strategioita. Microsoft tukee vahvasti EU:n tavoitetta ottaa käyttöön lisää datakeskuskapasiteettia, ja olemme sitoutuneet investoimaan Euroopan tekoälykehityksen edellyttämän infrastruktuurin kasvattamiseen.

Seuraavat suositukset koskevat CADA:n datakeskuskapasiteettipilaria. Kussakin suosituksessa esitetään keskeinen perustelu, lyhyt selitys sekä harkittavaksi suositeltu etenemistapa.

1. **11 artikla – Nopean kehittämisen alueiden kytkeminen EU:n datakeskusten luokitusjärjestelmään:** Pääsy nopean kehittämisen alueille on sidottava EU:n datakeskusten luokitusjärjestelmän kestävyysindikaattoreihin

Keskeinen perustelu: ***Pääsy datakeskusten nopean kehittämisen alueille tulisi sitoa EU:n datakeskusten luokitusjärjestelmän kestävyysindikaattoreihin eikä EU:n raportointiasetukseen. Luokitusjärjestelmä on tarkoituksenmukaisempi ja paremmin yhdenmukaistettu väline, jolla voidaan tunnistaa alan parasta tasoa edustava kestävyyssuorituskyky ja kannustaa siihen, ja juuri tätä tasoa nopean kehittämisen alueiden tulisi viime kädessä edistää.***

Pidämme tervetulleena sitä painoarvoa, jonka CADA antaa datakeskusten suorituskyvyn ja toiminnan kestävyydelle, muun muassa sen laajemman kehyksen kautta, jota komission energian pääosasto (DG ENER) parhaillaan kehittää alan kasvun ohjaamiseksi. Samalla EU-tason yhdenmukaistamisessa voitaisiin päästä pidemmälle, jos pääsy nopean kehittämisen alueille sidottaisiin EU:n datakeskusten luokitusjärjestelmään eikä raportointiasetukseen. Luokitusjärjestelmä on tarkoituksenmukaisempi väline alan parasta tasoa edustavan toiminnan tunnistamiseen ja palkitsemiseen, ja juuri tähän tasoon nopean kehittämisen alueilla tulisi viime kädessä kannustaa. Tämä auttaisi varmistamaan, että nopeutetun lupamenettelyn piiriin pääsevät ne hankkeet, joiden toiminta täyttää korkeimmat kestävyysvaatimukset, ja vähentäisi samalla jäsenvaltioiden välisen pirstoutumisen riskiä. Ilman tällaista lähestymistapaa jäsenvaltiot saattavat tukeutua toisistaan poikkeaviin, raportointiasetuksesta poimittuihin KPI:hin, myös sellaisiin indikaattoreihin, jotka eivät ole kestävyyssuorituskyvyn kannalta keskeisiä. Pääsyn edellytysten sitominen yhteiseen EU:n luokitusjärjestelmään sen sijaan tukisi yhdenmukaisempaa kehystä, vahvistaisi tasapuolisia toimintaedellytyksiä koko sisämarkkinoilla ja antaisi jäsenvaltioille mahdollisuuden määrittää ilmasto-oloihinsa ja paikallisiin olosuhteisiinsa soveltuvat KPI:t ja nojata samalla unionin tasolla tunnustettuihin yhteisiin kestävyysindikaattoreihin.

Suositus

Jotta lupamenettelykehyksen vaikuttavuutta voitaisiin vahvistaa ja kestäville investoinneille luoda todellinen kannustin, nopean kehittämisen alueille pääsyn edellytykset tulisi sitoa EU:n datakeskusten luokitusjärjestelmään sisältyviin datakeskusten kestävyysindikaattoreihin. Tämä kannustaisi alan parasta tasoa edustavaan kestävyyssuorituskykyyn, tukisi sääntelyn yhdenmukaistamista koko unionissa ja auttaisi parantamaan datakeskusten toiminnan yleistä laatua ja kestävyyttä Euroopassa.

2. **11 artikla – Nopean kehittämisen alueiden kytkeminen sähköverkkoon pääsyyn:** Nopean kehittämisen alueet on kytkettävä sähköverkkoon pääsyyn valmiusjärjestysperiaatteen (first-ready, first-served) mukaisesti

Keskeinen perustelu: ***Nopean kehittämisen alueet tulisi kytkeä oikea-aikaiseen ja ennakoitavaan pääsyyn sähköverkkoon valmiusjärjestysperiaatteen (first-ready, first-served, FRFS) mukaisesti. Pelkällä nopeutetulla lupamenettelyllä ei saada aikaan Euroopan tarvitsemaa datakeskus- ja pilvi-infrastruktuuria, elleivät nopean kehittämisen alueilla sijaitsevat hankkeet pysty myös turvaamaan itselleen selkeää ja luotettavaa väylää verkkoliityntään*.**

Datakeskusten kehittämistä ja pilvi-infrastruktuurin käyttöönottoa koskevassa kokonaisvaltaisessa lähestymistavassa on otettava huomioon, että infrastruktuurikapasiteetti ei riipu ainoastaan nopeammista lupamenettelyistä vaan myös energian ja verkkoliityntöjen oikea-aikaisesta ja ennakoitavasta saatavuudesta. Pidämme tervetulleena CADA:n tavoitetta nopeuttaa nimetyillä nopean kehittämisen alueilla sijaitsevien datakeskushankkeiden lupamenettelyjä. **Tämän kehyksen vaikuttavuus riippuu kuitenkin viime kädessä siitä, pystyvätkö nämä alueet tarjoamaan myös selkeän ja luotettavan väylän verkkoliityntään**.

Jos tällaista kytköstä ei ole, nopean kehittämisen alueet saattavat yksinkertaistaa hallinnollisia menettelyjä ilman, että ne mahdollistavat Euroopan tekoäly- ja digitaalitavoitteiden tukemiseen tarvittavien datakeskusten ja pilvi-infrastruktuurin tosiasiallisen rakentamisen. Tästä syystä nopean kehittämisen alueilla tehtävät sähköverkon liittymispyynnöt tulisi arvioida ja verkkokapasiteetti kohdentaa **valmiusjärjestysperiaatteen (first-ready, first-served, FRFS)** perusteella eikä pelkän **saapumisjärjestysperiaatteen (first come, first served, FCFS)** mukaisesti. Tämä auttaisi varmistamaan, että sähköverkkoon pääsyssä etusijalle asetetaan hankkeet, jotka osoittavat todellista valmiutta, kypsyyttä ja toteutuskykyä, mikä tukisi vaikuttavampaa ja paremmin koordinoitua lähestymistapaa datakeskuskapasiteettiin, pilvi-infrastruktuurin käyttöönottoon ja energiainfrastruktuuriin. Tässä yhteydessä katsomme, että oikeudellisesti sitomaton ohjeistus ei riitä, vaan EU-lainsäädäntöön tulisi sisällyttää kriteeristö ja menettelyvaiheet, jotka tukisivat valmiusjärjestysperiaatteen (FRFS) johdonmukaisempaa ja yhdenmukaisempaa tulkintaa eri jäsenvaltioissa.

Suositus

- CADA:ssa tulisi luoda selkeä kytkös nopean kehittämisen alueiden ja verkkoliityntämenettelyjen välille sisällyttämällä EU-lainsäädäntöön kriteeristön ja menettelyvaiheet, jotka tukevat valmiusjärjestysperiaatteen (FRFS) johdonmukaisempaa ja yhdenmukaisempaa tulkintaa eri jäsenvaltioissa. Sääntelyssä tulisi käsitellä seuraavia seikkoja: **Selvyys siitä, millaista näyttöä hankkeen kypsyyden osoittaminen edellyttää**, johon päästäisiin määrittelemällä tarkemmin, minkä tyyppistä näyttöä voidaan toimittaa, jotta sekä hakijoiden että verkonhaltijoiden hallinnollinen taakka kevenisi.
- **Vaiheistettu (porttimallinen) lähestymistapa avoimuuden, ennakoitavuuden ja investointivarmuuden turvaamiseksi**, jossa liittymisjonossa etenemiselle luotaisiin jäsennelty, monivaiheinen malli ja parannettaisiin näin prosessin näkyvyyttä ja luotettavuutta hankekehittäjien kannalta.
- Ehdottamamme yhdenmukainen ohjeistus on esitetty tämän kannanoton liitteessä I.

Tällainen lähestymistapa vahvistaisi nopean kehittämisen alueiden vaikuttavuutta, parantaisi lupamenettelyjen ja energiainfrastruktuurin suunnittelun yhteensovittamista ja auttaisi nopeuttamaan Euroopan pilvi- ja tekoälytavoitteiden tukemiseen tarvittavan digitaalisen infrastruktuurin käyttöönottoa.

3. 13 artikla – Hallinto- ja lupamenettelyjen helpottaminen: Lupamenettelyn digitalisointi

Keskeinen perustelu: ***Datakeskushankkeiden lupamenettelykehyksessä tulisi hyödyntää täysimääräisesti tekoälyn tarjoamia mahdollisuuksia nopeamman, tehokkaamman ja paremmin tietoon perustuvan hallinnollisen päätöksenteon tukemiseksi. Vaikka CADA:ssa ja ympäristöomnibusissa (Omnibus VIII) otetaan tärkeitä askelia lupamenettelyjen sujuvoittamiseksi, niissä ei tunnusteta riittävästi sitä roolia, joka tekoälyjärjestelmillä voi olla näiden menettelyjen helpottamisessa.***

CADA:n 13 artiklassa määritellään nopean kehittämisen alueille sijoittuvien datakeskushankkeiden lupamenettely, ja ympäristöomnibusiin sisältyvä ympäristöarviointien nopeuttamista koskeva asetus puolestaan yksinkertaistaa tämän menettelyn ennakkoseulontaa ja ympäristöarviointia koskevaa osaa. Pidämme näitä pyrkimyksiä tervetulleina, muun muassa tavoitetta luoda peruslupa (aggregated baseline permit), joka oikeuttaa datakeskusten käyttöönottoon ja kattaa kaikki hankkeen edellyttämät luvat ja hallinnolliset hyväksynnät. Tuemme myös 12 kuukauden määräajan asettamista luvan saamiselle hakemuksen jättämisestä lukien sekä keskitetyn tietopisteen nimeämistä.

Ympäristöomnibus ja CADA eivät kuitenkaan kumpikaan hyödynnä riittävästi tekoälyjärjestelmien mahdollisuuksia parantaa hallintopäätösten tekemistä. Tekoäly voi tukea julkishallintoa sisäisten pullonkaulojen purkamisessa, tehokkuuden parantamisessa ja hallinnon asiantuntemuksen vahvistamisessa. Kun lupapäätösten tarve kasvaa, tekoälyä hyödyntävät työkalut voivat auttaa viranomaisia käsittelemään hakemuksia tehokkaammin ja säilyttämään samalla valvonnan ja säännösten noudattamisen korkean tason.

Suositus

Jotta lupamenettelykehyksen tehokkuutta ja vaikuttavuutta voitaisiin edelleen vahvistaa, komission tulisi tunnustaa nimenomaisesti asetuksessa (EU) 2024/1689 määriteltyjen tekoälyjärjestelmien käyttö asiaankuuluvissa hallintomenettelyissä. Kannustamme komissiota erityisesti seuraaviin toimiin:

- tekoälyjärjestelmien käytön sisällyttäminen ympäristöomnibusiin sisältyvän ympäristöarviointien nopeuttamista koskevan asetuksen 10 artiklaan;
- tekoälyjärjestelmien käytön sisällyttäminen CADA:n 13 artiklan 5 kohtaan hallinto- ja lupamenettelyjä helpottavana välineenä.

Tämä auttaisi viranomaisia sujuvoittamaan menettelyjä, parantamaan hallinnollisia valmiuksiaan ja nopeuttamaan Euroopan pilvi- ja tekoälytavoitteiden tukemiseen tarvittavan digitaalisen infrastruktuurin käyttöönottoa.

4. 13 artikla – Hallinto- ja lupamenettelyjen helpottaminen: Perusluvan soveltamisalan ja toiminnan selkeyttäminen

Keskeinen perustelu: ***Peruslupa voi muodostua CADA:n lupamenettelykehyksen kulmakiveksi lisäämällä oikeusvarmuutta ja nopeuttamalla hankkeiden käyttöönottoa. Näiden tavoitteiden saavuttamiseksi asetuksessa tulisi määritellä selkeästi luvan oikeusvaikutukset, soveltamisala ja toiminta sekä varmistaa yhdenmukainen lähestymistapa kaikissa jäsenvaltioissa.***

Tuemme tavoitetta ottaa nopean kehittämisen alueilla sijaitseville datakeskushankkeille käyttöön peruslupa ja 12 kuukauden määräaika lupamenettelylle. Jotta kehys kuitenkin aidosti lisäisi

oikeusvarmuutta ja nopeuttaisi menettelyjä, asetuksessa tulisi selkeyttää perusluvan oikeusvaikutuksia, soveltamisalaa ja toimintaa.

Perusluvan tulisi olla yksi hallintopäätös, jota koordinoidaan keskitetyn tietopisteen kautta ja joka sitoo kaikkia lupamenettelyyn osallistuvia toimivaltaisia viranomaisia. Sen soveltamisala tulisi yhdenmukaistaa positiivisella luettelolla peruslupaan sisältyvistä luvista, joihin kuuluisivat muun muassa alueidenkäytön suunnittelua, rakentamista, ympäristöä, vesitaloutta, lämmön talteenottoa ja verkkoliityntää koskevat luvat.

Pirstoutumisen välttämiseksi asetuksessa tulisi myös vahvistaa yhdenmukaiset ja tyhjentävät hakemusvaatimukset sekä määritellä selkeästi, milloin hakemus katsotaan täydelliseksi, jolloin 12 kuukauden määräaika lupamenettelylle alkaa kulua. Lisäksi lupa tulisi myöntää kehysparametrien (ns. envelope-parametrien) perusteella; niihin kuuluisivat muun muassa hankealueen pinta-ala, vedenkäyttö ja jäähdytyksen suunnitteluarvojen vaihteluvälit, ja ne määriteltäisiin delegoidulla säädöksellä. Näin hankkeissa voitaisiin ottaa huomioon teknologian kehitys ja vaiheittainen käyttöönotto ilman, että lupamenettelyjä tarvitsisi avata uudelleen.

Lisää selkeyttä tarvitaan myös siihen, miten muutoksia käsitellään hankkeen toteutuksen aikana. Hyväksyttyjen kehysparametrien rajoissa tehtäviin muutoksiin tulisi riittää pelkkä ilmoitusmenettely, ja luvan voimassaoloon, voimassaolon jatkamiseen, siirrettävyyteen ja muutoksenhakumenettelyihin tulisi soveltaa selkeitä ja ennakoitavia sääntöjä.

Lopuksi asetuksessa tulisi vahvistaa, että hankkeiden, jotka hyötyvät ympäristöomnibusin mukaisista ympäristöarviointia koskevista vapautuksista, ei tarvitse toistaa kyseisiä arviointeja osana peruslupamenettelyä.

Suositus

CADA:ssa tulisi selkeyttää perusluvan oikeusvaikutuksia, soveltamisalaa ja toimintakehystä seuraavin tavoin:

- säätämällä, että peruslupa on **yksi hallintopäätös**, jota koordinoidaan keskitetyn tietopisteen kautta ja joka sitoo kaikkia toimivaltaisia viranomaisia;
- yhdenmukaistamalla perusluvan soveltamisalan **positiivisella luettelolla peruslupaan sisältyvistä luvista**, joihin kuuluisivat muun muassa alueidenkäytön suunnittelua, rakentamista, ympäristöä, vesitaloutta, lämmön talteenottoa ja verkkoliityntää koskevat luvat;
- määrittelemällä **yhdenmukaiset ja tyhjentävät hakemusvaatimukset** ja täsmentämällä, milloin hakemus katsotaan täydelliseksi, jolloin 12 kuukauden määräaika lupamenettelylle alkaa kulua;
- sallimalla, että luvat myönnetään **delegoidulla säädöksellä ennalta määriteltyjen kehysparametrien** perusteella, mikä mahdollistaa teknologisen kehittymisen ja vaiheittaisen käyttöönoton ilman, että lupamenettelyä tarvitsee avata uudelleen;
- selkeyttämällä, että hyväksyttyjen kehysparametrien rajoissa tehtäviin muutoksiin riittää **pelkkä ilmoitusmenettely**, ja luomalla samalla ennakoitavat säännöt luvan voimassaolosta, voimassaolon jatkamisesta, siirrettävyydestä ja muutoksenhausta;
- vahvistamalla, että hankkeiden, jotka hyötyvät ympäristöomnibusin mukaisista ympäristöarviointia koskevista vapautuksista, **ei tarvitse toistaa näitä arviointeja** osana peruslupamenettelyä.

Tällaiset täsmennykset vahvistaisivat oikeusvarmuutta, vähentäisivät hallinnollista monimutkaisuutta ja varmistaisivat, että peruslupa toteuttaa tehokkaasti CADA:n taustalla olevat nopeuttamistavoitteet.

5. **14 artikla – Strategisten datakeskushankkeiden nimeäminen:** Selkeytettävä, että hankkeen nimeäminen strategiseksi oikeuttaa samoihin lupamenettelyetuihin

Keskeinen perustelu: ***Kun datakeskushankkeita nimetään strategisiksi hankkeiksi, niiden tulisi saada pääsy paitsi julkisiin tukitoimenpiteisiin ja EU:n rahoitusvälineisiin myös samoihin lupamenettelyjen yksinkertaistamistoimiin, jotka ovat käytettävissä osana ympäristöarviointien nopeuttamista koskevassa asetuksessa ehdotettua lupamenettelyjen välineistöä. Tämän kytköksen selkeyttäminen on välttämätöntä, jotta strategisia hankkeita koskeva kehys tukisi tehokkaasti digitaalisen infrastruktuurin nopeaa käyttöönottoa siellä, missä laskentakapasiteettia tarvitaan eniten.***

CADA:n 14 artikla valtuuttaa komission nimeämään päätöksellä strategisiksi hankkeiksi avointen kiinnostuksenilmaisupyyntöjen kautta valittuja datakeskushankkeita edellyttäen, että ne täyttävät vähintään kaksi luetelluista kriteereistä. Ymmärryksemme mukaan tällaisen nimeämisen tarkoituksena on helpottaa pääsyä julkisiin tukitoimenpiteisiin ja EU:n rahoitusmahdollisuuksiin.

Artiklassa ei kuitenkaan todeta selkeästi, että näiden hankkeiden tulisi hyötyä myös siitä sujuvoitetusta lupamenettelystä, josta säädetään ympäristöomnibusiin sisältyvässä ympäristöarviointien nopeuttamista koskevassa asetuksessa. Tämä epäselvyys uhkaa heikentää yhtä strategisten hankkeiden nimeämisen keskeisistä tavoitteista eli merkittävien laskentakapasiteettivajeiden korjaamista alueilla, joilla tällaisia vajeita on todettu.

Strategisten hankkeiden pääsy lupamenettelyjen yksinkertaistamistoimien piiriin varmistaisi, että nimeäminen tuottaa konkreettisia käyttöönottoon liittyviä etuja eikä pelkästään taloudellisia etuja tai rahoitusetuja. Se parantaisi myös johdonmukaisuutta EU:n laajemmassa teollisuuspoliittisessa kehyksessä.

Suositus

Komission tulisi selkeyttää, että datakeskushankkeen nimeäminen strategiseksi hankkeeksi antaa hankkeelle mahdollisuuden hyötyä niistä lupamenettelyjen yksinkertaistamistoimista, jotka ovat käytettävissä ympäristöomnibusiin sisältyvän ympäristöarviointien nopeuttamista koskevan asetuksen nojalla.

Tämä täsmennys olisi tärkeä kahdesta syystä:

- **jotta vältettäisiin useita ja mahdollisesti toisistaan poikkeavia tulkintoja strategisen hankkeen aseman seurauksista**, mikä parantaisi oikeusvarmuutta ja ennakoitavuutta hankekehittäjien kannalta;
- **jotta varmistettaisiin johdonmukaisuus muiden EU:n lainsäädäntökehysten kanssa**, joihin kuuluu esimerkiksi teollisuuden vauhdittamissäädös (Industrial Accelerator Act), jonka nojalla strategiset hankkeet voivat hyötyä lupamenettelyjen yksinkertaistamistoimista riippumatta siitä, sijaitsevatko ne nopean kehittämisen alueilla.

Strategisten datakeskushankkeiden pääsy samoihin lupamenettelyetuihin vahvistaisi 14 artiklan vaikuttavuutta ja auttaisi nopeuttamaan Euroopan digitaali- ja tekoälytavoitteiden tukemiseen tarvittavan laskentainfrastruktuurin käyttöönottoa.

6. **14 artikla – Strategisten datakeskushankkeiden nimeäminen:** Ympäristöomnibusin kunnianhimon säilyttäminen

Keskeinen perustelu: ***Ympäristöomnibusiin sisältyvän ympäristöarviointien nopeuttamista koskevan asetuksen kunnianhimo olisi säilytettävä ja sitä olisi mahdollisuuksien mukaan vahvistettava. Asetus on ratkaisevan tärkeä tekijä, joka mahdollistaa CADA:lla ja muulla alakohtaisella lainsäädännöllä luotavan laajemman lupamenettelykehyksen, ja se on välttämätön, jotta voidaan nopeuttaa sen datakeskusinfrastruktuurin käyttöönottoa, jota tarvitaan Euroopan tekoäly- ja digitaalitavoitteiden tukemiseen.***

Ympäristöomnibusiin sisältyvä ympäristöarviointien nopeuttamista koskeva asetus on keskeinen väline, joka mahdollistaa koko sen uuden lupamenettelykehyksen, jota komissio on luomassa alakohtaisella lainsäädännöllä. Erityisesti suurissa infrastruktuurihankkeissa ympäristöarvioinnit ovat usein yksi lupamenettelyn monimutkaisimmista ja eniten aikaa vievistä osista, ja niihin sisältyy useita vaiheita, kuten ennakkoseulonta, julkinen kuuleminen ja laajat hallinnolliset menettelyt.

Ympäristöomnibus vastaa näihin haasteisiin asettamalla ympäristöarviointimenettelyille kiinteät määräajat ja tarjoamalla strategisiksi nimetyille hankkeille erityisiä välineitä, joihin kuuluu muun muassa hankkeiden katsominen erittäin tärkeän yleisen edun mukaisiksi. Näiden toimenpiteiden tarkoituksena on vähentää viivästyksiä ja lisätä ennakoitavuutta hankekehittäjien kannalta.

Jos tämän asetuksen kunnianhimoa heikennetään lainsäädäntöprosessin aikana, CADA:n nojalla nimetyt strategiset datakeskushankkeet eivät välttämättä enää voi hyötyä täysimääräisesti ympäristöomnibusissa esitetyistä yksinkertaistamistoimista. Tämä rajoittaisi myös ympäristöarviointien keskitetyn asiointipisteen roolia arviointeihin liittyvässä koordinoinnissa, helpottamisessa, seurannassa ja tiedon jakamisessa. Tämän seurauksena lupamenettelyt voisivat pidentyä ja monimutkaistua, mikä hidastaisi tekoälymanner-toimintasuunnitelman tavoitteiden saavuttamiseen tarvittavan laskentainfrastruktuurin käyttöönottoa.

Suositus

Lainsäätäjien tulisi varmistaa, että ympäristöarviointien nopeuttamista koskevan asetuksen kunnianhimo säilytetään ja sitä mahdollisuuksien mukaan vahvistetaan koko lainsäädäntöprosessin ajan.

Kehyksen tulisi erityisesti:

- säilyttää ne sujuvoitetut menettelyt ja määräajat, jotka on vahvistettu ympäristöarvioinneille;
- säilyttää strategisten hankkeiden käytettävissä olevat välineet, mukaan lukien erittäin tärkeän yleisen edun mukaisiin hankkeisiin liittyvät toimenpiteet;
- varmistaa, että CADA:n nojalla nimetyt strategiset datakeskushankkeet voivat hyötyä täysimääräisesti ympäristöomnibusissa esitetystä yksinkertaistamisen keinovalikoimasta;
- vahvistaa kehystä edelleen sisällyttämällä digitaalisia ratkaisuja entistä laajemmin lupamenettelyihin, mikä mahdollistaa tehokkaammat, avoimemmat ja ennakoitavammat hallintomenettelyt.

Ympäristöomnibusin kehyksen säilyttäminen vahvana ja tehokkaana on välttämätöntä, jotta saadaan aikaan nopeampi ja johdonmukaisempi lupajärjestelmä ja tuetaan Euroopan tavoitetta kasvattaa laskentakapasiteettia ja digitaalista infrastruktuuria laajamittaisesti.

Johtopäätökset

Eurooppa on digitaalitaloutensa kehityksessä ratkaisevassa vaiheessa. Pilvipalveluiden ja tekoälyn kehittämisen säädös tarjoaa tilaisuuden rakentaa digitaaliselle suvereniteetille tulevaisuuteen suuntautuvan mallin, jossa strateginen autonomia ja avoimuus ovat tasapainossa, ja samalla luoda tarvittavat edellytykset Euroopan pilvi-, tekoäly- ja datakeskusinfrastruktuurin laajentamiselle.

Tämän saavuttamiseksi EU:n päättäjien tulisi omaksua joustava ja riskeihin suhteutettu lähestymistapa, joka perustuu teknisiin suojatoimiin, operatiiviseen määräysvaltaan ja avoimeen hallintotapaan. Toiminnallinen suvereniteettimalli, jossa todennettava riskien vähentäminen asetetaan rajoittavien kriteerien edelle, voi varmistaa, että eurooppalaiset julkisen sektorin elimet ja instituutiot säilyttävät tosiasiallisen määräysvallan digitaaliseen omaisuuteensa ja voivat samalla edelleen hyötyä maailmanlaajuisista innovaatioista.

Samalla Euroopan suvereniteettitavoitteiden rinnalla on oltava kehys, joka mahdollistaa infrastruktuurin laajamittaisen käyttöönoton. CADA:n onnistuminen riippuu viime kädessä paitsi siitä, miten suvereniteettivaatimukset määritellään, myös siitä, luoko asetus ennakoitavan ja investoinneille suotuisan toimintaympäristön pilvi- ja tekoälyinfrastruktuurin kehittämiselle. Tämä edellyttää koko unionissa koordinoitua, digitalisoitua ja yhdenmukaistettua lupamenettelykehystä, jossa on selkeät etenemispolut hankkeen nimeämisestä sen toteuttamiseen.

Sääntelykehyksen, ohjeiden ja hankintavälineiden tulisi siksi tukea asiakkaiden laajempia valinnanmahdollisuuksia, edistää avoimia ja kilpailtuja markkinoita ja olla yhdenmukaisia kansainvälisten standardien kanssa. Julkisia hankintoja koskevien linjausten tulisi varmistaa pääsy kehittyneimpiin, turvallisiin ja kestäviin teknologioihin, jotka edistävät EU:n digitaalisen vuosikymmenen tavoitteiden saavuttamista. Sen sijaan, että EU ottaisi käyttöön rajoittavia toimenpiteitä, jotka kaventavat pääsyä uusimpiin teknologioihin, sen tulisi keskittyä toimitusketjujen monipuolistamiseen, infrastruktuurikapasiteetin laajentamiseen, kriittisten teknologioiden saatavuuden varmistamiseen ja yhteistyön edistämiseen luotettavien teknologiatoimittajien kanssa. Näin viranomaiset ja asiakkaat voivat valita ratkaisut objektiivisten ja riskiperusteisten kriteerien pohjalta, joita ovat muun muassa hallintotapa, turvallisuus, avoimuus, häiriönsietokyky, kestävyys ja suorituskyky.

Euroopan taloudellisen häiriönsietokyvyn, teknologisen turvallisuuden ja tekoälyalan kilpailukyvyn vahvistaminen vaatii sekä vankkoja suvereniteettia koskevia suojatoimia että käytännön edellytyksiä infrastruktuuri-investoinneille. Avoimet ja kilpaillut markkinat, joita tukevat tehokkaat lupamenettelyt, luotettava energiansaanti, yhdenmukaistetut kestävyyskehykset ja vahvat julkisen ja yksityisen sektorin kumppanuudet, ovat edelleen tehokkain tapa saavuttaa nämä tavoitteet. Tällainen lähestymistapa auttaisi eurooppalaisia julkisia hankkijoita tekemään tietoon perustuvia päätöksiä, ja samalla vältettäisiin tahattomat seuraukset, kuten toimittajien monipuolisuuden väheneminen, kustannusten nousu, infrastruktuurin käyttöönoton viivästyminen ja innovoinnin hidastuminen.

Microsoft on sitoutunut tukemaan Euroopan digitaalista tulevaisuutta investoimalla jatkossakin pilvi- ja tekoälyinfrastruktuuriin, suvereeneihin pilvivalmiuksiin, kestävyysinnovaatioihin ja kumppanuuksiin koko eurooppalaisessa ekosysteemissä. CADA:n tasapainoinen ja käytännönläheinen täytäntöönpano voi samanaikaisesti vahvistaa Euroopan strategista autonomiaa, nopeuttaa kriittisen digitaalisen infrastruktuurin käyttöönottoa ja lujittaa eurooppalaisen digitaali-

talouden kilpailukykyä. Päättäjien, teollisuuden, energiantoimittajien, infrastruktuurin ylläpitäjien ja muiden sidosryhmien välisen yhteistyön jatkaminen on välttämätöntä, jotta pilvipalveluiden ja tekoälyn kehittämisen säädös saavuttaa kunnianhimoisen tavoitteensa tehdä Euroopasta maailmanlaajuisesti johtava toimija pilvilaskennassa, tekoälyssä ja digitaalisessa infrastruktuurissa.

Liite I

Suositukset verkkoliityntöjä koskevaksi yhdenmukaiseksi ohjeistukseksi

Pääsy sähköverkkoon on EU:n sähkömarkkinoiden kulmakivi erityisesti datakeskusten käyttöönoton kannalta. Kannatamme tasapuolisia toimintaedellytyksiä eri jäsenvaltioissa ja eri toimialoilla, jotta sähköverkkoon pääsyä koskevat sääntelykehykset olisivat selkeitä, vakaita, ennakoitavia ja johdonmukaisia. Tällaiset kehykset ovat välttämättömiä pitkän aikavälin suunnittelulle ja investoinneille, ja ne ovat Euroopan kilpailukyvyn kannalta ratkaisevan tärkeitä.

Kun sähköistyminen lisääntyy ja verkkoliityntöjen kysyntä kasvaa, selkeät menettelyt, joilla ratkaistaan pääsy sähköverkkoihin, käyvät yhä tärkeämmiksi. Nykyisin liittymien toimitusajat ovat usein huomattavasti pidempiä siirtoverkonhaltijan (TSO) verkkoon liittymää hakevilla asiakkailla kuin jakeluverkonhaltijan (DSO) verkkoon liittymää hakevilla – joissakin tapauksissa odotusaika on jopa 12 vuotta. Lisäksi hakemuksen käsittelyn aikana tehtävät menettelymuutokset voivat palauttaa aikataulut alkuun, mikä kasvattaa viivästyksiä entisestään.

Kuten Euroopan parlamentin äskettäisessä sähköverkkoja koskevassa valiokunta-aloitteisessa mietinnössä (INI) ja Euroopan komission verkkoliityntöjä koskevissa suuntaviivoissa on tuotu esiin, liittymispyyntöjen käsittelyssä sovellettava saapumisjärjestysperiaate (first come, first served, FCFS) ei enää ole tarkoituksenmukainen tilanteessa, jossa eri sektoreiden hiilestä irtautuminen ja sähköistyminen kasvattavat liittymien kysyntää. Sähköverkkoon pääsyä koskevissa tulevissa ratkaisuissa tulisi aina varmistaa pitkän aikavälin luotettavuus ja pääsy verkkoon kaikille asiakkaille. Ihannetapauksessa tämä tulisi koordinoida EU-tasolla, jotta vältetään sääntelyn pirstoutuminen EU:n jäsenvaltioiden välillä, ja siihen tulisi sisältyä FCFS-periaatteen kattava uudistaminen siten, että siirrytään valmiusjärjestysperiaatteeseen (first-ready, first-served, FRFS). Uudistukseen tulisi kuulua hakemusten käsittelyssä sovellettava vaiheistettu (porttimallinen) lähestymistapa yhdistettynä hankekohtaisiin välitavoitteisiin, joiden avulla jonossa voidaan edetä ja liittymispäivästä voidaan pitää kiinni. Tämä on keino hillitä aidosti liittymisjonoihin kohdistuvaa spekulointia ja asettaa etusijalle hankkeet, jotka osoittavat valmiutensa saavuttamalla etukäteen sovitut välitavoitteet.

Kannustamme EU-tason ja kansallisia päättäjiä laatimaan verkkoliityntöjä koskevat kehykset siten, että ne nojaavat objektiivisiin, avoimiin ja toimialasta riippumattomiin kriteereihin. Selkeä, kriteeripohjainen lähestymistapa on välttämätön, jotta voidaan luoda investointivarmuutta ja hallita liittymisjonoja tehokkaasti. Vaikka priorisointimekanismeilla voi olla oma roolinsa, harkinnanvaraisten tai laadullisten tekijöiden tuominen jäsennellyn, valmiusjärjestysperiaatteeseen perustuvan kehyksen rinnalle uhkaa heikentää selkeyttä, johdonmukaisuutta ja ennakoitavuutta hankekehittäjien kannalta.

Suositus:

Suosittelemme, että Euroopan komissio sisällyttää EU:n lainsäädäntöön selkeät kriteerit ja menettelyvaiheet, jotka tukevat *valmiusjärjestysperiaatteen (first-ready, first-served, FRFS)* johdonmukaisempaa ja yhdenmukaisempaa tulkintaa eri jäsenvaltioissa. Tällaisessa ohjeistuksessa olisi hyödyllistä käsitellä seuraavia seikkoja:

- **Selvyys siitä, millaista näyttöä hankkeen kypsyyden osoittaminen edellyttää**
  Tarkemmat määrittelyt siitä, millaista näyttöä hankkeen kypsyyden osoittamiseksi voidaan toimittaa, keventäisivät sekä hakijoiden että verkonhaltijoiden hallinnollista taakkaa. Tämä

auttaisi myös minimoimaan lisäselvityspyyntöjen ja täsmennysten tarpeen, mikä sujuvoittaisi arviointimenettelyä.

- **Vaiheittainen (”porttimallinen”) lähestymistapa avoimuuden, ennakoitavuuden ja investointivarmuuden turvaamiseksi**
  Liittymisjonossa etenemistä koskevan jäsennellyn, monivaiheisen lähestymistavan käyttöönotto parantaisi menettelyn näkyvyyttä ja luotettavuutta hankekehittäjien kannalta. Selkeästi määritelty vaiheporttijärjestelmä antaisi hakijoille mahdollisuuden edetä menettelyssä sitä mukaa kuin ne täyttävät sovitut objektiiviset kriteerit, mikä vähentäisi investointiriskiä ja tukisi lupamenettelyjen aikataulujen toteutumista. Jos tällaista ennakoitavuutta ei ole, vaatimus tehdä mittavaa valmistelutyötä ilman varmuutta jonossa etenemisestä voi karkottaa toteuttamiskelpoisia hankkeita.

Harkittavaksi voitaisiin ottaa esimerkiksi kolmivaiheinen malli:

Vaihe 1: Hakemusten alustava seulonta

Tämän ensimmäisen vaiheen tulisi toimia alustavana seulontamekanismina, jonka avulla pyritään tunnistamaan varhain ne hankkeet, joiden on aidosti tarkoitus edetä, erotuksena spekulatiivisista hakemuksista. Tämän tavoitteen tueksi voitaisiin ottaa käyttöön rajattu määrä oikeasuhtaisia ja objektiivisia indikaattoreita, jotka osoittavat hankkeen toteuttamisaikomuksen ja kypsyyden:

- **Alustava näyttö hallintaoikeudesta hankealueeseen**
  Hakijoiden tulisi osoittaa, että niillä on edellytykset tehdä liittymispyyntö hankkeeseen liittyvälle maa-alueelle. Koska täyden näytön esittäminen maanomistuksesta ei välttämättä ole tässä vaiheessa mahdollista, kansallisista käytännöistä riippuen voitaisiin hyväksyä vähemmän vaativia näytön muotoja. Näitä voisivat olla esimerkiksi aiekirje, jossa vahvistetaan, että hakija käy virallisia neuvotteluja maanomistajan kanssa, valtakirja tai muut määritellyn ajan voimassa olevat ehdolliset sopimukset tai yksinoikeussopimukset.

- **Näyttö hakijan legitimiteetistä toimijana**
  Hakijoita voitaisiin vaatia osoittamaan legitimiteettinsä kyseisen alan toimijana. Tähän voi tarvittaessa kuulua loppuasiakkaan tai hankkeen taustalla olevan tahon yksilöiminen, edellyttäen että luottamuksellisuus turvataan riittävin suojatoimin.

- **Alustava taloudellinen sitoumus**
  Hakemusvaiheessa voitaisiin edellyttää oikeasuhtaista taloudellista sitoutumista, esimerkiksi hakemusmaksua, joka voidaan palauttaa sitä mukaa kuin hanke osoittaa etenevänsä edelleen. Tätä voitaisiin täydentää taloudellisilla lisävakuuksilla, kuten emoyhtiön takauksella, hakemuksen uskottavuuden vahvistamiseksi.

- **Hankkeen suuntaa-antavat parametrit (hankealueen rajat ja energiaprofiili)**
  Hakijoiden tulisi pystyä toimittamaan alustavat tiedot hankkeen alueellisesta laajuudesta, mukaan lukien hankealueen rajat, sekä suuntaa-antavat tiedot odotetusta energiantarpeesta tai energiatiheydestä. Näin verkonhaltijat voisivat arvioida jo varhaisessa vaiheessa, onko haettu maa-ala oikeassa suhteessa siihen liittyvään energiantarpeeseen.

Ehdotamme, että tämä arviointi pidetään melko lyhyenä (enintään 2 kuukautta asiakirjojen vastaanottamisesta). Tämän vaiheen päättyessä hakijan tulisi olla saanut alustava arvio siitä, voidaanko kyseiselle maa-alueelle toteuttaa liittymä. Kun hakemus on läpäissyt vaiheen 1 hyväksytysti, se voi edetä vaiheeseen 2.

Vaihe 2: Tarkennettu näyttö hankkeen ja rahoituksen valmiudesta

Tässä vaiheessa hakijoita voitaisiin vaatia osoittamaan hankkeen korkeampi kypsyysaste toimittamalla verkonhaltijalle lisää teknisiä, suunnittelua koskevia ja taloudellisia tietoja. Tämän vaiheen avulla voitaisiin vahvistaa, että hanke on valmis etenemään vaiheistetussa menettelyssä, ja erottaa muista ne hankkeet, joilla on selkeä toteutuspolku.

Keskeisiä näytön osatekijöitä voivat olla muun muassa:

- **Yksityiskohtaiset teknistä suunnittelua ja hankesuunnittelua koskevat asiakirjat**
  Hakijoiden tulisi toimittaa pidemmälle kehitetyt tekniset eritelmät ja hankkeen suunnitteluasiakirjat, jotta hankkeen toteutettavuutta ja järjestelmäintegraation vaatimuksia voidaan arvioida selkeämmin.
- **Hankkeen suuntaa-antavat aikataulut ja toteutuksen välitavoitteet**
  Hakijoiden tulisi esittää pääpiirteittäin hankkeen odotetut aikataulut, mukaan lukien kehittämisen ja toteutuksen keskeiset välitavoitteet, osoittaakseen, että niillä on uskottava ja jäsennelty toteutussuunnitelma.
- **Näyttö varmistetusta rahoituksesta tai sopimussitoumuksista (soveltuvin osin)**
  Hakijoita voitaisiin tarvittaessa vaatia osoittamaan edistymistä rahoituksen varmistamisessa tai keskeisten sopimusjärjestelyjen solmimisessa, mikä vahvistaisi entisestään hankkeen toteuttamiskelpoisuutta.

Kun verkonhaltija on tarkastanut ja vahvistanut nämä seikat, hakemus voisi edetä vaiheeseen 3.

Vaihe 3: Näyttö lupa- ja ympäristömenettelyjen käynnistämisestä

Tässä vaiheessa keskityttäisiin osoittamaan, että hanke on virallisesti siirtynyt lupamenettelyyn, joka on hankekehityksessä usein eniten aikaa vievä ja vaikeimmin ennakoitava vaihe. Monissa jäsenvaltioissa ympäristöarviointien ja lupapäätösten aikataulut voivat vaihdella huomattavasti ilman ennakoitavia määräaikoja, ja hakijoiden on tehtävä mittavaa valmistelutyötä kootakseen ja jättääkseen täydelliset hakemukset.

Jotta tähän vaiheeseen saataisiin enemmän selkeyttä ja kurinalaisuutta, hakijoita voitaisiin vaatia toimittamaan asiaankuuluvat lupa-asiakirjat määritellyssä määräajassa (esim. 18 kuukauden kuluessa vaiheen 3 alkamisesta). Samalla toimivaltaisia viranomaisia olisi kannustettava saattamaan arviointinsa päätökseen ennakoitavassa ja yhdenmukaisessa ajassa, mikä lisäisi koko menettelyn ennakoitavuutta.

Keskeisiä näytön osatekijöitä voivat olla muun muassa:

- **Ympäristövaikutusten arviointien toimittaminen**

Hakijoiden tulisi osoittaa, että vaaditut ympäristöarviointimenettelyt on virallisesti käynnistetty toimittamalla asiaankuuluvat asiakirjat.

- **Lupahakemusten jättäminen**

Hakijoiden tulisi esittää näyttöä siitä, että kaikki rakentamisen aloittamiseksi tarvittavat lupahakemukset on virallisesti jätetty toimivaltaisille viranomaisille.

Kun tämä vaihe on läpäisty hyväksytysti, hakija voisi saada alustavan tai ehdollisen liittymispäivän eli suuntaa-antavan paikan liittymisjonossa; paikka vahvistettaisiin, kun kaikki rakentamiseen tarvittavat luvat on saatu.

- **Sovellettavuus sekä uusiin hakemuksiin että olemassa oleviin liittymisjonoihin:** Ohjeistusta tulisi soveltaa paitsi tuleviin liittymispyyntöihin myös olemassa oleviin jonoihin. Vaikka verkonhaltijoiden voi olla tarpeen jatkaa pyyntöjen priorisointia myös sen jälkeen, kun kypsyyskriteerit on otettu käyttöön ja toteuttamiskelvottomat ”haamuhankkeet” on poistettu, selkeät linjaukset siitä, miten sekä saapuvia hakemuksia että aiemmin muodostuneita jonoja hallitaan, auttaisivat merkittävästi vähentämään yleistä ruuhkautumista ja parantamaan järjestelmän tehokkuutta.
- **Välitavoitejärjestelmän käyttöönotto jonojen hallinnassa spekulatiivisten hankkeiden karsimiseksi.** Liittymisjonojen tehokkuuden ja uskottavuuden parantamiseksi suosittelemme, että liittymissopimuksiin otetaan jäsennelty, välitavoitteisiin perustuva kehys, joka auttaa karsimaan spekulatiiviset hankkeet ja asettamaan etusijalle ne, joilla on selkeä ja osoitettavissa oleva toteutuspolku. Tällaisessa mallissa paikan säilyminen liittymisjonossa edellyttäisi, että hakija osoittaa sitoumuksensa ja saavuttaa sarjan ennalta määriteltyjä välitavoitteita, joista hakija ja verkonhaltija ovat sopineet ja jotka on kirjattu liittymissopimukseen. Edistymistä näiden välitavoitteiden saavuttamisessa arvioitaisiin säännöllisesti, ja jonossa eteneminen edelleen – ja jonossa pysyminen – edellyttäisi, että vaaditut kriteerit täytetään sovituissa määräajoissa. Välitavoitteita voisivat olla esimerkiksi seuraavat, loogisessa ja peräkkäisessä järjestyksessä:
  - **Maankäyttöä ja rakentamista koskevien lupien saaminen**
    Sen osoittaminen, että hanke on saanut tarvittavat maankäyttöä ja rakentamista koskevat luvat.
  - **Hankealueen oikeudellinen hallinta**
    Näytön esittäminen siitä, että maa-alue on turvattu omistuksella, vuokrasopimuksilla tai optiojärjestelyillä.
  - **Hankkeen toteutusvalmiuden osoittaminen**
    Sen vahvistaminen, että hanke etenee aktiivisesti kohti toteutusta, esimerkiksi seuraavin tavoin:
    - liittymistöiden yksityiskohtainen tekninen suunnittelu;
    - rakentamis- ja toteutustavan vahvistaminen;
    - näyttö taloudellisista ja sopimusperusteisista sitoumuksista hankkeen jatkamiseksi;
    - laitoksen rakentamisen tai siihen liittyvien verkkoliityntätöiden aloittaminen.

Tällainen kehys lisäisi avoimuutta, parantaisi jonokuria ja varmistaisi, että rajallinen verkkokapasiteetti kohdennetaan hankkeille, joilla on uskottava ja oikea-aikainen toteutuspolku.