

DIGI- SUVERENITEETTI

käytännössä

Mitä yritysten kannattaa tietää
digisuvereniteetistä juuri nyt

Digisuvereniteetti: mikä se on ja miksi se on
nyt ajankohtainen
Tekoälyn vaikutukset
Kartoita oma tilanteesi -kysymyspatteristo

Q&A w/ Janne Kalliola

digisuvereniteetin asiantuntija & Koodia Suomesta -puheenjohtaja

Tästä oppaasta saat tarvitsemasi tiedot digisuvereniteetistä. Oppaassa on myös digisuvereniteetin asiantuntija Janne Kalliolan kanssa tehty UKK-osio. Lisäksi saat kättä pidempää oman yrityksesi tai organisaatiosi digisuvereniteetin huomioimiseen ja kartoittamiseen käytännössä.

Lyhyesti meistä

Marvel Consulting on suomalainen IT-konsultointiyritys. Pääkonttorimme on Espoossa, mutta konsulttimme toimivat erilaisissa projekteissa eri puolilla Suomea. Yrityksemme on toiminut vuodesta 2019 lähtien, ja asiakkaitamme ovat sekä julkiset organisaatiot että yritykset, aina startupeista suuryrityksiin. Erikoistumme erityisosaamista ja asiantuntijakokemusta vaativiin IT-projekteihin.

Yhteys meihin

✉ info@marvelconsulting.fi

🌐 marvelconsulting.fi

in [Marvel Consulting Group](https://www.linkedin.com/company/marvel-consulting-group)

📷 [@marvelconsultingfi](https://www.instagram.com/marvelconsultingfi)



QR-KOODILLA VERKKOSIVUILLEMME



NÄITÄ AIHEITA KÄSITTELEMME

Mitä digisuvereniteetti tarkoittaa	04
Digisuvereniteetti ja datasuvereniteetti	05
Miksi digisuvereniteetti on ajankohtainen juuri nyt	06
Tekoälyn vaikutukset	09
Suomalaisia ja eurooppalaisia vaihtoehtoja	10
Digisuvereniteetti Q&A: Janne Kalliolan haastattelu	11
Miten edetä käytännössä	16
Kartoita oma digisuvereniteettitilanteesi	17
Mitä seuraavaksi	19

Mitä digisuvereniteetti tarkoittaa?

Digitaalinen suvereniteetti, eli digisuvereniteetti, tarkoittaa digitaalista itsenäisyyttä. Yrityksien ja organisaatioiden kontekstissa digisuvereniteetti viittaa organisaation kykyyn hallita omaa dataansa, järjestelmiään ja teknologisia riippuvuuksiaan. Käytännössä kyse on siitä, missä data sijaitsee, kuka sitä käsittelee ja millä ehdoilla.

Miksi digisuvereniteettiin kannattaa perehtyä juuri nyt?

Aihe on noussut keskiöön viime vuosina useasta syystä. Pilvipalveluiden käyttö on kasvanut nopeasti, lainsäädäntö on kiristynyt ja geopoliittinen tilanne on lisännyt kiinnostusta teknologiseen omavaraisuuteen sekä riskienhallintaan. Digisuvereniteetti on tärkeää huomioida liiketoiminnan jatkuvuuden kannalta, jos esimerkiksi yrityksen käyttämä ulkomainen palvelu yhtäkkiä lakkautetaan. Esimerkiksi Microsoft katkaisi palveluitaan YK:n kansainväliseltä tuomioistuimelta Trumpin hallituksen pyynnöstä.

Digisuvereniteetti ei kuitenkaan tarkoita eristäytymistä tai välttämättä edes kaikkien ulkomaisten palveluiden hylkäämistä. Sen ydin on hallinnan lisäämisessä ja tietoisten valintojen tekemisessä.

Digisuvereniteetti ja datasuvereniteetti

Digisuvereniteetti ja datasuvereniteetti saattavat helposti mennä sekaisin. Eikä täysin syyttä: digi- ja datasuvereniteetti ovat läheisesti liitoksissa toisiinsa.

Datasuvereniteetti keskittyy siihen, missä data sijaitsee, kuka sitä hallitsee ja miten sitä voidaan käyttää. Se liittyy erityisesti lainsäädäntöön, tietosuojaan ja datan käsittelyn läpinäkyvyyteen.

Digisuvereniteetti on laajempi kokonaisuus. Se kattaa datan lisäksi myös esimerkiksi järjestelmät, infrastruktuurin ja toimittajasuhteet. Kyse on organisaation kyvystä tehdä itsenäisiä teknologisia valintoja ja säilyttää IT-ympäristönsä hallinta.

Datasuvereniteetin voi siis
nähdä osana
digisuvereniteettiä.



Miksi digisuvereniteetti on ajankohtainen juuri nyt?

Monet organisaatiot ovat siirtäneet kriittisiä toimintojaan pilveen viime vuosina. Myös valtiot ovat siirtäneet tietojärjestelmiään pilveen. Samalla riippuvuus yksittäisistä toimittajista on kasvanut, ja esimerkiksi Supo suosittaa arvioimaan, minkä tasoiset riippuvuudet ulkomaisista palveluntarjoajista ovat hyväksyttäviä, erityisesti valtiolle kansallisen turvallisuuden kannalta.

Tänä vuonna esimerkiksi Ranska on ilmoittanut lopettavansa Microsoft Teamsin ja Zoomin käytön hallinnossaan ja alkavansa käyttämään ranskalaista Visiota.

Digisuvereniteetti Suomessa

Digisuvereniteettiin kiinnitetään huomiota myös Suomen hallinnon tasolla. Tässä muutamia esimerkkejä:

- Yhteiskunnan uudistamisen ministerityöryhmä käsitteli hiljattain kokouksessaan digitaalisen suvereniteetin tiekarttaa, jonka keskiössä ovat kriittisten palvelujen jatkuvuus, siirrettävyys, avoimet rajapinnat ja poistumiskyky
- Helsingin kaupunki rakentaa uuden tietojärjestelmän kotimaisen UpCloudin kanssa
- Kuntaliiton kartoituksen mukaan kunnat ovat yksimielisesti eurooppalaisen digisuvereniteetin edistämisen kannalla; digisuvereniteetti nähdään riippuvuuksien hallintana täydellisen omavaraisuuden sijaan

Digisuvereniteetin merkitys korostuu myös näistä syistä:

1

Toimittajariippuvuus kasvaa huomaamatta

Pilvipalvelut ja SaaS-ratkaisut nopeuttavat kehitystä, mutta sitovat organisaatiota usein yhteen toimittajaan ja sen tarjontaan. Irtautuminen voi olla hidasta, kallista tai teknisesti haastavaa.

2

Datanhallintaan kohdistuu yhä enemmän vaatimuksia

Organisaatioiden on tiedettävä tarkasti, missä data sijaitsee, kuka sitä käsittelee ja millä ehdoilla, erityisesti kansainvälisten palveluiden kohdalla.

Eri maiden ja alueiden lainsäädännön erot vaikuttavat dataan ja sen käsittelyyn. Esimerkiksi Yhdysvaltojen lainsäädäntö (kuten Cloud Act) voi vaikuttaa amerikkalaiseen yhtiöön enemmän kuin EU:n lainsäädäntö (kuten GDPR), riippumatta siitä, missä dataa säilötään fyysisesti. Jos yhdysvaltalaiset viranomaiset vaativat yhdysvaltalaista yhtiötä luovuttamaan dataa, saattaa yhtiö joutua tekemään niin, vaikka data ei fyysisesti olisikaan Yhdysvaltojen rajojen sisällä.

3

Tietoturva ja riskienhallinta korostuvat

Ulkoistetut palvelut eivät poista vastuuta. Organisaation on edelleen ymmärrettävä riskinsä ja varmistettava, että kriittinen data ja järjestelmät ovat hallinnassa kaikissa tilanteissa.

4

Liiketoiminnan jatkuvuus vaatii joustavuutta

Muutokset toimittajissa, hinnoittelussa tai geopoliittisessa tilanteessa voivat suoraan vaikuttaa liiketoimintaan. Mitä joustamattomampi ympäristö on, sitä vaikeampi muutoksiin on reagoida nopeasti.

Digisuvereniteetin nostamien kysymysten ja huolenaiheiden myötä monet yritykset ja organisaatiot ovat palanneet tai suunnittelevat palaamista kotimaisiin konesaleihin. Julkinen sektori toimii usein edelläkävijänä, mutta samat kysymykset koskevat yhä useammin myös yksityistä sektoria, erityisesti regulaatioherkillä toimialoilla.



Tekoälyn vaikutukset

Tekoälyn yleistyminen ja käyttöönotto tuovat digi- ja datasuvereniteettiin oman ulottuvuutensa.

Tekoälyä käytettäessä on datan sijainnin lisäksi erityisen tärkeää huomioida:

- miten dataa käytetään ja
- millaisia päätelmiä siitä voidaan tehdä tekoälyavusteisesti.

Organisaation on ymmärrettävä, mitä dataa käytetään tekoälymallien kouluttamiseen, missä nämä mallit sijaitsevat ja kenen hallinnassa ne ovat. Esimerkiksi generatiivisen tekoälyn palveluissa keskeinen kysymys on, voiko organisaation data päätyä osaksi palveluntarjoajan mallien kehitystä.

Myös lainsäädäntö vaikuttaa tekoälyn käyttöön. Esimerkiksi EU:n tekoälyasetus, AI Act, korostaa tarvetta hallita dataa sekä huomioida tekoälykäytön riskejä ja vastuuta. AI Act jaottelee tekoälyjärjestelmiä niiden riskien perusteella ja jopa täysin kieltää tekoälyjärjestelmiä, joiden tarkoituksena on hyödyntää ihmisten haavoittuvuuksia.

Organisaation on pystyttävä osoittamaan miten tekoälyä käytetään, millaista dataa hyödynnetään ja miten riskit on huomioitu.

Suomalaisia ja eurooppalaisia vaihtoehtoja

Tästä löydät muutamia suomalaisia ja eurooppalaisia vaihtoehtoja erilaisille digitaalisille palveluille. Lisää voit löytää eri tarpeisiin [European Alternatives -sivustolta](#).

Pilvipalvelu

UpCloud on suomalainen yritys, jonka omistus on kokonaan Euroopassa. Yrityksellä on Euroopassa 10 konesalia, joista kaksi on Suomessa. Tämä mahdollistaa datan pysymisen Suomen rajojen sisällä. Yritys tarjoaa 24/7 henkilökohtaista tukea asiakkailleen.

Viestintä ja yhteistyö

Stackfield on saksalainen yritys, joka tarjoaa päästä päähän -salauksen ja sovelluksia monille työpöytä- ja mobiilialustoille. Palvelu tarjoaa myös ääni- ja videopuheluita suoraan sovelluksessa.

Verkkosivujen analytiikka

Mouseflow on tanskalainen verkkoanalytiikkapalvelu, joka tarjoaa ominaisuuksia, kuten lämpökarttoja sekä istunnon toiston.

Dokumenttien, raporttien ja esityksien luominen

CryptPad tarjoaa dokumenttien muokkauspalvelun, jota voi ylläpitää itse (open source). CryptPad on nollatietoinen palvelu. Tunnetuinta versiota ylläpitävät palvelun pääkehittäjät Ranskassa (cryptpad.fr).



Digisuvereniteetti Q&A: Janne Kalliolan haastattelu

Janne Kalliola on asiantuntija digi- ja datasuvereniteetin sekä vihreän IT:n asioissa. Hän toimii Koodia Suomesta -yhdistyksen puheenjohtajana sekä tarjoaa konsultointia yrityksensä Coontin kautta.



Tässä usein kysyttyjä kysymyksiä digisuvereniteetista.
Janne Kalliola vastaa!

Miksi digisuvereniteetti on ajankohtainen asia?

“Useat teemat ovat johtaneet digisuvereniteetin nousemiseen isommin esille. Yksi niistä on Yhdysvaltain hallinnon toiminnan muutos. Euroopassa on herätty siihen, että täällä ollaan aika paljon yhdysvaltalaisten firmojen kanssa naimisissa, hyvässä ja pahassa. Lisäksi datan merkittävyys on kasvanut. Datatalouden ja datakäsittelyn merkittävyys on kasvanut. Tekoälyn merkittävyys on kasvanut isosti.

Voi havaita, ettei eurooppalaisilla yrityksillä ole enää samaa osuutta markkinassa. EU onkin ruvennut suitsimaan yhdysvaltalaisten firmojen toimintaa, koska monilla aloilla liiketoiminta on hyvin harvojen käsissä (duopoli tai jopa monopoli). Käytännössä käyttämällä EU:n ulkopuolisten yritysten palveluita rahoitamme niiden tuotekehitystä. Tämä johtaa siihen, että näiden yritysten tuotekehitys etenee nopeampaa tahtia, ja sen sijaan, että käytetty raha tulisi takaisin oman valtion tai EU:n alueen kehitykseen, se jää muualle.”



Missä tilanteissa digisuvereniteetin merkitys korostuu yrityksille?

“On eri tilanteita ja näkökulmia siihen, milloin digisuvereniteetin merkitys korostuu. Yksi kulma on lainsäädännön kehikko ja siihen liittyvät riskit, esimerkiksi Yhdysvaltojen Cloud Act, joka on ristiriidassa EU:n GDPR:n kanssa. On riski, että jos yhdysvaltalainen firma joutuu Cloud Actin pohjalta antamaan tietoja, niin se samalla voi rikkoa eurooppalaisen päämiehensä, asiakkaansa, GDPR-velvoitetta. Näitä ekstraterritoriaalisia lakeja tulee koko ajan enemmän, ja on juridisesti hankalampaa olla useamman lainsäädännön alaisena yhtäaikaaisesti. Juridiset riskit siis kasvavat, vaikka riskien materialisoituminen on tietenkin toinen kysymys.

Toinen kulma on se, että raha kiertää toiselle talousalueelle ja pysyy siellä. Sen sijaan, että raha pysyisi Suomen tai EU:n alueen sisällä, mistä se voisi palata takaisin ja tukea kehitystä Suomessa, se jää ulkomaille.”

Mitä suomalaiset yritykset tai organisaatiot tekevät digisuvereniteetin suhteen hyvin, ja mitä taas pitäisi parantaa?

“Monet tahot haluavat viedä digisuvereniteettiä eteenpäin ja kehittää sitä. Ja meillä on Suomessa hyvät mahdollisuudet siihen, koska olemme korkean teknologian maa ja meiltä jo löytyy monia hyviä ratkaisuja. Mutta samaan tapaan kuin ilmastonmuutoksen torjunnassa, tulisi myös digisuvereniteetin kehittämisessä suuren massan lähteä tekemään asioita, jotta työn vaikuttavuus kasvaa.

Digisuvereniteetti voi tuntua kaukaiselta tai abstraktilta asialta, jonka vaikutukset eivät näy omassa arjessa heti. Helppous ja mukavuus voivat mennä kehittämisen edelle. Käytännössä siis kaikkien pitäisi tehdä jotain.”

“Suomessa hyvät mahdollisuudet siihen (digisuvereniteetin kehittämiseen), koska olemme korkean teknologian maa ja meiltä jo löytyy monia hyviä ratkaisuja.”



Mikä on yleisin väärinkäsitys digisuvereniteetistä?

“Yleinen harhaluulo on, että yhdysvaltalaiset ratkaisut ovat merkittävästi parempia tai edullisempia kuin eurooppalaiset vaihtoehdot – todellisuudessa meiltä löytyy vähintään yhtä laadukkaita tai laadukkaampiakin ratkaisuja. Koheesion taso ratkaisuissa saattaa tosin olla alempi, eikä kaikkia tarvittavia ominaisuuksia välttämättä saa yhdeltä palveluntarjoajalta. Mutta yhden tarjoajan varassa oltaessa on vähäisemmät mahdollisuudet neuvottelemiselle tai kilpailuttamiselle, ja palvelun vaihtaminen voi olla vaikeaa. Lisäksi hinnoittelumallit näillä palveluntarjoajilla ovat usein sellaisia, että asiakas joutuu maksamaan enemmän kuin useampia palveluntarjoajia hyödyntäessä.

Toinen iso väärinkäsitys on se, että me ei voida enää tehdä mitään. Ilman että asialle yritetään tehdä jotakin, ei voida tietää, pystytäänkö siihen vaikuttamaan. Käytännössä yrittämällä saisi kuitenkin vähintään sen, että meillä Suomessa kompetenssi kasvaa – ja parhaassa tapauksessa myös digitaalinen suvereniteetti saavutetaan tai sen taso paranee. Matkan varrellakin tapahtuu hyviä asioita.”

Missä tilanteissa organisaation kannattaa oikeasti olla huolissaan omasta digisuvereniteetin tilasta?

“Ulkoisissa ongelmatilanteissa, esimerkiksi GDPR:n liittyvissä ongelmatilanteissa ulkomaisten palveluntarjoajien kanssa. Tämän lisäksi voi olla sisäisiä ongelmia, esimerkiksi se, ettei organisaatio tiedä, missä sen dataa käsitellään, missä se kulkee ja kuka sitä käsittelee. Hyvä kontrolli datasta puuttuu.”

Mikä on yleisin digisuvereniteettiin liittyvä virhe, jonka tekeminen kannattaa välttää?

“Kaikki tai ei mitään -ajattelu, se, että yritetään muuttaa kaikki kerralla. Äkkiliikkeitä kannattaa välttää ja lähestyä asiaa askel askeleelta. Riskejä ja toimenpiteitä kannattaa luokitella sekä priorisoida ennen toimintaa. Vaiheittainen, mutta päättäväinen eteneminen kannattaa. Muutamassa vuodessa voi päästä digisuvereniteetissä pitkälle.”



Millaisia riskejä on olemassa organisaatioille, jotka eivät huomioi digisuvereniteettiä?

“Riskeihin kuuluvat juridiset riskit, jotka voivat olla suuria, mutta joiden todennäköisyys on yleensä pieni. Suuri riski on myös arvaamattomuus ja se, ettei omaan toimintaan ole tarkkaa näkyvyyttä. Mitä paremmin oman toimintansa tuntee, sitä paremmin sitä voi kontrolloida. Esimerkiksi tietomurtojen riski vähentyy, kun ymmärrys on suurempi ja toimittajilta on voitu esimerkiksi vaatia selvityksiä, sen sijaan, että niiden toimintaan luotetaan sokeasti.

Pitkällä tähtäimellä, jos oman talousalueen sisäistä osaamista ei tueta, kompetenssitasot laskevat ja köyhtymisen riski kasvaa.”

Miten Suomen tilanne vertautuu muuhun Eurooppaan?

“Protonin taulukon ([Europe's tech sovereignty watch](#)) mukaan Suomi on 92 % riippuvainen Yhdysvaltojen tarjoamista digipalveluista. Jos siis Yhdysvalloista katkeaisi yhteydet, nämä palvelut lakkaisivat toimimasta. Tässä Suomi on Euroopan neljänneksi korkeimmalla tasolla, eli melko kärjessä. Tämä prosentti kertoo myös siitä, kuinka paljon me Suomessa laitamme rahaa muualle, vaikkakin asiaan vaikuttaa myös maan digitaalinen edistyneisyys; mitä edistyneempi maa on digitaalisuudessa, sen tiukemmin se on usein Yhdysvaltojen varassa.”

“Suomi on 92 % riippuvainen
Yhdysvaltojen tarjoamista
digipalveluista.”





Miten digisuvereniteetti ja tietoturva liittyvät toisiinsa?

“Yhdysvaltalaisia järjestelmiä usein pidetään tietoturvallisempina. Todellisuudessa suomalaiset ja eurooppalaiset toimijat suhtautuvat tietoturvaan yhtä vakavasti, ja esimerkiksi suomalaiset koodarit ovat maailman tasolla vertailtaessa todella hyviä. Suuri käyttäjämäärä voi toki johtaa siihen, että ongelmat paljastuvat ja ne korjataan nopeammin.

Palveluja hajautettaessa tietoturvan tarve usein kasvaa, kun vendorien ja integraatioiden määrä kasvaa. Hajauttaminen kuitenkin mahdollistaa sen, että jos yksi järjestelmä vaaraantuu tai siihen murtaudutaan, se ei välttämättä vaikuta muihin järjestelmiin. Tietoturvan haasteet ovat erilaisia yhden toimittajan mallissa verrattuna hajautettuun malliin.”

Miten Koodia Suomesta ottaa digisuvereniteetin huomioon?

“Koodia Suomesta on rakentamassa koalitiota ([Data Sovereignty Coalition](#)), jonka ydinajatuksena on se, että tehdään enemmän yhteistyötä Suomen sisällä; että suomalainen tukisi suomalaista. Ja sitten sen jälkeen eurooppalaista ja sitten vasta Euroopan ulkopuolisia palveluita. Tavoitteena on rakentaa yhdessä moniulotteinen pilvipalveluratkaisu tai ratkaisukomponentteja, jotka toimivat yhdessä. Näistä sitten koostettaisiin vaihtoehtoja hyperscalereille. Koodia Suomesta toimii tässä fasilitaattorina, ei siis ongelmanratkaisijana, vaan ratkaisijoita yhteen tuovana ja innostavana tahona. Tavoitteena on herättää suuren yleisön mielenkiintoa. Lisäksi tuemme digitaalinen itsenäisyys -kansalaisaloitetta.”

“Todellisuudessa suomalaiset ja eurooppalaiset toimijat suhtautuvat tietoturvaan yhtä vakavasti, ja esimerkiksi suomalaiset koodarit ovat maailman tasolla vertailtaessa todella hyviä.”

Miten edetä käytännössä

Digisuvereniteetin kehittäminen kannattaa aloittaa oman nykytilan ymmärtämisestä.

NYKYTILAN KARTOITUS

Kartoita oma digisuvereniteettitilanteesi. Apuna voit käyttää esimerkiksi seuraavalta sivulta löytyvää kysymyspatteristoa.

RISKIEN TUNNISTAMINEN

Tunnista yrityksellesi tai organisaatiollesi oleellimmat digisuvereniteettiin liittyvät riskit. Arvioi ja analysoi niiden mahdollisia vaikutuksia sekä niiden todennäköisyyttä. Mieti esimerkiksi näitä asioita:

- Olemmeko riippuvaisia jostakin tietystä toimittajasta?
- Koskeeko toimintaamme lainsäädännölliset vaatimukset, joita emme vielä täytä?

PRIORISOINTI

Kaikkea ei tarvitse muuttaa kerralla. Keskity kriittisimpiin kehityskohteisiin ensimmäisenä nykytilasi kartoituksen ja riskianalyysisi perusteella.

ROADMAP

Suunnittele vaiheittainen eteneminen ja realistinen aikataulu tarvittaville muutoksille.



Kysymyspatteristo:

Kartoita oma digisuvereniteettitilanteesi

Oman yrityksen tai organisaation digisuvereniteetin arvioiminen saattaa tuntua vaikealta.

Tätä helpottaa se, että arviointi jaetaan teemoihin:

data, infrastruktuuri, toimittajariippuvuus ja hankintamenettely, strategia sekä lainsäädäntö ja vaatimustenmukaisuus.

DATA

Missä datanne sijaitsee?

Kuka omistaa datan ja hallinnoi sitä?

Voidaanko data siirtää tarvittaessa?

Onko datan käyttöoikeudet dokumentoitu oikein?

INFRASTRUKTUURI

Millainen infrastruktuurinne on: pilvi, on-prem vai hybridi?

Kuinka helposti ympäristö voidaan vaihtaa?

TOIMITTAJARIIPPUUUS & HANKINTAMENETTELY

Onko käytössä yksi vai useampi toimittaja?

Onko exit-strategia olemassa?

Kuinka nopeaa tai kallista vaihtaminen olisi?

Voidaanko palvelut korvata ilman merkittäviä uudelleenrakennuksia?

Millainen hankintamenettelyenne on; millaisia kriteerejä teillä on softan hankinnalle?

STRATEGIA

Onko digisuvereniteetti huomioitu IT-strategiassa?

Arvioitko riskejä säännöllisesti?

Onko organisaatiollanne selkeä omistajuus digisuvereniteetille?

LAINSÄÄDÄNTÖ JA VAATIMUSTENMUKAISUUS

Mitkä lait ja säädökset vaikuttavat datanne käsittelyyn ja muuhun toimintaan?

Täyttyvätkö nykyiset vaatimukset?

Oletteko varautuneet lainsäädännön muutoksiin?

Miten tulkita vastauksiasi

Kaikkiin kysymyksiin ei tarvitse vastata täydellisesti, eikä “täydellinen digisuvereniteetti” ole useimmille yrityksille realistinen tai tarkoituksenmukainen tavoite. Tämän arvioinnin tarkoituksena on auttaa sinua tunnistamaan ja pohtimaan, missä kohtaa hallinta on riittävällä tasolla ja mitkä asiat vaatisivat lisätoimenpiteitä.

Tilanteesi voi olla esimerkiksi:

Riskialtis	Hallittu	Edistynyt
Ette tiedä tarkasti, missä datanne sijaitsee tai miten sitä käsitellään. Olette vahvasti sidoksissa yhteen toimittajaan ilman selkeää exit-strategiaa. Muutokset ympäristöön olisivat hitaita ja kalliita.	Ymmärrätte keskeiset riippuvuudet ja datanne sijainnin. Olette tunnistaneet kriittiset riskit. Pystytte toimimaan jossain määrin joustavasti.	Datanne sijainti, käyttö ja hallinta ovat hyvin hallussa. Toimittajariippuvuuksia on aktiivisesti vähennetty. Arkkitehtuurinne kestää muutoksia. Digisuvereniteetti on osa strategista päätöksentekoa.
Muutostilanteissa reagointi on hidasta. Vaatimustenmukaisuus voi olla heikolla tasolla.	Hyvä perusta, mutta kehityskohteita löytyy. Riskit on tunnistettu ja kehitystyö niiden välttämiseen aloitetaan.	Teillä on kyky reagoida muutoksiin nopeasti ja hallitusti. Riskit on tunnistettu ja kehitystyö on jatkuva.

Mitä seuraavaksi

Mikäli sisäistä asiantuntijuutta digisuvereniteettiasioihin liittyen ei vielä löydy, voi olla järkevää tukeutua ulkoisen asiantuntijan apuun.

Myös mahdollisia muutoksia tehtäessä saattaa ulkoinen apu olla tarpeen, joko lyhyemmän aikaa tai pitkäkestoisemmin. Ota tällöin yhteys meihin ja ratkaistaan tilanteesi yhdessä!



✉ info@marvelconsulting.fi

🌐 marvelconsulting.fi

🌐 [Marvel Consulting Group](https://www.linkedin.com/company/marvel-consulting-group/)

📷 [@marvelconsultingfi](https://www.instagram.com/marvelconsultingfi)



MARVELCONSULTING.FI

Huomioithan, että oppaamme tarkoituksena on antaa sinulle eväitä digisuvereniteetin huomioimiseen omassa toiminnassasi, ei olla virallinen tai lakisääteinen opas. Lähteinä käytimme asiantuntijoidemme lisäksi esimerkiksi Euroopan komission ja Valtioneuvoston sivuja sekä eri uutissivustoja. Mikäli sinulla on lisäkysymyksiä, voit olla meihin yhteydessä!