

Digitale soevereiniteit: zit je zelf aan het stuur?

Bestuurbaarheid is de voorwaarde die bepaalt welke uitkomsten uw organisatie zich kan veroorloven.

Soevereiniteit, 'demystified'

Veel organisaties zien digitale soevereiniteit als een simpele knop: kies een Europese leverancier, zet data op een Nederlandse server, klaar. Bij Dux zien we dat anders. Achter digitale soevereiniteit zit een reeks keuzes in het landschap, niet allemaal technisch. Geen eenmalige keuze maar een doorlopend proces wat de hele organisatie raakt.

Soverein zijn is niet iets dat je op een dinsdagmiddag regelt met een contractwissel. Het is een continu proces van controle, besluitvorming en het managen van afhankelijkheden door de hele keten heen. Het gaat om het behouden van keuzevrijheid en regie, ongeacht waar de technologie vandaan komt en wat er geopolitiek gebeurt.

Dat is ook meteen een veelgemaakte denkfout: soevereiniteit verwarren met "geen vendor lock-in hebben". Geen lock-in is een gevolg van **goede architectuurkeuzes**. Soevereiniteit is het bredere vermogen om, wat er ook gebeurt, in charge te blijven.

Een capability, geen product

Waar sommige leveranciers soevereiniteit verkopen als kant-en-klaar product, Sovereignty-as-a-Service, praat Dux erover als een capability: het **vermogen** van een organisatie om in de driver's seat te blijven zitten. De risk appetite van de organisatie is leidend voor de inrichting, van het IT-landschap tot de lagen daarboven. De leverancier bepaalt dat niet. Welke processen, data en stuurinformatie vereisen volledige soevereiniteit, en waar is een hybride vorm prima acceptabel? Dat is een afweging die per organisatie, en vaak per behoefte, anders uitvalt.

De kernvraag is bestuurlijk: wie bepaalt of jouw organisatie kan blijven functioneren als het erop aankomt?

Waarom het geen IT-vraagstuk is

Digitale soevereiniteit wordt vaak bij de IT-afdeling neergelegd, maar hoort daar niet thuis. Naast technologie spelen er lagen die minstens zo bepalend zijn: juridische, operationele, economische en publieke waarden.



Stel dat een land alles uitbesteedt aan één grote buitenlandse partij. Op een gegeven moment weet niemand meer hoe de eigen stroomvoorziening of de eigen ziekenhuizen precies werken. De kennis en het gezag zijn dan verdwenen. Dezelfde logica geldt voor organisaties: kan de organisatie zelfstandig blijven functioneren als er internationaal grote spanningen ontstaan? Dat is een vraag voor de hele organisatie, niet iets dat je kunt delegeren aan een systeembeheerder.

Wat soevereine architectuur vraagt

In de praktijk vraagt digitale soevereiniteit niet om één tool of leverancier, maar om samenhangende keuzes rondom risicobeheer, dataopslag, integraties, (cloud)strategie, toegangsbeheer, governance, security, continuïteit en exitmogelijkheden. Drie principes komen daarbij steeds terug:

Een toekomstbestendige architectuur vraagt om...



Risico classificaties: Niet alles vraagt hetzelfde beschermingsniveau. Kritieke data en processen krijgen de zwaarste bewaking afhankelijk van je risk appetite, in eigen beheer of een soevereine omgeving. Minder gevoelige onderdelen kunnen in een reguliere cloudomgeving.



Een modulaire opbouw met open standaarden: Componenten die vervangbaar zijn en niet vastzitten aan één leverancier houden de exit-optie reëel en het ontwerpprincipe 'plug and play' werkbaar.



Een bewaakte onderhandelingspositie: Zolang vervangen mogelijk blijft, houdt de organisatie regie over de eigen keten, ook over de volledige levensduur van het landschap. Dit benadrukt dus het belang van goed applicatieportfoliomanagement.



Principes voor 'hoe wij het hier doen': De kaders die de organisatie houvast geven bij het inrichten van het bedrijfs- en applicatielandschap. Soevereiniteitskeuzes zijn het resultaat van die principes, bepaald door de kaders vooraf, niet gecontroleerd achteraf.



Waarom er geen standaardoplossing bestaat

Elke sector heeft een eigen risicoprofiel en eigen maatschappelijke verantwoordelijkheden. Een ziekenhuis dat geen seconde uit de lucht mag zijn en met uiterst gevoelige patiëntgegevens werkt, staat voor heel andere afwegingen dan een webshop in schoenen. Omdat de risico's en de regelgeving, denk aan NIS2, per sector verschillen, bestaat er geen tovermiddel dat overal hetzelfde werkt.

De noodzaak voor soevereiniteit wordt bepaald door de impact op de primaire processen en de geldende regelgeving. Een algemene richtlijn die voor iedereen gelijk is, bestaat niet.

Plan B?

Als een grote techpartij morgen besluit de stekker eruit te trekken, bijvoorbeeld door een geopolitiek conflict, kan de organisatie dan binnen drie maanden ergens anders weer opstarten? Of is dan alles kwijt?

De vraag die er echt toe doet

Organisaties die serieus met digitale soevereiniteit aan de slag willen, hoeven zich niet eerst af te vragen welke leverancier het beste past. De eerste vragen zijn fundamenteeler: wat hebben we nodig, welke risico's horen daarbij, en hebben we daar een plan (B) voor?

Digitale soevereiniteit is meer dan alleen een leverancierskeuze. Het is ook de mate waarin een organisatie zelf kan sturen op haar data, processen en infrastructuur, tevens wanneer de context verandert. Die sturing ontstaat niet vanzelf en is het resultaat van governance die vooraf bepaalt welke risico's acceptabel zijn en welke niet. Organisaties die dat nu inrichten, hebben een antwoord klaarliggen wanneer de vraag zich aandient.





Over de auteur

Morgan Djotaroeno is consultant en bouwt bij Dux Group aan het digitale fundament van organisaties, zij vertaalt strategie naar de inrichting van data, processen en governance zodat organisaties beter sturen en resultaten behalen.

☎ +31 6 41 76 39 74

✉ m.djotaroeno@duxgroup.nl

Over Dux Group

Dux Group, geboren en gebouwd in Rotterdam. Recht door zee, geen franje: geen woorden maar data.

Wij maken digitale transitie concreet en menselijk. Want verandering draait voor 90% om mensen en maar 10% om technologie. Daarom brengen wij data, AI, cloud en security niet als hype, maar als praktische oplossingen die organisaties vandaag al vooruithelpen.

We zorgen dat mensen data vertrouwen, ermee experimenteren en nieuwe manieren van werken omarmen. Zo bouwen we organisaties die groeien in resultaat, efficiëntie én zelfvertrouwen.

Klaar voor verandering?

Neem dan contact met ons op

info@duxgroup.nl