



WHITEPAPER

Digitale soevereiniteit in het Nederlandse Zorglandschap.

intermax 

Inhoudsopgave

Digitale soevereiniteit in het Nederlandse Zorglandschap.

Inleiding	3
Het verschil tussen digitale soevereiniteit en digitale autonomie	5
Recente discussies over digitale afhankelijkheid en geopolitieke ontwikkelingen	6
Digitale soevereiniteit in de Nederlandse zorgsector: implicaties van cloudadoptie	8
Risico's en uitdagingen voor de zorgsector	11
Implicaties van digitale soevereiniteit voor de zorgsector	13
Strategieën voor digitale soevereiniteit in de zorg	15
Praktische handvatten voor zorginstellingen	16
Conclusie en toekomstperspectief	17
Aanbevelingen voor beleidsmakers	18
Gebruikte bronnen	19

Inleiding

Digitale soevereiniteit is volgens ons al bijna geworden tot het 'buzzword' van 2025. Over het algemeen is er consensus dat soevereiniteit ziet op het vermogen en de controle van een land, organisatie of individu om digitale infrastructuur, data en diensten te beheren en te beschermen volgens eigen wet- en regelgeving, zonder ongewenste afhankelijkheid of invloed van externe partijen.

Maar belangrijker is wellicht nog het bereiken van digitale autonomie. Afhankelijk zijn van een leverancier in een monopolie of duopolie is op langere termijn negatief. Het Nederlandse zorglandschap – en wij bedoelen hier feitelijk alle zorginstellingen en toeleveranciers aan de zorg mee – is voor 100% afhankelijk van hun IT-infrastructuur. We kunnen niet meer zonder, dus laten we zorgen dat het 'goed zit'!

Laten we zorgen dat het goed zit!



Het verschil tussen digitale soevereiniteit en digitale autonomie

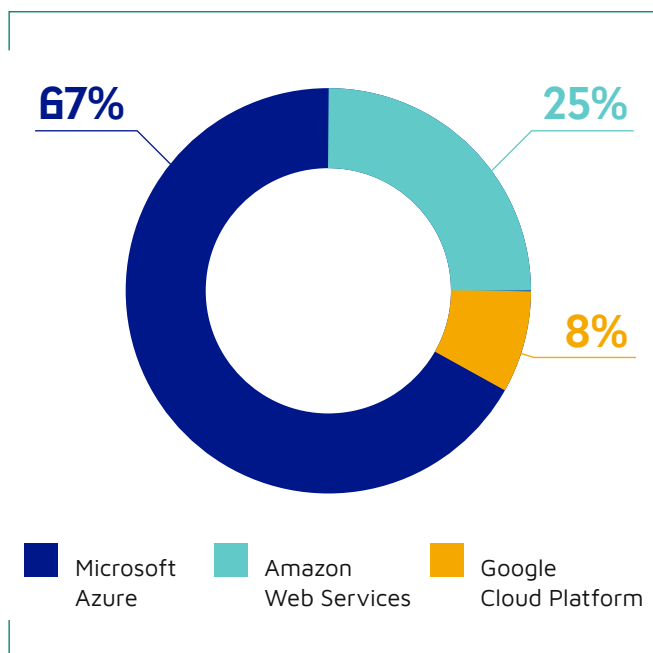
Waar digitale soevereiniteit streeft naar volledige onafhankelijkheid en afdwingbare jurisdictie over het digitale domein, is digitale autonomie een meer haalbare tussenstap. Het gaat om het vermogen zelfstandig keuzes te maken in het digitale domein, zonder per se totale controle na te streven.

IN PRAKTISE ZIN VERTAALT DIGITALE AUTONOMIE ZICH IN:

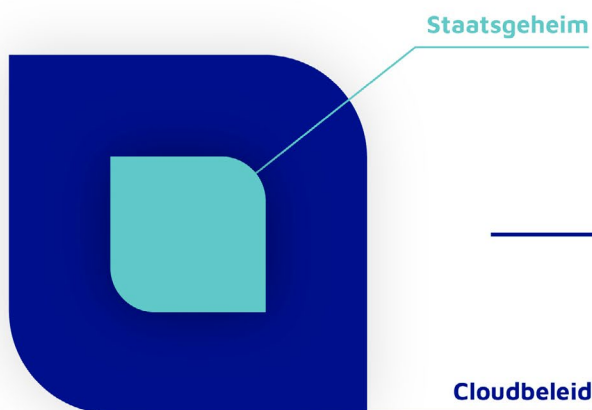
- ▶ Controle over eigen digitale infrastructuur
- ▶ Gebruik van (open-source) software die aanpasbaar is aan eigen wensen
- ▶ Veilige communicatie en digitale weerbaarheid
- ▶ Verminderde afhankelijkheid van buitenlandse technologiebedrijven

Cloudtechnologie is voornamelijk van Amerikaanse leveranciers en Microsoft Azure is met afstand marktleider voor public clouddiensten in Nederland. Microsoft Azure heeft een uitzonderlijk groot marktaandeel in de Nederlandse cloudmarkt: 67% van de public cloud-markt wordt ingenomen door Azure, Amazon Web Services (AWS) volgt met 25% en Google Cloud Platform (GCP) heeft een marktaandeel van slechts 8%^[3].

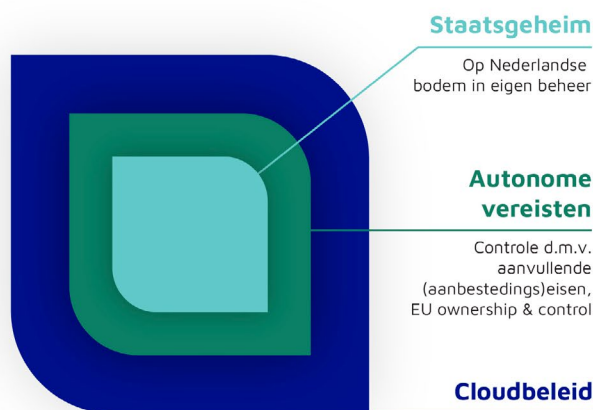
De technologie, functionaliteit en kwaliteit van hun dienstverlening is ongeëvenaard, en dat is niet verwonderlijk gezien de investeringen die Microsoft de afgelopen jaren



in cloudtechnologie en datacenters heeft gedaan. In het kwartaal eindigend op 30 juni 2024 investeerde Microsoft \$19 miljard in kapitaaluitgaven, waarvan bijna alles naar cloud- en AI-gerelateerde projecten ging. Ongeveer de helft daarvan werd gebruikt voor de bouw en leasing van datacenters; de rest ging naar hardware zoals CPU's en GPU's. In het eerste kwartaal van fiscaal jaar 2025 (juli-september 2024) verdubbelde Microsoft bijna zijn investeringen naar \$20 miljard om te voldoen aan de groeiende vraag naar cloud en AI^[41]. Wel moet worden opgemerkt dat de toekomstige investeringen met name naar AI-infrastructuur gaan, en niet in het algemeen meer naar cloudtechnologie.



Huidige situatie



Nieuwe situatie

Recente discussies over digitale afhankelijkheid en geopolitieke ontwikkelingen

Naar aanleiding van diverse recente rapporten, onder andere dat van Draghi^[42], de initiatiefnota 'Wolken aan de horizon'^[43], het Rekenkamer rapport 'het Rijk in de Cloud'^[44] en de negen (!) recent aangenomen moties in de Tweede Kamer over het gebruik van public cloud en niet-Europese cloudleveranciers voor overheidsdata is er een forse maatschappelijke discussie ontstaan.

Tegenstanders van het gebruik van niet-Europese cloudleveranciers (hiermee worden tenminste Microsoft, Amazon, Google, Oracle, IBM en Alibaba bedoeld) menen dat het zelfs 'roekeloos' en 'gevaarlijk' om essentiële overheidsdiensten en maatschappelijke functies aan Amerikaanse cloudproviders toe te vertrouwen, vooral gezien recente politieke ontwikkelingen in de VS. Tech-expert Bert Hubert wijst erop dat deze afhankelijkheid Europa kwetsbaar maakt voor Amerikaanse sancties, politieke druk en mogelijke inmenging in data en dienstverlening. Hij benadrukt dat marktwerking tot nu toe niet heeft geleid tot een volwaardig Europees alternatief, en dat bedrijven en overheden vastzitten aan Amerikaanse diensten vanwege lock-in en het ontbreken van gelijkwaardige Europese alternatieven.

BELANGRIJKE NUANCES, TEGENWERPINGEN EN UITDAGINGEN HIERBIJ ZIJN ONDER ANDERE:

- ▶ De CLOUD Act gaat niet specifiek over cloud, maar over data
- ▶ Datasoevereiniteit ligt in eigen handen
- ▶ Europese digitale onafhankelijkheid is complex
- ▶ Lokale cloudplatformen zijn geen directe vervanging voor hyperscalers
- ▶ De geopolitieke tarievendiscussie gaat over goederen, niet over diensten
- ▶ EU-regio's afsluiten is onrealistisch
- ▶ Organisaties verlaten hyperscalers niet massaal
- ▶ Ook de Nederlandse overheid heeft haar cloudbeleid (nog) niet gewijzigd

De CLOUD Act gaat niet specifiek over cloud, maar over data

De Amerikaanse CLOUD Act betreft toegang tot data in het algemeen, niet alleen data in de cloud. Europese wetgeving zoals de GDPR blijft van kracht en cloudproviders hoeven encryptie niet te verbreken. Tot nu toe is er geen buiten de VS opgeslagen data aan de Amerikaanse overheid overgedragen op basis van deze wet.

Datasoevereiniteit ligt in eigen handen

Met sterke encryptie-opties en eigen sleutelbeheer bij hyperscalers blijft de klant zelf baas over zijn data. Nieuwe initiatieven zoals de European Sovereign Cloud van AWS vergroten de juridische autonomie voor Europese klanten. Tegenstanders menen echter dat een soevereine cloud van een Amerikaans bedrijf nog steeds geen garantie geeft op volledige soevereiniteit.

Europese digitale onafhankelijkheid is complex

Volledige onafhankelijkheid van Amerikaanse technologie is lastig, omdat ook Europese cloudproviders afhankelijk zijn van Amerikaanse hardware en software. Bovendien gebruiken we massaal Amerikaanse SaaS-diensten, die niet eenvoudig te vervangen zijn. Tegenstanders menen dat het feit dat het niet eenvoudig is, geen argument mag zijn om je er dan maar bij neer te leggen.

Lokale cloudplatformen zijn geen directe vervanging voor hyperscalers

Europese aanbieders zijn geen 1-op-1 alternatief voor hyperscalers qua schaal, security, innovatie en dienstenaanbod. Ze kunnen wel geschikt zijn voor specifieke workloads, maar de vergelijking gaat niet volledig op. Wel is dankzij de opkomst van technologie als Kubernetes en cloud native platforms het overstappen veel eenvoudiger geworden.

De geopolitieke tarievendiscussie gaat over goederen, niet over diensten

Importtarieven raken vooral goederen, niet digitale diensten. Hyperscalers leveren hun diensten lokaal via Europese entiteiten, waardoor ze moeilijk te belasten zijn met importtarieven. Discussies over extra belastingen op winsten lopen nog. Tegenstanders zijn hier kritisch op, want

uiteindelijk is politieke druk op Amerikaanse bedrijven door de Amerikaanse overheid – die ook de grootste klant is van de hyperscalers – nog steeds mogelijk en niet geheel onrealistisch. Wie betaalt, bepaalt immers.

EU-regio's afsluiten is onrealistisch

Het volledig afsluiten van Europese cloudregio's door Amerikaanse hyperscalers is zeer onwaarschijnlijk vanwege de grote financiële belangen en de afhankelijkheid van beide kanten. Volledige digitale isolatie bestaat bovendien niet zolang er internetverbinding is. Wel hebben we al gezien dat individuen of specifieke organisaties afgesloten kunnen worden. Het risico is dus niet nul. En regionale of wereldwijde storingsen hebben weinig met soevereiniteit te maken, maar zijn ook een realistisch scenario voor (tijdelijke) afsluiting.

Organisaties verlaten hyperscalers niet massaal

Hoewel de interesse in Europese providers groeit, blijven veel organisaties gewoon klant bij hyperscalers. Migraties naar Europese clouds zijn vaak al voor recente geopolitieke ontwikkelingen ingezet. Nieuwe cloudprojecten worden soms uitgesteld, maar exits zijn nog zeldzaam. Wij zien echter een forse toename in vragen omtrent uitwijkomgevingen, disaster recovery scenario's en onderzoeken naar een 'terugverhuizing' naar Nederland of Europa. Niet alleen vanwege sentimenten, maar ook concreet vanwege

Ook de Nederlandse overheid heeft haar cloudbeleid (nog) niet gewijzigd

Er zijn wel politieke moties en discussies over een Nederlandse cloud, maar formeel beleid of wetgeving is nog niet aangepast. Initiatieven zoals Cloud Kootwijk zijn nog geen officiële overheidsprojecten en een Nederlandse cloud zal qua schaal niet vergelijkbaar zijn met hyperscalers. Dat hoeft ook niet per se, want het nabouwen van bijvoorbeeld Azure is natuurlijk onbegonnen werk^[45].

Digitale Soevereiniteit in de Nederlandse Zorgsector: implicaties van grootschalige cloudadoptie

De groeiende afhankelijkheid van niet-Europese cloudproviders brengt ook voor de Nederlandse zorgsector zowel kansen als uitdagingen met zich mee. Uit analyse blijkt dat zorginstellingen in een complex speelveld opereren waarbij ze moeten balanceren tussen innovatiemogelijkheden van cloudtechnologie en toenemende risico's rond digitale soevereiniteit. De cloudadoptie in de zorg stijgt snel (van 27% naar verwachte 51% binnen drie jaar), maar zonder duidelijke strategie voor data-autonomie. Zorginstellingen worden geconfronteerd met juridische dilemma's door conflicterende Europese en Amerikaanse wetgeving, cyberrisico's (zoals datalekken, ransomware, DDoS aanvallen etc.), en vendor lock-in zonder eenvoudige of snel realiseerbare exit-strategie. Deze situatie vraagt om een bewuste benadering van cloudgebruik in de zorg, met duidelijke data-classificatie, multicloud-strategieën, en nauwere samenwerking tussen zorginstellingen om hun onderhandelingspositie te versterken.

De huidige stand van cloudadoptie in de Nederlandse zorgsector

De Nederlandse zorgsector bevindt zich midden in een digitale transformatie waarin cloudtechnologie een steeds prominentere rol speelt. De adoptiecurve vertoont een sterk stijgende lijn, met 76% van de mondiale healthcare-beslissers die al in meer of mindere mate cloud-platforms hebben geadopteerd - een verdubbeling ten opzichte van vorig jaar^[2]. Voor Nederlandse zorginstellingen geldt dat ongeveer 44% leert omgaan met AI-toepassingen die vaak cloudgebaseerd zijn en circa 40% al met testen bezig is^[2].

De cloud wordt in diverse varianten toegepast binnen de zorgsector. Van Software-as-a-Service (SaaS) oplossingen voor administratieve processen tot volledige infrastructuurmigraties waarbij kritische systemen zoals elektronische patiëntendossiers (EPD's) naar de cloud worden verplaatst. Gelre ziekenhuizen fungeerde hierbij als pionier door als eerste ziekenhuis in Nederland en Europa het EPD naar de Microsoft Azure-cloud te brengen^[4]. In de GGZ-sector was GGZ Breburg in 2020 de eerste instelling

die haar complete IT-infrastructuur naar het Microsoft Azure platform overbracht^[8].

Drijvende krachten achter cloudadoptie

De beweging naar de cloud wordt gedreven door verschillende factoren. Enerzijds zijn er praktische overwegingen: "Het datacenter van Breburg wordt per 1 januari 2020 opgeheven, dus zag de instelling zich genooddaakt met een nieuwe oplossing te komen", zoals beschreven in het geval van GGZ Breburg^[8]. Anderzijds zijn er strategische voordelen die zorginstellingen zien in cloudtechnologie.

Een heel belangrijke driver is natuurlijk de opkomst van e-health toepassingen. De flexibiliteit die cloudoplossingen bieden sluit goed aan bij de doelen van het Integraal Zorgakkoord (IZA), waaronder het leveren van passende zorg en het mogelijk maken van continu leren en verbeteren^[15].

Van traditionele IT naar cloudinfrastructuur

De transitie van traditionele, lokale IT-infrastructuur naar de cloud verloopt niet overal even snel. Hoewel ziekenhuizen (cure) nog last hebben van 'cloudwatervrees', wordt de cloud wel omarmd door verzorgingshuizen, GGZ-en andere instellingen die onder 'care' worden geschaard. Deze observatie wijst op een belangrijk verschil tussen verschillende types zorginstellingen, waarbij kleinere en meer flexibele organisaties sneller de stap naar de cloud zetten en SaaS sneller zullen inzetten.

Wereldwijd is er een trend naar multicloud-omgevingen. Onderzoek van leverancier van cloudtechnologie en hardware Nutanix toont aan dat "de verwachting is dat de adoptie zal stijgen van 27% naar 51% in de komende drie jaar"^[19]. Deze groei komt overeen met de wereldwijde trend om te evolueren naar multicloud-omgevingen die een mix van private en public clouds omvatten.

Potentiële voordelen van cloud-technologie voor zorginstellingen

De adoptie van cloudtechnologie brengt significante voordelen met zich mee voor zorginstellingen, variërend van operationele efficiëntie tot verbeterde zorgkwaliteit. Deze voordelen verklaren waarom steeds meer zorginstellingen de stap naar de cloud zetten.

- ▶ **Kostenefficiëntie en schaalbaarheid**
- ▶ **Geavanceerde data-analyse en AI voor betere en slimmere zorg**
- ▶ **Verbeterde gegevensuitwisseling en samenwerking**
- ▶ **Ontzorging van IT-beheer**

Kostenefficiëntie en schaalbaarheid

Een van de meest aangehaalde voordelen is kostenefficiëntie. SaaS is relatief goedkoop. De software wordt immers niet speciaal voor de zorginstelling ontwikkeld, maar deze deelt de kosten met de andere 'abbonementen'. Dit financiële aspect is belangrijk voor zorginstellingen die onder constante druk staan om zorg betaalbaar te houden.

Daarnaast biedt cloud schaalbaarheid die traditionele IT-infrastructuur niet kan evenaren. SaaS-oplossingen zijn schaalbaar. Komen er een aantal nieuwe medewerkers? Dan neem je gewoon een ruimere licentie af. Deze flexibiliteit is waardevol in een sector waar capaciteitsbehoeften kunnen fluctueren door beleidsveranderingen, fusies of crisissituaties zoals de covid-19 pandemie.

Geavanceerde data-analyse en AI voor betere en slimmere zorg

Cloudgebaseerde oplossingen maken geavanceerde analyses mogelijk die voorheen onbereikbaar waren voor veel zorginstellingen. Bijvoorbeeld het Milton Keynes Hospital in het Verenigd Koninkrijk toont hoe zij "profiteren van cloudgebaseerde geavanceerde analyse-tools voor de verwerking van grote hoeveelheden patiëntgegevens"^[15].

DOOR GEBRUIK TE MAKEN VAN DEZE TOOLS KUNNEN ZORGVERLENERS:

- ▶ Complexe analyses uitvoeren en trends identificeren op basis van uitgebreide datasets
- ▶ Voorspellende analyses uitvoeren voor ziektepreventie
- ▶ Gepersonaliseerde behandelplannen ontwikkelen

Maar ook steeds meer ziekenhuizen en zorginstellingen in Nederland constateren dat de cloud hen de flexibiliteit biedt om snel nieuwe analysemethoden te implementeren en de patiëntenzorg continu te verbeteren.

Ook wij bieden een soeverein AI-platform voor het veilig toepassen van eigen LLM's en computer vision technologie voor Nederlandse zorginstellingen, in samenwerking met UbiOps. Zo kunnen zorginstellingen op basis van hun eigen data een 'private GPT' gebruiken, die antwoorden geeft op basis van een taalmodel dat verrijkt is met de eigen gegevens van de zorginstelling.

Verbeterde gegevensuitwisseling en samenwerking

Een cruciaal voordeel in de gefragmenteerde zorgketen is de mogelijkheid om gegevens veilig uit te wisselen. "Het samenbrengen van databronnen maakt het mogelijk om medische gegevens te integreren, veilig uit te wisselen en te analyseren – en in het huidige zorgstelsel kunnen ziekenhuizen niet meer zonder dat"^[4]. Deze capaciteit sluit aan bij de doelen van het Integraal Zorgakkoord en de aankomende European Health Data Space (EHDS).

Ziekenhuizen zetten steeds meer in op "digitale zorg op afstand, ketenzorg en samenwerking met de patiënt"^[4].

De cloud maakt dit mogelijk door verschillende databronnen met elkaar te laten communiceren, wat in stand-alone systemen veel moeilijker te realiseren is.

Ontzorging van IT-beheer

Voor veel zorginstellingen betekent de overstap naar de cloud ook een verlichting van IT-beheer. Het is niet meer nodig om de software te installeren en configureren. Dat verlicht het technisch beheer. Dit voordeel is bijzonder relevant in een sector waar de focus ligt op zorgverlening en niet op IT-infrastructuur. Ook personeels- en kennisgebrek bij de zorginstelling geeft een extra 'push' om naar de cloud te gaan.

Deze ontzorging wordt geïllustreerd door de case van GGZ Breburg: "In de oude opzet liep de instelling tegen verschillende zaken aan. Van schaarse middelen tot het zelf moeten onderhouden van de hardware en een ICT-omgeving die 24/7 draaide terwijl het merendeel van de medewerkers van 8 tot 5 werkt"^[8]. De overstap naar de cloud bood de instelling meer tijd voor innovatie en het verbeteren van de werkplekervaring voor gebruikers.



"Ziekenhuizen
zetten steeds
meer in op
digitale zorg
op afstand,
ketenzorg en
samenwerking
met de patient."

Risico's en uitdagingen voor de zorgsector

Tegenover de veelbelovende voordelen van cloudtechnologie en het gebruik van (niet-Europese) public cloud providers en hyperscalers staan significante risico's en uitdagingen, die vooral in de zorgsector zwaar wegen vanwege de gevoelige aard van gezondheidsgegevens en de kritische functie van zorgsystemen.

Cybersecurity en datalekken

De zorgsector kampt met een toenemend aantal cyberaanvallen en datalekken. Onderzoek van SOTI toont aan dat "96% van de Nederlandse zorgverleners in de eerstelijnszorg sinds 2021 te maken heeft gehad met ten minste één datalek"^[10]. Deze alarmerende statistiek onderstreept de kwetsbaarheid van de sector.

De specifieke aard van deze datalekken is divers.

41% van de organisaties heeft sinds 2021 te maken gehad met een datalek door een externe bron.

Ook steeg het aantal datalekken door medewerkers met **53%**^[10].

Daarnaast rapporteert Z-CERT dat zij in 2023 **3** ransomware-aanvallen bij Nederlandse zorgaanbieders hebben geregistreerd^[11].

De gevolgen van dergelijke incidenten reiken verder dan alleen financiële schade. "Deze inbreuken gaan verder dan financiële kosten en boetes. Ze brengen niet alleen gevoelige informatie van patiënten en medewerkers in gevaar, maar kunnen ook het vertrouwen tussen patiënten en hun zorgverleners ondermijnen"^[10].

Nu is het hebben van een datalek niet per se gekoppeld aan welke cloudtechnologie gebruikt wordt. Ook is een datalek zelden toe te wijzen aan een cloudprovider. Wel is door de toegenomen complexiteit en de veelheid aan (cloud- en IT) leveranciers de kans op een datalek toegenomen. Wie weet exact nog welke data waar staat en wie er toezicht op zou moeten houden?

Regie op data als gevolg van goede dataclassificatie en het strak handhaven van informatiebeveiligingsbeleid in samenwerking en nauw overleg met leveranciers is van eminent belang.

Juridische complexiteit en geopolitieke risico's

Een fundamenteel risico voor Nederlandse zorginstellingen die gebruikmaken van niet-Europese cloudproviders betreft de juridische jurisdictie waaronder hun data valt. "De CLOUD Act maakt het mogelijk dat de federale rechtshandhaving in de Verenigde Staten technologiebedrijven via een bevelschrift of dagvaarding kan dwingen de gevraagde



gegevens van gebruikers te verstrekken, ook al zijn die gegevens opgeslagen op buitenlands grondgebied"^[14].

Deze juridische realiteit creëert een potentieel conflict met Europese wetgeving zoals de AVG/GDPR. Een juridisch expert stelt dat dit "gebruikers in conflict kan brengen met de Europese wet- en regelgeving. Praktisch gezien kunnen de consequenties nog groter zijn"^[18].

De geopolitieke dimensie van dit probleem wordt steeds relevanter. "Clouddiensten van grote techreuzen bevinden zich vaak onder Amerikaanse wet- en regelgeving, zoals de Patriot Act en CLOUD Act, waardoor gegevens mogelijk toegankelijk worden voor buitenlandse overheden. Dit vormt een risico voor de privacy en veiligheid van gevoelige medische gegevens"^[16]. Bovendien kunnen "internationale spanningen leiden tot sancties, cyberaanvallen of beperkingen die de werking van deze diensten kunnen verstoren."

Ook het stopzetten van diensten als gevolg van overheidsingrijpen of het fors verhogen van tarieven en veranderen van voorwaarden in licenties is een actueel en concreet risico, zo zien we bij ICC^[46]. De Nederlandse Bank waarschuwt hier nu ook voor bij monde van Klaas Knot. Hij wijst er op dat financiële instellingen volop gebruikmaken van digitale dienstverlening van grote Amerikaanse techbedrijven. Denk aan de opslag en beveiliging van klantgegevens. DNB waarschuwt dat betalingsverkeer in de problemen komt als de toegang tot dit soort diensten beperkt wordt^[47].

Continuïteitsrisico's en afhankelijkheid

Een van de grootste risico's voor zorginstellingen is de afhankelijkheid die ontstaat bij cloudgebruik. "Een van de grootste risico's van clouddiensten in de zorg is de afhankelijkheid van een stabiele internetverbinding. Bij een internetstoring kunnen zorginstellingen geen toegang krijgen tot cruciale patiëntendossiers, medische apparatuur die verbonden is met de cloud, of andere belangrijke systemen"^[16]. In een sector waar onderbrekingen levensbedreigende gevolgen kunnen hebben, is dit een serieus risico.

Daarnaast ontstaat er vaak een vendor lock-in situatie zonder duidelijke exit-strategie. Zoals het whitepaper over digitale

soevereiniteit van brancheorganisatie van Nederlandse cloudbedrijven DCC^[1] opmerkt: "Een clouddienst stopzetten is niet zo eenvoudig als de krant opzeggen. Je hele bedrijfsvoering is er omheen gebouwd. Je security is erop ingericht. Je data zit in een proprietary formaat dat niet heel makkelijk omgezet kan worden naar iets anders."

Kostenoverschrijdingen en verborgen uitgaven

Hoewel kostenbesparingen vaak worden aangehaald als voordeel van cloudtechnologie, blijkt de praktijk regelmatig anders. "Een offerte kan er leuk uitzien, maar de werkelijke prijs per maand kan schommelen tussen het twee- en vijfvoudige. Een ding is zeker: het zal nooit goedkoper uitkomen dan verwacht", waarschuwt DCC.

Voor Gelre ziekenhuizen bleek het kostenplaatje van het EPD in de cloud gunstiger uit te vallen dan gedacht^[4]. Toch is dit niet voor elke zorginstelling het geval: "We moeten het per individuele situatie bekijken. Als een ziekenhuis net naar een nieuw datacenter is gegaan of net een contract met een datacenterprovider heeft gesloten, dan wil die dat eerst uitnutten en wordt het een ander verhaal"^[4].

"Internationale spanningen leiden tot sancties, cyberaanvallen of beperkingen die de werking van deze diensten kunnen verstoren."

Implicaties van digitale soevereiniteit voor de zorgsector

Het concept van digitale soevereiniteit heeft verstrekkende gevolgen voor de Nederlandse zorgsector. De centrale vraag is in hoeverre zorginstellingen controle hebben en moeten hebben over hun data, systemen en digitale infrastructuur.

- ▶ Zorgsector als vitale infrastructuur
- ▶ CLOUD Act en zorginstellingen
- ▶ Balans tussen innovatie en soevereiniteit
- ▶ European Health Data Space (EHDS) en cloudgebruik

Zorgsector als vitale infrastructuur

De zorgsector kan worden beschouwd als een vitale infrastructuur die essentieel is voor het functioneren van de samenleving. Dit maakt dat zorginstellingen extra aandacht zouden moeten besteden aan digitale soevereiniteit. De covid-19 pandemie heeft dit nog eens benadrukt: onderbrekingen in zorgprocessen kunnen direct levensbedreigende gevolgen hebben.

Het beheren van patiëntgegevens brengt daarnaast een bijzondere verantwoordelijkheid met zich mee die verder gaat dan reguliere data. "Het doel van Mijn Gezondheidsoverzicht is dat iedere inwoner van Nederland toegang krijgt tot persoonlijke gegevens over de eigen gezondheid"^[20]. De vraag wie uiteindelijk controle heeft over deze gegevens is niet alleen een technische maar ook een ethische kwestie.

CLOUD Act en zorginstellingen

De Amerikaanse CLOUD Act heeft specifieke implicaties voor de zorgsector. Uit onderzoek uitgevoerd voor het NCSC blijkt: "De twee centrale vragen van dit memorandum zijn: Hoe vaak is de CLOUD Act ingeroepen voor verzoeken van persoonlijke



gegevens van EU-inwoners? En in welke mate leiden CLOUD Act-verzoeken tot onthulling van persoonlijke gegevens van EU-inwoners?"^[7]

Voor zorginstellingen die patiëntgegevens beheren is dit een cruciale vraag. Uit de studie blijkt dat het aantal verzoeken en onthullingen "in lijn zijn met de bevindingen in de gegevensbeschermingseffectbeoordeling (DPIA is korter!) uitgevoerd op Microsoft Teams door het Ministerie van Justitie en Veiligheid (SLM)"^[7]. Dit suggereert dat er daadwerkelijk gegevensverzoeken plaatsvinden onder de CLOUD Act die relevant kunnen zijn voor zorginstellingen.

Balans tussen innovatie en soevereiniteit

Zorginstellingen staan voor de uitdaging om een balans te vinden tussen het benutten van innovatieve cloudtechnologie en het behouden van digitale soevereiniteit. "De focus op continuïteit en disaster recovery stimuleert cloud-adoptie. Omdat de gezondheidszorg zwaar gereguleerd wordt, hebben organisaties de verwachting dat de adoptie zal stijgen"^[19].

Tegelijkertijd moeten zorginstellingen rekening houden met hun verantwoordelijkheid om patiëntgegevens te beschermen. "Om deze risico's te beperken, is het belangrijk dat zorginstellingen nadenken over lokale alternatieven en hybride oplossingen"^[16]. Een hybride of multicloud-strategie, zoals beschreven in het whitepaper, kan een pragmatische benadering zijn voor zorginstellingen.

European Health Data Space (EHDS) en cloudgebruik

De aanstaande European Health Data Space (EHDS) zal belangrijke implicaties hebben voor hoe zorginstellingen omgaan met cloudtechnologie. "De voorbereidingen voor implementatie zijn gestart en de eerste onderdelen uit de EHDS moeten al begin 2027 zijn gerealiseerd"^[12].

De EHDS stelt eisen aan gegevensuitwisseling in de zorg en kan derhalve de keuzes voor cloudproviders beïnvloeden. Het rapport van DigitalHealthEurope beveelt aan om "vereisten te definiëren voor cybersecurity, encryptietechnieken en anonimisering", en om "de fysieke locatie van de cloudserviceprovider in overweging te nemen", waarbij "het hebben van een in Europa gebaseerde provider van strategisch belang is"^[9].



Strategieën voor digitale soevereiniteit in de zorg

In het licht van de geschetste risico's en kansen kunnen zorginstellingen verschillende strategieën adopteren om hun digitale soevereiniteit te vergroten zonder de voordelen van cloudtechnologie te verliezen.

Multicloud-aanpak

Een multicloud-strategie, waarin diensten van verschillende cloudaanbieders worden gecombineerd, biedt zorginstellingen flexibiliteit en vermindert afhankelijkheid van één leverancier. "92% van de respondenten zegt dat eenvoudiger beheer van multi cloud-infrastructuren een voorwaarde is voor succes. Om de grootste uitdagingen, zoals interoperabiliteit, security, kosten en data-integratie, aan te pakken, is 90% het erover eens dat de hybrid multicloud het ideale IT-model is"^[19].

Voor zorginstellingen betekent dit concreet dat zij kritieke patiëntgegevens kunnen opslaan op Europese of Nederlandse clouds, terwijl ze voor minder gevoelige toepassingen gebruik kunnen maken van grote internationale providers die specifieke functionaliteiten bieden die lokaal niet beschikbaar zijn.

Data-classificatie en risicogestuurd cloudgebruik

Een belangrijke strategie is het classificeren van data naar gevoeligheid en daarop het cloudgebruik afstemmen. Niet alle zorgdata is even privacy-gevoelig, en verschillende soorten gegevens vereisen verschillende beveiligingsniveaus en soevereiniteitsoverwegingen.

Zoals het rapport van DigitalHealthEurope aanbeveelt: "Definieer vereisten voor een gemeenschappelijke benadering van elektronische contracten, inclusief geïnformeerde toestemming van burgers"^[9]. Door duidelijke kaders te stellen voor verschillende dataklassen kunnen zorginstellingen genuanceerde beslissingen nemen over

welke gegevens in welke cloud kunnen worden opgeslagen.

Samenwerkingsverbanden tussen zorginstellingen

De zorgsector kan haar collectieve positie versterken door samen te werken bij de inkoop en het gebruik van clouddiensten. Door de krachten te bundelen kunnen zorginstellingen betere voorwaarden bedingen bij cloudproviders en gezamenlijk investeren in oplossingen die digitale soevereiniteit waarborgen.

Branchevereniging DCC suggereert bijvoorbeeld een "bijkorf model, waarmee de overheid via één loket toegang heeft tot een aantal bedrijven, waarvan het de garantie heeft dat ze voldoen aan een aantal van tevoren gedefinieerde eisen." Een vergelijkbaar model zou kunnen worden ontwikkeld specifiek voor de zorgsector.

Investerings in lokale en Europese cloud-alternatieven

De zorgsector kan bijdragen aan het versterken van Europese cloud-alternatieven door gericht te investeren in lokale oplossingen. Het EU4Health programma, met een budget van €5,3 miljard^[6], biedt mogelijkheden om Europese cloudoplossingen voor de zorgsector te ontwikkelen.

Zoals de DCC verderop nog stelt: "Als wij inderdaad van mening zijn dat het wél belangrijk is dat Nederland een koploper moet blijven en dat Europa een serieuze tech-sector nodig heeft, dan moeten wij accepteren dat die keuze consequenties heeft en dat de eerste daarvan is dat de belangrijkste en grootste klant zijn boodschappen waar mogelijk bij de eigen sector doet."

"90% is het erover eens dat de hybrid multicloud het ideale IT-model is"

Praktische handvatten voor zorginstellingen

Voor zorginstellingen die hun cloudstrategie willen heroverwegen in het licht van digitale soevereiniteit, zijn de volgende praktische handvatten relevant.

Bewuste cloud-strategie ontwikkelen

ZORGINSTELLINGEN DOEN ER GOED AAN EEN BEWUSTE CLOUDSTRATEGIE TE ONTWIKKELEN WAARIN SOEVE-REINITEITSASPECTEN EXPLICIET WORDEN MEEGENOMEN. DIT BETEKENT:

1. Een brede vertegenwoordiging bij de strategieontwikkeling, inclusief zorgprofessionals, IT-specialisten, juridische experts en bestuurders
2. Expliciete afweging van verschillende cloudmodellen: private, public of hybride
3. Inventarisatie van gevoelige en minder gevoelige data en processen
4. Vaststellen van minimale eisen rond soevereiniteit voor verschillende typen data

Uitvoeren van gedegen risicoanalyse

Voordat clouddiensten worden afgenomen, is een gedegen risicoanalyse essentieel. Het rapport van de Algemene Rekenkamer concludeerde dat "bij twee derde van de afgenomen diensten nooit een risico-analyse heeft plaatsgevonden, zelfs niet voor cruciale diensten zoals die van de Belastingdienst of paspoortuitgaven". Zorginstellingen kunnen leren van deze observatie.

EEN RISICOANALYSE ZOU MINIMAAL MOETEN OMVATTEN:

- ▷ Beoordeling van impact bij dataverlies of -lek
- ▷ Scenario's voor systeemuitval en continuïteitsmaatregelen
- ▷ Evaluatie van juridische risico's, inclusief conflicten tussen jurisdicties
- ▷ Vendor lock-in risico's en exit-mogelijkheden

Ontwikkelen van exit-strategieën

Wij benadrukken hier ook het belang van exit-strategieën, wat bijzonder relevant is voor zorginstellingen. In samenwerking tussen de overheid en de Nederlandse cloudbedrijven kunnen Nederlandse service providers helpen met een inventarisatie van de behoeften, en op basis daarvan omgevingen creëren waarin de continuïteit van de dienstverlening geborgd kan worden."

PRAKTISCHE ELEMENTEN VAN EEN EXIT-STRATEGIE VOOR ZORGINSTELLINGEN OMVATTEN:

- ▷ Regelmatige databack-ups in standaard, overdraagbare formaten
- ▷ Documentatie van systeemconfiguraties en workflows
- ▷ Contractuele bepalingen die dataportabiliteit en autonomie garanderen
- ▷ Periodieke tests van de overstap naar alternatieve systemen
- ▷ Reeds bij het aangaan van het contract bepalen hoe de exit zou werken en wie er voor de kosten opdraait

Contractuele waarborgen en certificeringen

BIJ HET AANGAAN VAN CONTRACTEN MET CLOUD-PROVIDERS KUNNEN ZORGINSTELLINGEN SPECIFIEKE WAARBORGEN OPNEMEN DIE DIGITALE SOEVE-REINITEIT BEVORDEREN:

- ▷ Transparantie over datalokalisiteit en gegevensstromen
- ▷ Duidelijke procedures bij verzoeken van buitenlandse autoriteiten
- ▷ Compliance met zorgspecifieke normen zoals NEN 7510 en toekomstige Europese normen op dit specifieke onderwerp
- ▷ Garanties voor ondersteuning bij een eventuele migratie naar andere providers

Verder kan er gewerkt worden aan "een raamovereenkomst waar Nederlandse (en eventueel Europese) bedrijven op in kunnen tekenen, zodat overheidsinstanties niet telkens nieuwe onderhandelingen hoeven aan te gaan om diensten af te nemen bij de eigen industrie." Een vergelijkbare aanpak zou voor zorginstellingen waardevol kunnen zijn.

Conclusie en toekomstperspectief

De Nederlandse zorgsector staat voor een cruciale uitdaging wat betreft cloudadoptie en digitale soevereiniteit. De balans vinden tussen innovatiekracht en onafhankelijkheid, tussen efficiëntie en controle, is geen eenvoudige opgave. Tegelijkertijd is het een noodzakelijke die bepalend zal zijn voor de toekomstbestendigheid van onze zorgsector.

Balanceren tussen innovatie en controle

De zorg heeft cloud nodig om te innoveren en te voldoen aan de groeiende vraag naar efficiëntere en effectievere zorg. Zoals onderzoek aantoont, heeft de cloud "het potentieel de Nederlandse zorgsector te transformeren door innovatieve en efficiënte zorgoplossingen te bieden die aansluiten bij de doelen van het IZA"^[5]. Tegelijkertijd moet de zorgsector waakzaam blijven over wie uiteindelijk controle heeft over essentiële zorgdata en -systemen.

Van onbewust naar bewust cloudgebruik

De huidige situatie lijkt zich te kenmerken door een situatie die "nooit beleidsmatig als zodanig is besloten" maar "organisch is ontstaan". Voor de zorgsector betekent dit dat er een transitie nodig is van onbewust naar bewust cloudgebruik, waarin digitale soevereiniteit een expliciete afweging wordt.

Deze transitie vereist een combinatie van betere bewustwording, concrete richtlijnen, samenwerkingsverbanden binnen de sector, en ondersteuning vanuit beleidsmakers. De komst van de EHDS biedt een kans om deze discussie te verdiepen en gezamenlijke kaders te ontwikkelen.

Naar een duurzaam Europees zorg-cloudecosysteem

Op de lange termijn zou de zorgsector kunnen bijdragen aan het versterken van het Europese cloud-ecosysteem door strategische investeringen en gerichte samenwerking. Het EU4Health programma biedt hiervoor mogelijkheden, evenals nationale innovatiefondsen.

Door te investeren in lokale oplossingen en te kiezen voor Europese providers waar mogelijk, kan de zorgsector bijdragen aan het creëren van "een situatie waarin de sector kan groeien, verder kan innoveren, onderwijs en onderzoek kan aantrekken en uiteindelijk op steeds meer fronten een aantrekkelijk alternatief voor de Amerikaanse hyperscalers kan bieden."

De zorgsector heeft een unieke positie en verantwoordelijkheid in het digitale soevereiniteitsdebat. Door nu bewuste keuzes te maken, kan zij bijdragen aan een toekomstbestendig, innovatief én soeverein digitaal zorglandschap in Nederland en Europa.



Aanbevelingen voor beleidsmakers

Om zorginstellingen te ondersteunen bij het navigeren van deze complexe uitdagingen, zijn gerichte beleidsinterventies noodzakelijk.

Ontwikkelen van zorgspecifieke soevereiniteitskaders

Beleidsmakers zouden in samenwerking met de zorgsector specifieke kaders kunnen ontwikkelen voor digitale soevereiniteit in de zorg. Deze kaders zouden rekening moeten houden met de specifieke kenmerken van zorgdata en -processen, en praktische handvatten moeten bieden voor verschillende typen zorginstellingen.

Er dient apart aandacht te zijn voor de verwerking van bijzondere persoonsgegevens in AI-platforms, zeker wanneer deze door niet-Europese leveranciers worden beheerd. Zoek naar Europese alternatieven of investeer in een eigen 'private AI platform', bijvoorbeeld voor het gebruik van LLM's.

Stimuleren van innovatie in Europese zorg-cloudoplossingen

Via gerichte subsidieprogramma's en innovatiefondsen kunnen beleidsmakers de ontwikkeling van Europese cloudoplossingen specifiek voor de zorgsector stimuleren. Het EU4Health programma biedt hiervoor een kader, maar aanvullende nationale initiatieven kunnen dit versterken.

Faciliteren van kennisdeling en samenwerking

Beleidsmakers kunnen platforms creëren voor kennisdeling tussen zorginstellingen over cloud-adoptie en digitale soevereiniteit. Door best practices te delen en gezamenlijk problemen aan te pakken, kan de sector als geheel sneller leren en evolueren.

De uitdagingen van cloudadoptie en digitale soevereiniteit in de zorgsector vereisen een gezamenlijke aanpak van zorginstellingen, cloudproviders en beleidsmakers. Alleen door samen te werken kunnen we een zorgsysteem creëren dat zowel innovatief als soeverein is, en dat de privacy en veiligheid van patiëntgegevens waarborgt terwijl het de mogelijkheden van cloudtechnologie ten volle benut.





Gebruikte bronnen

Alle bronnen zijn terug te vinden op de website van Intermix.
Bekijk de pagina door de knop te volgen.



www.intermix.nl/whitepaper-digitale-soevereiniteit-in-het-nederlandse-zorglandschap-referenties



ISA E 3402 TYPE II &
SOC2 ASSURANCE

Contact

Intermax

Schouwburgplein 30 – 34
3012 CL Rotterdam
+31(0) 10 – 710 4444
info@intermax.nl

2025 © Intermax Cloudsourcing B.V.

Over Intermax

Het is onze missie de IT van maatschappelijk cruciale organisaties beschikbaar en veilig te houden. De techniek die we daarvoor gebruiken is niet uniek – de manier waarop we de techniek inzetten voor onze klanten wel. Dat begint met onze focus op het aangaan van die langetermijnrelaties met onze klanten. We kennen onze klanten persoonlijk; we kennen het verhaal achter hun organisatie, maar ook de mensen die er het werk doen. Met aandacht zoeken we uit wat hen beweegt, wat hun belangen zijn en welke uitdagingen ze hebben. Dit stelt ons in staat hen nog beter te helpen. Dat is al 30 jaar de Intermax Manier.