WHITEPAPER | 2026

Digitale soevereiniteit in het Nederlandse zorglandschap.

intermax

Inhoudsopgave

Digitale soevereiniteit in het Nederlandse zorglandschap.

Managementsamenvatting

De digitale infrastructuur van jouw zorginstelling maakt waarschijnlijk gebruik van Amerikaanse cloudtechnologie. Dat is geen vergissing. Het is het logische gevolg van jarenlange innovatie en schaalvoordelen van deze providers. Maar het betekent wel dat je afhankelijkheden hebt geaccepteerd die je mogelijk nooit bewust hebt afgewogen.

Het publieke debat over digitale soevereiniteit wordt gedomineerd door alarmerende koppen en politieke stellingname. Dit whitepaper biedt wat daarin ontbreekt: een nuchter kader voor zorginstellingen, gebaseerd op feiten en praktijkvoorbeelden.

Drie inzichten die je niet in de krant leest:

Je risico hangt af van je inrichting, niet van het label 'cloud'. De CLOUD Act, het meest besproken risico, is alleen relevant wanneer een provider daadwerkelijk toegang heeft tot je data. Bij een EPD dat op Azure-infrastructuur draait met eigen encryptiesleutels ziet Microsoft alleen versleutelde bestanden. Dat is een fundamenteel ander risicoprofiel dan e-mail in Microsoft 365. Die nuance ontbreekt vrijwel volledig in het publieke debat.

Meer autonomie betekent meer verantwoordelijkheid. Elke stap richting eigen beheer verlaagt je privacyrisico, maar verhoogt de eisen aan je eigen security en operationele capaciteit. Zowel Amerikaanse als Nederlandse Cloudproviders investeren in beveiliging op een niveau dat een zorginstelling niet kan evenaren. De scenariotabel in dit whitepaper maakt per hostingvariant zichtbaar wat je wint én wat je opgeeft.

Volledige onafhankelijkheid bestaat niet. De mondiale IT-keten zit vol wederzijdse afhankelijkheden: van Taiwanese chips tot Chinese zeldzame aardmetalen tot Nederlandse ASML-machines. De vraag is niet hoe je volledig onafhankelijk wordt, maar voor welke diensten en data je bewust een ander pad kiest.

Dit whitepaper sluit af met vijf concrete acties. Drie daarvan kun je morgen al starten: breng je dienstenlandschap in kaart met het drielagenmodel, stel bij de eerstvolgende contractverlenging de juiste vragen over exit-clausules en dataportabiliteit, en zoek aansluiting bij collega-instellingen om gezamenlijk sterker te staan.

Over de schrijvers

Ludo Baauw is oprichter en Group CEO van Intermax Group en regelmatig in de media en politiek te zien als expert op het gebied van digitale autonomie, soevereiniteit en cybersecurity. Ludo zag jaren geleden dat afhankelijkheid een strategisch risico is en heeft toen maatregelen genomen om autonoom te ondernemen. Zo was Intermax één van de eerste IT-bedrijven die een eigen, Nederlandse cloud voor vitale organisaties, verdeeld over meerdere datacenters had.

Ludo Baauw

Sander Winthagen is Managing Director van Intermax. Met zijn brede kennis en expertise bij verschillende internationale bedrijven in de cloud- en hostingsector biedt hij een genuanceerde en nuchtere kijk op de huidige cloudsituatie. Sander staat bekend om zijn persoonlijke en pragmatische aanpak, innovatieve werkwijze en heldere visie op IT.

Sander Winthagen

Inleiding

Een zorginstelling heeft in essentie één opdracht: bijdragen aan de gezondheid, het herstel of de kwaliteit van leven van de mensen die zij bedient. De vorm verschilt per ziekenhuis, revalidatiecentra of andere vormen van zorg, maar de kern is overal dezelfde: de mens centraal, niet de instelling.

Alles wat een zorginstelling doet staat in dienst van die opdracht. Of het nu een opname van enkele dagen is of een jarenlange zorgrelatie, jouw zorginstelling wil de best mogelijke ervaring bieden. Niet alleen omdat dat menselijk is, maar ook omdat we weten dat het bijdraagt aan herstel en welbevinden.

De dagelijkse uitdagingen om die opdracht waar te maken zijn al enorm. Financiële druk om zorg betaalbaar te houden. Personeelstekorten die steeds nijpender worden. Het voorkomen van infecties, medicatiefouten en verkeerde behandelbeslissingen. Het verhogen van diagnostische nauwkeurigheid en de kwaliteit van zorgplannen. Dát is waar de aandacht en het budget naartoe gaat, en terecht.

IT en cloudtechnologie beloven hier enorm bij te helpen. AI-gestuurde diagnostiek die de arts ondersteunt. Efficiëntere bedrijfsvoering die schaarse middelen vrijmaakt. Betere gegevensuitwisseling in de keten die de patiënt ten goede komt. E-health toepassingen die zorg op afstand mogelijk maken. De cloud maakt dingen mogelijk die vijf jaar geleden ondenkbaar waren, en zorginstellingen stappen daar logischerwijs in.

En dan komt er nog een thema op je bord: digitale soevereiniteit. Met het aantreden van het kabinet-Jetten en een historisch hoofdstuk over digitalisering in het coalitieakkoord is het onderwerp verheven van beleidsdiscussie tot regeringsprioriteit. De kernvragen zijn simpel: waar staat jouw data, wie kan erbij, welke regels gelden daar, en kun je er te allen tijde bij?

De verleiding is groot om digitale soevereiniteit laag op de agenda te zetten. Er zijn urgentere dossiers die direct om aandacht vragen. En voor een deel is dat ook een verdedigbare keuze. Kies je voor meer budget naar extra middelen binnen de zorginstellingen, extra personeel e.d., of verbeterde informatiebeveiliging?

We snappen het wel. Maar soevereiniteit is geen doel op zich; het is risicomanagement. En risicomanagement is iets wat zorginstellingen elke dag doen. Je weegt infectierisico's, operatierisico's, financiële risico's. Soevereiniteitsrisico's horen in diezelfde afweging thuis: niet bovenaan, niet onderaan, maar op de plek die past bij de waarschijnlijkheid en de impact.

Dit whitepaper helpt je daarbij. Het biedt bestuurders en IT-verantwoordelijken in de zorgsector een helder overzicht van wat digitale soevereiniteit concreet betekent voor jouw instelling, welke risico's reëel zijn en welke overdreven, en welke maatregelen verstandig zijn zonder dat ze een fortuin kosten. Na het lezen beschik je over de kennis om gefundeerde keuzes te maken. Keuzes die passen bij een organisatie die haar schaarse middelen wil inzetten waar ze het meeste verschil maken: bij de patiënt.

1. Digitale soevereiniteit en digitale autonomie

Wat is digitale soevereiniteit?

Over het begrip digitale soevereiniteit bestaat brede consensus: het betreft 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.

Het verschil met 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. Concreet: weten waar je data staat, bepalen wie erbij kan, en de mogelijkheid hebben om van leverancier te wisselen als dat nodig is.

Digitale autonomie als beleidskeuze

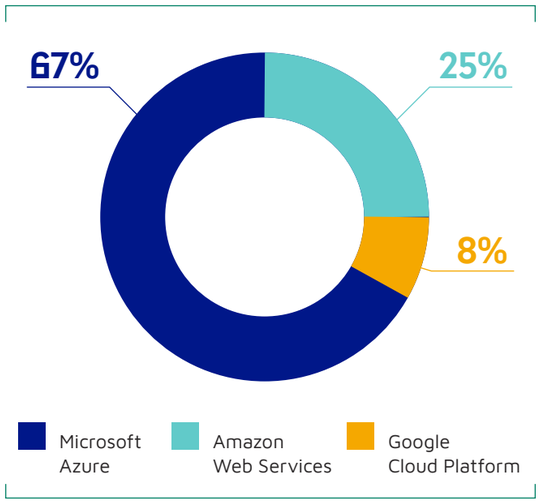
Het kabinet-Jetten kiest bewust voor de term 'digitale autonomie' boven 'digitale soevereiniteit'. Waar soevereiniteit een absoluut begrip is, erkent autonomie een spectrum: Nederland kan geleidelijk autonomer worden in het digitale domein. Het coalitieakkoord spreekt van het 'doelgericht afbouwen' van strategische afhankelijkheden, niet van een radicale breuk met bestaande leveranciers.

2. Het debat en de context

De achtergrond: Amerikaanse dominantie

De Nederlandse cloudmarkt wordt gedomineerd door Amerikaanse leveranciers. Microsoft Azure neemt 67% van de public cloud-markt in, Amazon Web Services (AWS) volgt met 25% en Google Cloud Platform (GCP) heeft 8%. De technologie, functionaliteit en schaal van hun dienstverlening is op dit moment ongeëvenaard; het resultaat van jarenlange miljarden-investeringen in datacenters en AI-infrastructuur.

Die dominantie heeft geleid tot een stevig maatschappelijk debat. Het Draghi-rapport over Europese concurrentiekracht, de initiatiefnota 'Wolken aan de horizon' en het Rekenkamer-rapport 'het Rijk in de Cloud' schetsen stuk voor stuk een beeld van te grote afhankelijkheid. De discussie die hierover is ontstaan volg je waarschijnlijk al volop in de media. Waar het in dit whitepaper om gaat is: welke nuances mist dat debat, en wat betekent het concreet voor jouw instelling?



Nuances die ertoe doen

Bij de discussie over cloudafhankelijkheid passen enkele belangrijke nuances die in het publieke debat onderbelicht blijven:

- De cloud maakt je niet kwetsbaar, maar de inrichting van je IT-omgeving wel.
- Europese sovereign clouds van hyperscalers: een zinvolle tussenstap, geen volledige oplossing.
- Keuzevrijheid is er, maar volledige onafhankelijkheid bestaat nergens.
- De rode knop is er helemaal niet, het zijn meerdere kleine hendeltjes.

De cloud maakt je niet kwetsbaar, maar de inrichting van je IT-omgeving wel. De CLOUD Act geeft Amerikaanse autoriteiten de bevoegdheid om data op te vragen bij Amerikaanse techbedrijven, maar alleen wanneer die provider de data daadwerkelijk in bezit, bewaring of controle heeft. Die technische toegang verschilt fundamenteel per scenario. Gebruik je Microsoft 365 voor e-mail? Dan kan Microsoft aan een order voldoen. Draai je een eigen applicatie op Azure-infrastructuur met eigen encryptiesleutels (customer-managed keys)? Dan ziet Microsoft versleutelde data, maar biedt het nog geen 100% garantie dat Microsoft niet bij de gegevens kan. En host je je e-mail zelf op een eigen Exchange-server in een eigen datacenter? Dan is Microsoft puur een softwareleverancier zonder enige toegang tot je data. Een CLOUD Act-order levert dan niets op. Jouw inrichting bepaalt dus in grote mate jouw risicoprofiel. In hoofdstuk 3 werken we drie scenario's uit die elk een andere risicoafweging vragen.

Europese sovereign clouds van hyperscalers: een zinvolle tussenstap, geen volledige oplossing. Initiatieven zoals de European Sovereign Cloud van AWS en soortgelijke programma's van Microsoft en Google draaien volledig in Europa: Europees personeel, Europese datacenters, Europese operatie. Dat neemt reële risico's weg. Bij een verstoring van transatlantische internetverbindingen blijven de diensten beschikbaar. En in een extreem scenario biedt het Europese overheden de theoretische mogelijkheid om de Europese operatie van deze hyperscalers onder eigen jurisdictie te brengen. Maar is wel degelijk een risico aan verbonden. Voor diensten die de provider namens jou beheert, zoals e-mail of collaboratiesoftware, blijft het moederbedrijf onderworpen aan Amerikaans recht. Een CLOUD Act-order aan het hoofdkantoor in de VS maakt niet halt bij de grens van de Europese operatie. De zogeheten soevereine cloud van hyperscalers is daarmee een zinvolle tussenstap voor bepaalde workloads, maar geen volledige oplossing voor het jurisdictievraagstuk.

Keuzevrijheid is er, maar volledige onafhankelijkheid bestaat nergens. De mondiale IT-keten zit vol wederzijdse afhankelijkheden: Amerikaanse cloudproviders draaien op chips die voornamelijk in Taiwan worden geproduceerd, chipfabrikanten zijn afhankelijk van zeldzame aardmetalen die grotendeels in China worden geraffineerd, en diezelfde chipfabrikanten kunnen niet zonder de lithografiemachines van het Nederlandse ASML. Voor elk land en bedrijf is volledige digitale onafhankelijkheid in die context een illusie. Wat wél realistisch is: bewuste keuzes maken per dienst. Voor hosting, opslag, backup en specifieke applicaties bestaan volwassen Europese en Nederlandse alternatieven. Voor collaboratiesoftware, AI-platformen of gespecialiseerde SaaS-tools zijn de hyperscalers voorlopig zonder realistisch alternatief. De vraag is daarom niet "hoe word ik volledig onafhankelijk?" maar "voor welke diensten en data kies ik bewust een ander pad, en waar accepteer ik de afhankelijkheid?"

De rode knop is er helemaal niet, het zijn meerdere kleine hendeltjes. In het publieke debat wordt gewaarschuwd voor het scenario waarin de Amerikaanse overheid Europese cloudregio's in één keer uitzet. Dat is om twee redenen zeer onwaarschijnlijk

Ten eerste het economische zelfbelang: Microsoft alleen al genereert naar schatting meer dan $25 miljard per jaar aan cloudrevenue uit Europa. Geen enkel Amerikaans bedrijf vernietigt vrijwillig tientallen miljarden aan jaaromzet. In ieder geval niet zonder enige gevolgen.

Ten tweede de escalatielogica: het platleggen van digitale infrastructuur waarop Europese ziekenhuizen, overheden en bedrijven draaien, zou neerkomen op een digitale oorlogshandeling. In zo'n scenario kan Europa niet anders dan met volledige tegensancties reageren, denk

aan nationalisatie van Europese datacenters, bevriezing van intellectueel eigendom en het beëindigen van alle handelsrelaties met de Amerikaanse techsector. Het is zeer onwaarschijnlijk dat een Amerikaanse regering een dergelijk scenario zal triggeren.

Toen AI-bedrijf Anthropic weigerde veiligheidsbeperkingen op zijn modellen te verwijderen voor het Pentagon, bestempelde de Amerikaanse overheid het bedrijf binnen dagen als "supply chain risk" en kregen alle federale instanties opdracht per direct te stoppen met het gebruik van hun technologie. Niet vanwege een zakelijk geschil, maar omdat het bedrijf politiek botste met de defensieagenda van de Trump-administratie. De boodschap is helder: technologische afhankelijkheid wordt een hefboom zodra er politieke druk ontstaat. De vraag voor zorginstellingen is niet óf dit mechanisme ook bij cloudproviders kan spelen, maar hoe kwetsbaar je eigen inrichting je maakt wanneer dat gebeurt. In hoofdstuk 3 werken we die risico's concreet uit.

Wat komt eraan: beleid dat jou raakt

Het kabinet-Jetten heeft digitale soevereiniteit voor het eerst tot regeringsprioriteit verheven. Ongekend in de Nederlandse politiek is dat het coalitieakkoord een volledig hoofdstuk bevat over digitalisering. Het kabinet erkent expliciet dat Nederland te afhankelijk is geworden van een aantal buitenlandse techbedrijven. Digitale autonomie wordt het leidende principe voor alle nieuwe overheids-ICT. Met de aanstelling van staatssecretaris Willemijn Aerdts (D66) voor Digitale Economie en Soevereiniteit en de oprichting van de Nederlandse Digitale Dienst (NDD), een centrale organisatie met doorzettingsmacht over rijksbrede IT-inkoop, wordt dit beleid ook institutioneel verankerd.
Hoewel het coalitieakkoord zich primair richt op de rijksoverheid, werken de nieuwe standaarden en eisen onvermijdelijk door naar de zorgsector. De concrete maatregelen die voor zorginstellingen relevant zijn:

- Europese infrastructuur als uitgangspunt: De overheid kiest nadrukkelijk voor Europese digitale infrastructuur bij nieuwe projecten.
- Soevereiniteit als inkoopeis: Aanbesteding wordt gecentraliseerd, met security-by-design, zero trust, open source en soevereiniteit als leidende principes.
- Toetsing van grote projecten: IT-projecten van meer dan €5 miljoen worden vooraf getoetst aan centrale IT-standaarden.
- Nationale stresstests: Er komt een framework om afhankelijkheden van buitenlandse cloudproviders te testen. Tech-expert Bert Hubert spreekt van een "Microsoft-out oefening" om te kijken wat er nog functioneert als Amerikaanse cloudproviders wegvallen.

De financiering blijft overigens een aandachtspunt: in de budgettaire tabel van het coalitieakkoord zijn geen structurele middelen voor digitalisering opgenomen, terwijl de geschatte kosten voor de Nederlandse Digitaliseringsstrategie circa €950 miljoen bedragen.

Cloud in de zorgsector: de huidige stand van zaken

De Nederlandse zorgsector zit al volop in de cloud en dat gaat niet meer terug. De cloud wordt in diverse varianten toegepast: van SaaS-oplossingen voor administratieve processen tot volledige infrastructuurmigraties. Gelre ziekenhuizen fungeerde als pionier door als eerste ziekenhuis in Nederland het EPD naar Microsoft Azure te brengen. Inmiddels draaien volgens Chipsoft ten minste drie Nederlandse ziekenhuizen hun volledige EPD in de Azure-cloud. In de GGZ-sector was GGZ Breburg in 2020 de eerste instelling die haar complete IT-infrastructuur naar Azure overbracht, deels uit noodzaak, omdat het eigen datacenter werd opgeheven.

De beweging wordt gedreven door zowel praktische als strategische overwegingen. Cloudoplossingen bieden flexibiliteit en functionaliteit die aansluit bij de doelen van het Integraal Zorgakkoord (IZA): passende zorg, efficiëntere bedrijfsvoering en betere gegevensuitwisseling. Tegelijkertijd werken de beleidsmaatregelen uit het coalitieakkoord onvermijdelijk door naar de zorgsector: zorginstellingen die publieke taken uitvoeren krijgen te maken met soevereiniteit, security-by-design en zero trust als leidende inkoopcriteria. De vraag is niet meer óf de zorg de cloud gebruikt, maar hóe, en met welke waarborgen.

De vraag is niet meer óf de zorg de cloud gebruikt, maar hoe.

3. Risico's en uitdagingen

Als bestuurder of IT-verantwoordelijke manage je dagelijks een breed palet aan risico's. Infectiepreventie, medicatieveiligheid, personeelscapaciteit, financiële continuïteit, brandveiligheid; het zijn stuk voor stuk thema's die structurele aandacht vragen en waar beproefde raamwerken voor bestaan. Digitale soevereiniteit is geen fundamenteel ander type vraagstuk: het is een extra risicocategorie die in datzelfde raamwerk thuishoort. De vraag is niet of je er aandacht aan besteedt, maar hoeveel. En dat hangt af van de waarschijnlijkheid en de impact, precies zoals bij elk ander risico.
Wat de discussie lastig maakt is dat er in het publieke debat twee fundamenteel verschillende risico's door elkaar lopen:

- Privacyrisico: kan iemand ongeoorloofd bij mijn data?
- Continuïteitsrisico's: kan mijn dienstverlening van buitenaf worden verstoord?
- Systeemrisico's: in het debat onderbelicht, maar voor de zorgsector misschien wel het meest relevant. Door concentratie bij een beperkt aantal providers ontstaat er een systeemrisico.

A. Privacyrisico's: wie kan bij jouw data?

De kernvraag bij privacyrisico's is: kunnen buitenlandse overheden of inlichtingendiensten toegang krijgen tot persoonsgegevens die jouw organisatie beheert, en zo ja, met welke juridische waarborgen?

Het Amerikaanse wettelijke kader

Nederlandse zorginstellingen die gebruikmaken van Amerikaanse cloudproviders worden geconfronteerd met drie elkaar overlappende Amerikaanse wettelijke kaders die toegang tot hun data mogelijk maken: De CLOUD Act, FISA Section 702 en Executive Order 12333.

De CLOUD Act maakt het mogelijk dat de federale rechtshandhaving in de VS technologiebedrijven kan dwingen gevraagde gegevens van gebruikers te verstrekken, ook al zijn die gegevens opgeslagen op buitenlands grondgebied. Belangrijk: dit geldt alleen voor data die de techprovider daadwerkelijk in bezit, bewaring of controle heeft. Verderop in dit hoofdstuk werken we uit wat dat concreet betekent voor verschillende typen IT-omgevingen. In juni 2025 bevestigde Microsoft deze realiteit onder ede voor een Franse rechtbank: het bedrijf gaf toe dat het digitale soevereiniteit niet kan garanderen voor diensten die het beheert, als de Amerikaanse overheid via de CLOUD Act toegang eist. Uit het transparantierapport van Microsoft over de tweede helft van 2024 blijkt dat Amerikaanse opsporingsdiensten 59 bevelschriften hebben uitgegeven voor content-data die buiten de VS was opgeslagen. Dit zijn geen theoretische scenario's meer, het gebeurt echt.

FISA Section 702 autoriseert Amerikaanse inlichtingendiensten om zonder individueel rechterlijk bevel de elektronische communicatie te verzamelen van niet-Amerikaanse personen buiten de VS, en dat is inclusief alle Europese burgers en organisaties. Bij de laatste verlenging in 2024 werd het toepassingsbereik significant uitgebreid: vrijwel alle cloudproviders, datacenters en IT-dienstverleners vallen nu onder het bereik. FISA 702 maakt geen onderscheid naar type data: medische gegevens, financiële informatie en persoonlijke communicatie vallen allen onder hetzelfde regime.

Het minst bekende instrument is Executive Order (EO) 12333 uit 1981. Dit presidentieel decreet autoriseert de National Security Agency (NSA) om buitenlandse "signals intelligence" te verzamelen, inclusief data die via onderzeese kabels de Atlantische Oceaan oversteekt. Anders dan de CLOUD Act en FISA vereist EO 12333 geen rechterlijke toetsing. Het Europees Hof van Justitie oordeelde in het Schrems II-arrest dat EO 12333 niet verenigbaar is met Europees recht. Voor zorginstellingen betekent dit concreet: zelfs wanneer patiëntgegevens op servers in de EU staan, kunnen deze worden onderschept zodra ze via trans-Atlantische verbindingen worden verstuurd.

Belangrijk: Amerikaanse wetgeving maakt geen uitzondering voor medische gegevens. Waar de AVG/GDPR bijzondere bescherming biedt aan gezondheidsdata als "bijzondere categorie persoonsgegevens", kent het Amerikaanse rechtssysteem geen vergelijkbare bescherming tegen inlichtingenverzoeken.

De CLOUD Act in de praktijk: wat betekent dit voor jouw zorginstelling?

De CLOUD Act wordt in het publieke debat vaak gepresenteerd alsof de Amerikaanse overheid met één druk op de knop bij alle data kan die op Azure staat. Dat beeld verdient nuancering. Een order onder de CLOUD Act moet aan strikte voorwaarden voldoen:

- het moet gaan om de opsporing of preventie van ernstige criminaliteit (inclusief terrorisme).
- de order moet een specifiek persoon, account of apparaat identificeren (een "fishing expedition" door een complete database is dus niet toegestaan).
- er moet een rechterlijke toetsing aan voorafgaan.
- de order moet voldoen aan het binnenlandse recht van het uitvaardigende land.

Bovendien heeft de ontvangende techprovider het recht om de order aan te vechten, met name wanneer er een conflict ontstaat met het recht van het land waar de klant is gevestigd.

Minstens zo belangrijk is het technische onderscheid tussen wat een provider wél en niet kan overhandigen. Om dit scherp te krijgen, helpt het om drie scenario's naast elkaar te leggen:

Scenario 1: Microsoft-beheerde clouddiensten (hoogste blootstelling). Microsoft beheert als Online Service Provider bepaalde diensten direct: Exchange Online (e-mail), Microsoft Teams (chat en vergaderingen), OneDrive en SharePoint (bestanden), en Entra ID (identiteitsbeheer). Bij deze diensten heeft Microsoft technisch toegang tot de inhoud. Een CLOUD Act-order gericht op het e-mailverkeer van een specifieke ziekenhuismedewerker, bstuurder of IT-medewerker, bijvoorbeeld omdat die persoon verdacht wordt van een ernstig misdrijf, is technisch gezien uitvoerbaar: Microsoft kan die mailbox openen en de inhoud leveren.

Scenario 2: Eigen applicaties op Azure-infrastructuur (beperkte blootstelling). Een EPD-systeem zoals HiX van Chipsoft dat op Azure draait is een fundamenteel ander verhaal. Dat systeem gebruikt Azure als infrastructuur (bijv. voor rekenkracht en opslag), maar de data zit in een applicatiedatabase die door Chipsoft en het ziekenhuis wordt beheerd. Microsoft levert de virtuele machines en de opslagcapaciteit, maar heeft geen inhoudelijke toegang tot de applicatielaag. Wat Microsoft ziet zijn versleutelde blobs, geen patiëntendossiers. Om bij die data te komen is niet alleen een order aan Microsoft nodig, maar ook medewerking van de applicatieleverancier en mogelijk het ziekenhuis zelf. Als het ziekenhuis bovendien eigen encryptiesleutels beheert, dan wordt het technisch een stuk moeilijker, maar biedt het echter geen garantie.

Scenario 3: Zelf gehoste software in een eigen of gehuurd datacenter (geen blootstelling). Draai je bijvoorbeeld je eigen Exchange-server in je eigen datacenter of in een gehuurd rack bij een Nederlands datacenterbedrijf? Dan is Microsoft puur een softwareleverancier: ze leveren je een licentie, maar ze hosten en beheren je data niet. Een CLOUD Act-order aan Microsoft levert in dat geval niets op, want Microsoft heeft de data niet "in bezit, bewaring of controle". En dat is de wettelijke voorwaarde om aan een order te kunnen voldoen. Het zelf hosten van diensten elimineert het CLOUD Act-risico voor die specifieke dienst volledig.

Een veelgehoorde zorg is of je blootgesteld bent aan de CLOUD Act als je servers staan in een datacenter dat eigendom is van een Amerikaans bedrijf, zoals bijvoorbeeld Equinix. Het korte antwoord: nee, niet op een manier die hout snijdt. Een CLOUD Act-order vereist dat de ontvanger de gevraagde data kan identificeren en overhandigen. Een co-locatieprovider die je rackruimte en stroom levert weet niet welke data op jouw servers staat, kan niet in je versleutelde schijven kijken, en heeft geen idee of er gegevens van een specifiek persoon op staan. Een order die zegt "geef ons de e-mails van persoon X" is aan een colocatieprovider simpelweg niet uitvoerbaar.

De praktische les: jouw CLOUD Act-blootstelling is geen vast gegeven. Je bepaalt die grotendeels zelf door de keuzes die je maakt in de inrichting van je IT-omgeving.

- Welke diensten neem je af als SaaS (waar de provider bij je data kan)?
- Welke draai je als eigen applicatie op cloudinfrastructuur (waar de provider alleen de onderlaag ziet)?
- En welke host je volledig zelf (waar de provider er helemaal niet bij kan)?

Die drie lagen vragen om drie verschillende risicoafwegingen. Daarbij is het relevant dat er op dit moment nog geen executive agreement tussen de VS en de EU bestaat onder de CLOUD Act. Dat betekent dat providers bij een CLOUD Act-verzoek in een directe conflictsituatie komen met de AVG/GDPR. In de praktijk lijken Microsoft en andere providers tot nu toe dergelijke verzoeken te hebben afgewezen of doorverwezen naar het traditionele Mutual Legal Assistance Treaty (MLAT)-proces, juist vanwege het risico op hoge GDPR-boetes.

Een eerlijke nuancering: ook Europese inlichtingendiensten hebben toegang

Het zou oneerlijk zijn om dit als een uitsluitend Amerikaans probleem te presenteren. Ook Europese inlichtingendiensten, waaronder de Nederlandse Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD), beschikken onder de Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017) over vergaande bevoegdheden, inclusief de mogelijkheid tot bulkinterceptie van communicatie.

Het wezenlijke verschil zit in de juridische waarborgen. In Nederland toetst de Toetsingscommissie Inzet Bevoegdheden (TIB) vooraf of de inzet van bijzondere bevoegdheden rechtmatig is. De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) houdt achteraf onafhankelijk toezicht. In de VS ontbreken dergelijke waarborgen voor niet-Amerikaanse burgers grotendeels: FISA 702 kent alleen een jaarlijkse goedkeuring door de FISA-rechtbank voor het programma als geheel, niet voor individuele verzoeken. EO 12333 kent helemaal geen externe rechterlijke toetsing.

Het gaat dus niet om de vraag of inlichtingendiensten toegang kunnen krijgen. Dat kunnen ze aan beide zijden van de Atlantische Oceaan. Het gaat om het niveau van juridische bescherming dat jouw data en organisatie geniet als dat gebeurt. En dat beschermingsniveau verschilt fundamenteel.

B. Continuïteitsrisico's: kan jouw dienstverlening van buitenaf worden verstoord?

Naast privacyrisico's is er een tweede categorie die voor zorginstellingen minstens zo relevant is: het risico dat cloud-diensten worden stopgezet, beperkt of onbetaalbaar worden gemaakt door factoren buiten jouw invloed. Dit risico kent verschillende verschijningsvormen.

Stopzetting van diensten door sancties of politieke druk

Het ICC-incident van mei 2025 is tot op heden het meest concrete voorbeeld. De volledige digitale werkomgeving van het Internationaal Strafhof (ICC) in Den Haag draaide op Microsoft 365. Toen de VS sancties oplegden aan ICC-hoofdaanklager Karim Khan, blokkeerde Microsoft de toegang tot zijn officiële Outlook-account (onderdeel van die M365-suite). Microsoft stelde dat zij vanwege de Amerikaanse sanctiewetgeving geen diensten meer mochten leveren aan gesanctioneerde individuen.

De impact reikte verder dan één geblokkeerd account. Naar verluidt gaf Microsoft het ICC een ultimatum: het hof blokkeerde zelf de toegang van Khan tot zijn M365-account, of Microsoft zou gedwongen zijn de diensten voor de volledige organisatie van 900 medewerkers stop te zetten, om te voorkomen dat zij indirect een gesanctioneerd persoon zouden faciliteren. Het ICC zag zich genoodzaakt Khans account te deactiveren. Het ICC heeft vervolgens besloten Microsoft 365 volledig te verlaten en over te stappen op openDesk, een Europees open source platform.

Het is belangrijk om dit risico iets te nuanceren. Het ICC is een politiek uiterst gevoelige organisatie die direct in het vizier lag van Amerikaanse sancties. Een Nederlands ziekenhuis of een zorginstelling is dat niet. De kans dat een cloudprovider de dienstverlening aan een politiek oncontroversiele zorginstelling stopzet vanwege sancties is op dit moment zeer klein. Maar het ICC-incident toont wel aan dat het mechanisme bestaat: een Amerikaans bedrijf kan, onder druk van Amerikaanse wetgeving, diensten stopzetten voor organisaties op Nederlands grondgebied, zonder tussenkomst van een Nederlandse rechter.

Eenzijdige prijsverhogingen en gewijzigde voorwaarden

Een reëler en veel voorkomender continuïteitsrisico dan sancties is de eenzijdige wijziging van licentievoorwaarden en prijzen. Cloudproviders hanteren doorgaans contracten waarin zij het recht voorbehouden om tarieven en voorwaarden periodiek aan te passen. In de praktijk zien zorginstellingen regelmatig forse prijsverhogingen bij contractverlenging, soms van 20% tot 40% per jaar. De onderhandelingspositie is beperkt: overstappen is duur en tijdrovend, en de provider weet dat.

Vendor lock-in en platformafhankelijkheid

Het gebruik van platformspecifieke diensten versterkt de afhankelijkheid. Zodra je gebruikmaakt van proprietary diensten van een cloudprovider, denk aan specifieke database-services, AI-platformen, identity management of monitoring-tools, groeit de lock-in exponentieel. Jouw data zit in proprietary formaten, jouw workflows zijn gebouwd op platformspecifieke API's, en jouw team heeft specialistische kennis opgebouwd die niet overdraagbaar is.

Zoals de DCC 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 eenvoudig omgezet kan worden naar iets anders."

Elke platformspecifieke dienst die je afneemt vergroot de exit-barrière. Een bewuste cloudstrategie houdt hier rekening mee door bij elke dienst de vraag te stellen: bestaat hier een open-standaard-alternatief voor, en wat kost het om over te stappen?

C. Systeemrisico's: wat als de hele sector tegelijk wordt geraakt?

De derde risicocategorie is wellicht de meest onderschatte en tegelijk de minst politiek beladen. Systeemrisico ontstaat wanneer een groot deel van een sector afhankelijk is van dezelfde infrastructuur, ongeacht of die infrastructuur Amerikaans, Europees of Nederlands is.

Concentratierisico bij één provider

Als 67% van de Nederlandse public cloud-markt op Microsoft Azure draait, en een groot deel van de ziekenhuizen hun EPD aan Microsoft-infrastructuur heeft gekoppeld, dan is er sprake van een concentratierisico. Een regionale storing bij Azure (iets wat de afgelopen jaren meerdere keren is voorgekomen) treft dan niet één ziekenhuis, maar potentieel tientallen tegelijk. Dit heeft niets met geopolitiek te maken: het is een klassiek risicomanagement-vraagstuk.

De Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten (AFM) waarschuwen hier expliciet voor in de financiële sector. Zij constateren dat de concentratie bij een handvol cloudproviders een systeemrisico vormt: als AWS of Microsoft Azure tegelijk last hebben van een storing, kan betaalverkeer bij meerdere banken tegelijk uitvallen. DNB-president Klaas Knot stelt: "We moeten nu denken aan scenario's waar we 80 jaar niet aan hebben gedacht."

Vertaling naar de zorgsector

Voor de zorgsector is dit argument minstens zo sterk als voor de financiële sector. Stel dat een Azure-storing samenvalt met een griepgolf of een andere piek in de zorgvraag: meerdere ziekenhuizen hebben tegelijk geen toegang tot hun EPD, hun communicatiesystemen of hun planningssoftware. De gevolgen zijn niet alleen financieel, maar direct medisch.

Dit risico vraagt om diversificatie op sectorniveau, niet alleen op organisatieniveau. Wanneer zorginstellingen samenwerken bij inkoop en cloudstrategie, is het verstandig om ook afspraken te maken over spreiding over meerdere providers. Niet elke instelling hoeft op hetzelfde platform te draaien. Diversificatie op sectorniveau vermindert de kans dat een technische storing of geopolitieke gebeurtenis de hele Nederlandse zorg tegelijk raakt.

Niet alles naar Europa

Het is belangrijk om te benadrukken dat systeemrisico niet verdwijnt door over te stappen naar een Europese provider. Als alle ziekenhuizen gezamenlijk migreren naar één Europese cloud, verplaats je het concentratierisico zonder het op te lossen. De kern van de oplossing zit in spreiding en uitwijkmogelijkheden over verschillende clouds. Zowel Amerikaans, Nederlands of Europees.

Kan je het tegenwoordig nog zelf doen?

In het soevereiniteitsdebat gaat het vrijwel altijd over de risico's van blijven bij of bewegen naar een hyperscaler. Zelden wordt de vraag gesteld: wat zijn de risico's van alles zelf doen?

Het meest onderschatte risico is security. Niet alleen de Amerikaanse hyperscalers, maar ook gespecialiseerde Europese en Nederlandse aanbieders investeren structureel in beveiliging op een niveau dat een individueel ziekenhuis niet kan evenaren. Ze draaien 24/7 Security Operations Centers, hebben gespecialiseerde teams die nieuwe dreigingen monitoren, en passen beveiligingsupdates toe op een schaal die voor een enkele organisatie ondoenlijk is. Als je besluit om diensten zelf te hosten om soevereiniteitsredenen, dan neem je ook de volledige verantwoordelijkheid voor de beveiliging van die diensten op je. In een arbeidsmarkt waar IT-security-specialisten schaars zijn, is dat voor een zorginstelling een reëel probleem.

Dat betekent niet dat zelf hosten onverantwoord is. Het betekent wel dat de risicoafweging twee kanten op werkt. Minder afhankelijkheid van een externe provider betekent meer afhankelijkheid van eigen kennis en capaciteit. De vraag is niet alleen "vertrouw ik deze provider met mijn data?" maar ook "kan ik het zelf aantoonbaar beter?" Bij het uitbesteden aan een cloudprovider, of dat nu een hyperscaler is of een Nederlandse aanbieder, bieden compliance-programma's zoals ISO 27001, NEN 7510 en SOC 2 Type II-rapportages het comfort dat de beveiliging onafhankelijk is getoetst. Die transparantie verlies je als je alles in eigen beheer neemt, tenzij je diezelfde standaarden op jezelf toepast.

De risico's uit het vorige hoofdstuk vragen niet om paniek, maar om regie. Hieronder vijf concrete acties die je als zorginstelling kunt nemen. Niet alles tegelijk, maar als startpunt voor een bewuste cloudstrategie.

4. Naar een bewuste cloudstrategie; van paniek naar regie

1. Ken je risico's per dienst

De belangrijkste les uit hoofdstuk 4: je risicoprofiel is geen vast gegeven, maar het resultaat van keuzes die je maakt. Het drielagenmodel maakt dat concreet. Loop je huidige dienstenlandschap langs en bepaal per dienst in welk scenario je zit:

1. Ken je risico's per dienst
2. Spreid je risico
3. Zorg dat je weg kunt
4. Versterk je positie als sector
5. Anticipeer op wat er aankomt

- **Scenario 1**:
  wordt de dienst volledig beheerd door de provider?
- **Scenario 2**:
  draai je eigen applicaties op Cloud infrastructuur?
- **Scenario 3**:
  of host je het zelf?

Die classificatie bepaalt welke risico's reëel zijn en welke niet. Weeg daarbij ook de keerzijde mee: als je diensten naar eigen beheer terughaalt, neem je ook de security-verantwoordelijkheid op je (zie hoofdstuk 3). Kan jouw organisatie dat aantoonbaar waarmaken?

Het goede nieuws: dit hoeft niet van nul te beginnen. Je instelling heeft al processen voor risicomanagement, informatiebeveiliging en privacy. Het gaat erom dat je de soevereiniteitsvraag toevoegt aan die bestaande afwegingen: wie heeft toegang, onder welke jurisdictie, en wat als de dienst wegvalt? Betrek hierbij de IT-afdeling, de Functionaris Gegevensbescherming en de juridische afdeling, en herhaal de analyse minimaal jaarlijks.

Belangrijk aandachtspunt: het rapport van de Algemene Rekenkamer concludeerde dat bij twee derde van de door de Rijksoverheid afgenomen clouddiensten nooit een risicoanalyse heeft plaatsgevonden, zelfs niet voor cruciale diensten zoals die van de Belastingdienst. Dat is een fout die de zorgsector niet hoeft te herhalen.

Van risico-analyse naar plaatsingskeuze

Als je het drielagenmodel combineert met de kriticiteit (hoe essentieel een systeem is voor de zorgverlening) en privacygevoeligheid van je systemen, ontstaat een concreet plaatsingsmodel dat helpt bij het maken van keuzes. Niet alles hoeft op dezelfde plek te staan.

Sommige IT wil je binnen de muren van je instelling houden. Denk aan de systemen die direct nodig zijn voor het verlenen van acute zorg: de IT op de spoedeisende hulp, de IC-systemen, en de communicatiemiddelen voor zorgverleners zoals telefonie en pagers. Daar wil je waarschijnlijk zelfs niet afhankelijk zijn van een internetverbinding die kan uitvallen door graafwerkzaamheden. Dit zijn systemen waarbij beschikbaarheid letterlijk levens kan kosten: die houd je lokaal.

Andere systemen wil je in een Nederlandse of Europese cloud plaatsen om privacy te waarborgen en continuïteitsrisico's te beperken. De productieomgeving van je EPD is daar een goed voorbeeld van: gevoelige patiëntgegevens, hoge beschikbaarheidseisen, en de wens om binnen de Europese jurisdictie te blijven. Een Nederlandse of Europese cloudprovider biedt hier de combinatie van professioneel beheer en juridische zekerheid.

En dan zijn er systemen die prima in de publieke cloud van een Amerikaanse hyperscaler kunnen draaien. Een test- of acceptatieomgeving van je EPD (met een geanonimiseerde dataset) heeft geen privacyrisico en is niet bedrijfskritisch, maar profiteert wel enorm van de elasticiteit van een hyperscaler: opschalen als je test, afschalen als je klaar bent. Hetzelfde geldt voor het gebruik van AI-diensten zoals Large Language Models (LLM's). De LLM-platformen van hyperscalers bieden functionaliteit die bij Europese aanbieders niet of nauwelijks beschikbaar is. Mits je goede guardrails inricht kun je hier veilig gebruik van maken, denk aan tooling om persoonlijke gegevens te maskeren voordat ze naar het model worden gestuurd.

De rode draad: niet elk systeem vraagt om dezelfde mate van soevereiniteit. Door per systeem bewust te kiezen waar het thuishoort, vermijd je zowel de valkuil van alles bij één hyperscaler plaatsen als de valkuil van alles terughalen naar eigen beheer.

Scenariovergelijking: vijf manieren om een EPD te hosten

Om de afweging concreet te maken, zetten we vijf realistische scenario's naast elkaar. Per scenario beoordelen we het privacyrisico, het continuïteitsrisico, het securityprofiel en de benodigde eigen expertise. Het beeld dat ontstaat is helder: er is geen 'beste' keuze, elke optie verschuift het risico.

De tabel maakt zichtbaar wat in het debat vaak impliciet blijft: hoe meer je naar eigen beheer gaat, hoe lager je privacyrisico en je afhankelijkheid van buitenlandse jurisdicties, maar hoe hoger de eisen aan je eigen organisatie. Dat is geen reden om niet te bewegen, maar wel om eerlijk te zijn over wat elke keuze vraagt.

Niet elk systeem vraagt om dezelfde mate van soevereiniteit.

Scenario	Privacyrisico	Continuïteitsrisico	Beveiligingsniveau	Benodigde eigen expertise
Amerikaans SaaS-EPD (volledig beheerd door Amerikaanse leverancier)	Hoog CLOUD Act volledig van toepassing, provider heeft directe toegang tot patiëntdata	Hoog Sanctierisico (klein maar reëel), volledige leveranciersafhankelijkheid, eenzijdige prijswijzigingen	Zeer hoog Miljarden-investeringen in security, 24/7 SOC, continue threat monitoring	Laag Leverancier beheert vrijwel alles
Nederlands SaaS-EPD op Azure (Nederlandse leverancier host op Amerikaanse cloudinfrastructuur)	Gemiddeld Nederlandse leverancier beheert applicatielaag, Microsoft ziet alleen versleutelde infrastructuur. Met customer-managed keys is de kans op CLOUD Act-blootstelling wel aanwezig, maar minder	Gemiddeld Azure-afhankelijkheid voor infrastructuur, Nederlandse leveranciersrelatie voor applicatie. Dubbel prijsrisico	Hoog Azure-infrastructuurbeveiliging gecombineerd met applicatiebeveiliging door Nederlandse leverancier	Laag-gemiddeld Leverancier beheert het meeste, je moet het shared-responsibility-model begrijpen
Nederlands SaaS-EPD op Nederlandse cloud	Laag Volledig binnen Nederlandse/ Europese jurisdictie, geen CLOUD Act-blootstelling	Laag-gemiddeld Geen sanctierisico, afhankelijk van twee Nederlandse partijen	Hoog Kleiner klantenbestand, beperktere attack surface, geen publiek toegankelijke beheerportalen. Compliance-programma's (ISO 27001, NEN 7510, SOC 2 Type II) borgen onafhankelijke toetsing	Laag-gemiddeld Vergelijkbaar met vorig scenario
Nederlandse EPD-software, zelf gehost op eigen infrastructuur	Laag Data volledig onder eigen controle, geen cloud-blootstelling	Laag voor externe verstoringen, hoger voor interne risico's (hardwarefalen, capaciteitstekort). Afhankelijk van softwareleverancier voor updates	Afhankelijk van eigen capaciteit Vereist forse investering in eigen security-team, tooling en processen	Hoog Je beheert infrastructuur, netwerk, security, patching, back-ups en disaster recovery
Open source EPD, zelf gehost in eigen datacenter	Laagst Volledige controle, geen leveranciersafhankelijkheid voor datatoegang	Gemengd Geen vendor lock-in, maar ook geen leveranciersondersteuning. Volledige eigen verantwoordelijkheid	Volledig afhankelijk van eigen capaciteit Geen leverancier die meekijkt of bijspringt bij incidenten	Zeer hoog Je beheert alles, inclusief applicatie-expertise

Tabel Scenariovergelijking

2. Spreid je risico

In hoofdstuk 3C beschreven we het systeemrisico: als een groot deel van de zorgsector op dezelfde infrastructuur draait, kan één storing tientallen instellingen tegelijk treffen. Dat risico los je niet op door allemaal naar dezelfde Europese cloud te verhuizen. Dan verplaats je de concentratie zonder het probleem op te lossen.

Een multicloud-aanpak vermindert die kwetsbaarheid. Met deze aanpak spreid je bewust diensten over meerdere providers. Dat betekent niet dat je alles dubbel draait. Het begint bij het identificeren van je meest kritieke systemen en het borgen dat daar een uitwijkscenario voor bestaat. Als je EPD op Azure draait, overweeg dan of je back-up- en disaster-recovery-omgeving bij een andere provider kan. Als je e-mail bij Microsoft 365 afneemt, onderzoek dan wat je nodig hebt om binnen een redelijke termijn naar een alternatief over te stappen.

3. Zorg dat je weg kunt

Exit-strategieën zijn niet iets wat je bedenkt op het moment dat je weg moet. Dan ben je te laat. Het coalitieakkoord spreekt niet voor niets van "doelgericht afbouwen" van strategische afhankelijkheden, en de aangekondigde nationale stresstests ("Microsoft-out oefeningen") maken duidelijk dat ook de overheid verwacht dat organisaties hierop voorbereid zijn.

De kern van een goede exit-strategie: zorg dat je data overdraagbaar is en dat je contractueel het recht hebt om te vertrekken. Dat betekent: back-ups in open formaten, gedocumenteerde systeemconfiguraties, contractuele dataportabiliteit, en periodieke "dry runs" waarin je de overstap naar een alternatief test. Leg bij contracten ook exit-procedures, doorlooptijden en kostenverdeling vooraf vast, en eis dat leveranciers data kunnen exporteren in open standaarden (zoals HL7 FHIR voor zorginformatie).

Leg daarnaast in je leverancierscontracten de waarborgen vast die je nodig hebt: transparantie over datalocatie en gegevensstromen, notificatieplicht bij verzoeken van buitenlandse autoriteiten, een rechtskeuzebeding voor Nederlands/Europees recht, compliance met NEN 7510 en ISO 27001, en audit-rechten. Eis een actueel overzicht van subverwerkers met vetorecht bij wijzigingen. De financiële sector loopt hierin voorop, DNB en AFM eisen dit al van banken. Zorginstellingen werken met minstens even gevoelige gegevens en kunnen van die aanpak leren.

4. Versterk je positie als sector

Individueel sta je als zorginstelling niet sterk tegenover een techgigant met honderden miljarden omzet. Collectief wel. Brancheorganisaties zoals de NVZ, NFU en ActiZ kunnen gezamenlijke inkoopvoorwaarden ontwikkelen met ingebouwde soevereiniteitseisen. Dat versterkt de onderhandelingspositie, verlaagt transactiekosten en voorkomt dat elke instelling afzonderlijk het wiel uitvindt.

5. Anticipeer op wat er aankomt

De regelgeving rond digitale soevereiniteit is in beweging. De EHDS-verordening (in werking sinds maart 2025) stelt vanaf 2029 eisen aan interoperabiliteit en dataportabiliteit van EPD-systemen. De Cyberbeveiligingswet (de Nederlandse implementatie van NIS2) scherpt de eisen aan voor informatiebeveiliging in vitale sectoren, waaronder de zorg. En de inkoopeisen uit het coalitieakkoord (security-by-design, zero trust, open source, soevereiniteit) werken door naar zorginstellingen die met publiek gefinancierde systemen werken.

Anticipeer hierop door nu al leveranciers te selecteren die open standaarden ondersteunen en die bereid zijn om aan soevereiniteitseisen te voldoen. Dat verlaagt niet alleen de exit-drempel, maar ook toekomstige compliance-kosten. De instellingen die hier nu mee beginnen, hoeven straks niet in een keer alles om te gooien.

5. Conclusie

Dit whitepaper begon met de kernopdracht van zorginstellingen: patiënten en cliënten komen binnen met een klacht en vertrekken beter dan ze binnenkwamen. De patiënt staat altijd centraal. Ook bij IT-keuzes. Digitale soevereiniteit is geen doel op zich, maar een risico dat je weegt naast infectierisico's, financiële risico's en personeelstekorten.

De huidige afhankelijkheid van Amerikaanse cloudproviders is nooit beleidsmatig besloten, maar organisch ontstaan. Dat hoeft geen probleem te zijn, mits je weet wat de risico's zijn en bewust hebt gekozen. De drie risicocategorieën uit dit whitepaper: **privacy, continuïteit en systeemrisico**. Elk vragen om een andere afweging. Het drielagenmodel laat zien dat je blootstelling geen vast gegeven is maar het resultaat van je eigen inrichtingskeuzes. En de scenariotabel maakt zichtbaar dat elke stap richting meer autonomie ook meer verantwoordelijkheid vraagt.

Drie dingen kun je morgen al doen. Loop je huidige dienstenlandschap langs met het drielagenmodel en bepaal per dienst waar je staat. Stel bij de eerstvolgende contractverlenging de vraag of je exit-clausules, dataportabiliteit en notificatieplicht hebt vastgelegd. En zoek contact met collega-instellingen via NVZ, NFU of ActiZ om gezamenlijk soevereiniteitseisen te formuleren. Collectief sta je sterker.

De zorgsector hoeft niet in paniek te raken en hoeft niet alles morgen om te gooien. Maar bewust niets doen is ook een keuze. En dan wel eentje die je over vijf jaar moet verantwoorden. De instellingen die nu beginnen met een bewuste cloudstrategie, investeren niet in technologie maar in de toekomstbestendigheid van hun zorgverlening.

Gebruikte bronnen

Alle bronnen zijn terug te vinden op de website van Intermax.
Bekijk de pagina door de QR-code te scannen.

ontdek.intermax.nl/bronvermeldingen-whitepaper-zorg

intermax

intermax

MANAGEMENTSYSTEEM CERTIFICATIE
DNV
ISO 9001 • ISO 14001
ISO 20000 • ISO 22301
ISO 27001 • NEN 7510

ISAE 3402 TYPE II &
SOC2 ASSURANCE

Contact

Intermax
Rotterdam
+31(0) 10 – 710 4444
info@intermax.nl

Over Intermax

Bij Intermax geloven we dat technologie pas waarde krijgt als ze bijdraagt aan iets groters. Aan zorg die altijd beschikbaar is. Aan overheidsdiensten die betrouwbaar functioneren. Aan infrastructuren die de samenleving dragen, en waarop iedereen blind moet kunnen vertrouwen, juist als het spannend wordt.

Wij leveren cloudoplossingen die volledig aansluiten bij hun wensen en behoeften. Of het nu gaat om private, public of hybrid cloud; wij zorgen voor een veilige, betrouwbare en schaalbare omgeving die de Nederlandse maatschappij verder helpen.

Kortom: waar IT nooit mag uitvallen, staan wij altijd aan.