ZA CERT

Data soevereiniteit & digitale autonomie in de zorg

Een samenwerking met:

NVZ Nederlandse Vereniging van Ziekenhuizen

Inhoudsopgave

Waarom digitale Autonomie en data soevereiniteit nodig zijn

Onze patiënten en medewerkers moeten erop kunnen vertrouwen dat hun gegevens bij ons in veilige en vertrouwde handen zijn. Daarom moeten we onze digitale autonomie vergroten. In dit document lees je hoe je daarmee aan de slag gaat. Het doel hiervan is om de regie te behouden over onze persoonsgegeven in Europa.

Internationale spanningen nemen toe

De internationale situatie zet Europa en Nederland steeds meer onder druk. Onze waarden, welvaart en veiligheid komen steeds meer onder druk te staan. De spanningen in de wereld en geopolitieke grimmigheid nemen toe. Denk aan de oorlogen in Oekraïne, Gaza, Libanon en het Midden-Oosten, zeker na de militaire acties van Israël en de VS in Iran.

Landen en machthebbers treden harder op. Ze zijn minder terughoudend om hun eigen belangen door te drukken. Conflicten worden vaker uitgevochten, soms militair, soms economisch of politiek.

Ook Europa en Europese bedrijven merken dat. Zij raken steeds vaker betrokken bij de strijd tussen grootmachten als de VS, Rusland en China.

Landen zijn sterk met elkaar verbonden door handel, technologie en geld. Die verbondenheid helpt de economie, maar maakt landen ook kwetsbaar. Want wat eerst bedoeld was voor samenwerking, kan ook worden gebruikt om druk uit te oefenen. Handel, digitale systemen en financiële netwerken worden zo steeds vaker een machtsmiddel. Die ontwikkeling noem je ook wel: weaponization of everything.

De rol van de VS verandert

De huidige Amerikaanse koers draait vooral om de veiligheid en belangen van het eigen land. Zaken die de VS niet direct raken, krijgen minder aandacht van Washington.

Europa blijft voor de VS strategisch belangrijk. Ook ziet Amerika Europa als cultureel verwant. Tegelijk kijkt de Amerikaanse regering kritischer naar Europa dan vroeger. Europa wordt vaker gezien als een probleem: minder sterk dan voorheen en volgens Washington afgeremd door supranationale organisaties zoals de Europese Unie.

Ook de relatie met internationale organisaties verandert. De houding van de VS tegenover organisaties zoals de NAVO en het Internationaal Strafhof (ICC) lijkt vooral af te hangen van wat de regering-Trump zelf nodig vindt. Zo legde de VS sancties op aan het ICC en probeert het de werking van het hof te bemoeilijken.

Een voorbeeld daarvan is de blokkade van de Microsoft-mailbox van een hoofdaanklager van het ICC in mei 2025. Dit laat zien hoe afhankelijk Europa is van grote Amerikaanse cloud- en communicatiediensten. Als die toegang wordt beperkt, kan dat direct gevolgen hebben voor Europese organisaties en instellingen.

In dit document verstaan we onder:

- **Digitale autonomie** betekent dat een organisatie zelf keuzes kan maken over data en digitale voorzieningen. De organisatie blijft flexibel en verkleint ongewenste afhankelijkheden. Dat betekent niet dat alles in eigen bezit of beheer hoeft te zijn. Het betekent wel dat de organisatie bewust kan kiezen, kan bijsturen en zelf bepaalt hoe zij cybersecurity beheerst.
- **Datasoevereiniteit** is de regie en controle hebben over data, die de organisatie verwerkt, onafhankelijk van derden.

Digitale autonomie

Digitale autonomie betekent dat we zelf bewuste keuzes kunnen maken over onze digitale systemen. Denk aan communicatie, informatievoorziening, infrastructuur en de processen die daarbij horen. Het gaat dus om de vraag: hoeveel grip hebben we zelf op onze digitale omgeving?

Daarbij spelen ook economische factoren een rol: is er genoeg vraag en aanbod? Is er echte concurrentie? Zijn er alleen standaardproducten of is maatwerk mogelijk? Zijn er goede alternatieven? Kunnen we makkelijk overstappen naar een andere leverancier? En blijven de kosten beheersbaar? Als dat niet zo is, ontstaat afhankelijkheid.

Zorgorganisaties zijn verplicht om de digitale infrastructuur zo in te richten dat informatie veilig wordt beheerd en zoveel mogelijk onder Europese of Nederlandse wet- en regelgeving valt. Ook moeten ze goed beschermd zijn tegen ongeoorloofde toegang of verkeerd gebruik. Hier komen **digitale autonomie** en **datasoevereiniteit** samen: we hebben niet alleen veilige systemen nodig, maar ook zeggenschap over onze data.

Op dit moment zijn we sterk afhankelijk van grote software-, cloud- en communicatie-leveranciers, van vaak Amerikaanse aanbieders. Dat maakt ons economisch en strategisch kwetsbaar. Onder andere door stijgende kosten en monopolies: een klein aantal heeft veel macht. Die afhankelijkheid speelt ook in de zorg, bijvoorbeeld bij elektronische patiëntendossiers en andere zorgspecifieke systemen.

Hoe versterk je digitale autonomie?

Digitale autonomie versterken vraagt om gerichte keuzes. We moeten investeren in open standaarden, open source en Europese alternatieven. Ook moeten we bewuste keuzes maken over datasoevereiniteit: welke data bewaren we waar en onder welke regels?
Dit vraagt om leiderschap met een lange adem: risicogestuurd en gericht op de lange termijn door doelgericht en gefaseerd toe te werken naar digitale autonomie. Zeggenschap, privacy en uitwisselbaarheid van systemen moeten daarbij centraal staan. Dat is nodig om veilige, betrouwbare en innovatieve zorg te kunnen blijven bieden.

Aan de slag

Digitale autonomie is een strategisch onderwerp. Het gaat niet alleen over ICT, contracten of compliance. Het raakt direct aan de continuïteit van je organisatie. De keuzes die een zorgorganisatie hierin maakt, hebben invloed op veel onderdelen van de zorg. Denk aan datatoegang, leveranciers, innovatie, cybersecurity, inkoop, kosten, continuïteit en het vertrouwen van patiënten en medewerkers. Daarom hoort digitale autonomie thuis op de strategische agenda.

Tegelijk is digitale autonomie geen doel dat je in één keer bereikt. Het vraagt om een gefaseerde aanpak. Neem het onderwerp daarom op in de meerjarige IT-strategie, de inkoopstrategie en het strategisch risicomanagement. Zo kun je stap voor stap afhankelijkheden verkleinen en meer grip krijgen op data, systemen en leveranciers. Wacht daar niet te lang mee: de risico's zijn nu al zichtbaar en nemen verder toe.

Daarbij moet je afwegingen maken. Investeren in digitale autonomie kan tijdelijk betekenen dat er minder ruimte is voor andere ontwikkelingen of innovatie. Toch is die investering nodig. Zonder voldoende autonomie wordt innovatie op termijn juist kwetsbaarder, omdat je minder vrij bent om eigen keuzes te maken.

Ook de overheid geeft hierin een duidelijk signaal af. In het regeerakkoord wordt gestuurd op het afbouwen van technologische afhankelijkheid. Dat gaat niet alleen over data, maar ook over digitale apparatuur, infrastructuur en leveranciers.

De richting is daarmee helder: meer grip, minder ongewenste afhankelijkheid en meer weerbaarheid. Waar dat kan, ligt de voorkeur bij Europese oplossingen en samenwerkingen. Niet omdat Europees automatisch beter is, maar omdat het organisaties kan helpen om data, continuïteit en zeggenschap beter te beschermen.

Tot slot is het belangrijk om niet te wachten, maar te starten. Digitale autonomie is niet alleen van belang voor de korte termijn, maar vraagt juist om structurele aandacht met het oog op de lange termijn. Door nu stappen te zetten, bouw je gericht aan meer grip, weerbaarheid en continuïteit voor de toekomst.

Hoe te beginnen

Digitale autonomie vraagt om richting én praktische keuzes. Het begint met een strategisch besluit, maar moet daarna worden vertaald naar beleid, inkoop, contracten, techniek en risicomanagement.

- **Stap 1: maak een strategische keuze**

  Bepaal eerst welke mate van digitale autonomie je wilt bereiken. Dat hoeft niet voor alle data, systemen en processen hetzelfde te zijn. Voor zeer gevoelige patiëntdata kan een hogere mate van autonomie nodig zijn dan voor minder kritieke processen. Om strategische verantwoorde keuzes te maken verwijzen we naar de bijlagen waarin verschillende invalshoeken uitgewerkt zijn. Leg ook een stip op de horizon vast. Wanneer wil je welk niveau van digitale autonomie bereikt hebben? Werk dit uit in een tijdlijn, zodat duidelijk wordt welke keuzes op korte, middellange en lange termijn nodig zijn.

- **Stap 2: breng het in kaart**

  Breng daarna de huidige situatie in kaart. Controleer of je bestaande leveranciers, systemen en contracten passen bij de digitale autonomie die je wilt hebben. Pas waar nodig de eisen voor nieuwe aanschaf en aanbesteding aan. Neem digitale autonomie standaard mee in inkoopcriteria, contractvoorwaarden en leveranciersbeoordelingen.

- **Stap 3: werk met scenario's**

  Gebruik vervolgens scenario's om te bepalen waar de grootste risico's zitten. Kijk waar de huidige situatie afwijkt van het gewenste eindbeeld. Welke leveranciers, systemen of processen vormen de grootste afhankelijkheid? Waar is overstappen moeilijk?

Werk per risico uit wat het gewenste tijdpad is. Bepaal welke maatregelen nodig zijn om de risico's te mitigeren. Ook als je door externe ontwikkelingen gedwongen wordt snel te reageren. Bepaal welke stappen je kunt plannen per SEAL-categorie en welke maatregelen je nodig hebt als je door externe ontwikkelingen gedwongen wordt eerder over te stappen.

Dit document is tot stand gekomen naar aanleiding van vragen van bestuurders aan de NVZ. Dit document is gemaakt door een werkgroep van (C)ISO's van de NVZ en Z-CERT.

Bronnen

1. National Security Statement of the United States of America – november 2025
2. Het nieuwe wereldbeeld van Amerika – Clingendael Spectator, 18 dec 2025, Instituut Clingendael
3. Visie Digitale autonomie en soevereiniteit van de overheid – Ministerie van Binnenlandse Zaken, juni 2025

Invalshoek: Verstoring clouddienst

Context

Zorgorganisaties maken steeds meer gebruik van clouddiensten. Daardoor ontstaat er een nieuwe afhankelijkheid: als een clouddienst, datacenter of softwareplatform uitvalt, kan dit direct gevolgen hebben voor de zorgverlening.

Bij clouddiensten is dit risico groter wanneer leveranciers buiten de Europese Economische Ruimte zijn gevestigd of onder buitenlandse wetgeving vallen. Een overheid buiten Europa kan invloed uitoefenen op de leverancier. Daardoor kan toegang tot diensten of data onder druk komen te staan.

Deze afhankelijkheid raakt niet alleen individuele zorgorganisaties. Als veel organisaties dezelfde cloudleverancier of digitale infrastructuur gebruiken, kan een verstoring ook sectorbreed gevolgen hebben. Een grote storing bij een dominante cloud- of infrastructuurpartij kan meerdere ziekenhuizen en ketenpartners tegelijk raken.

In de bijlage is een casus uitgewerkt waarin wordt beschreven wat er kan gebeuren als een zorgorganisatie met een Microsoft 365-omgeving geen toegang meer heeft tot Microsoft 365.

Risico's

- **Uitval van een clouddienst, datacenter of softwareplatform**
  Als een kritische clouddienst niet beschikbaar is, kan dat direct leiden tot problemen in de organisatie. Denk aan uitval van applicaties, data, communicatie, authenticatie of digitale werkplekken. Bij systemen die volledig cloudafhankelijk zijn, is er vaak minder directe controle dan bij systemen die lokaal of met een goede fallback zijn ingericht.
- **Geopolitieke invloed op leveranciers**
  Leveranciers die onder buitenlandse jurisdictie vallen, kunnen te maken krijgen met maatregelen van hun eigen overheid. Dat kan gevolgen hebben voor toegang tot diensten, support, updates, licenties of data.
- **Sectorbrede uitval**
  Veel zorgorganisaties gebruiken dezelfde cloudleveranciers, communicatieplatforms of infrastructuurdiensten. Daardoor kan één grote storing meerdere organisaties tegelijk raken.

Wat kun je in de praktijk doen?

- **Neem SEAL of een vergelijkbaar beoordelingskader mee bij aanschaf**

  Gebruik bij de aanschaf van clouddiensten een beoordelingskader zoals SEAL[4]. Zo zie je snel welke eisen gelden voor beschikbaarheid, datalocatie, beveiliging, toegang, jurisdictie en exitmogelijkheden. Dit helpt om bewuster te kiezen en risico's vooraf mee te wegen.

- **Richt redundantie in**

  Zorg dat kritische applicaties en data niet afhankelijk zijn van één locatie, datacenter of platform. Spreid waar nodig over meerdere datacenters of regio's. Als één locatie uitvalt door technische storing, stroomuitval of calamiteit, kan je dienstverlening automatisch doorgaan vanuit een andere locatie. Hier heb je een goed ingerichte failover-voorziening voor nodig, waarbij systemen automatisch overschakelen naar een reserve-omgeving.

- **Maak een disaster recovery-strategie (DR)**

  Bepaal per systeem hoe snel het hersteld moet zijn en hoeveel dataverlies maximaal acceptabel is. Maak back-ups en test periodiek of systemen en data binnen de afgesproken tijd kunnen worden hersteld.

- **Beperk afhankelijkheid van één leverancier**

  Onderzoek of een multicloudstrategie (meerdere cloudproviders gebruiken om afhankelijkheid te beperken), open standaarden of containertechnologie kan helpen om minder afhankelijk te zijn van één leverancier. Zo blijft het makkelijker om applicaties en data te verplaatsen als dat nodig is.

- **Zorg voor continue monitoring**

  Bewaak beschikbaarheid, prestaties en storingen actief. Zo zie je afwijkingen eerder en kun je maatregelen nemen voordat zorgprocessen worden geraakt.

- **Bescherm data met encryptie**

  Zorg dat data versleuteld wordt opgeslagen (data at rest) en verzonden (data in transit). Voor zeer gevoelige gegevens is het verstandig om zelf de encryptiesleutels te beheren. Daarmee voorkom je dat de cloudleverancier zelfstandig toegang heeft tot leesbare data. Pas waar mogelijk end-to-end-encryptie toe. Zo blijven gegevens versleuteld tijdens de hele verwerking en kunnen alleen geautoriseerde gebruikers bij het ziekenhuis deze ontsleutelen.

- **Beperk toegang volgens het least-privilege-principe**

  Geef medewerkers, leveranciers en beheerders alleen toegang tot systemen en gegevens die zij nodig hebben voor hun taak. Leg vast wie toegang heeft, waarvoor en onder welke voorwaarden.

- **Pas just-in-time-toegang toe**

  Verleen gebruikers en beheerders alleen tijdelijk toegang tot systemen en gegevens wanneer dit nodig is voor hun taak. Zorg dat rechten automatisch worden ingetrokken na gebruik en dat aanvragen worden goedgekeurd en gelogd. Hiermee verklein je het risico op misbruik van permanente toegang en beperk je de impact van gecompromitteerde accounts.
- **Gebruik MFA en PAM voor beheerdersaccounts**

  Pas Multi-Factor Authentication toe, op z'n minst voor accounts met verhoogde rechten. Gebruik daarnaast Privileged Access Management om beheerderstoegang tijdelijk, gecontroleerd en geregistreerd toe te kennen.
- **Werk volgens Zero Trust**

  Vertrouw geen gebruiker, apparaat of systeem automatisch. Controleer voortdurend of toegang terecht is. Dit verkleint het risico op ongewenste toegang tot clouddata en kritische systemen.
- **Leg afspraken contractueel vast**

  Maak duidelijke afspraken over beschikbaarheid, gegevensbescherming, audits, incidentmeldingen, support, subleveranciers, exitmogelijkheden en migratie. Leg ook vast wat er gebeurt bij overname, faillissement, geopolitieke maatregelen of het beëindigen van diensten.

Bronnen

4. https://www.norea.nl/nieuws/europese-commissie-publiceert-cloud-sovereignty-framework

Invalshoek: Handelsbetrekkingen

Context

Internationale ontwikkelingen en geopolitieke verschuivingen hebben direct invloed op de zorg. De zorg is afhankelijk van veel digitale systemen, leveranciers, energie, goederen en internationale ketens. Als handelsrelaties veranderen of onder druk komen te staan, kan dat gevolgen hebben voor de continuïteit, veiligheid en betaalbaarheid van zorg.

Daarom is het nodig om voortdurend alert te zijn en kritische afhankelijkheden te verminderen. De uitkomsten daarvan moeten worden meegenomen in strategische keuzes over digitale autonomie. Het gaat daarbij niet alleen om de vraag welke systemen we gebruiken, maar ook om de vraag hoe kwetsbaar we zijn als leveranciers, landen of ketens onder druk komen te staan.

Risico's

- **Cybercrime en statelijke dreiging**

  Cybercrime wordt niet alleen ingezet voor financieel gewin, maar ook als drukmiddel om organisaties of de samenleving te ontregelen. Voor de zorg is dit een groot risico, omdat digitale verstoring direct gevolgen kan hebben voor patiënten, medewerkers en de continuïteit van zorg.
- **Energievoorziening en kosten**

  Internationale spanningen maken duidelijk hoe afhankelijk de zorg is van energie en brandstoffen. Problemen met beschikbaarheid of stijgende prijzen kunnen de bedrijfscontinuïteit, zorgkosten en afspraken met zorgverzekeraars onder druk zetten. Daarnaast krijgen zorgorganisaties te maken met veranderende wet- en regelgeving, die steeds zwaardere eisen stelt aan zelfvoorziening en noodvoorzieningen.
- **Grondstoffen, goederen en producten**

  Grondstoffen, chips en andere onderdelen worden steeds vaker onderdeel van internationale machtsverhoudingen. Dat kan ook de zorg raken. Door de digitalisering is de zorg afhankelijk van apparatuur, onderdelen, software en digitale infrastructuur. Leveringsproblemen kunnen leiden tot schaarste, langere levertijden en hogere kosten voor materialen en onderdelen.

Wat kun je in de praktijk doen?

- **Beoordeel alternatieven**

  Breng in kaart welke alternatieven er zijn voor belangrijke leveranciers, systemen, onderdelen en diensten voor de kortere, middelange en lange termijn.

- **Maak beleid voor voorraden**

  Bepaal welke onderdelen, apparatuur en middelen nodig zijn om de zorg te kunnen blijven leveren bij verstoringen. Werk hierbij met forecasting en leveringszekerheid van IT-leveranciers: kijk vooruit naar verwachte vervanging, groei, onderhoud en mogelijke schaarste. Zo kun je eerder zien waar knelpunten ontstaan. Dit helpt om tijdig te bestellen, budget te reserveren en alternatieven te organiseren.
- **Reserveer budget voor prijsstijgingen**

  Houd rekening met stijgende kosten voor energie, onderdelen, apparatuur en digitale diensten.

Invalshoek: Datatoegang

Context

In de zorg werken we met zeer gevoelige gegevens. Patiënten en medewerkers moeten erop kunnen vertrouwen dat deze data goed beschermd is. Daarom is controle over data een belangrijk onderdeel van digitale autonomie en soevereinitieit.

Bij datatoegang gaat het om vragen als: waar staat onze data? Wie kan erbij? Onder welke wetgeving valt de data? En welke leveranciers of subleveranciers hebben toegang?

Risico's

- **Andere wetgeving buiten de EU**

  Leveranciers met een hoofdkantoor buiten de EU kunnen te maken krijgen met wetgeving uit dat land. Dat heet extraterritoriale wetgeving . Daarnaast zijn er landen, zoals de VS en China, die vinden dat hun wetgeving voorrang heeft op de wetgeving van de staat/land waar de activiteiten plaatsvinden Een bekend voorbeeld is de Amerikaanse CLOUD Act. Ook de Foreign Intelligence Surveillance Act kan toegang tot data mogelijk maken. Daardoor kunnen buitenlandse overheden in bepaalde situaties toegang krijgen tot gegevens, ook als die data in Europa staat. Dit komt voor in de praktijk .
- **Juridische afspraken bieden geen volledige zekerheid**

  Zorgorganisaties maken afspraken met leveranciers in contracten en verwerkersovereenkomsten. Dat is belangrijk, maar het biedt geen absolute garantie. Statelijke actoren kunnen soms toegang krijgen tot data zonder dat de organisatie dat weet. Daarnaast is data verwijderen niet altijd definitief. Als een organisatie vraagt om data te verwijderen, betekent dat niet altijd dat alle gegevens volledig weg zijn. Sommige leveranciers werken met 'best effort deletion'. Dat betekent dat zij hun best doen om data te verwijderen, maar geen volledige verwijdering garanderen. Hierdoor kan het zijn dat data toch nog bestaat en ingezien kan worden door andere partijen.
- **Follow the sun: toegang via subleveranciers en supportteams**

  Veel leveranciers werken met subleveranciers of internationale supportteams. Bij het zogenoemde follow-the-sun-principe wordt ondersteuning 24 uur per dag geleverd vanuit verschillende tijdzones. Ook als data in de EU staat, kunnen medewerkers of systemen buiten Europa mogelijk toegang krijgen tot data of metadata, omdat deze in andere geografische zones wordt verwerkt en geëxporteerd.

Wat kun je in de praktijk doen?

- **Overweeg leveranciers onder Europese jurisdictie**

  Kijk bij nieuwe contracten en aanbestedingen ook naar onder welke wetgeving een leverancier valt. Een Europese leverancier kan helpen om risico's rond buitenlandse wetgeving te verkleinen.

- **Maak duidelijke afspraken over opslag en toegang**

  Leg contractueel vast waar data wordt opgeslagen, wie toegang heeft en onder welke voorwaarden. Neem hierin ook subleveranciers mee.

- **Richt strategische data governance in**

  Maak duidelijke afspraken over hoe de organisatie met data omgaat. Leg vast wie waarvoor verantwoordelijk is en hoe deze afspraken worden nageleefd en geëvalueerd.
  Dataclassificatie is hierbij onmisbaar. Zo wordt duidelijk welke gegevens extra bescherming nodig hebben. Op basis daarvan kun je bepalen wat wel en niet mag met bepaalde data, welke leveranciers geschikt zijn en welke beveiligingsmaatregelen nodig zijn.

- **Werk samen met andere zorgorganisaties**

  Individuele zorgorganisaties hebben vaak beperkte invloed op grote leveranciers. Door samen op te trekken, kunnen zorgorganisaties sterker onderhandelen. Eerdere afspraken tussen de onderwijssector met onder andere Google laten zien dat collectieve druk kan leiden tot betere afspraken.

Bronnen

5. Regeerakkoord 2026-2030, 2026; Van Eeden et al., 2025; VNG, 2025

6. https://www.audittrail.nl/digitale-soevereiniteit-op-strategische-risicoagenda/

7. Van Eeden et al., 2025

Invalshoek: Innovatiekracht

Context

Innovatie in de zorg is belangrijk om aan de toenemende zorgvraag te kunnen voldoen. Hoeveel digitale autonomie een organisatie heeft, kan namelijk effect hebben op die innovatiekracht van een organisatie. En als een organisatie voldoende grip heeft op data, systemen en leveranciers, kan zij sneller vernieuwen. Als die grip ontbreekt, kan innovatie juist worden afgeremd.

Risico's

- **Beperkte uitwisseling van gegevens (interoperabiliteit)**
  Gegevensuitwisseling en samenwerking zijn belangrijk in de zorg. Dat geldt binnen één zorgorganisatie, maar ook tussen zorgorganisaties. Als systemen niet goed met elkaar kunnen samenwerken, wordt innovatie moeilijker schaalbaar. Dit risico wordt groter als een organisatie weinig invloed heeft op data, koppelingen of de ontwikkelagenda van leveranciers.
- **Afhankelijkheid van één leverancier**
  Zorgorganisaties kiezen soms voor totaaloplossingen van één grote leverancier. Zo ontstaat het risico van vendor lock-in. De organisatie wordt dan sterk afhankelijk van één leverancier. Daardoor kan het lastig worden om innovaties van andere leveranciers te gebruiken of om over te stappen . Ook word je als organisatie afhankelijk van het innovatietempo van één leverancier . Bij grote leveranciers is die ontwikkelagenda vaak moeilijk te beïnvloeden. Daar staat tegenover dat grote leveranciers vaak wel meer middelen hebben om te investeren in innovatie.
- **Nationale belangen kunnen innovaties belemmeren**
  Landen kunnen ervoor kiezen om belangrijke technologieën eerst voor zichzelf te houden of de toegang voor andere landen te beperken. Daardoor kunnen organisaties buiten dat land later of minder makkelijk toegang krijgen tot nieuwe technologie.

Voorbeeld: Het behouden van een superieure positie in kritieke en opkomende technologieën is een van de zes speerpunten uit de cyberstrategie van president Trump. Het beschermen van het nationale intellectueel eigendom is hierbij essentieel.

Wat kun je in de praktijk doen?

- **Investeer in open source en open standaarden.**
  Ook vanuit de overheid wordt ingezet op open-source technologieën .
- **Neem exit clausules op in het contract**
  En zorg dat contracten duidelijke afspraken bevatten over data-export en migratie.
- **Werk samen met andere zorgorganisaties**
  Zo kun je invloed uitoefenen op leveranciers om te zorgen voor innovatie.
- **Weeg één leverancier af tegen meerdere leveranciers**
  Eén leverancier kan overzicht en eenvoud bieden. Meerdere leveranciers kunnen juist zorgen voor meer keuzevrijheid, innovatie en minder afhankelijkheid op de lange termijn.
- **Kijk vooral naar de lange termijn**
  De impact op innovatie verschilt op korte en lange termijn. Een oplossing die nu handig lijkt, kan later vernieuwing beperken.

Bronnen

8. Rathenau Instituut, 2024; Van Eeden et al., 2025; VNG, 2025

9. Van Eeden et al., 2025

10. https://nos.nl/artikel/2618372-anthropic-schakelt-geavanceerde-ai-modellen-uit-op-last-van-regering-trump

11. Trump, 2026

12. ICT&health, 2026; Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2025

Invalshoek: Leverancier binnen de EU wordt overgenomen door partij buiten de EU

Context

Heb je eerder gekozen voor een leverancier binnen de EU om je gegevens te verwerken, en wordt deze overgenomen door een organisatie buiten de EU? Dan kunnen nieuwe risico's ontstaan. Die risico's gaan bijvoorbeeld over databescherming, toegang tot gevoelige informatie, geopolitieke beïnvloeding en de continuïteit van dienstverlening.

Een recent voorbeeld is de dreigende overname van Solvinity door het Amerikaanse Kyndryl. Solvinity beheert onder meer DigiD. Het kabinet heeft deze overname geblokkeerd .

Risico's

- **Toegang door overheden buiten de EU**
  Na een overname door een partij buiten de EU kan het risico ontstaan dat niet-Europese overheden toegang krijgen tot gevoelige data, waaronder zorgdata.
- **Onvoorspelbare interventies in dienstverlening**
  Er kan meer onzekerheid ontstaan over de continuïteit van diensten. Denk aan plotselinge wijzigingen, beperkingen of stopzetting van diensten, zoals we eerder zagen bij grote internationale providers.
- **Conflicten tussen Europese en buitenlandse wetgeving**
  Er kunnen spanningen ontstaan tussen Europese regels, zoals de AVG en NIS2, en buitenlandse regels die toegang tot data kunnen eisen.
- **Minder zekerheid over patiëntdata**
  Een overname kan invloed hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van patiëntdata.
- **Groter risico voor de zorgcontinuïteit**
  Als diensten veranderen, duurder worden of tijdelijk niet beschikbaar zijn, kan dat gevolgen hebben voor zorgprocessen en de vraag of je goede zorg kunt blijven bieden.
- **Nieuwe Europese wetgeving kunnen gevolgen hebben**
  Nieuwe Europese wetgeving, zoals CSA2, kan ervoor zorgen dat je leveranciers uit landen buiten de EU niet meer mag gebruiken in kritieke sectoren. Daardoor moet je mogelijk verplicht migreren of overstappen naar andere technologieën.

Wat kun je in de praktijk doen?

- **Zorg voor een uitgewerkte exitstrategie**

  Maak vooraf duidelijk hoe de organisatie kan overstappen naar een andere leverancier. Werk dit uit in een migratieroadmap. Zo voorkom je dat de organisatie te afhankelijk wordt van één leverancier.
- **Leg vast dat toegang vanuit derde landen niet is toegestaan**

  Maak contractuele afspraken over wie toegang heeft tot data en vanuit welke landen.
- **Versleutel data en beheer zelf de sleutels**

  Versleutel data in transit en in rest (tijdens verzending en opslag). Zorg dat de organisatie zelf de encryptiesleutels beheert. Daarmee verklein je het risico dat derden toegang krijgen tot leesbare data.
- **Onderzoek een multi-vendorstrategie**

  Bekijk of het mogelijk is om niet volledig afhankelijk te zijn van één leverancier. Meerdere leveranciers kunnen zorgen voor meer flexibiliteit en minder afhankelijkheid.
- **Neem meldplicht bij overname op in contracten**

  Leg in het inkoopcontract vast dat een leverancier een mogelijke overname minimaal drie maanden vooraf moet melden bij de zorginstelling. Zorg ook dat de Algemene Inkoopvoorwaarden Gezondheidszorg (AIVG) en de ICT-module daarvan van toepassing zijn .
- **Voer jaarlijks periodiek een leveranciersassessment uit**

  Beoordeel jaarlijks periodiek of leveranciers nog voldoen aan je eisen.
- **Neem digitale autonomie op in strategisch risicomanagement**

  Behandel digitale autonomie niet alleen als ICT-onderwerp, maar als onderdeel van strategisch risicomanagement. Zo worden risico's rond leveranciers, data, continuïteit en geopolitiek structureel meegenomen in besluitvorming.

Bronnen

13. Staatssecretaris verbiedt Amerikaanse overname Solvinity, bedrijf achter DigiD

14. Zie artikel 21.1g van de AIVG

Bijlage 1: Invalshoeken

Digitale autonomie is complex.

Keuzes op dit gebied raken meerdere risico's tegelijk. Denk aan veiligheid, continuïteit, kosten, leveranciersafhankelijkheid, privacy en zeggenschap over data.

Daarom helpt het om digitale autonomie vanuit verschillende invalshoeken te bekijken. Per invalshoek laten we zien welke risico's er zijn en hoe je daar in de praktijk mee om kunt gaan.

Bijlage 2: Amerikaanse wetgeving

Amerikaanse wetgeving en Europese data

De CLOUD Act is in 2018 van kracht geworden. Deze Amerikaanse wet geeft Amerikaanse opsporingsdiensten toegang tot bedrijfs- en klantgegevens van cloud- en communicatieproviders. Het maakt daarbij niet uit waar die gegevens fysiek zijn opgeslagen.

De wet geldt voor Amerikaanse bedrijven en hun dochterondernemingen. Dus ook voor grote cloudproviders zoals AWS, Google Cloud en Microsoft Azure. Gegevens die zijn opgeslagen in datacenters in de EU zijn daardoor niet automatisch beschermd tegen toegang door Amerikaanse autoriteiten. Dat betekent dat ook handelsgeheimen, intellectueel eigendom en andere gevoelige informatie kunnen worden ingezien.

FISA 702 en toegang door inlichtingendiensten

In 2008 werd FISA 702 goedgekeurd als onderdeel van de USA Patriot Act. Sindsdien hebben Amerikaanse inlichtingendiensten in bepaalde situaties geen gerechtelijk bevel meer nodig om toegang te krijgen tot gegevens van aanbieders van elektronische communicatiediensten. Dat geldt wanneer het doelwit geen Amerikaanse burger is en zich buiten de VS bevindt.

De onthullingen van Edward Snowden in 2013 lieten zien hoe ver de NSA en andere Amerikaanse inlichtingendiensten hierin kunnen gaan. Daaruit bleek dat Amerikaanse bedrijven zoals Microsoft, Google, Apple en Facebook toegang gaven tot live communicatie en opgeslagen informatie van Europese burgers.

EU-VS Data Privacy Framework

Het EU-VS Data Privacy Framework is in 2023 ingevoerd als opvolger van het Privacy Shield. Het doel was om gegevensuitwisseling tussen de EU en de VS beter te regelen. Het Europees Parlement uitte kort na de invoering echter al zorgen over de juridische houdbaarheid van dit framework.

Volgens de nieuwe regels mogen Amerikaanse autoriteiten alleen toegang krijgen tot Europese gegevens als dit strikt noodzakelijk is voor specifieke en legitieme veiligheidsdoeleinden. Een belangrijke vernieuwing is het tweedelige rechtsbeschermingsmechanisme. De Civil Liberties Protection Officer is daarbij het eerste aanspreekpunt. Deze functionaris moet erop toezien dat Amerikaanse inlichtingendiensten grondrechten naleven en privacy respecteren.

Daarnaast is het Data Protection Review Court opgericht. Dit is een tweede instantie die klachten kan beoordelen. Deze rechtbank bestaat uit ervaren juristen die geen deel uitmaken van de Amerikaanse overheid. Zij mogen geheime documenten van inlichtingendiensten inzien en bindende besluiten nemen. Zij kunnen bijvoorbeeld bepalen dat onrechtmatig verzamelde gegevens moeten worden verwijderd.

Toch zijn er zorgen over de onafhankelijkheid van dit systeem. De leden van deze instantie worden namelijk benoemd na goedkeuring door het hoogste hoofd van de Amerikaanse geheime diensten.

Kwetsbaarheid van het toezicht

De regering-Trump heeft eind januari 2025, kort na haar aantreden, drie Democratische leden van de Privacy and Civil Liberties Oversight Board ontslagen. Deze toezichthouder heeft minimaal drie actieve leden nodig om besluiten te kunnen nemen. Sindsdien kan dit centrale toezichthoudende orgaan niet goed functioneren. Daarmee staat ook het tweedelige rechtsbeschermingsmechanisme onder druk.

Daar komt bij dat de juridische basis van het EU-VS Data Privacy Framework kwetsbaar is. Het framework is grotendeels gebaseerd op Executive Order 14086 van president Biden. President Trump zou dit besluit met een nieuw presidentieel decreet kunnen intrekken. Daardoor kan de juridische grondslag van de ene op de andere dag wegvallen.

Certificering van Amerikaanse bedrijven

Amerikaanse bedrijven die persoonsgegevens uit de EU willen verwerken, kunnen zich vrijwillig laten certificeren bij het Amerikaanse ministerie van Handel. Dat gebeurt onder het Data Privacy Framework. Om gecertificeerd te worden, moeten bedrijven publiek beloven dat zij zich aan de DPF-principes houden. Daarmee zeggen zij toe dat zij ook voldoen aan Europese normen voor gegevensbescherming. Deze belofte is vervolgens afdwingbaar onder Amerikaanse wetgeving. Het Amerikaanse ministerie van Handel controleert de naleving.

Als EU-burgers vermoeden dat hun gegevens worden misbruikt, kunnen zij contact opnemen met de bevoegde privacytoezichthouder. De klachtenprocedure biedt verschillende rechtsmiddelen. Deze worden geregeld door het Europees Comité voor gegevensbescherming.

Conclusie: bescherming blijft onzeker

De CLOUD Act, FISA 702 en het Data Privacy Framework lijken samen onvoldoende waarborgen te bieden voor de bescherming van bedrijfsgegevens en persoonsgegevens van Europese organisaties en inwoners bij het gebruik van Amerikaanse cloud- en communicatiediensten.

De Amerikaanse wetgeving bevat mogelijkheden waardoor Amerikaanse inlichtingendiensten toegang kunnen krijgen tot Europese data in communicatie- en cloudsystemen van Amerikaanse bedrijven. Dat kan gebeuren zonder dat Europese organisaties daarvan op de hoogte zijn.

Omdat Amerikaanse inlichtingendiensten worden aangestuurd door de Amerikaanse regering, zijn deze risico's niet alleen theoretisch. Daarom is nader onderzoek nodig naar het verminderen van de afhankelijkheid van Amerikaanse cloud- en communicatieproviders. Op basis van de Europese privacywetgeving, de AVG, kan dit onderzoek zelfs noodzakelijk zijn.

Bijlage 3: Casus - EU krijgt geen toegang meer tot Microsoft

Trigger

Een geopolitiek incident kan leiden tot een juridische maatregel of handelsmaatregel. Daardoor kan Microsoft verplicht worden, of zelf besluiten, om diensten voor EU-klanten tijdelijk of gedeeltelijk te blokkeren. Ook kan het gaan om beperkingen voor specifieke accounts, tenants, organisaties of functies.

Zo'n blokkade kan verschillende vormen aannemen:

- **Soft cut:** Microsoft beperkt bijvoorbeeld updates, licenties, support of bepaalde cloudfuncties.
- **Hard cut:** Organisaties krijgen geen toegang meer tot Microsoft 365, Entra ID of Azure-diensten. Daardoor vallen onder meer authenticatie, e-mail, Teams, SharePoint en OneDrive uit.
- **Targeted cut:** Alleen specifieke organisaties, afdelingen, rollen of personen worden geraakt, bijvoorbeeld als gevolg van sancties.

Scenario: hard cut van Microsoft Cloud

Trigger

In dit scenario leidt een geopolitiek of juridisch conflict tot maatregelen waardoor Microsoft diensten moet beperken. Het kan ook gaan om maatregelen waardoor Microsoft bepaalde licenties of tenants in de EU niet langer mag bedienen. In het zwaarste geval wordt toegang tot authenticatie en cloudplatforms geblokkeerd. Dit kan gebeuren via sancties, handelsmaatregelen of juridische bevelen.

Het belangrijkste risico is niet alleen waar de data staat. Ook als data in Europa wordt opgeslagen, kan de toegang tot digitale voorzieningen worden beïnvloed door buitenlandse wetgeving, externe rechtsmacht en geopolitieke ontwikkelingen.

Mogelijke effecten

Een hard cut kan grote gevolgen hebben voor de dagelijkse werking van een ziekenhuis:

- Medewerkers kunnen niet meer inloggen via Entra ID (voorheen Azure AD);
- Microsoft 365, Outlook, Teams, SharePoint en OneDrive zijn niet of beperkt bereikbaar;
- Toegang tot de Azure Portal, Azure-diensten en Microsoft security tooling in de cloud valt weg;
- Single Sign-On en Multi-Factor Authenticatie via Entra werken niet meer;
- Alle applicaties die Entra gebruiken voor authenticatie of conditional access kunnen problemen krijgen;

- Microsoft 365-data kan fysiek nog bestaan, maar is op dat moment niet bereikbaar of slechts beperkt te exporteren.

Daarmee ontstaat niet alleen een technisch probleem, maar ook een probleem voor samenwerking, communicatie, informatievoorziening en zorgcontinuïteit.

Operationele tijdlijn

- **0 tot 1 uur:** Er ontstaan massaal inlogproblemen. SSO en MFA werken niet meer. Teams en Outlook vallen uit. De servicedesk raakt snel overbelast.
- **1 tot 6 uur:** Klinische processen die afhankelijk zijn van kantoorapplicaties lopen vast. Denk aan roosters, protocollen, overdrachten en interne coördinatie. De crisisorganisatie wordt opgeschaald.
- **6 tot 72 uur:** Werken via papier, telefoon en noodprocedures wordt de norm. De organisatie moet zorg prioriteren. Niet-spoedeisende zorg kan worden uitgesteld. Door workarounds neemt de kans op fouten toe.

Impactkaart voor ziekenhuizen: Wat valt er stil?

Directe uitval

- **Entra ID:** Dit is vaak de grootste kwetsbaarheid. Als Entra ID wordt gebruikt voor SSO, MFA en conditional access, kunnen veel applicaties niet meer worden geopend. Dat geldt soms ook voor applicaties die lokaal of on-premise draaien, maar Entra gebruiken als identity provider.
- **E-mail en agenda:** Exchange Online valt uit. Daardoor raken interne coördinatie, ketencommunicatie, afspraken en spreekurenplanning ontregeld.
- **Teams:** Chat, vergaderen en eventueel telefonie via Teams Phone vallen weg. Dat raakt onder meer MDO's, afstemming tussen SEH en OK en interne crisiscommunicatie.
- **SharePoint en OneDrive:** Protocollen, formulieren, roosters, werkinstructies en beleidsdocumenten zijn niet meer bereikbaar als deze alleen daar staan.

Tweede-orde effecten

Naast de directe uitval ontstaan er ook indirecte problemen. Juist deze effecten worden vaak onderschat.

- **Autorisaties en groepen:** Als Entra leidend is voor groepsrechten en rollen, vallen autorisatiestructuren weg. Het herstel daarvan kan ingewikkeld zijn.

- **Servicedesk en ITSM:** Als ITSM, CMDB of ticketing via SSO of SaaS werkt, wordt ook de incidentafhandeling vertraagd.
- **Security monitoring:** Cloudgebaseerde logging, meldingen en beveiligingstools werken minder goed of vallen uit. Daardoor heeft de organisatie minder zicht op cyberdreigingen, juist op het moment dat zij in crisismodus zit.

Wat blijft mogelijk beschikbaar?

Niet alles hoeft stil te vallen. Sommige voorzieningen kunnen blijven werken, afhankelijk van de inrichting.

- On-premise EPD's en klinische systemen kunnen beschikbaar blijven als er lokale authenticatie of een lokale Active Directory-fallback is.
- Telefonie, DECT en paging kunnen blijven werken als deze niet afhankelijk zijn van Teams of een cloudafhankelijke beheerlaag.

Advies aan de sector: vergroot de weerbaarheid

Deze casus laat zien dat het risico niet alleen bij individuele ziekenhuizen ligt. Omdat veel zorgorganisaties op dezelfde digitale voorzieningen steunen, is ook sectorbrede weerbaarheid nodig.

Sectorbrede maatregelen

- **Maak een standaard draaiboek 'Hard Cut Microsoft'**
  Zorg voor een sectorbreed draaiboek voor alle ziekenhuizen. Gebruik dezelfde begrippen, rollen, tijdlijnen en escalatieroutes.
- **Richt sectorbrede noodcommunicatie in**
  Zorg voor een kleine, Europees gehoste noodvoorziening voor crisisrollen. Denk aan noodmail en noodchat. Deze voorziening is niet bedoeld voor dagelijkse zorgdata, maar voor coördinatie in crisissituaties. Combineer dit met een vaste telefoonboom.
- **Maak een referentiearchitectuur voor identiteit**
  Voorkom dat Entra de enige identity provider is voor klinische kernprocessen. Ontwerp met een tweede route, lokale fallback of break-glass-toegang voor kritieke systemen.
- **Neem exit- en portabiliteitseisen op in contracten**
  Leg in aanbestedingen en contracten vast dat data exporteerbaar is, dat open formaten worden gebruikt en dat rechtenstructuren kunnen worden hersteld. Dit is belangrijk omdat juist Entra en rechtenstructuren lastig te herstellen kunnen zijn.

- **Oefen twee keer per jaar**

  Organiseer jaarlijks meerdere oefeningen met ziekenhuizen, Z-CERT en NCSC. Combineer tabletop-oefeningen met technische tests. Leg verbeterpunten vast en volg op of deze daadwerkelijk worden uitgevoerd.

Oefenen en meten

Een CISO kan deze casus vertalen naar meetpunten die ook richting de raad van bestuur te rapporteren zijn.

- **RTO en RPO per kritiek zorgdomein**

  Bepaal per domein, zoals SEH, OK, IC, lab, radiologie en apotheek, hoe lang veilig kan worden doorgewerkt zonder Microsoft 365 en Entra.
- **Beschikbaarheid van nooddocumentatie**

  Meet welk percentage protocollen, formulieren en werkinstructies offline beschikbaar is en actueel blijft.
- **Identity resilience score**

  Breng in kaart hoeveel kritieke systemen niet volledig afhankelijk zijn van cloud-only authenticatie.
- **Oefenfrequentie en opvolging**

  Meet hoe vaak wordt geoefend en hoeveel verbeteracties binnen 90 dagen zijn afgerond.

Referentielijst

1. ICT&health. (2026, February 9). VWS zet open source centraal in de toekomst van digitale zorg. https://www.Icthealth.Nl/Nieuws/Vws-Zet-Open-Source-Centraal-in-de-Toekomst-van-Digitale-Zorg.
2. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2025). Visie Digitale autonomie en soevereiniteit van de overheid.
3. Rathenau Instituut. (2024). Digitale afhankelijkheid zet onze autonomie onder druk.
4. Regeerakkoord 2026-2030. (2026).
5. Trump, D. (2026). President Trump's cyber strategy for America.
6. Van Eeden, Q., Karstens, B., & Van Huijstee, M. (2025). Koers zetten richting digitale autonomie Handelingsopties voor beleidsmakers en inkopers.
7. VNG. (2025). Position paper Digitale autonomie.

De Nederlandse zorg digitaal veilig