



interconnect.nl

Whitepaper



De 5 dimensies van een soevereine cloud

Een praktische vertaling van het DICTU
Toetsingsinstrument Sovereiniteit Clouddiensten

Inleiding

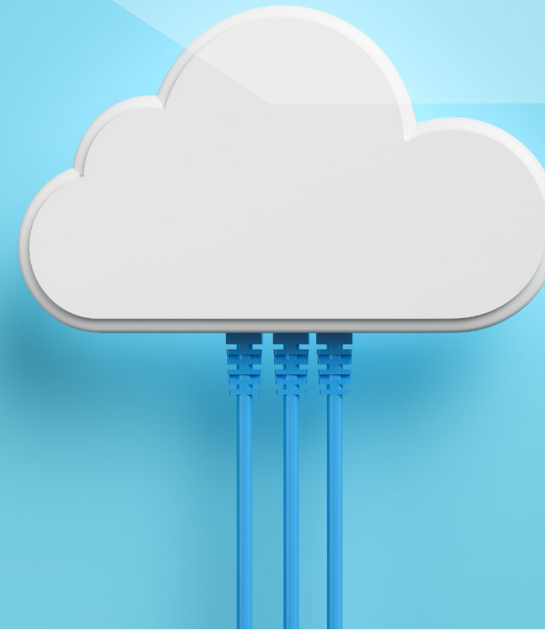
DE 5 DEMENSIES VAN EEN SOEVEREINE CLOUD

Wilt u meer informatie of persoonlijk advies? Neem dan contact op met solutions@interconnect.nl

Steeds meer organisaties brengen bedrijfskritische applicaties en data onder in de cloud. Dat biedt flexibiliteit, schaalbaarheid en toegang tot innovatieve technologieën. Tegelijkertijd neemt de afhankelijkheid van cloudleveranciers toe. Daarmee ontstaat een belangrijke vraag: hoe houdt u grip op uw data?

Het beoordelen van datasoevereiniteit is in de praktijk niet altijd eenvoudig. Het vraagt om meer dan alleen inzicht in de locatie van uw data. Een doordachte cloudstrategie gaat daarom verder dan prestaties, kosten en schaalbaarheid.

Ook de mate waarin u de regie behoudt over uw data speelt een belangrijke rol. Zonder bewuste afwegingen kunnen afhankelijkheden ontstaan die pas zichtbaar worden wanneer u wilt overstappen, nieuwe wetgeving van kracht wordt of een leverancier zijn dienstverlening wijzigt. Juist daarom is het belangrijk om datasoevereiniteit vanaf het begin mee te nemen in uw cloudstrategie.



Om organisaties hierbij te ondersteunen, ontwikkelde de **Dienst ICT Uitvoering (DICTU)**, onderdeel van het ministerie van Economische Zaken, het Toetsingsinstrument Sovereiniteit Clouddiensten. Dit instrument biedt een uitgebreid beoordelingskader waarmee organisaties datasoevereiniteit vanuit verschillende perspectieven kunnen beoordelen. Tegelijkertijd maakt juist die uitgebreidheid het soms lastig om de vertaalslag naar de dagelijkse praktijk te maken.

Deze paper vertaalt de belangrijkste inzichten uit het DICTU-toetsingsinstrument naar een compacte en praktische leidraad. Aan de hand van herkenbare situaties uit de praktijk ontdekt u welke vijf dimensies samen de mate van datasoevereiniteit bepalen. Niet om één cloudstrategie als de juiste te presenteren, maar om u te helpen de juiste vragen te stellen. Want hoe beter u begrijpt welke afwegingen een rol spelen, hoe beter u kunt bepalen welke cloudomgeving past bij de behoeften en risicobereidheid van uw organisatie.

1. Juridische soevereiniteit

Onder welke wetgeving valt uw cloudleverancier?

Wanneer u een cloudleverancier kiest, kijkt u waarschijnlijk naar prestaties, beveiliging en uiteraard kosten. Maar minstens zo belangrijk is een andere vraag: onder welke wetgeving valt de organisatie achter uw cloudomgeving?

Dat lijkt misschien vanzelfsprekend, want uw data staat immers in Nederland of Europa. Toch zegt de locatie van een datacenter niet automatisch iets over de wetgeving waaraan een cloudleverancier uiteindelijk verantwoording moet afleggen. De vestigingsplaats van het moederbedrijf, de eigendomsstructuur en het toepasselijke recht kunnen namelijk net zo bepalend zijn voor de mate waarin uw organisatie de regie houdt over haar data.

Het DICTU Toetsingsinstrument Soevereiniteit Clouddiensten noemt dit de dimensie 'Juridische soevereiniteit' en kijkt naar drie onderdelen:

1. **Vestiging**
Waar is het moederbedrijf van uw cloudleverancier juridisch gevestigd?
2. **Zeggenschap en eigenaarschap**
Wie heeft uiteindelijk de controle over de organisatie achter de cloudomgeving?
3. **Toepasselijk recht**
Onder welke wetgeving valt uw cloudleverancier en welke gevolgen kan dat hebben voor uw data?

In de praktijk

Uw organisatie kiest bewust voor een cloudleverancier met een Nederlands datacenter, zodat uw data binnen Nederland blijft. Tijdens een leveranciersgesprek blijkt echter dat het moederbedrijf buiten Europa is gevestigd. Daarmee ontstaat de vraag of uitsluitend Europese wetgeving van toepassing is, of dat ook buitenlandse wetgeving invloed kan hebben op uw data. Pas op dat moment wordt duidelijk dat de locatie van een datacenter slechts één onderdeel is van een juridisch complexe afweging.

Waarom is dit belangrijk?

Juridische afhankelijkheden zijn vaak niet zichtbaar wanneer u een cloudomgeving selecteert. Pas wanneer wetgeving verandert, een verzoek om datatoegang wordt ingediend of een conflict tussen mogendheden ontstaat of dreigt te ontstaan, blijkt welke juridische kaders daadwerkelijk van toepassing zijn. Door vooraf inzicht te krijgen in de vestigingsplaats, zeggenschap en het toepasselijke recht van uw cloudleverancier, kunt u beter beoordelen of de cloudomgeving aansluit bij de eisen en verantwoordelijkheden van uw organisatie.

Vragen die u zichzelf kunt stellen

- Waar is het moederbedrijf van mijn cloudleverancier juridisch gevestigd?
- Wie heeft uiteindelijk de zeggenschap over de organisatie?
- Onder welke wetgeving valt mijn cloudleverancier?
- Kan buitenlandse wetgeving invloed hebben op de toegang tot mijn data?
- Loop ik risico speelbal te worden in een conflict, bijvoorbeeld tussen staten of over IP?
- Sluit dit aan bij de eisen en risicobereidheid van mijn organisatie?

Kort samengevat

De locatie van uw data vertelt slechts een deel van het verhaal. Voor een goede beoordeling van een soevereine cloud is het minstens zo belangrijk om te kijken naar de vestigingsplaats, de zeggenschap en het toepasselijke recht van uw cloudleverancier.

2. Data & AI

Is uw data voldoende beschermd?

In het vorige hoofdstuk las u dat een soevereine cloud verder gaat dan de locatie van uw data. Ook de juridische context van uw cloudleverancier speelt een belangrijke rol. Maar zelfs wanneer de juridische aspecten goed zijn geregeld, blijft één belangrijke vraag over: in welke mate is uw data daadwerkelijk beschermd?

De bescherming van data gaat namelijk verder dan een veilige opslaglocatie of het gebruik van encryptie. Uw data wordt opgeslagen, verwerkt en geback-upt. Daarnaast worden metadata en logbestanden verzameld en kunnen gegevens worden gebruikt voor analyses of AI-toepassingen. Het is daarom belangrijk om te weten waar uw data zich bevindt, wie er technisch toegang toe heeft en welke bescherming uw leverancier biedt wanneer derden toegang proberen te krijgen.

Het DICTU Toetsingsinstrument Sovereiniteit Clouddiensten noemt dit de dimensie 'Data & AI' en kijkt naar drie onderdelen:

1. Opslag en verwerking van data

Worden al uw gegevens, inclusief back-ups, metadata en logbestanden, uitsluitend binnen Europa opgeslagen en verwerkt? Daarbij kijkt DICTU ook of data buiten Europa wordt gebruikt voor analyses of AI-training.

2. Technische bescherming

Kan de cloudleverancier technisch toegang krijgen tot ongecodeerde data of houdt u zelf de regie over het beheer van encryptiesleutels?

3. Juridische bescherming

Welke afspraken zijn gemaakt wanneer een buitenlandse overheid toegang tot uw data vraagt? Informeert de leverancier u hierover en biedt hij waar mogelijk juridisch verweer?

In de praktijk

Een organisatie kiest bewust voor een cloudleverancier die alle primaire data binnen Europa opslaat. Tijdens een leveranciersgesprek blijkt echter dat metadata buiten Europa wordt verwerkt voor analyses en dat de leverancier de encryptiesleutels beheert. Hoewel de data veilig lijkt opgeslagen, blijkt de bescherming van gegevens uit meer te bestaan dan alleen de locatie van het datacenter.

Waarom is dit belangrijk?

Data behoort vaak tot de meest waardevolle bedrijfsmiddelen van een organisatie. Daarom is het belangrijk om niet alleen te kijken waar gegevens worden opgeslagen, maar ook hoe ze gedurende de hele levenscyclus worden beschermd.

Door inzicht te krijgen in de opslag en verwerking van data, de technische toegangsbeveiliging en de juridische bescherming, kunt u beter beoordelen in hoeverre u daadwerkelijk de regie houdt over uw gegevens.

Vragen die u zichzelf kunt stellen

- Worden al mijn data, inclusief back-ups, metadata en logbestanden, uitsluitend binnen Europa opgeslagen en verwerkt?
- Wie beheert de encryptiesleutels van mijn data?
- Kan mijn cloudleverancier technisch toegang krijgen tot ongecodeerde data?
- Welke afspraken zijn gemaakt wanneer een buitenlandse overheid toegang tot mijn data vraagt?
- Word ik hierover geïnformeerd en biedt mijn leverancier waar mogelijk juridisch verweer?

Kort samengevat

De bescherming van uw data gaat verder dan de locatie van een datacenter of het gebruik van encryptie. Ook de opslag en verwerking van gegevens, het beheer van encryptiesleutels en de juridische bescherming van uw data bepalen in hoeverre u daadwerkelijk de regie houdt over uw cloudomgeving.

3. Technische soevereiniteit

Hoe afhankelijk bent u van uw cloudleverancier?

In de vorige hoofdstukken zag u dat een soevereine cloud verder gaat dan de locatie van uw data. Ook de juridische context van uw cloudleverancier en de bescherming van uw gegevens spelen een belangrijke rol. Maar zelfs wanneer deze aspecten goed zijn geregeld, volgt de volgende belangrijke vraag: houdt u ook de regie over de technologie waarop uw cloudomgeving is gebouwd?

Technologie kan uw organisatie vrijheid geven, maar ook afhankelijk maken. Veel cloudplatformen bieden krachtige functionaliteiten die innovatie versnellen en beheer vereenvoudigen. Tegelijkertijd kunnen deze technologieën ervoor zorgen dat een overstap naar een andere leverancier steeds complexer wordt. Het is daarom belangrijk om te begrijpen welke afhankelijkheden ontstaan en of deze aansluiten bij de strategie van uw organisatie.

Het DICTU Toetsingsinstrument Soevereiniteit Clouddiensten noemt dit de dimensie 'Technologie' en kijkt naar vier onderdelen:

1. Interoperabiliteit & portabiliteit

Maakt uw cloudomgeving gebruik van open standaarden, zodat data en workloads eenvoudig kunnen worden uitgewisseld of verplaatst naar een andere cloudomgeving?

2. Open source

Maakt de cloudomgeving gebruik van open-sourcesoftware voor de kerncomponenten? Open source kan de afhankelijkheid van één leverancier verkleinen en maakt het eenvoudiger om workloads naar een andere omgeving te verplaatsen. De grootste meerwaarde ontstaat wanneer de software wordt ondersteund door een actieve, onafhankelijke community.

3. Softwaretransparantie

Is inzichtelijk hoe de gebruikte software werkt? En is de broncode of de werking van software en algoritmen controleerbaar, zodat u niet afhankelijk bent van een 'black box'?

4. Operationele omkeerbaarheid

Kan een andere partij de dienstverlening overnemen wanneer de samenwerking eindigt of de leverancier uitvalt? En is daarvoor voldoende documentatie beschikbaar?

In de praktijk

Uw organisatie draait al enkele jaren succesvol op een cloudplatform. De dienstverlening voldoet aan alle verwachtingen en nieuwe functionaliteiten worden snel geïntroduceerd. Wanneer u onderzoekt of een deel van de omgeving naar een andere cloudleverancier kan worden verplaatst, blijkt dat applicaties sterk afhankelijk zijn van platformspecifieke diensten. Een overstap is mogelijk, maar vraagt aanzienlijk meer tijd, expertise en investeringen dan vooraf werd verwacht.

Waarom is dit belangrijk?

Technologische afhankelijkheid ontstaat vaak geleidelijk. Organisaties kiezen begrijpelijkerwijs voor oplossingen die vandaag het beste aansluiten bij hun behoeften. Pas wanneer een overstap, uitbreiding of migratie aan de orde is, wordt duidelijk hoeveel vrijheid de gekozen technologie nog biedt.

Door vooraf inzicht te krijgen in de samenwerking met andere systemen, de gebruikte technologie en de mogelijkheid om over te stappen, kunt u beter beoordelen of uw cloudomgeving ook op de lange termijn aansluit bij de ambities van uw organisatie.

Vragen die u zichzelf kunt stellen

- Is mijn cloudomgeving gebaseerd op open standaarden?
- Kan ik mijn data en applicaties eenvoudig verplaatsen naar een andere leverancier?
- Ben ik afhankelijk van technologie van één leverancier?
- Is inzichtelijk hoe de gebruikte software en algoritmen werken?
- Kan een andere partij de dienstverlening overnemen wanneer dat nodig is?

Kort samengevat

Technologische soevereiniteit draait om keuzevrijheid. Door inzicht te krijgen in de gebruikte technologie en de mate van afhankelijkheid, kunt u beter beoordelen of uw cloudomgeving ook in de toekomst blijft aansluiten bij de behoeften van uw organisatie.

4. Operationele soevereiniteit

Wie heeft de controle over uw cloudomgeving?

In de vorige hoofdstukken keek u naar de juridische context van uw cloudleverancier, de bescherming van uw data en de technologie waarop uw cloudomgeving is gebouwd. Dan volgt de volgende vraag: wie beheert uw cloudomgeving eigenlijk in de praktijk?

Een cloudomgeving draait namelijk niet vanzelf. Achter de schermen worden systemen beheerd, updates uitgevoerd en storingen opgelost. Daarbij spelen niet alleen technologie en processen een rol, maar ook de mensen die toegang hebben tot uw omgeving en de locatie van waaruit deze werkzaamheden worden uitgevoerd. Juist deze operationele kant bepaalt in belangrijke mate hoeveel controle u daadwerkelijk behoudt.

Het DICTU Toetsingsinstrument Soevereiniteit Clouddiensten noemt dit de dimensie 'Operationeel' en kijkt hierbij naar drie onderdelen:

1. Infrastructuur en beheer

Worden de infrastructuur én de beheeromgeving (control plane) volledig vanuit Europa beheerd?

2. Personeel met beheertoegang

Wie heeft toegang tot uw cloudomgeving? En worden beheerwerkzaamheden uitgevoerd door personeel dat onder de Europese jurisdictie valt?

3. Continuïteit van de dienstverlening

Hoe waarborgt uw cloudleverancier de continuïteit wanneer geopolitieke ontwikkelingen of verstoringen in de toeleveringsketen optreden?

In de praktijk

Uw organisatie maakt gebruik van een cloudomgeving die volledig in Europa draait. Tijdens een audit blijkt echter dat een deel van het beheer wordt uitgevoerd vanuit een land buiten Europa en dat specialistische beheerders toegang hebben tot uw productieomgeving. De infrastructuur staat dan wel in Europa, maar de operationele controle blijkt breder te zijn georganiseerd dan u vooraf had verwacht.

Waarom is dit belangrijk?

De operationele controle over een cloudomgeving is vaak minder zichtbaar dan de techniek waarop deze draait. Toch kan juist deze controle bepalend zijn voor de continuïteit en betrouwbaarheid van de dienstverlening. Door inzicht te krijgen in waar de infrastructuur wordt beheerd, wie toegang heeft tot uw omgeving en hoe uw leverancier omgaat met verstoringen in de supply chain, kunt u beter beoordelen in hoeverre uw cloudomgeving aansluit bij de eisen van uw organisatie.

Vragen die u zichzelf kunt stellen

- Worden de infrastructuur en de beheeromgeving volledig vanuit Europa beheerd?
- Wie heeft beheertoegang tot mijn cloudomgeving?
- Vallen deze beheerders onder de Europese jurisdictie?
- Heeft mijn cloudleverancier een strategie om verstoringen in de supply chain op te vangen?
- Is de operationele continuïteit van de dienstverlening voldoende geborgd?



Kort samengevat

Operationele soevereiniteit draait om de vraag wie uw cloudomgeving beheert en onder welke omstandigheden dat gebeurt. Door inzicht te krijgen in de infrastructuur, het beheer en de continuïteit van de dienstverlening, kunt u beter beoordelen hoeveel operationele regie u daadwerkelijk behoudt.

5. Menselijke soevereiniteit

Wie heeft toegang tot uw cloudomgeving?

In de vorige hoofdstukken heeft u gekeken naar de juridische, technische en operationele aspecten van een soevereine cloud. Maar uiteindelijk zijn het mensen die cloudomgevingen ontwerpen, beheren en doorontwikkelen. Daarom is het belangrijk om niet alleen te weten **wie** toegang heeft tot uw systemen en data, maar ook **of deze mensen beschikken over de juiste kennis, ervaring en bevoegdheden**.

Een veilige en soevereine cloudomgeving vraagt namelijk om meer dan goede technologie. Ook de mensen die ermee werken spelen een belangrijke rol. Zijn medewerkers voldoende gescreend? Beschikken zij over de juiste certificeringen? En heeft uw cloudleverancier voldoende kennis en capaciteit in huis om de dienstverlening zelfstandig te ontwikkelen en te beheren?

Het DICTU Toetsingsinstrument Soevereiniteit Clouddiensten noemt dit de dimensie 'Mens' en kijkt hierbij naar twee onderdelen:

1. Training, certificering en screening

Zijn medewerkers met toegang tot kritieke systemen aantoonbaar gescreend, goed opgeleid en beschikken zij over de juiste certificeringen om hun werkzaamheden veilig en verantwoord uit te voeren?

2. Capaciteit en vaardigheden

Beschikt de cloudleverancier over voldoende interne kennis, capaciteit en expertise om de cloudomgeving zelfstandig te bouwen, beheren en verder te ontwikkelen, zonder structureel afhankelijk te zijn van externe partijen?

In de praktijk

Uw cloudomgeving draait stabiel en voldoet aan alle technische eisen. Tijdens een leveranciersaudit blijkt echter dat specialistische kennis grotendeels is ondergebracht bij externe partijen en dat niet inzichtelijk is welke medewerkers toegang hebben tot kritieke systemen. De technologie is op orde, maar de afhankelijkheid van mensen en expertise blijkt groter dan vooraf werd aangenomen.

Waarom is dit belangrijk?

Een cloudomgeving is nooit sterker dan de mensen die deze beheren. Goed opgeleide en gescreende medewerkers verkleinen niet alleen veiligheidsrisico's, maar zorgen er ook voor dat kennis binnen de organisatie behouden blijft. Daarnaast geeft voldoende interne capaciteit meer zekerheid dat een cloudleverancier zelfstandig kan blijven innoveren, beheren en ondersteuning kan bieden wanneer dat nodig is.

Vragen die u zichzelf kunt stellen

- Zijn medewerkers met toegang tot mijn cloudomgeving aantoonbaar gescreend en gecertificeerd?
- Heeft mijn cloudleverancier voldoende interne kennis en capaciteit om de dienstverlening zelfstandig te beheren?
- In welke mate is de leverancier afhankelijk van externe partijen voor beheer of doorontwikkeling?
- Is duidelijk welke medewerkers toegang hebben tot kritieke systemen en data?
- Sluit de kennis en expertise van de leverancier aan bij de behoeften van mijn organisatie?

Kort samengevat

Menselijke soevereiniteit draait om vertrouwen in de mensen achter de technologie. Door inzicht te krijgen in de kennis, betrouwbaarheid en capaciteit van het personeel, kunt u beter beoordelen in hoeverre uw cloudomgeving ook op de lange termijn veilig, beheersbaar en toekomstbestendig is.

Een soevereine cloud vraagt om meer dan een keuze voor een leverancier. Het vraagt om inzicht in de afwegingen die bepalend zijn voor de regie over uw data, technologie en cloudomgeving. De vijf dimensies uit deze paper bieden daarvoor een praktisch uitgangspunt.

OVER INTERCONNECT

Sinds 1995 ondersteunt Interconnect organisaties bij het bouwen aan een betrouwbare en toekomstbestendige IT-infrastructuur. Als honderd procent Nederlands Data & Cloud Center helpen we IT-professionals met veilige cloud- en datacenteroplossingen die aansluiten op de behoeften van vandaag én morgen.

Onze twee Tier 3-datacenters in Eindhoven en 's-Hertogenbosch vormen samen het grootste datacenter van Zuid-Nederland. Vanuit deze locaties profiteert u van volledig Nederlandse datasoevereiniteit, een uptimegarantie van 99,9% en een hoogwaardige, veilig beheerde infrastructuur met bijna 8.000 vierkante meter datacenterruimte.

Of het nu gaat om colocatie, cloudoplossingen of een hybride IT-omgeving: we denken graag met u mee over een oplossing die past bij uw organisatie, zodat u zich kunt richten op wat voor u belangrijk is.

NEEM HIER
CONTACT OP
MET ONZE
SPECIALISTEN

Heeft u vragen over Private Cloud van Interconnect?

Wij helpen u graag verder

Heeft deze whitepaper u nieuwe inzichten gegeven of zijn er nog vragen die u graag wilt bespreken? Onze specialisten denken graag met u mee en helpen u verder met informatie die past bij uw situatie. Neem contact op via **073 - 88 000 00**, solutions@interconnect.nl of het contactformulier op onze website.