



DIGITALE SOEVEREINITEIT IN DE CLOUD: EEN WAKE-UP CALL

DIBRAN MULDER | CTO CAESAR GROEP

INLEIDING: DE AFHANKELIJKHEID VAN BIG TECH

Europese organisaties – van overheidsinstellingen tot universiteiten – zijn het afgelopen decennium in rap tempo in een toenemende mate afhankelijk geworden van BigTech en hun cloudoplossingen. Menig organisatie draait zijn hele automatisering op Amerikaanse clouddiensten zoals Microsoft 365. Een open brief van bezorgde medewerkers aan de Radboud Universiteit wees er recent op dat de universiteit “voor al haar (kantoor)werk afhankelijk is van Microsoft Office 365 en andere (Amerikaanse) bedrijven”, met alle risico’s van dien in het huidige geopolitieke klimaat [cs.ru.nl]. Ook binnen de Rijksoverheid zien we deze trend: volgens de Algemene Rekenkamer draait meer dan de helft van de belangrijkste cloudservices bij het Rijk inmiddels op de public clouds van Amazon, Microsoft of Google. Het kwalijke is dat dit vaak gebeurde zonder een bewuste strategische afweging [rekenkamer.nl].

WAAROM IS DIT EEN PROBLEEM?

Deze cloudgiganten bieden innovatie, schaalvoordelen en hoge beveiligingsstandaarden. Toch groeit de vrees dat deze diepe afhankelijkheid van Big Tech onze digitale soevereiniteit ondermijnt. Digitale soevereiniteit betekent dat een land of organisatie zelf zeggenschap houdt over zijn digitale infrastructuur en data, conform eigen waarden en wetten. Als cruciale IT volledig in handen is van buitenlandse partijen, komt die zeggenschap in het geding. Geopolitieke verschuivingen kunnen dan ineens voelbaar worden in jouw serverruimtes en applicaties.

DIBRAN MULDER
CTO CAESAR GROEP



GEVOLGEN: VAN VERSTORING TOT CHANTAGE

De risico's van een eenzijdige cloudafhankelijkheid zijn allerm minst theoretisch. De open brief aan de Radboud medewerkers schetst scherpe scenario's: trans-Atlantische verbindingen kunnen verbroken worden, Microsoft kan gedwongen worden het virtuele kantoor te sluiten, waardoor al het werk stilvalt, en alle (persoonlijke) data kunnen door deze bedrijven ingezien en gebruikt worden. Met andere woorden: als morgen de VS vanwege een conflict besluit sancties op te leggen, zou een Amerikaanse cloudprovider de toegang tot jouw data en systemen kunnen blokkeren.

Dit is niet langer fictie – het is al gebeurd. Toen de Amsterdam Trade Bank in 2022 onder Amerikaanse sancties viel vanwege Russische banden, “blokkeerde Microsoft direct de toegang tot de clouddiensten van de bank, waardoor ATB niet meer bij klantgegevens, e-mails en administratie kon” [[voxweb.nl](#)]. De bank ging failliet en zelfs de curator kreeg aanvankelijk geen toegang tot de systemen, er moest een gerechtelijk uitspraak aan te pas komen voordat Microsoft toegang gaf aan de curatoren [[rechtspraak.nl](#)]. Zo'n abrupte uitschakeling van diensten is een

nachtmerrie voor elke CIO: van de ene op de andere dag geen e-mail, geen gegevens, geen applicaties meer.

Behalve directe verstoring is er ook het risico van politieke chantage. Als buitenlandse grootmachten weten hoe afhankelijk je bent van hun technologie, kunnen ze die hefboom gebruiken. Hoepman, associate professor, vatte het kernachtig samen: we zijn kwetsbaar voor sanctiedruk, “dit kan niet alleen gebeuren, het is zelfs al gebeurd” [[voxweb.nl](#)]. In het genoemde voorbeeld van de Trade Bank werd een drukmiddel daadwerkelijk ingezet. Maar ook als het niet zo ver komt, hangt de dreiging als een zwaard van Damocles boven organisaties.

Daarnaast speelt een sluipender gevaar: verlies van autonomie en privacy. De open brief benadrukt dat de afhankelijkheid van Big Tech publieke waarden als academische vrijheid en autonomie ondermijnt. De digitale diensten vormen de ruggengraat van onderwijs en bedrijfsvoering, zonder dat de organisaties zelf invloed hebben op die diensten. Denk aan de uitrol van AI-features als Microsoft's Copilot in Office: universiteiten moeten maar accepteren dat zo'n tool ineens verschijnt, nog voordat zij een eigen visie op generative AI hebben geformuleerd. De cloud-leverancier bepaalt de koers, niet de afnemer – een omkering van de regie.

JURIDISCHE RISICO'S: DE EXTRA- TERRITORIALE TENTAKELS VAN DE CLOUD ACT

Een belangrijke dimensie van digitale soevereiniteit is juridische controle. Hier wringt de schoen het hardst bij Amerikaanse cloudaanbieders, door wetten als de U.S. CLOUD Act. Deze wet uit 2018 verplicht Amerikaanse cloudbedrijven om – op bevel van Amerikaanse opsporingsdiensten – gegevens van klanten te overhandigen, ook als die data op Europese bodem staat opgeslagen [ncsc.nl]. Veel Europese bestuurders gingen er lang van uit dat data in een EU-datacenter automatisch onder alleen EU-wetgeving valt. Maar volgens een analyse van het Nationaal Cyber Security Centrum is dat schijnveiligheid: “Europese bedrijven en dataopslag in Europa (zijn) niet immuun voor niet-Europese wetgeving, zoals de Amerikaanse CLOUD-Act”. Met andere woorden, ook data die keurig in Amsterdam staat, kan via de Amerikaanse moedermaatschappij juridisch toegankelijk zijn voor de VS.

Dit effect zorgt voor een spanningsveld met Europese regelgeving (zoals de GDPR/AVG) en zet organisaties klem

tussen twee jurisdicties. In het ergste geval kan een bedrijf als Microsoft klem komen te zitten tussen voldoen aan een Amerikaans dataverzoek en het schenden van EU-privacywetgeving. Microsoft benadrukt dat het dergelijke verzoeken kritisch beoordeelt en waar mogelijk aanvecht, maar het punt blijft: de uiteindelijke controle ligt bij de Amerikaanse wetgever en rechtspraak, niet bij de Europese klant.

Het nieuws dat Donald Trump in 2025 weer tot president is gekozen, een scenario dat de open-briefschrijvers expliciet noemen, heeft deze zorgen verder aangewakkerd [voxweb.nl]. Plots is het niet ondenkbaar dat een Amerikaanse overheid minder terughoudend omgaat met internationale jurisdictie of zelfs rechterlijke uitspraken naast zich neerlegt. Juridische deskundigen waarschuwen dat het complex en lastig is voor een afnemer om precies vast te stellen welke diensten onderhevig zijn aan buitenlandse wetgeving. Vaak lopen er onzichtbare lijntjes in de Cloud-leveringsketen die alsnog in de VS uitkomen.

Het NCSC-rapport concludeert dat organisaties moeten beseffen dat het feitelijk niet goed mogelijk is extraterritoriale invloeden volledig uit te sluiten en dat dit gedegen risicoanalyses vergt [ncsc.nl]. Simpel gezegd: zolang je van een buitenlands bedrijf afhankelijk bent, geef je een stukje van je soevereiniteit op.

EUROPESE WAKE-UP CALLS EN INITIATIEVEN

Gelukkig groeit het bewustzijn in Europa. De hierboven genoemde open brief (ondertekend door honderden medewerkers) is één signaal. De Radboud Universiteit heeft publiekelijk erkend dat de zorgen terecht zijn en werkt “aan een nieuwe strategie waarin digitale soevereiniteit een belangrijk thema is” [ru.nl]. Men voelt de urgentie om minder afhankelijk te worden van Big Tech. Dit besef beperkt zich niet tot academische kringen: in januari 2025 luidde de Algemene Rekenkamer de noodklok over ondoordacht cloudgebruik door ministeries, “zonder afwegingen” en met “zorgwekkend gebrek aan controle”. Die waarschuwing is een oproep aan de hele publieke sector om digitale autonomie hoger op de agenda te zetten.

Ook op Europees niveau speelt dit. In toenemende mate wordt er gesproken over Europese alternatieven, zoals Scaleway, OVHCloud en dergelijke. Caesar Groep investeert ook in dienstverlening die meer focust op open source en Europese soevereiniteit.

De eerste softwareproducten draaien al op Europese servers op basis van open

source software [LinkedIn]. Tegelijk ontstaan er samenwerkingsverbanden en platforms om Europese alternatieven te versterken.

De ondertekenaars van de open brief roepen op tot investeringen in non-profit open-source oplossingen – bijvoorbeeld het Europese Nextcloud voor documentendiensten, of Jitsi voor videobellen [voxweb.nl]. Ook pleiten zij voor samenwerking via SURF en internationale consortia: hoe groter de beweging richting soevereine IT, hoe makkelijker de overstap wordt.

“

‘Het risico is levensgroot dat universiteiten of overheden dan op een bepaald moment geconfronteerd worden met het afsluiten van bepaalde diensten of dat we geen toegang meer hebben tot gegevens. Dat moet je voor zijn.’

Jaap-Henk Hoepman, associate professor Radboud Universiteit (2025)

We zien al dat in Frankrijk en Duitsland “andere universiteiten bezig zijn met dergelijke stappen”, en binnen Radboud zelf draait een volledige faculteit – de bètafaculteit – nog op eigen mailservers en lokaal beheerde diensten als bewijs dat het kan.

BIG TECH'S REACTIE: TOEZEGGINGEN EN EUROPESE BELOFTES

De groeiende Europese assertiviteit is Big Tech niet ontgaan. Microsoft in het bijzonder is in de spotlight komen te staan, aangezien het met Azure en Microsoft 365 diep verankerd is in Europese bedrijfsvoering en overheid. Op 30 april 2025 kondigde Brad Smith (president van Microsoft) vijf nieuwe "European Digital Commitments" aan. Deze beloftes moeten Europese klanten geruststellen "dat Microsoft tot aan de rechter zal vechten voor de soevereiniteit van haar klanten" ondanks de onrust rond Amerikaanse regelgeving en data-toegang.

ENKELE KERNPUNTEN:

- **Uitbreiding van Europese cloud infrastructuur:** Microsoft belooft de komende twee jaar de capaciteit van zijn Europese datacenters met 40% uit te breiden, verspreid over 16 landen. Tussen 2023 en 2027 verdubbelt daarmee hun EU-capaciteit. Het idee is duidelijk: data en diensten "dicht bij huis" houden,

onder Europese regelgeving, om zo zowel prestaties als vertrouwen te verhogen. Meer lokale datacenters suggereren ook minder afhankelijkheid van trans-Atlantische dataverkeer.

- **Soevereine cloud constructies:** Microsoft werkt aan speciale sovereign cloud oplossingen in samenwerking met lokale partijen. Brad Smith wijst op het Franse project "Bleu" (met Capgemini en Orange) en een vergelijkbare opzet in Duitsland (met SAP's dochter Delos en Arvato). Deze zorgen ervoor dat Azure-diensten onder toezicht van een lokale entiteit komen, met extra encryptielaag en alleen lokaal personeel met toegang – in theorie dus afgeschermd van de Amerikaanse moeder. Tevens wordt aangekondigd dat alle Europese datacenteractiviteiten voortaan een aparte bestuurslaag met uitsluitend EU-personen krijgen, die opereert onder Europees recht. Dit "European cloud for Europe" model moet de band met Europa cementeren.
- **Digital Resilience Commitment (juridische zelfbescherming):** In een duidelijke knipoog naar de Cloud Act-zorgen belooft Microsoft dat geen enkele overheid ter wereld de toegang voor Europese klanten mag afsnijden zonder gevecht.

Mocht Microsoft ooit de opdracht krijgen zijn clouddiensten in de EU te staken, dan zal het bedrijf “onmiddellijk en met volle kracht zo’n maatregel aanvechten via alle juridische wegen, inclusief rechtszaken”. Deze belofte willen ze zelfs contractueel vastleggen met alle overheidsklanten in Europa, om het juridisch bindend te maken voor Microsoft Corp. Met andere woorden: Microsoft zegt bereid te zijn desnoods de eigen Amerikaanse overheid aan te klagen om continuïteit voor Europese klanten te waarborgen.

- **Back-up en continuïteit via Europese partners:** Voor het scenario dat een rechter Microsoft toch dwingt diensten te staken, heeft men een noodplan. Microsoft zal broncode back-uppen in Zwitserland, zodat aangewezen Europese partners de diensten kunnen overnemen als dat ooit nodig is. Dit moet voorkomen dat Europese gebruikers letterlijk zonder software komen te zitten; lokale partijen kunnen de cloud dan gaande houden.
- **Privacy en EU data boundary:** Microsoft wijst erop dat het inmiddels zijn “EU Data Boundary” heeft voltooid, een project dat klanten de mogelijkheid geeft om

hun data uitsluitend binnen EU-datacenters te houden, ook voor SaaS-diensten als Microsoft 365 en Dynamics 365. Technisch betekent dit dat een Europese klant niet meer bang hoeft te zijn dat bijvoorbeeld een document of mailbox ongemerkt op een Amerikaanse server belandt; standaard blijft alles in de EU. Dit is vooral relevant voor naleving van de AVG en komt voort uit eerdere druk vanuit de Schrems II-uitspraak.



Today we commit to further strengthen and expand solutions that allow European customers to control and protect their data.

Brad Smith, Vice Chair & President Microsoft (2025)

Deze toezeggingen zijn uniek – geen andere Amerikaanse cloudprovider is vooralsnog zo ver gegaan in het formaliseren van Europese garanties. Smith benadrukt dat Microsoft al vaker naar de rechter is gestapt namens klanten, zowel onder Obama, Biden als in de eerste Trump-periode. Die geschiedenis moet vertrouwen wekken dat het bedrijf zijn beloften zal nakomen: “When necessary, we’re prepared to go to court” is de duidelijke boodschap.

DE KEERZIJD: KRITISCHE KANTTEKENINGEN BIJ DE BELOFTEN

Hoe geruststellend Microsoft's Europese koerswijziging ook klinkt, het is belangrijk de beperkingen onder ogen te zien. Ten eerste blijft Microsoft een Amerikaans bedrijf. Het mag dan Europese datacenters uitbaten en een EU-directie instellen, uiteindelijk valt het moederbedrijf onder Amerikaans recht. De CLOUD Act verdwijnt niet door PR-beloftes en ook niet door rechtzaken. Microsoft's bereidheid om te procederen is bemoedigend, maar zoals analisten opmerken: dat helpt alleen zolang de Amerikaanse rechtsstaat normaal functioneert. Wat als een toekomstige regering in Washington rechterlijke uitspraken naast zich neerlegt of de wet aanscherpt? Brad Smith riep in mei '25 zelf op dat de EU en VS snel tot een data-akkoord moeten komen om dit in verdragen te gieten – een impliciete erkenning dat hun beloften geen volledige oplossing zijn.

Bovendien richten de Microsoft-commitments zich vooral op extreme scenario's ("suspend or cease operations"). In de praktijk zijn dataverzoeken vaak minder zichtbaar. Bijvoorbeeld: wetshandavingsverzoek onder geheimhoudingsplicht zal Microsoft niet publiek maken.

De transparantierapporten van Microsoft laten zien dat men duizenden dataverzoeken per halfjaar ontvangt van overheden wereldwijd. In de meeste gevallen gaat dit om rechtmatige strafonderzoeken, maar Europese gebruikers hebben weinig zicht op hoeveel verzoeken uit de VS betrekking hebben op hun data. Microsoft kan zo'n verzoek eventueel juridisch aanvechten, maar garanderen dat geen enkel bitje ooit overhandigd wordt, kan het bedrijf niet.

Ook de contractuele garantie om te procederen is interessant, maar hoe hard is die als puntje bij paaltje komt? En wat gebeurt er in de tussentijd als Microsoft aan het procederen is? Juridisch blijft Microsoft gehouden aan Amerikaanse wetgeving; een contract met klanten maakt geen einde aan die plicht.



Het is in feite een belofte om eerst te vechten voor de klant – niet om te winnen. Sommige critici noemen dit dan ook een “slimme PR-zet” om vertrouwen te behouden. Want stel, Microsoft verliest zo’n juridische strijd: dan zijn Europese klanten alsnog de klos, en in het voorbeeld van de Amsterdam Trade Bank, dan helpt het Zwitserse-escapemechanisme je ook niet. En stel het komt toch tot een extreem scenario, kunnen Franse of Duitse partners zonder Microsoft dezelfde dienst draaiende houden op korte termijn? Dat is nooit grootschalig getest.

Een ander heikel punt is dat continuïteit niet hetzelfde is als soevereiniteit. Wigo4it, de IT-organisatie van de G4-gemeenten, reageerde op de kritiek van de Rekenkamer door te stellen dat men wél “in control” is in de cloud. Inderdaad heeft Wigo4it met een doordachte cloudstrategie, DevOps-autonomie en transparantie laten zien dat grip op kosten, prestaties & security mogelijk is.

Maar zelfs een showcase als Wigo4it – volledig in de publieke multi-cloud draaiend – ontkomt niet aan de eerdergenoemde juridische afhankelijkheid.

Operationele controle is dus niet gelijk aan juridische controle. Ook Wigo4it blijft uiteindelijk vertrouwen op de goede wil en stabiliteit van haar Amerikaanse leveranciers.

Ten slotte is er het lock-in probleem. Jarenlang hebben organisaties SaaS-oplossingen omarmd zonder een exit-strategie. Zoals Microsoft-watcher Mary Jo Foley opmerkt: het is één ding om stoer te praten over “terug naar eigen bodem” of “Eurostacks bouwen”, maar iets heel anders om het echt te dóen – het is uitermate complex en kostbaar om je weer los te maken van de cloud wanneer je “erin gezogen” bent. Big Tech wéét dit en heeft ecosystemen gecreëerd die diep in de bedrijfsprocessen verankerd zitten.

Microsoft's new European digital commitments

- 1 We will help build a broad AI and cloud ecosystem across Europe.
- 2 We will uphold Europe's digital resilience even when there is geopolitical volatility.
- 3 We will continue to protect the privacy of European data.
- 4 We will always help protect and defend Europe's cybersecurity.
- 5 We will help strengthen Europe's economic competitiveness, including for open source.

DE WEG VOORUIT: HANDELEN VANUIT DIGITALE AUTONOMIE

Voor CIO's en enterprise architecten is het tijd om wakker te worden en actie te ondernemen. "Niets doen is geen optie. Het risico is aanwezig dat op een bepaald moment diensten worden afgesloten of dat we geen toegang meer hebben tot gegevens. Dat moet je voor zijn," waarschuwde Jaap-Henk Hoepman terecht. Wat betekent dit concreet op strategisch en praktisch niveau?

- **Voer een soevereiniteits-risicoanalyse uit**

Neem je cloudportfolio onder de loep. Welke kritieke processen en data rusten op buitenlandse cloudplatformen? Wat zou er gebeuren als die morgen niet meer beschikbaar zijn, al dan niet tijdelijk? Breng juridische risico's in kaart. Denk ook aan supply chain: misschien host u in een EU-cloud, maar draait er een essentieel component van een Amerikaans derde partij in de achtergrond. Gebruik scenario-denken: "Wat als dienst X wegvalt of leverancier Y overgenomen wordt door een niet-EU partij?"

- **Ontwikkel een exit-strategie en doe dry-runs**

Zorg dat je niet gevangen zit als de situatie verandert. Dit betekent contractueel én technisch voorbereiden op exit. Leg in contracten vast dat je data soepel kunt exporteren in de juiste formaten. Investeer in portabiliteit van jouw applicaties – containeriseer workloads, gebruik open standaarden. Test: neem een representatieve applicatie of dataset en probeer die eens te migreren naar een alternatieve omgeving (een andere cloud of on-premises). Hoeveel moeite kost dat, welke afhankelijkheden kom je tegen? Zo'n "dry-run" onthult waar de pijnpunten zitten. Sommige organisaties houden zelfs een soort brandoefening: een weekend draaien vanaf back-ups en alternatieve systemen, om te zien of de continuïteitsplannen werken. Liever nu de tekortkomingen ontdekken dan tijdens een echte crisis. Zulke oefeningen levert je direct inzicht in hoe wendbaar jouw organisatie is.



- **Werk samen en deel kennis**

Digitale soevereiniteit is geen probleem dat één organisatie alleen kan oplossen. Zoek aansluiting bij sectorinitiatieven (zoals SURF voor onderwijs, of overheidscoalities via de VNG of EU-programma's). Door best practices te delen – van DPIA's op cloudservices tot handleidingen voor het opzetten van Nextcloud – versnellen we elkaars leercurve. Bovendien geeft collectieve actie richting aan de markt: als meerdere universiteiten gezamenlijke eisen stellen aan leveranciers, staan ze sterker dan individueel. Hoepman stelde: "Hoe meer instellingen onafhankelijk worden van Big Tech, hoe minder groot dat pressiemiddel wordt". Samen kunnen we een vuist maken richting zowel Big Tech als politiek.

- **Betrek bestuur en politiek**

Uiteindelijk raken deze kwesties aan organisatiebrede en maatschappelijke belangen. Zorg dat raden van bestuur en toezichthouders begrijpen dat dit geen IT-fantoomrisico is, maar een reëel strategisch risico. De case van de Amsterdam Trade Bank laat zien dat digitale afhankelijkheid ineens een existentiële bedreiging kan vormen voor een organisatie. Maak digitale soevereiniteit onderdeel van de strategisch risicoanalyse. Pleit ook richting de overheid voor duidelijkere kaders: bijvoorbeeld cloud-aanbestedingsregels die soevereiniteit meewegen, of internationale verdragen (zoals Brad Smith bepleit) om jurisdictieconflicten op te lossen.



CONCLUSIE: GRIP OP DE TOEKOMST

Europese digitale soevereiniteit in de context van cloud computing is geen abstracte geopolitieke droom – het is een noodzaak voor continuïteit, veiligheid en autonomie. De afgelopen jaren zijn we, vaak ongemerkt, in een comfortabele afhankelijkheid gewiegd door de gebruiksvriendelijkheid van de public cloud. Die heeft ontegenzeggelijk veel goeds gebracht, maar de balans is weg. We bevinden ons in een situatie waarin een handvol buitenlandse techgiganten de ruggengraat van onze digitale samenleving vormt. Dit maakt ons kwetsbaar op manieren die pas recent ten volle doordringen.

De eerste wake-up calls zijn niet voor niets afkomstig uit kringen die verantwoordelijkheid dragen voor publieke waarden: universiteiten, auditoren, cybersecurity-experts. Digitale soevereiniteit gaat immers niet alleen over IT, maar over wie de macht heeft in de informatiesamenleving. Willen we dat Europese waarden – privacy, vrijheid, rechtsbescherming – geborgd blijven, dan moeten we zorgen dat de onderliggende infrastructuur niet als wisselgeld kan dienen in een geopolitiek spel. Juridische controle over je data en diensten is daarbij net zo cruciaal als technische controle. Voor

CIO's en enterprise architecten betekent dit een verschuiving in denken: van cloud first naar een cloud-agnostisch first strategie. Ja, we willen profiteren van de public cloud, maar niet tegen elke prijs. Het vraagt om visie en daadkracht om nu veranderingen door te voeren die misschien lastig zijn, maar later het verschil kunnen maken tussen autonomie en afhankelijkheid. Durf een stip op de horizon te zetten – zoals de Radboudmedewerkers: over drie jaar minder afhankelijk van Big Tech.

Uiteindelijk is digitale soevereiniteit geen stap terug, maar een stap vooruit naar duurzame digitalisering. Het is bemoedigend dat Microsoft en consorten onze zorgen serieus genoeg nemen om zich publiekelijk vast te pinnen op beloften – maar we moeten zelf aan het stuur blijven.

De oproep is duidelijk: neem je verantwoordelijkheid als verantwoordelijken van de digitale toekomst van je organisatie. Ga in gesprek over deze risico's, initieer die proof-of-concepts met alternatieven, en zorg dat jouw organisatie niet onvoorbereid is als de ellende toeslaat. Digitale soevereiniteit verwerf je niet van vandaag op morgen. In een wereld vol “donkere wolken” boven de cloud, is het onze taak om ervoor te zorgen dat de zon blijft schijnen over onze digitale autonomie.

Dit whitepaper is geschreven door Dibran Mulder,
CTO van Caesar Groep



[linkedin.com/in/dibranmulder](https://www.linkedin.com/in/dibranmulder)



caesar.nl



d.mulder@caesar.nl