

Europese Cloudoplossingen: grip op data en geopolitiek

Digitale diensten zijn tegenwoordig onmisbaar voor organisaties. Maar achter het gemak van de cloud gaat ook een kwetsbaarheid schuil: Europa is sterk afhankelijk van Amerikaanse aanbieders. In een tijd van geopolitieke spanningen en veranderende wetgeving is die afhankelijkheid niet langer vrijblijvend. Steeds meer Nederlandse organisaties vragen zich af: wat als Amerikaanse bedrijven ineens hun services staken? Europese cloudoplossingen bieden een serieus alternatief, waarbij privacy, controle en continuïteit vooropstaan.

Toenemende zorgen over afhankelijkheid

Veel Nederlandse organisaties maken gebruik van cloudplatforms zoals Amazon Web Services (AWS), Microsoft Azure en Google Cloud. Deze leveranciers zijn technologisch toonaangevend, maar vallen onder Amerikaanse wetgeving. De zogenoemde Cloud Act verplicht deze bedrijven om data over te dragen aan de Amerikaanse overheid, zelfs als die gegevens in Europa zijn opgeslagen.

Daarmee ontstaat een spanningsveld: aan de ene kant de Europese privacywetgeving (AVG, artikel 48), aan de andere kant de Amerikaanse verplichtingen. Bovendien maken recente geopolitieke ontwikkelingen duidelijk hoe snel internationale verhoudingen kunnen veranderen. Sinds de herverkiezing van President Trump is het wantrouwen vanuit Europa verder toegenomen. In januari 2025 werd het onafhankelijke toezicht op het EU-VS Data Privacy Framework in de VS verzwakt, wat opnieuw vragen oproept over de rechtsgeldigheid van datatransfers. De situatie is daarmee actueler dan ooit.

Van privacy naar strategisch risico

Wat begon als een vraagstuk rondom naleving van wet- en regelgeving, is inmiddels uitgegroeid tot een strategisch aandachtspunt. Het risico dat Amerikaanse wetgeving botst met Europese normen is allesbehalve theoretisch: in 2015 en 2020 verklaarde het Europees Hof al twee keer een trans-Atlantisch gegevensverdrag ongeldig (Schrems I en II). Ook de opvolger, het EU-US Data Privacy Framework uit 2023, wordt door veel experts als juridisch kwetsbaar gezien. Daardoor is het risico op onderbreking van de IT-services, sancties of verplichte datami-graties reëel geworden.

Maar het speelt niet alleen in de rechtszaal: cloud-infrastructuur is inmiddels een geopolitiek thema. Data, technologie en digitale diensten kunnen in conflictsituaties worden gebruikt als machtsmiddel. Organisaties die volledig leunen op niet-Europese clouddiensten lopen dus niet alleen juridische, maar vooral ook operationele risico's.

Digitale soevereiniteit: meer dan alleen data-opslag

Digitale autonomie betekent dat je zelf controle houdt over je gegevens, infrastructuur en processen. Europese cloudoplossingen vallen onder de jurisdictie van de EU, voldoen aan de AVG en bieden betere garanties als het gaat om zeggenschap. Maar soevereiniteit draait om meer dan alleen de locatie van je data. Het gaat ook om:

Operationele controle: Wie beheert de cloud-omgeving en regelt het toegangsbeheer?

- Encryptie en sleutelbeheer: Heb je ook technisch gezien de controle over je data (en beschik je ook nog over de 'sleutels' als de ICT-dienstverlening wordt opgeschort)?
- Exitmogelijkheden: Kun je overstappen zonder vast te zitten aan technische of contractuele beperkingen?

Steeds meer organisaties zien in dat cloudbeleid niet alleen een IT-keuze is, maar ook een onderdeel van de bedrijfsstrategie en risicomanagement. Wie nu al nadenkt over alternatieven, versterkt zijn weerbaarheid in een onzekere wereld.



Europese alternatieven in opkomst

Het goede nieuws is dat het aanbod van Europese cloudoplossingen snel groeit. Enkele voorbeelden:

- **Gaia-X:**
een Europees initiatief dat werkt aan een federatief cloudnetwerk met gedeelde normen voor privacy en interoperabiliteit.
- **Nextcloud (Duitsland):**
een open source alternatief voor Google Workspace of Microsoft 365.
- **Stack-IT (Duitsland):**
een platform van de Schwarz Group (Lidl/Kaufland), dat samenwerkt met Google Cloud voor lokale opslag met client-side encryptie.
- **OVHcloud (Frankrijk):**
een grote speler met datacenters in Europa, gericht op open standaarden en gecertificeerd met onder andere ISO27001 en SecNumCloud.
- **Hetzner (Duitsland):**
levert betrouwbare infrastructuurdiensten tegen scherpe prijzen.
- **Scaleway (Frankrijk):**
richt zich op AI-capaciteit en digitale soevereiniteit, volledig binnen Europese controle.
- **Open Telekom Cloud (Duitsland/Nederland):**
voldoet aan de AVG, is afgestemd op Gaia-X en biedt mogelijkheden voor confidential computing.

Hoewel deze aanbieders qua schaal nog niet kunnen concurreren met de grote Amerikaanse hyperscalers, geven deze organisaties wel controle, betere naleving van (Europese) wetgeving en meer transparantie terug. Het belangrijkste is echter dat ze Europees zijn en dus een minder groot risico als het gaat om geopolitieke afhankelijkheid.

Wetgeving dwingt tot heroverweging

De Europese Unie werkt actief aan het versterken van digitale autonomie door middel van een breed scala aan Europese regelgeving. De GDPR-standaard (in het Nederlands: AVG) is internationaal door veel landen in meer of mindere mate overgenomen en daarmee een wereldwijde standaard geworden. In het verlengde daarvan zijn de afgelopen jaren vele richtlijnen en verordeningen gevolgd. Denk daarbij aan de Digital Services Act (DSA), Chips Act, Data Act,

AI Act, Cybersecurity Act, NIS2, uiteraard de DORA en nog meer.

Amerikaanse 'Big Tech' organisaties voeren intensieve lobby-campagnes in Brussel om invloed te houden op de regelgeving (en bij voorkeur om deze terug te dringen), maar de zorg om onze onafhankelijkheid en de bescherming van onze privacy blijft een belangrijke drijfveer voor de Europese politiek. Uiteraard, gaat het ook om stimulering van Europese ICT-bedrijven.

Het grote aantal wetten gericht op de cyber-industrie en daarmee samenhangende services maken Europese cloudoplossingen niet alleen aantrekkelijker, maar zorgen er ook steeds vaker voor dat ze nodig zijn om aan de regels te blijven voldoen.

Wat kan een organisatie nu doen?

Voor de meeste organisaties lijkt digitale soevereiniteit op korte termijn een volkomen illusie. De afgelopen jaren zijn we met onze ICT-systemen massaal richting de cloud gegaan en dat betekent vrijwel per definitie Amerikaanse 'Big Tech'. Ook gebruiken we massaal Microsoft Office en dan liggen producten als Teams, Sharepoint en OneDrive voor de hand of Google met haar Gmail and Google Suite. Daar zijn in het laatste jaar ook nog CoPilot en Gemini bijgekomen. Neem daar maar eens afscheid van. Dat begint met het ontwarren van alles dat nu is geïntegreerd.

Overstappen betekent een enorme investering. Laten we eerlijk zijn: deze producten zijn ook gewoon kwalitatief goed en de integratie van services maken ze erg efficiënt. Voor de overstap moet je beschikken over voldoende en goed opgeleide specialisten, alsmede goede alternatieven. Deze zijn beide schaars. Voor organisaties die hun afhankelijkheid willen verminderen zijn er verschillende mogelijkheden, maar de aanpak zal altijd stap-voor-stap moeten gaan. Denk daarbij aan:

- **Hybride of multicloudstrategie:**
Combineer Europese en niet-Europese cloudproviders. Gebruik een Europese cloud voor gevoelige of strategische gegevens en andere platforms voor minder kritieke onderdelen.

- **Datalocatie en encryptie:**

Kies voor aanbieders die data fysiek binnen de EU opslaan en zorg dat je voor het sleutelbeheer niet afhankelijk bent.

- **Evalueer contracten en exitstrategieën:**

Zorg ervoor dat overstappen haalbaar blijft. Hoe meer je integreert, des te meer je ook vastzit aan één leverancier.

Tussen droom en werkelijkheid liggen wetten en in dit geval heel veel praktische bezwaren. Een eerste stap is misschien wel bewustwording en een meer risicogewogen ICT-strategie bij nieuwe uitbestedingen.

Conclusie

De afhankelijkheid van niet-Europese cloudaanbieders is lange tijd als vanzelfsprekend gezien. Maar nu privacy, geopolitiek en technologie steeds nauwer met elkaar verbonden zijn, wordt digitale soevereiniteit steeds belangrijker. Iedereen voelt aan dat uitbesteding aan landen zoals China of andere landen met een ander rechtssysteem wellicht te risicovol is voor bedrijfskritieke gegevens. Misschien denken we

over een aantal jaar ook wel zo over de Verenigde Staten. Dan wordt het tijd om vandaag te beginnen met de voorbereiding. Hoewel Amerikaanse tech-reuzen Europese wetgeving proberen te verzachten en bijvoorbeeld Microsoft een charme-offensief is begonnen, kunnen we er niet omheen dat de risico's aan het veranderen zijn.

Europese cloudoplossingen zijn allang geen niche meer, maar vormen een serieus alternatief voor organisaties die verantwoordelijkheid willen nemen voor hun data, processen en continuïteit. Een complete overstap is niet meteen nodig. Maar het is wel het moment om kritisch naar de huidige cloudstrategie te kijken en naar verdere integratie van producten (hoe efficiënt ook). Misschien wordt het dan ook tijd om te kiezen voor oplossingen die passen bij de risico's én de waarden van deze tijd. ◆

Coen van Diepen

Stagiair Information Security

