

Baas over eigen data



Hoe Nederlandse organisaties
omgaan met datasoevereiniteit,
afhankelijkheid en digitale
autonomie

Management-samenvatting

Datasoeveriniteit is uitgegroeid tot een strategisch vraagstuk voor Nederlandse organisaties. Cloudadoptie, internationale ketens en de snelle inzet van generatieve AI hebben de digitale slagkracht vergroot, maar ook de afhankelijkheid van externe leveranciers en buitenlandse infrastructuur. Het onderzoek van Proximus NXT laat zien dat organisaties zich hiervan bewust zijn, maar dat dit bewustzijn zich nog onvoldoende vertaalt naar structurele regie over data.



Belangrijkste inzichten

- **Leveranciersafhankelijkheid** vormt de grootste kwetsbaarheid. Veel organisaties zijn sterk afhankelijk van één of enkele cloudleveranciers. Deze afhankelijkheid beperkt de flexibiliteit bij verstoringen, veranderende wetgeving of strategische heroriëntatie.
- **Exit-strategieën en datamobilititeit zijn onvoldoende geborgd binnen samenwerkingen met cloudproviders.** Een aanzienlijk deel van de organisaties beschikt niet over concrete overstapplannen voor data en workloads. Zonder exit-gereedheid blijft datasoevereiniteit in de praktijk kwetsbaar.
- **Inzicht in datalocatie is hoog, maar controle blijft beperkt.** Organisaties weten steeds beter waar hun data staat, maar ervaren gebrek aan transparantie en zorgen over buitenlandse toegang, zelfs wanneer data binnen de EU is opgeslagen.
- **Generatieve AI vergroot kansen én risico's.** AI-tools worden breed ingezet, vaak sneller dan beleid en technische waarborgen kunnen volgen. Zonder duidelijke governance ontstaat een nieuwe laag van afhankelijkheid en datarisico's.
- **Ambitie en urgentie lopen uiteen.** Organisaties vinden datasoevereiniteit belangrijk en zijn bereid te investeren in Europese alternatieven, maar slechts een minderheid maakt het een topprioriteit voor de korte termijn.
- **Datasoevereiniteit is ook een collectief vraagstuk.** Zorgen over geopolitieke ontwikkelingen en beperkte overheidsbescherming versterken de roep om Europese en soevereine digitale infrastructuur.

Er is een duidelijke paradox: datasoevereiniteit wordt breed erkend als essentieel, maar nog te weinig verankerd in concrete keuzes en dagelijkse praktijk. Zonder samenhangende aanpak waarin cloudstrategie, governance, AI-gebruik en exit-gereedheid samenkomen, blijft regie over data fragiel.

Aanbevelingen

- Maak datasoevereiniteit een expliciet strategisch uitgangspunt
- Borg exit-strategieën en datamobilititeit
- Gebruik hybrid cloud als structureel regiemodel
- Versterk governance en dataclassificatie
- Richt generatieve AI gecontroleerd en transparant in
- Kies waar mogelijk voor Europese en soevereine cloudoplossingen

Inleiding

Organisaties zijn niet langer in de experimentele fase als het gaat om cloudplatformen, hybride omgevingen en AI-gedreven toepassingen. Bij vele vormt dit inmiddels het hart van de bedrijfsvoering en is het dagelijkse realiteit. Waar data staan, wie erbij kan, hoe het wordt verwerkt en of je het kunt meenemen naar een andere omgeving zijn geen technische detailvragen meer. Het raakt direct continuïteit, compliance, risicobeheersing én strategische autonomie. De groeiende afhankelijkheid van internationale hyperscalers en generatieve AI-technologieën maakt dit spanningsveld nog complexer.

Organisaties profiteren van innovatie, flexibiliteit en schaalbaarheid, maar geven tegelijkertijd een deel van hun autonomie weg. Datasoevereiniteit is daarmee uitgegroeid tot een strategisch thema dat IT-teams en compliance-specialisten raakt. Proximus NXT ziet dit vraagstuk dagelijks terug bij klanten die de balans zoeken tussen vernieuwing en controle. Daarom onderzochten we hoe Nederlandse organisaties omgaan met datasoevereiniteit:

- Hoeveel grip hebben zij op de locatie, toegankelijkheid en verplaatsbaarheid van hun data?
- In welke mate zijn ze afhankelijk van leveranciers en cloudplatformen?
- Welke governance-structuren hebben zij ingericht?
- Welke risico's én kansen zien zij rondom AI, cloudmigratie en datalocatie?

Dit onderzoeksrapport brengt de belangrijkste inzichten uit dat onderzoek samen. Het doel: helder maken waar organisaties vandaag staan, welke drempels en misvattingen er bestaan, en vooral welke stappen nodig zijn om datasoevereiniteit structureel te versterken. Want echte digitale vooruitgang ontstaat pas wanneer technologie en controle hand in hand gaan.

Wat is datasoevereiniteit?

Onder datasoevereiniteit verstaan we de mate waarin een organisatie zelf kan bepalen waar data wordt opgeslagen, wie toegang heeft tot de data, hoe data verplaatst kan worden tussen systemen of leveranciers, onder welke voorwaarden data wordt verwerkt en hoe onafhankelijk de organisatie is van cloudpartijen.

Over dit onderzoek

De cijfers in dit onderzoek zijn het resultaat van een online onderzoek onder 556 werkende Nederlanders die (mede-)beslissend of eindverantwoordelijk zijn voor ICT en/of automatisering binnen hun organisatie. Het onderzoek is in het vierde kwartaal van 2025 uitgevoerd.

Afhankelijkheid van leveranciers

Ondanks de brede adoptie van cloudtechnologie blijven veel organisaties sterk afhankelijk van een beperkt aantal leveranciers. Waar organisaties vroeger volledige controle hadden over hun infrastructuur, is die regie vandaag deels verschoven naar externe partijen. Dat heeft directe gevolgen voor de datasoevereiniteit binnen een organisatie.

Uit het onderzoek blijkt dat veel organisaties zich bewust zijn van deze afhankelijkheid, maar moeite hebben om deze daadwerkelijk te doorbreken. Leveranciersafhankelijkheid raakt daarmee niet alleen de technische architectuur, maar ook strategische keuzeruimte, risicobeheersing en continuïteit.

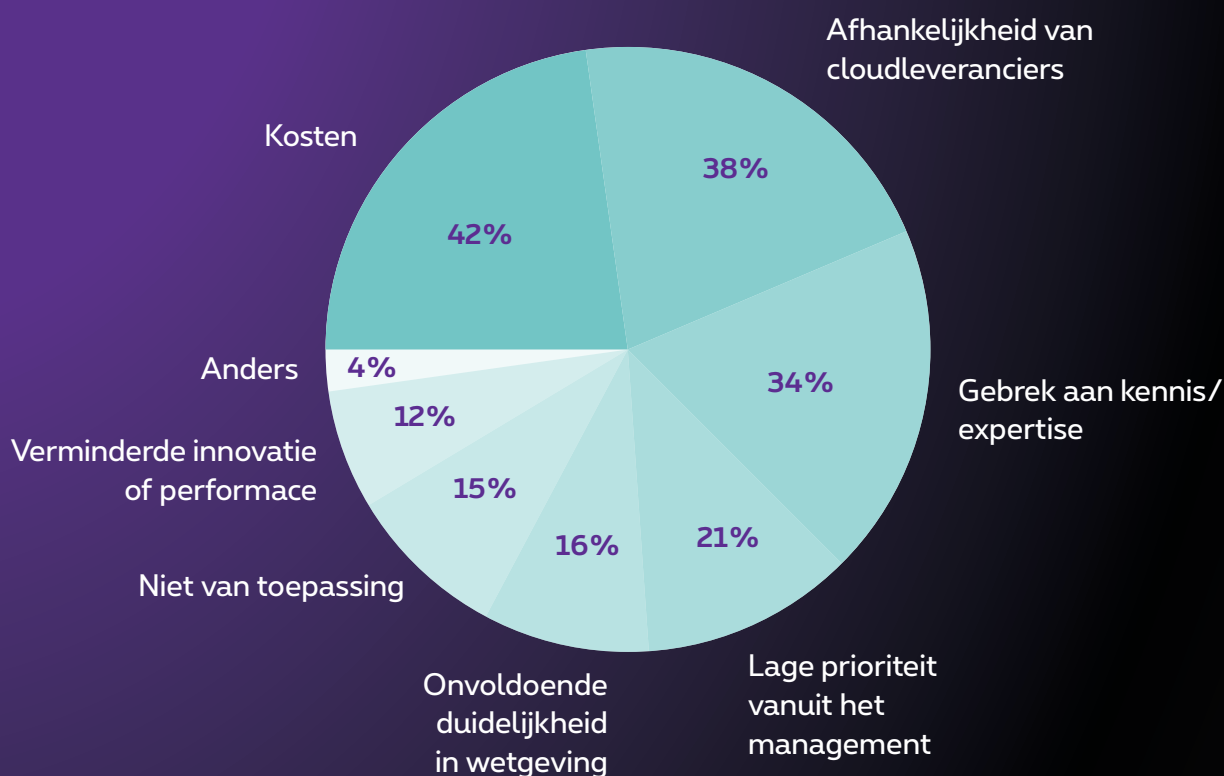
Onvoldoende voorbereid op uitval

32,2 procent van de organisaties geeft aan niet voorbereid te zijn op een langdurige uitval van een cloudleverancier. Dit betekent dat bij een structurele storing, geopolitieke verstoring of juridisch conflict de impact op de bedrijfsvoering groot kan zijn. Zonder uitgewerkt alternatief of overstapscenario ontstaat een situatie waarin data wel beschikbaar lijkt, maar feitelijk niet meer onder eigen controle staat. Daarbij fungeren cloudplatformen steeds vaker als basis voor meerdere kritieke processen tegelijk. Een storing of beperking bij één leverancier kan daardoor doorwerken in meerdere delen van de organisatie.

“De afhankelijkheid van cloudleveranciers wordt erkend, maar niet aangepakt.”



Wat zijn voor uw organisatie de grootste barrières om datasoeverein te worden?



Grootste barrière

Dat organisaties leverancierafhankelijkheid als problematisch ervaren, blijkt uit de cijfers. 38,2 procent van de respondenten noemt afhankelijkheid van cloudleveranciers expliciet als één van de grootste barrières om data-soeverein te worden.

Deze afhankelijkheid uit zich op verschillende niveaus:

- **Technisch:** workloads en data zijn sterk verweven met één platform
- **Operationeel:** processen zijn ingericht rondom specifieke cloudfunctionaliteit
- **Contractueel:** overstappen is complex, kostbaar of beperkt mogelijk

Multicloud als intentie, minder als realiteit

Het onderzoek laat zien dat organisaties zich bewust zijn van de risico's van afhankelijkheid en hier actief op proberen te sturen. 41,8 procent geeft aan bewust gebruik te maken van meerdere cloudleveranciers om technologische en veiligheidsrisico's te beperken.

Tegelijkertijd laten de resultaten zien dat multicloud geen universele oplossing is voor data-sovereiniteit. Het gebruik van meerdere cloudleveranciers vermindert weliswaar bepaalde risico's, maar vraagt ook om duidelijke keuzes, governance en regie om daadwerkelijk effect te hebben. Zonder heldere afspraken over data-locatie, verantwoordelijkheden en overstaps-cenarior blijft ook een multicloudomgeving afhankelijk van de onderliggende leveranciers en hun voorwaarden.

Exit-strategieën en data-portabiliteit

Datasoevereiniteit vraagt meer dan inzicht in waar data staat of door wie deze wordt verwerkt. Een belangrijke voorwaarde is data-portabiliteit: de mogelijkheid om data en workloads gecontroleerd te verplaatsen tussen omgevingen, maar ook leveranciers wanneer dat nodig is. Exit-strategieën vormen daarmee het sluitstuk van deze controle over data. Zonder een uitgewerkt overstapscenario blijft datasoevereiniteit in de praktijk kwetsbaar. Het onderzoek laat zien dat juist op dit punt veel organisaties achterblijven.

Beperkte voorbereiding op overstappen

Wanneer organisaties wordt gevraagd of zij beschikken over een exit- of overstapplan voor het geval een cloudleverancier niet langer voldoet, geeft 26,1 procent aan het hiermee (helemaal) oneens te zijn. Met andere woorden: ruim een kwart van de organisaties erkent expliciet dat zij géén concreet plan heeft om data en workloads te migreren bij veranderende omstandigheden.

Dat is opvallend, zeker in een context waarin cloudcontracten, wet- en regelgeving en technologische mogelijkheden continu in beweging zijn. Zonder exit-strategie zijn organisaties afhankelijk van:

- de technische inrichting van één platform;
- contractuele voorwaarden die overstappen bemoeilijken; en
- de beschikbaarheid van specifieke cloudfunctionaliteiten.

In hoeverre bent u het eens met onderstaande uitspraken over ICT?

Onze organisatie heeft een exit- of overstapplan voor als onze huidige cloudleverancier niet meer voldoet

Helemaal niet mee eens	7%
Niet mee eens	23%
Neutraal	28%
Mee eens	30%
Helemaal mee eens	12%

Data-portabiliteit als randvoorwaarde voor regie

Een gebrek aan exit-strategieën betekent niet dat organisaties niet kunnen migreren, maar wel dat migraties vaak reactief, kostbaar en risicovol worden. Data-portabiliteit vereist voorafgaande keuzes: gestandaardiseerde architecturen en dataformats, duidelijke verantwoordelijkheden en periodieke toetsing van overstapsenario's.

Het ontbreken van een exit-strategie beperkt de keuzeruimte van een organisatie. Je kunt minder snel inspelen op veranderende wetgeving en compliance-eisen of nieuwe technologische alternatieven.

De rol van hybrid cloud

De beperkte beschikbaarheid van exit- en overstapplannen laat zien dat veel organisaties moeite hebben om hun cloudomgeving zodanig in te richten dat overstappen daadwerkelijk mogelijk is. Dat roept de vraag op welke architecturale keuzes organisaties kunnen maken om die overstapbaarheid te vergroten.

Hybrid cloud kan hier een belangrijke rol in spelen. Een hybride cloudstrategie stelt organisaties in staat om workloads en data te verdelen over meerdere omgevingen – on-premise, private cloud en public cloud – in plaats van alles onder te brengen bij één leverancier.

Door kritieke data en gevoelige workloads bewust in een passende omgeving te positioneren, ontstaat:

- meer flexibiliteit om data en workloads te migreren;
- minder afhankelijkheid van één platform;
- en een beter uitgangspunt voor gecontroleerde overstappen.



“Zonder exit-strategie is datasoeveriniteit een theoretisch concept.”

Cloudkeuzes en datalocatie

Waar data zich fysiek bevindt, bepaalt welke wet- en regelgeving van toepassing is, wie juridisch toegang kan afdwingen en hoe groot de operationele en juridische afhankelijkheid van externe partijen wordt. Cloudkeuzes zijn daarmee een directe en bepalende factor voor datasoevereiniteit. Het onderzoek laat zien dat organisaties zich steeds bewuster worden van het belang van datalocatie, maar deze bewustwording niet altijd leidt tot structurele controle of risicoreductie.

Regie niet vanzelfsprekend

Een belangrijk positief signaal is dat ruim drie kwart van de organisaties (77,4%) aangeeft inzicht te hebben in waar hun bedrijfs- en klantdata fysiek wordt opgeslagen. Datalocatie staat daarmee duidelijk op de agenda van IT- en securityteams.

Tegelijkertijd laten de onderzoeksresultaten zien dat inzicht niet automatisch gelijkstaat aan daadwerkelijke regie. 31,5 procent van de organisaties ervaart een gebrek aan transparantie van cloudleveranciers over de locatie en toegang tot data, terwijl 47,2 procent zich zorgen maakt over een te grote afhankelijkheid van één of enkele cloudleveranciers voor de continuïteit van de bedrijfsvoering.

Het inzicht in datalocatie lijkt dus in veel gevallen gebaseerd op contractuele afspraken, terwijl de verwerking van data plaatsvindt binnen internationale cloudarchitecturen. Daardoor blijft de mate van controle voor veel organisaties afhankelijk van leveranciersvoorwaarden, juridische kaders en externe ontwikkelingen als wijzigingen in wetgeving of geopolitieke spanningen.



Cloudkeuzes om regie te versterken

Wanneer gevraagd wordt naar concrete maatregelen om datasoevereiniteit te waarborgen, geeft 33,8 procent van de organisaties aan gebruik te maken van lokale datacenters of on-premises opslag. Lokale infrastructuur speelt dus nog steeds een belangrijke rol, met name voor gevoelige of bedrijfskritische data.

Daarnaast past ongeveer een derde (33%) data-classificatie en segmentatie toe, waarbij gevoelige data bewust wordt gescheiden of niet in de cloud wordt geplaatst.

Organisaties lijken actief te zoeken naar manieren om risico's te beperken en controle te vergroten. Tegelijkertijd vereist dit governance, consistente toepassing en monitoring om effectief te blijven.

In dit kader kun je als organisatie kiezen voor een hybride cloudstrategie. Door data en workloads te verdelen over lokale infrastructuur, private cloud en public cloud kun je gevoelige data beter afbakenen, terwijl je gebruikmaakt van de schaalbaarheid en flexibiliteit van de public cloud. De hybride cloud fungeert daarmee niet als compromis, maar als een bewuste keuze om regie, flexibiliteit en compliance te combineren.

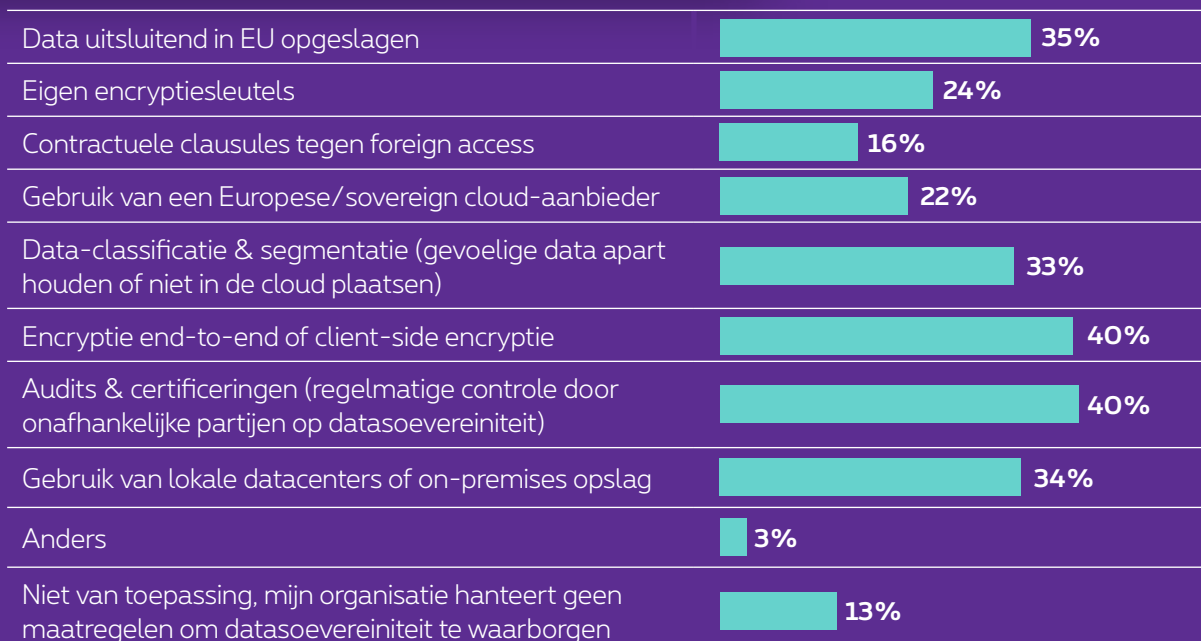
Data binnen Nederland en de EU

De geografische locatie van data speelt een steeds belangrijkere rol in de afwegingen van organisaties. 34,9 procent slaat data uitsluitend op binnen de Europese Unie, terwijl 21,1 procent gebruikmaakt van een Europese of sovereign cloud-aanbieder. De zorgen die organisaties hebben over wet- en regelgeving, jurisdictie en toegang tot data beïnvloeden deze keuzes.

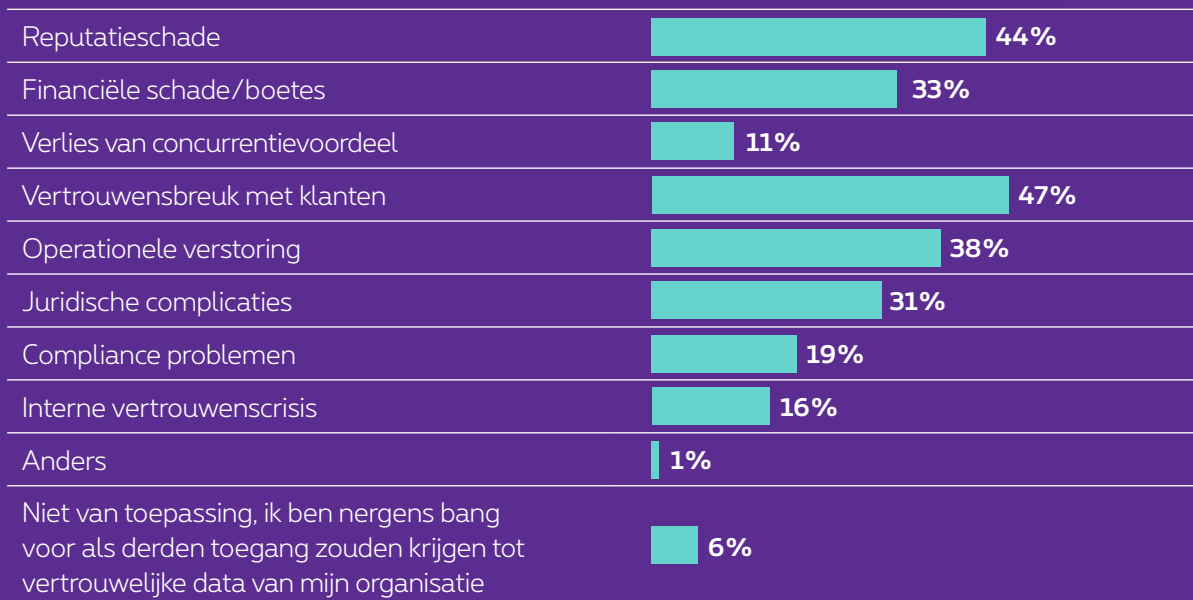
Tegelijkertijd accepteert 28,6 procent van de organisaties de risico's van dataopslag buiten Europa, zolang prijs en prestaties gunstig zijn. Deze cijfers laten zien dat organisaties continu balanceren tussen kosten, performance en soevereiniteit – een afweging die onder druk kan komen te staan bij veranderende wetgeving of geopolitieke ontwikkelingen.

Dat blijkt ook uit het feit dat 51,3 procent zich zorgen maakt dat niet-Europese autoriteiten toegang kunnen krijgen tot data, zelfs wanneer deze binnen de EU zijn opgeslagen. Daarmee wordt duidelijk dat datalocatie alleen niet altijd voldoende zekerheid biedt over juridische en operationele controle.

Welke maatregelen hanteert uw organisatie om datasoevereiniteit te waarborgen?



Waar bent u het meest bang voor als derden (bijvoorbeeld buitenlandse overheden) toegang zouden krijgen tot vertrouwelijke data van uw organisatie?



Wat organisaties écht vrezen bij ongewenste toegang tot data

De zorgen rond datalocatie en buitenlandse toegang zijn er niet zomaar. Wanneer organisaties het hebben over hun angst als het gaat om derden, zoals buitenlandse overheden, die toegang tot vertrouwelijke data zouden krijgen, ontstaat een scherp beeld van hun verwachtingen.

De top 5 risico's die organisaties noemen:

1. **Vertrouwensbreuk met klanten**
2. **Reputatieschade**
3. **Operationele verstoring**
4. **Financiële schade en boetes**
5. **Juridische complicaties**

Vertrouwen en reputatie scoren hoger dan directe financiële schade. Voor organisaties is datasoevereiniteit niet alleen een compliance- of IT-vraagstuk. Het raakt ook aan klantrelaties, samenwerking en maatschappelijke legitimiteit.

Het feit dat operationele verstoring hier ook genoemd wordt, betekent dat organisaties weten dat ongewenste toegang niet alleen een compliance-issue is, maar directe gevolgen kan hebben voor de dagelijkse bedrijfsvoering, van procesonderbrekingen tot het tijdelijk stilleggen van systemen.

“Inzicht in datalocatie is niet hetzelfde als regie over data.”

Gebruik van generatieve AI-tools

Generatieve AI, of GenAI, heeft zich in korte tijd ontwikkeld van experimentele technologie tot een vast onderdeel van de dagelijkse praktijk binnen organisaties. AI-tools worden ingezet voor analyse, contentcreatie, softwareontwikkeling en ondersteuning van bedrijfsprocessen. Vaak gebeurt dit via commerciële platform zoals ChatGPT, Gemini, Claude en Copilot, of via AI-functionaliteiten die geïntegreerd zijn in bestaande software en cloudomgevingen.

Hoewel het aantoonbare voordelen oplevert, stelt AI organisaties ook voor nieuwe vragen. Want waar AI-tools data verwerken, ontstaan automatisch nieuwe afhankelijkheden. Data wordt aangeboden aan externe modellen, de verwerkingslocatie is niet altijd transparant en de onderliggende infrastructuur wordt vaak beheerd door internationale leveranciers. Het gebruik van GenAI raakt daarmee direct aan datasoevereiniteit.

Gebruik groeit sneller dan beleid

GenAI wordt breed gebruikt, maar governance en beleidskaders houden deze ontwikkeling niet altijd bij. 41 procent van de organisaties heeft richtlijnen of beleid opgesteld voor het gebruik van generatieve AI met gevoelige data. Dat is een belangrijkste eerste stap, maar het betekent ook dat een meerderheid nog geen formeel kader heeft waarin gebruik, risico's en verantwoordelijkheden zijn vastgelegd.

17,2 procent geeft aan GenAI wel te gebruiken, maar zonder beleid of bewustwording binnen de organisatie. In deze situaties ontstaat een verhoogd risico op ongecontroleerd datagebruik, shadow-IT en onbedoelde blootstelling van vertrouwelijke informatie.

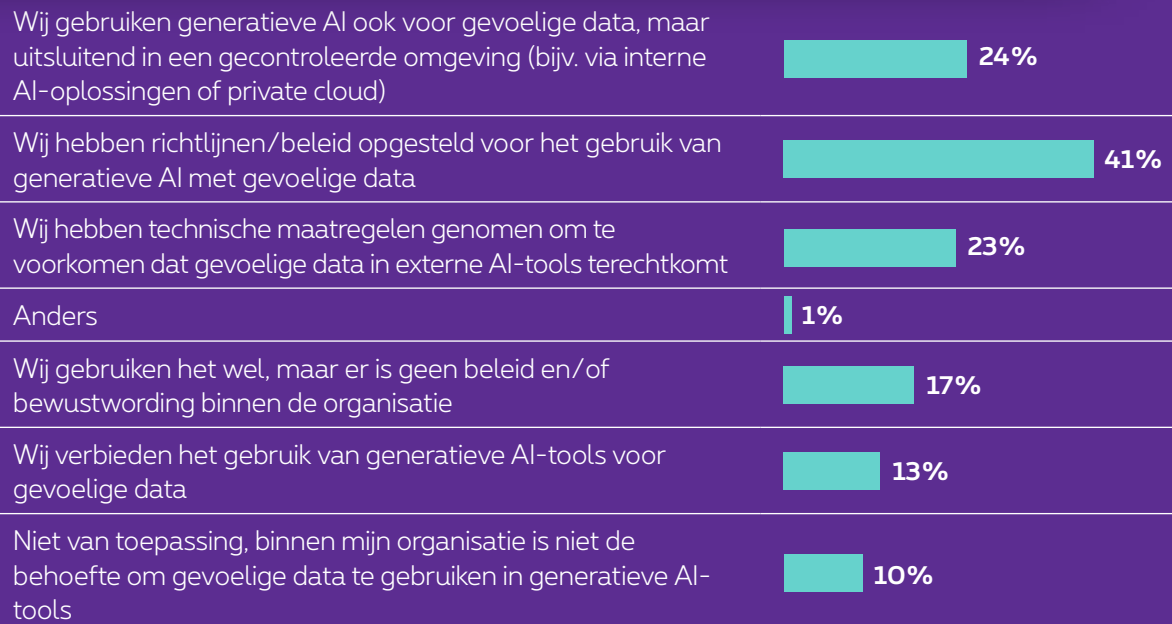
Gevoelige data en GenAI: spanning tussen waarde en risico

Opvallend is dat 24,2 procent van de organisaties aangeeft generatieve AI ook te gebruiken voor gevoelige data, maar uitsluitend in een gecontroleerde omgeving. Het besef dat AI waarde toe kan voegen groeit, mits het gebruik wordt afgebakend en technisch wordt ondersteund.

Tegelijkertijd blijkt dat slecht 22,7 procent technische maatregelen heeft genomen om te voorkomen dat gevoelige data in externe AI-tools terechtkomt. In veel organisaties wordt het beleid (waar aanwezig) nog niet structureel ondersteund door technische waarborgen, zoals datasegmentatie, monitoring of afgeschermd AI-omgevingen.

Aan de andere kant van het spectrum kiest 12,7 procent ervoor het gebruik van GenAI voor gevoelige data volledig te verbieden, terwijl 10,4 procent aangeeft geen behoefte te hebben om gevoelige data in AI-tools te gebruiken. Deze benadering vermindert risico's, maar beperkt ook de potentiële waarde van AI-toepassingen.

Wat doet uw organisatie met gevoelige data in generatieve AI-tools (zoals ChatGPT, Copilot, Gemini, Claude, etc.)?



Nieuwe vormen van leveranciersafhankelijkheid

Het gebruik van generatieve AI creëert een nieuwe laag van afhankelijkheid. Processen, workflows en besluitvorming worden steeds vaker ingericht rondom specifieke AI-platformen. Dat maakt overstappen complexer en vergroot het risico op vastzitten – niet alleen op infrastructuurniveau, maar ook functioneel.

Wanneer AI-modellen, prompts en contextdata niet eenvoudig overdraagbaar zijn, is er minder vrijheid om van leverancier te wisselen. Daarmee kan generatieve AI, zonder duidelijke governance, de datasoevereiniteit van organisaties verder onder druk zetten.

AI als versterker van datasoevereiniteit

Maar GenAI biedt ook kansen. Wanneer organisaties kiezen voor een gecontroleerde omgeving, duidelijke beleidskaders en transparantie over dataverwerking, kan AI juist bijdragen aan efficiëntere processen en snellere besluitvorming. Zonder dat de regie verloren gaat.

De sleutel ligt in bewuste keuzes: waar AI wordt ingezet, met welke data, onder welke voorwaarden en binnen welke architectuur.

“Generatieve AI kan de datasoevereiniteit van een organisatie zowel versterken als ondermijnen, afhankelijk van het gebruik en de governance.”

Overheid en digitale infrastructuur

Datasoeveriniteit is niet uitsluitend een vraagstuk voor individuele organisaties. Het raakt aan de inrichting van de digitale infrastructuur als geheel, en daarmee aan publieke belangen zoals nationale veiligheid. Het onderzoek laat zien dat organisaties deze bredere context meenemen in hun afwegingen. Maar tegelijkertijd is er twijfel: worden ze hierin wel voldoende ondersteund?

Geopolitiek als reëel risico

De zorgen over afhankelijkheid van buitenlandse cloud-infrastructuren worden versterkt door geopolitieke ontwikkelingen. 64,3 procent van de organisaties maakt zich zorgen dat geopolitieke conflicten effect zullen hebben op de continuïteit van hun digitale infrastructuur en dienstverlening.

Dit benadrukt dat datasoeveriniteit niet alleen gaat over privacy of compliance, maar ook over strategische bedrijfsvoering. Digitale infrastructuur is steeds vaker verweven met internationale wetgeving en handelsconflicten: factoren waar individuele organisaties nauwelijks invloed op hebben.



Beperkt vertrouwen in overheidsbescherming

Hoewel datasoevereiniteit steeds vaker onderwerp is van politiek debat, blijkt het vertrouwen in overheidsbescherming beperkt. 30,8 procent van de respondenten vindt namelijk dat de Nederlandse overheid de belangen van bedrijven onvoldoende beschermt op het gebied van datasoevereiniteit en cloudtechnologie. Organisaties voelen zich genoodzaakt zelf maatregelen te treffen, terwijl zij tegelijkertijd afhankelijk blijven van internationale infrastructuren waar overheden slechts beperkte invloed op hebben.

Europese alternatieven

De behoefte aan structurele Europese alternatieven is duidelijk. 69,5 procent vindt dat de overheid meer moet investeren in Europese cloud- en digitale infrastructuur. Organisaties zien het ontwikkelen van sterke Europese ecosystemen niet als protectionisme, maar als noodzakelijke voorwaarde voor keuzevrijheid en autonomie.

In hoeverre bent u het eens met onderstaande uitspraken over ICT?

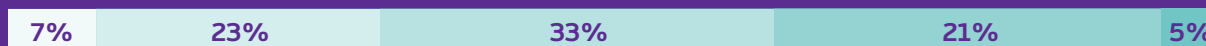
Datasoevereiniteit moet meer aandacht krijgen in de Nederlandse en Europese politiek



Ik maak me zorgen dat geopolitieke conflicten (Conflicten tussen landen of regio's die te maken hebben met hun geografische ligging, macht, grondstoffen, invloedssferen of strategische belangen) effect gaan hebben op de continuïteit van onze digitale infrastructuur en dienstverlening



Ik vertrouw erop dat de Nederlandse overheid de belangen van bedrijven voldoende beschermt op het gebied van datasoevereiniteit en cloudtechnologie



De overheid moet meer investeren in Europese alternatieven voor cloud en digitale infrastructuur



☐ Helemaal niet mee eens ☐ Niet mee eens ☐ Neutraal ☐ Mee eens ☐ Helemaal mee eens

Datasoeveriniteit in de toekomst

Datasoeveriniteit lijkt hoog op de agenda te staan, maar het onderzoek laat zien dat ambitie en daadwerkelijke prioritering niet altijd samenvallen. Organisaties onderschrijven het belang van autonomie, maar worstelen met keuzes en investeringen.

Hoge ambities, beperkte urgentie

Op strategisch niveau zijn organisaties uitgesproken:

42,9% vindt het essentieel om volledig autonoom te zijn op het gebied van cloudtechnologie en dataveiligheid;

43,4% is bereid hogere kosten te accepteren als dit bijdraagt aan Europese technologische en datasoeveriniteit;

76,4% vindt dat datasoeveriniteit meer aandacht moet krijgen in de Nederlandse en Europese politiek.

Tegelijkertijd blijkt de operationele urgentie lager. Slechts 36,1 procent noemt datasoeveriniteit een topprioriteit voor de komende twaalf maanden, terwijl 13 procent aangeeft überhaupt geen maatregelen te hanteren om datasoeveriniteit te waarborgen.

Dit suggereert dat datasoeveriniteit vaak wordt gezien als belangrijk, maar niet als urgent.

“De toekomst van datasoeveriniteit hangt af van keuzes die vandaag worden uitgesteld.”

Toekomstverwachtingen

Vooruitkijkend ontstaat een verdeeld beeld:

56,7% verwacht dat organisaties in de toekomst uitsluitend nog zaken zullen doen met cloudleveranciers die datasoeveriniteit kunnen garanderen;

27,8% verwacht binnen drie jaar over te stappen op Europese cloudoplossingen;

41,5% verwacht tegelijkertijd dat Europese bedrijven binnen vijf jaar volledig afhankelijk zijn van niet-Europese cloudleveranciers, tenzij er sterke Europese alternatieven komen.

Organisaties verwachten wel degelijk beweging, maar tegelijkertijd twijfelen ze aan de snelheid en schaal waarop Europese oplossingen zich zullen ontwikkelen.

Een kantelpunt in wording

De bereidheid om te investeren is aanwezig, het bewustzijn groeit en geopolitieke druk neemt toe. Wat ontbreekt, is samenhang: tussen beleid en praktijk, tussen publieke investeringen en private adoptie, en tussen strategische intenties en operationele prioriteiten.

Aanbevelingen

Datasoeveriniteit is geen afzonderlijk IT-vraagstuk, maar een structureel vraagstuk dat effect heeft op de continuïteit van en het vertrouwen in een organisatie. De resultaten van het onderzoek laten zien dat Nederlandse organisaties zich bewust zijn van het belang van datasoeveriniteit, maar dat dit bewustzijn zich nog onvoldoende vertaalt naar concrete maatregelen.

Afhankelijkheid van cloudleveranciers, beperkte exit-gereedheid, onvolwassen governance en snelle AI-adoptie zonder bijpassende kaders zorgen ervoor dat regie over data onder druk staat. Datasoeveriniteit is daarmee vooral een ambitie en nog te weinig een realiteit.

Om datasoeveriniteit daadwerkelijk te versterken, zijn 5 gerichte keuzes nodig.

1 **Positioneer datasoeveriniteit als strategisch uitgangspunt**

Maak datasoeveriniteit expliciet onderdeel van de IT- en cloud-strategie van jouw organisatie. Niet als compliance-eis, maar als randvoorwaarde voor continuïteit en vertrouwen. Beleg eigenaarschap op directie- of boardniveau.

3 **Gebruik hybrid cloud als regiemodel**

Zet hybrid cloud in om gevoelige data te beschermen, afhankelijkheden te beperken en flexibiliteit te behouden. Zie hybrid cloud niet als een tussen-oplossing, maar als structurele architectuurkeuze.

2 **Borg exit-strategieën en datamobiliteit**

Zorg dat overstappen mogelijk is vóórdat het nodig is. Ontwikkel en test exit-scenario's voor data en workloads, inclusief contractuele, technische en organisatorische aspecten. Zonder exit is er geen echte keuzevrijheid.



4

Versterk governance en dataclassificatie

Investeer in duidelijke datakaders: weet welke data waar mag staan, wie toegang heeft en onder welke voorwaarden data wordt verwerkt. Dataclassificatie en segmentatie vormen hierbij de basis

6

Kies bewust voor Europese en soevereine oplossingen

Stimuleer digitale autonomie door waar mogelijk te kiezen voor Europese of sovereign cloudoplossingen. Daarmee verklein je als organisatie geopolitieke risico's en vergroten zij hun strategische wendbaarheid.

Datasoevereiniteit vraagt geen radicale breuk met bestaande technologie, maar wel om bewuste keuzes. Organisaties die vandaag investeren in regie, creëren een digitale infrastructuur die klaar is voor de uitdagingen van morgen.

5

Richt generatieve AI gecontroleerd in

Combineer AI-beleid met technische maatregelen. Gebruik gecontroleerde omgevingen voor gevoelige data en voorkom ongewenste afhankelijkheid van één AI-platform. AI kan datasoevereiniteit versterken, mits bewust ingericht.

Meer weten over hoe wij
je kunnen helpen weer baas
over je eigen data te worden?

Of wil je advies over de juiste aanpak voor jouw organisatie?
Onze experts staan voor je klaar.

contact