



Whitepaper

Europese storage voor digitale soevereiniteit

“Zonder controle over je data, is er geen controle over je intelligentie.”

Deze uitspraak raakt de kern van een groeiend besef onder IT-leiders: digitale soevereiniteit is geen luxe meer, maar een noodzaak. Zeker nu organisaties strategisch inzetten op kunstmatige intelligentie. In mei 2025 blokkeerde Microsoft op verzoek van de Amerikaanse overheid de mailbox van de hoofdaanklager van het Internationaal Strafhof. Een ongekennde stap. Een Amerikaans technologiebedrijf dat een internationale rechtsinstantie op Europees grondgebied digitaal lamlegt, dat is een nieuwe ontwikkeling. Vakbladen en nieuwssites stonden er dan ook vol van. Vandaag de dag (juli 2025), spreekt de tweede kamer nog steeds over de gevaren van afhankelijkheid van Amerikaanse tech, blijkt uit de kamervragen naar aanleiding van de actie van Microsoft om de e-mail van de hoofdaanklager van het ICC af te sluiten..

Als toegang tot e-mail al kan worden ingezet als politiek drukmiddel, hoe kwetsbaar is dan de rest van onze IT-infrastructuur? Wat als de toegang tot je back-up wordt beperkt op aandringen van een buitenlandse overheid? Of wat als Amerikaanse bedrijven geen service meer mogen verlenen aan Europese organisaties? Deze casus toont haarscherp hoe snel organisaties de controle kunnen verliezen wanneer zij afhankelijk zijn van buitenlandse cloudproviders. Digitale autonomie is in een stroomversnelling geraakt: van abstract beleidsideaal naar concrete strategische prioriteit. En daarmee groeit ook de vraag naar Europese storage.



De controle paradox: gemak versus grip

Iedere organisatie streeft naar maximale grip op data, infrastructuur, compliance en continuïteit. Toch zien we in de praktijk een paradox: juist door te kiezen voor uitbesteding en cloudoplossingen die het beheer uit handen nemen, verliezen organisaties ongemerkt de controle die ze dachten te winnen. Deze controle paradox is het gevoel dat alles geregeld is in de cloud, terwijl men in werkelijkheid steeds minder zelf in de hand heeft.

De massale adoptie van ‘as-a-service modellen’ en een cloud first strategie biedt onmiskenbaar voordelen: schaalbaarheid, flexibiliteit en minder druk op interne teams. Maar gemak komt met een keerzijde, namelijk controleverlies. Dit zien we op drie vlakken:

Juridisch gezien valt data die in een buitenlandse cloud staat vaak onder een andere jurisdictie. Overheden of toezichthouders overzee kunnen toegang eisen, zelfs als de gegevens fysiek in Europa staan. Extraterritoriale wetten zoals de Amerikaanse CLOUD Act maken het mogelijk dat buitenlandse autoriteiten bij Europese bedrijfsdata kunnen zonder dat EU-instellingen daar invloed op hebben. Sterker nog, in extreme gevallen kan toegang tot data of applicaties volledig worden geblokkeerd op bevel van een vreemde mogendheid, zoals het voorbeeld van het ICC laat zien. Dit staat haaks op Europese regelgeving als de GDPR en brengt organisaties in een juridisch spanningsveld. Voor meer informatie over de juridische gevaren verwijs ik je graag naar de whitepaper “*Een kritische feitencheck over dataveiligheid: US Cloud Act, FISA en het Data Privacy Framework*” op www.comex.eu/kenniscentrum

Operationeel gezien geldt dat wie essentiële diensten als backup, e-mail of herstel volledig extern afneemt, merkt dat eigen ingrijpen lastiger wordt op kritieke momenten. Een internetstoring kan bijvoorbeeld betekenen dat een organisatie niet bij zijn clouddata kan. Denk aan de overstromingsramp in het Duitse Ahrtal in 2021: een ziekenhuis in het rampgebied verloor dagenlang toegang tot alle patiëntgegevens omdat de medische administratie volledig in de cloud draaide en de internetverbinding wegviel. De zorg stond stil. Geen toegang betekent geen controle. Ook geopolitieke ontwikkelingen kunnen operaties verstoren: sancties of plotselinge wijzigingen in dienstverlening kunnen ertoe leiden dat een extern beheerde applicatie niet meer beschikbaar is voor eindgebruikers. Wanneer een provider eenzijdig zijn SLA of licenties aanpast, staat de afnemer met de rug tegen de muur. Dit operationele risico wordt vaak pas zichtbaar als het misgaat.

Technisch gezien pronken cloudproviders met certificeringen en voldoen ze aan wetten als NIS2 en DORA, maar echte controle blijft bij de klant vandaan. Organisaties hebben doorgaans weinig zicht op hoe en waar hun data precies wordt opgeslagen, beschermd en bijgewerkt. Men vertrouwt op beloften van de leverancier. Cruciale securitymaatregelen zoals of data echt onveranderbaar is opgeslagen (immutability), of er een offline back-up (air gap) bestaat, of wanneer kritieke patches worden doorgevoerd, zijn zelden transparant of aantoonbaar onder eigen regie. Zelfs als cloudproviders aan alle documentatie voldoen.



De vraag is dus: *hoe weet u zeker dat uw cloud leverancier dezelfde urgentie voelt bij een security incident als u zelf? Wilt u afhankelijk zijn van externe servicecontracten en reactietijden, of liever zelf kunnen schakelen en binnen no time restoren om zo snel mogelijk weer operationeel te zijn?*

Deze controle paradox is de actuele realiteit. Hoe sterker we leunen op cloud en outsourcingmodellen, hoe urgenter de keerzijde wordt. Een onbedoeld bijeffect van modernisering is dat “wat je niet ziet, je wel kan raken”: zichtbare voordelen verbergen onzichtbare kwetsbaarheden. Hoe je deze paradox voor kunt blijven? Daar komen we later op terug.

Juridische en operationele risico's voor Nederlandse organisaties

Het verlies aan controle blijft niet zonder gevolgen. Voor Nederlandse en Europese organisaties brengt afhankelijkheid van buitenlandse cloudaanbieders aanzienlijke juridische en operationele risico's met zich mee.

Om te beginnen is er het risico in strijd met privacywetgeving. De Amerikaanse CLOUD Act en inlichtingenwet FISA 702 geven Amerikaanse autoriteiten vergaande bevoegdheden om toegang te krijgen tot data die is opgeslagen bij Amerikaanse cloudproviders, ook als die data zich fysiek op Europese bodem bevindt. Dit botst met de Europese GDPR (AVG): bedrijven die persoonsgegevens toevertrouwen aan een Amerikaanse cloud lopen het risico dat deze in handen van derden vallen, buiten de EU-regels om. In het ergste geval kan dit worden aangemerkt als een datalek of onrechtmatige overdracht, met boetes tot 20 miljoen euro of 4 procent van de wereldwijde jaaromzet tot gevolg.

Met de recente Schrems II-uitspraak is al duidelijk geworden dat ‘business as usual’ niet langer volstaat. Juridische kaders voor trans-atlantische data-uitwisseling zijn wankel. Het nieuwste EU VS Data Privacy Framework (DPF) was bedoeld om hierin zekerheid te scheppen, maar hangt grotendeels aan een zijden draadje van Amerikaanse goodwill. Na de wisseling van de wacht in Washington werd het toezichthoudend orgaan van het DPF praktisch lamgelegd, en een volgend Amerikaans bestuur kan de afspraken eenzijdig intrekken. Kortom: bedrijven kunnen niet blindvaren op tijdelijke politieke oplossingen voor blijvende privacy-eisen.

Voor meer informatie over dit vraagstuk verwijst ik je graag naar de whitepaper “EU-data in de handen van de VS: Een analyse van de status van trans-atlantische inspanningen op het gebied van gegevensbescherming” op www.comex.eu/kenniscentrum.

Daarnaast is er het risico van extraterritoriale inmenging. Buitenlandse wetgeving kan Nederlandse organisaties direct raken. FISA 702 bijvoorbeeld staat Amerikaanse inlichtingendiensten toe om, zonder gerechtelijk bevel, data op te vragen van niet-Amerikanen buiten de VS. Europese burgers en bedrijven genieten niet dezelfde beschermingen als Amerikanen onder de Amerikaanse grondwet. Dit betekent dat vertrouwelijke bedrijfsinformatie, intellectueel eigendom of klantgegevens in buitenlandse handen kunnen vallen zonder dat de organisatie het weet of hiertegen bezwaar kan maken.



Edward Snowden's onthullingen in 2013, ook wel bekend als de PRISM-affaire, toonden al aan hoe omvangrijk die surveillance kan zijn. Voor Nederlandse bedrijven in gevoelige sectoren vormt dit een continu compliance dilemma: voldoen aan de cloud-eisen van de business, zonder de nationale en EU-regels of de verwachtingen van burgers te schenden.

Ook de continuïteit en afhankelijkheid van buitenlandse partijen vormen een reëel risico. Het incident bij het Internationaal Strafhof staat niet op zichzelf. Het roept de vraag op hoe robuust de continuïteit van Nederlandse organisaties is als zij in de kern afhankelijk zijn van leveranciers van buiten de EU. Wat als morgen een belangrijke Amerikaanse leverancier onder druk van zijn overheid supportdiensten of toegang voor uw organisatie moet beperken? Dit lijkt ineens geen vergezochte situatie meer. Ook commerciële besluiten kunnen schade aanrichten: denk aan een cloudprovider die plots zijn prijzen verdubbelt of een dienst stopzet. Organisaties kunnen geconfronteerd worden met stilstand of hoge kosten om te migreren. Deze zogeheten 'Total Cost of Trust', de optelsom van verborgen risico's en kosten door blind vertrouwen in buitenlandse IT, blijkt vaak hoger dan gedacht. Denk bijvoorbeeld aan juridische exposure, kwetsbaarheid voor sancties, leveringsproblemen en verlies van controle over cruciale data. Dat is een prijs die pas duidelijk wordt als het te laat is.

Tot slot brengt ook toezicht en regelgeving de nodige verplichtingen met zich mee. Recentelijk ingevoerde Europese richtlijnen zoals NIS2 (voor netwerk en informatiebeveiliging) en DORA (voor digitale operationele weerbaarheid in de financiële sector) leggen de lat hoger voor governance en risicobeheersing. Organisaties moeten aantoonbaar weten waar hun data zich bevindt, wie er toegang toe heeft en hoe snel systemen hersteld kunnen worden na incidenten. Als kritieke processen buiten de deur staan, wordt het lastiger om aan te tonen dat u aan deze normen voldoet. U blijft als organisatie verantwoordelijk, ook als de uitvoering bij een leverancier ligt. Digitale soevereiniteit; zelf kunnen beschikken over uw data en systemen, wordt zo niet alleen een securityvraagstuk, maar ook een compliance verplichting.

Europese on-premises opslag: fundament voor hybride grip

Gelukkig betekent deze nieuwe realiteit niet dat men de cloud volledig moet afzweren. Integendeel, het draait om balans: herwin de regie door kritieke data en systemen weer onder eigen beheer te brengen, zonder de voordelen van de cloud op te geven. Steeds meer organisaties kiezen voor een hybride infrastructuur: een combinatie van cloud en lokale on-premises oplossingen, om zo flexibiliteit te behouden en de controle te versterken.

Europese on-premises storage kan dienen als solide basis voor zo'n hybride strategie. Door data op Europees geproduceerde en beheerde opslagplatformen te houden, profiteert men van meerdere voordelen. Neem bijvoorbeeld de **Europese storage van FAST LTA**:

Soevereine off-cloud AI applicatie



Silent AI

Ransomwareproof back-up en recovery met airgap



Silent Bricks

Compliant lange-termijn archivering zonder dataverlies



Silent Cubes

1

Ten eerste is er de **juridische zekerheid**. Gegevens opgeslagen op een Europese on-prem oplossing vallen volledig onder EU-recht. Dit voorkomt directe blootstelling aan de CLOUD Act of FISA 702, omdat er geen Amerikaanse entiteit is die gedwongen kan worden toegang te geven. Bovendien maakt lokaal beheer het eenvoudiger te voldoen aan GDPR-eisen en nationale regelgeving, omdat dataresidentie en soevereiniteit gewaarborgd zijn. Auditeurs en toezichhouders hebben meer vertrouwen als aantoonbaar is dat gevoelige data niet onder vreemde jurisdictie valt.

2

Ten tweede biedt het **operationele autonomie**. Een Europese on-prem storageoplossing geeft organisaties het heft in eigen handen bij calamiteiten. Air-gapped back-ups en archieven op eigen bodem blijven beschikbaar, ook als de internetverbinding uitvalt of een cloudprovider kampt met een storing. Een ransomwareaanval op een ziekenhuis in Düsseldorf in 2020 toonde aan hoe levensreddend dit kan zijn. Patiëntgegevens opgeslagen op hardwarematige WORM-storage konden niet ontoegankelijk gemaakt worden door de hackers en bleven beschikbaar. Een geruststellende gedachte voor elke continuitymanager. Daarnaast betekent een eigen oplossing ook onafhankelijkheid van de activiteiten van leveranciers: u bepaalt zelf de update-tijdstippen, recoveryprocedures en serviceafspraken.

3

Ten derde biedt het **technische controle en weerbaarheid**. Met on-prem storage heeft u volledige inzage in en zeggenschap over hoe data wordt bewaard en beschermd. Technologieën zoals immutability (onveranderbare opslag), hardwarematige WORM (Write Once Read Many) en air-gapped media (fysiek gescheiden back-ups) kunnen in eigen huis ingericht worden, zodat u zeker weet dat back-ups niet te manipuleren zijn en ransomware geen kans maakt. In het voorbeeld van het ziekenhuis in Düsseldorf bleek dat lokale WORM-storage van Europese makelij cruciaal was: 400 terabyte aan patiëntgegevens bleven veilig en beschikbaar ondanks een verwoestende cyberaanval. Zulke maatregelen zijn moeilijk af te dwingen in een pure cloudomgeving, maar on-prem vormt u zelf die laatste verdedigingslinie. Dit verhoogt de Zero Loss-doelstelling: geen dataverlies en geen controleverlies.

4

Tot slot is er het **voordeel van een korte keten en lokale support**. Europese storageoplossingen brengen ook praktische voordelen mee in de toeleveringsketen. Producten die binnen Europa worden ontworpen en gebouwd, kennen doorgaans kortere levertijden en minder beschikbaarheidsrisico's. Daarnaast is ondersteuning vaak directer en sneller beschikbaar via lokale partners. Er is geen afhankelijkheid van supportteams aan de andere kant van de wereld of van componenten die vastzitten in de douane. Dit verhoogt de bedrijfscontinuïteit en voorspelbaarheid. Cruciaal hierbij is dat het de afhankelijkheid van een enkele cloudleverancier (vendor lock-in) elimineert, omdat data op een standaard manier lokaal beschikbaar is en desgewenst eenvoudig naar andere omgevingen

Specialist in secundaire storage

Bij Comex zijn we al meer dan 30 jaar dé specialist in secundaire storage. We bieden betrouwbare oplossingen voor back-up, archivering en AI-infrastructuur, met volledige controle over uw data als fundament voor digitale soevereiniteit. Onze focus en aanpak?

- **Zero Loss storage:** Geen dataverlies, maximale controle en volledige compliance.
- **Digitale soevereiniteit:** Uw data blijft binnen Europese jurisdictie, beschermd tegen buitenlandse wetgeving zoals de U.S. CLOUD Act.
- **Hybride oplossingen:** Combinatie van lokale en cloudopslag voor optimale flexibiliteit en veiligheid.
- **Langdurige ondersteuning:** Tot 10 jaar service en support voor onze oplossingen.



Aanbevelingen: stappen naar digitale soevereiniteit

Digitale soevereiniteit verwerf je niet van de ene op de andere dag. Het vergt bewuste keuzes en concrete stappen. Organisaties die meer grip op hun data willen krijgen, doen er goed aan om planmatig te werk te gaan.

Breng datastromen en risico's in kaart

1

Een eerste stap is het in kaart brengen van datastromen en risico's. Voer een systematische inventarisatie uit van alle gegevensstromen naar buitenlandse, met name Amerikaanse, cloud- en SaaS-diensten. Analyseer welke data en processen gevoelig of bedrijfskritisch zijn. Dit vormt de basis om te bepalen waar de grootste soevereiniteitsrisico's zitten.

Cloudstrategie herzien, gevoelige data terughalen

2

Vervolgens is het belangrijk om de cloudstrategie te herzien en gevoelige data waar nodig terug te halen naar eigen infrastructuur. Overweeg om zeer gevoelige of bedrijfskritische gegevens te repatriëren naar on-premises oplossingen, zeker wanneer juridische of continuïteitsrisico's hoog zijn. Gegevens die u niet in-house kunt houden, voorziet u idealiter van end-to-end encryptie met zelfbeheer van de sleutels. Zo behoudt u de controle, zelfs als deze gegevens zich in de cloud bevinden. Houd hierbij altijd rekening met de eisen uit de GDPR bij het kiezen van cloudlocaties en leveranciers.

Omarm een hybride infrastructuur

3

Daarbij past het om een hybride infrastructuur te omarmen. Zoek een gezonde balans tussen cloud en eigen omgeving. Combineer het beste van twee werelden door de flexibiliteit en schaal van de cloud te benutten waar het kan, maar tegelijkertijd lokale opslag en back-ups te implementeren voor cruciale data. Zo creëert u redundantie en voorkomt u een enkel storingspunt. Cloud is immers een middel, geen alles-of-niets-doel op zich.

Implementatie immutability en air-gap

4

Een andere cruciale stap is het implementeren van immutability en air-gapped back-ups. Zorg dat er altijd een kopie van uw data is die niet aangevallen of gewist kan worden bij een incident. Onveranderbare opslag, zoals WORM of immutability, in combinatie met fysiek gescheiden back-ups (air-gap), biedt bescherming tegen ransomware, menselijke fouten en zelfs kwaadwillende insiders. Test regelmatig of deze back-ups daadwerkelijk toegankelijk en intact zijn. Ze vormen uw laatste verdedigingslinie.

Transparantie en aantoonbare compliance

5

Daarnaast is transparantie en aantoonbare compliance essentieel. Weet op elk moment waar uw gegevens zich bevinden en wie er toegang toe heeft. Documenteer deze keten zodat u auditors en toezichhouders kunt laten zien hoe data wordt opgeslagen en beschermd. Transparantie in data-opslag en -toegang is niet alleen technisch wenselijk, maar ook noodzakelijk voor regelgeving zoals NIS2 en DORA. U moet kunnen aantonen dat u in control bent, ongeacht of u cloud-diensten afneemt.

Kies voor Europese technologie en partners

6

Tot slot is het verstandig om bewust te kiezen voor Europese technologie en partners. Maak waar mogelijk gebruik van oplossingen die in Europa zijn ontwikkeld en gehost. Hiermee voorkomt u afhankelijkheid van buitenlandse wetgeving en zogenoemde black box-technologie. Bovendien profiteert u van kortere lijnen in ondersteuning en levering. Europese storage-oplossingen en IT-infrastructuur bieden een extra garantie dat uw data niet ongewild onderdeel wordt van een geopolitiek steekspel. Steeds meer organisaties in publieke en gereguleerde sectoren maken dan ook bewust de keuze voor IT van eigen bodem.

Digitale soevereiniteit vraagt om visie en actie. Controle is geen luxe, maar een noodzaak. Steeds meer organisaties realiseren zich dat datasoevereiniteit niet ophoudt bij een goed contract of een checkbox in de SLA, maar juist structurele grip vereist op de hele informatieketen. De manier waarop u data opslaat, beveiligt en kunt herstellen, zegt alles over uw weerbaarheid als organisatie. In een tijd waarin geopolitiek, cyberdreigingen en strenge wetgeving samenkomen, is het herwinnen van controle niet slechts een IT-project, maar een strategische investering in de toekomst van uw organisatie. Neem vandaag de regie terug, zodat u morgen met vertrouwen kunt blijven innoveren.



FAST LTA

FAST LTA
Rüdesheimer Str. 11
80686 München
info@fast-lta.de
www.fast-lta.de

Design,
Entwicklung
und Support
in **Deutschland**

