uniserver

Digitale soevereiniteit in Nederland 2026

Tussen innovatie en controle

Hoe Nederlandse organisaties navigeren in het tijdperk van AI en digitale autonomie

Onderzoeksrapport | Uniserver

Exclusieve inzichten van 1.023 IT-beslissers

Cloud | AI | Datasoevereiniteit | Compliance

Inhoud.

Management-samenvatting

Wat als je patiëntdossiers morgen door een Amerikaanse rechtbank worden opgevraagd? Wat als je concurrentiegevoelige R&D-data toegankelijk is voor inlichtingendiensten? Dit zijn geen hypothetische scenario's, dit is de juridische werkelijkheid voor elke organisatie die werkt met niet-Europese cloudproviders.

Dit rapport presenteert de resultaten van grootschalig onderzoek onder 1.023 IT-beslissers in Nederland. De uitkomsten tonen een sector op een strategisch kantelpunt: tussen de druk om te innoveren en de noodzaak om controle te behouden.

URGENTIE

68% van de organisaties maakt zich zorgen over ongewenste toegang tot data door buitenlandse overheden. Toch slaat **10%** data op in de VS, waar de CLOUD Act en FISA 702 directe toegang verlenen aan Amerikaanse autoriteiten– ongeacht waar je data fysiek staat. De juridische realiteit raakt je organisatie vandaag.

Vier bevindingen die alles veranderen

47%
Kiest voor private cloud, controle wint van public

74%
Heeft digitale autonomie in IT-strategie verankerd

83%
Bezorgd over datalekken bij AI-gebruik

73%
Bereid extra te investeren in soevereine infrastructuur

1. **Private cloud domineert, public cloud verliest terrein**

Met **47%** is private cloud veruit de populairste vorm van dataopslag, terwijl slechts **16%** voor public cloud kiest. Deze verschuiving weerspiegelt een fundamentele herwaardering: organisaties willen niet langer afhankelijk zijn van externe governance. De controle over wie toegang heeft tot data en waar deze fysiek staat is geen nice-to-have meer, het is een strategische eis.

2. **Digitale soevereiniteit is mainstream geworden**

74% van de organisaties heeft digitale autonomie expliciet verankerd in de IT-strategie. Nog opvallender: **78%** wil actief meer regie over dataopslag en toegang, en eveneens **78%** streeft naar minder afhankelijkheid van niet-Europese providers. Soevereiniteit is geen niche-thema meer voor overheden. Het is een breed gedragen prioriteit geworden, gedreven door geopolitieke spanningen en juridische risico's.

3. **AI-adoptie stagneert door veiligheids- en governancezorgen**

61% erkent een AI-inhaalslag nodig te hebben, maar **83%** maakt zich zorgen over datalekken en onvoldoende databeveiliging bij AI-gebruik. De grootste belemmeringen? Veiligheid (voor **34%** een grote zorg), bias in uitkomsten (**30%**), en gebrek aan interne kennis (**29%**). Organisaties willen AI wel inzetten, maar niet ten koste van controle over gevoelige data. Private AI binnen soevereine omgevingen biedt hier een uitweg.

4. Compliance-druk neemt toe, voorbereiding blijft achter
NIS2 is officieel sinds januari 2023 van kracht in de EU, maar moet in Nederland nog naar lokale wetgeving worden vertaald. De verwachting is dat dit in 2026 zal gebeuren waarbij de AI Act al wel gefaseerd is ingegaan. Toch voelt slechts **46%** zich voldoende voorbereid op AI-wetgeving. De sancties zijn enorm: tot €40 miljoen of **7%** van de wereldwijde omzet bij verboden AI-praktijken. Organisaties die nu niet handelen, lopen aanzienlijke juridische en financiële risico's.

DE CENTRALE BOODSCHAP

Innovatie vereist een stevig fundament. Organisaties die nu investeren in dataclassificatie, soevereine cloudkeuzes en private AI, creëren ruimte om te versnellen zonder telkens te moeten remmen. Regie is geen rem op innovatie, het is de voorwaarde om deze verantwoord te laten groeien.

Waarom dit rapport nu lezen?

Dit onderzoek biedt je:

- Een datagedreven kompas voor strategische IT-besluitvorming in 2026
- Sectorspecifieke inzichten voor zorg, overheid, ISV's en MSP's
- Concrete juridische risico-analyse van CLOUD Act en FISA 702
- Praktische routekaart met direct toepasbare aanbevelingen
- Realistische tijdlijnen en compliance-checklists voor NIS2 en AI Act

1. Inleiding: Het nieuwe IT-landschap

Het IT-landschap van 2026 wordt gekenmerkt door een scherpe paradox. Cloud computing en AI bieden organisaties ongekende mogelijkheden om te schalen en te innoveren. Tegelijkertijd zorgen geopolitieke ontwikkelingen, strengere regelgeving en toenemende cyberdreiging voor fundamentele vragen over datacontrole en digitale autonomie.

Die spanning is in de praktijk scherp voelbaar:

Voor organisaties is deze spanning niet langer theoretisch. Europese regelgeving zoals NIS2 en de AI Act, in combinatie met Amerikaanse wetgeving zoals de CLOUD Act en FISA 702, dwingt IT-beslissers tot concrete keuzes.

Dit onderzoek vertrekt vanuit één centrale vraag: hoe gaan Nederlandse organisaties om met de toenemende spanning tussen innovatie en controle, en welke strategische keuzes maken zij voor hun digitale toekomst?

ZORG - SCENARIO

Stel: het bestuur wil AI inzetten voor snellere diagnosestelling. De privacy officer stelt de onvermijdelijke vraag: waar komen gevoelige patiëntgegevens terecht, en wie heeft daar feitelijk toegang toe? De afweging: innovatie zonder juridisch risico vraagt om private AI op Nederlandse bodem, waar patiëntdata onder medisch beroepsgeheim blijft.

SECTORINZICHT: ONDERWIJS

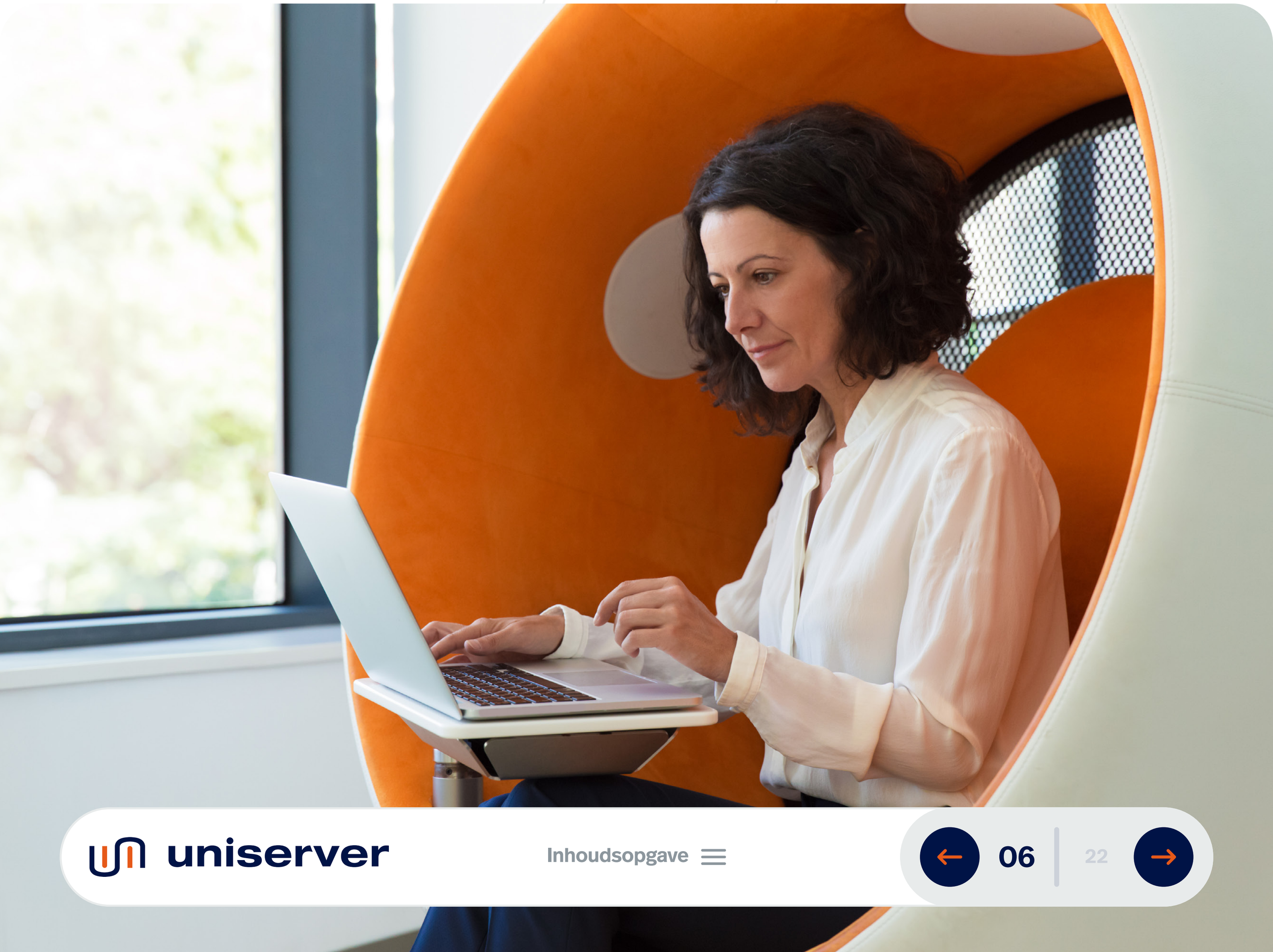
In het onderwijs heeft één datalek niet alleen operationele impact, maar ondermijnt het direct het publieke vertrouwen. De kernvraag voor onderwijsinstellingen: hoe versnellen we digitalisering zonder de controle te verliezen? Hybride cloud, met kritieke studentdata in private omgeving, biedt de balans tussen innovatie en bescherming van privacygevoelige onderwijsgegevens.

2. Onderzoeksmethode en respondenten

Eind 2025 is kwantitatief onderzoek uitgevoerd onder IT-(mede)beslissers in Nederland. De respondenten hebben online een vragenlijst ingevuld bestaande uit 16 vragen.

Categorie	Aantal (n)	Percentage
Totaal respondenten	1.023	100%
Zorg en welzijn	133	13,0%
Gemeenten en semi-overheid	78	7,6%
Overige sectoren	812	79,4%

De steekproef weerspiegelt een brede doorsnede van de Nederlandse zakelijke markt, met duidelijke vertegenwoordiging van sectoren waar regelgeving, continuïteit en dataveiligheid een centrale rol spelen.



3. De cloudmigratie: private wint terrein

De meest in het oog springende uitkomst van het onderzoek is de duidelijke dominantie van private cloud als voorkeursmodel. Dat staat haaks op het hardnekkige beeld dat public cloud inmiddels de standaard zou zijn.

De verschuiving naar private cloud

Cloudmodel	Percentage	Interpretatie
Private cloud	47%	Veruit populairst, controle en afscherming
Hybride cloud	18%	Balans tussen flexibiliteit en soevereiniteit
Public cloud	16%	Kleiner dan vaak verondersteld
On premise	15%	Legacy en specifieke controle-eisen

Met **47%** is private cloud de meest gebruikte vorm van dataopslag. Organisaties kiezen bewust voor exclusieve, afgeschermde omgevingen. Dat past bij de groeiende behoefte aan regie over gevoelige bedrijfsinformatie, governance en datasoevereiniteit.

SECTORINZICHT: ZORG

Ziekenhuizen en zorgorganisaties werken met elektronische patiëntendossiers onder strikte NEN 7510-eisen. Deze norm vereist aantoonbare controle over wie toegang heeft tot medische data. Gedeelde cloudinfrastructuur brengt compliance-risico's met zich mee. Private cloud op Nederlandse bodem en onder Nederlandse of Europese jurisdictie is niet alleen technisch de juiste keuze, het is de enige verdedigbare keuze richting patiënten, toezichthouders en onder het medisch beroepsgeheim.

FINANCIEEL - SCENARIO

Stel: een financiële dienstverlener overweegt bancaire data te migreren naar een gedeelde cloudomgeving. Het risico? Data kan via die infrastructuur onder niet-Europese jurisdictie vallen, buiten het toezicht van DNB en AFM. De keuze voor private cloud is hier niet ideologisch, maar direct gekoppeld aan risicomanagement en wettelijke toezichtseisen.

Datalocatie: Nederland en Europa domineren

68% van de organisaties slaat data op in Nederland. Dit wijst op een breed besef dat fysieke datalocatie directe gevolgen heeft voor juridische bescherming, toezicht en compliance. Dit betekent overigens niet dat deze data gevrijwaard is van niet-Europese jurisdictie. Om dat te bewerkstelligen moet de data verplaatst worden naar een partij die onder Europese wetgeving valt.

KRITISCH

10% van de organisaties slaat data op in de Verenigde Staten. Deze groep loopt aantoonbaar verhoogd juridisch risico, doordat Amerikaanse wetgeving van toepassing is op die data, ongeacht waar deze fysiek is opgeslagen. Dit betekent dat de CLOUD Act en FISA 702 directe toegang kunnen verlenen aan Amerikaanse autoriteiten.

SECTORINZICHT: OVERHEID

Voor gemeenten en overheidsorganisaties is datalocatie van burgergegevens cruciaal. Basisregistraties, het sociaal domein en belastingadministraties bevatten privacygevoelige informatie die onder Nederlands toezicht hoort. De BIO (Baseline Informatiebeveiliging Overheid) schrijft dit impliciet voor, en NIS2 zal dit verder aanscherpen met concrete verplichtingen voor kritieke infrastructuur.

4. **Digitale soevereiniteit:** van concept naar strategische prioriteit

Digitale autonomie en soevereiniteit zijn in 2026 stevig verankerd in de IT-strategie van Nederlandse organisaties. Voor **74%** is digitale autonomie expliciet onderdeel van de IT-strategie. Nog duidelijker is de behoefte aan regie: 78% wil meer controle over waar data worden opgeslagen en wie daar toegang toe heeft.

SECTORINZICHT: COMMERCIËLE SECTOREN

Soevereiniteit is geen niche-thema meer voor overheden of defensie. Softwareleveranciers merken dat klanten steeds vaker vragen naar SaaS-oplossingen op soevereine Nederlandse infrastructuur. Retailorganisaties met grote volumes klantdata en bouwbedrijven met concurrentiegevoelige projectinformatie willen expliciet weten onder welke jurisdictie hun data vallen en kiezen bewust voor Nederlandse of Europese cloudproviders.

Geopolitiek als katalysator

Geopolitieke ontwikkelingen fungeren als duidelijke versneller:

- **81%** vindt dat de geopolitieke context het belang van digitale onafhankelijkheid benadrukt
- **72%** maakt zich zorgen over soevereiniteit op maatschappelijk niveau
- **63%** maakt zich zorgen over soevereiniteit voor de eigen organisatie
- **83%** vindt het belangrijk dat IT- en cloudoplossingen voldoen aan Europese en Nederlandse normen

KRITIEKE INFRASTRUCTUUR - SCENARIO

Stel: een waterschap of energiebedrijf ontdekt dat hun SCADA-systemen draaien op een platform met niet-Europese jurisdictie. Het besef: hun kritieke infrastructuur kan doelwit zijn van statelijke bedreigingen en afhankelijkheid van buitenlandse platforms vergroot de impact van verstoringen. Voor deze sectoren is soevereiniteit geen ideologische keuze, het is een randvoorwaarde voor operationele continuïteit en nationale veiligheid.

De bereidheid om hiernaar te handelen is groot: **73%** van de organisaties is bereid extra te investeren om data onder te brengen in een volledig soevereine omgeving. Soevereiniteit is daarmee niet langer alleen een strategisch principe, maar een concrete investeringsrichting binnen de IT-agenda.

5. De juridische realiteit: CLOUD Act en FISA 702

JURIDISCHE WAARSCHUWING

Een datacenter in Amsterdam van een Amerikaanse cloudprovider biedt GEEN bescherming tegen Amerikaanse informatieverzoeken. De fysieke locatie van je data is minder relevant dan de juridische jurisdictie van je cloudprovider. Dit is geen theoretisch risico, dit is geldende wetgeving met directe consequenties.

Een belangrijk, maar vaak onderschat onderdeel van cloudstrategie is de impact van Amerikaanse wetgeving op data die wordt verwerkt door Amerikaanse cloudproviders. Deze wetgeving kan van toepassing zijn, ongeacht waar data fysiek is opgeslagen.

CLOUD Act: extraterritoriale toegang

De Clarifying Lawful Overseas Use of Data Act (CLOUD Act) geeft Amerikaanse autoriteiten de bevoegdheid om data op te vragen bij Amerikaanse cloudproviders, ook wanneer deze data buiten de Verenigde Staten is opgeslagen.

Wat dit concreet betekent: wanneer je data opslaat bij Amerikaanse partijen of zelfs in hun Europese datacenters, kunnen Amerikaanse autoriteiten via de CLOUD Act toegang eisen tot die data. Er is sprake van rechterlijke toetsing per individueel verzoek, maar de juridische grondslag voor toegang blijft bestaan.

FISA Section 702: structurele surveillance

FISA Section 702 gaat verder dan gerichte datavorderingen. Deze wet stelt Amerikaanse inlichtingendiensten in staat om communicatie van niet-Amerikanen buiten de Verenigde Staten te verzamelen, zonder individueel rechterlijk bevel. In 2024 is deze wet verlengd tot 2026.

HET SCHREMS II-ARREST

Het Europees Hof van Justitie verklaarde in 2020 het Privacy Shield ongeldig vanwege onvoldoende waarborgen tegen Amerikaanse surveillancewetgeving, waaronder FISA Section 702. Daarmee werd bevestigd dat deze wetgeving fundamenteel botst met Europese privacybescherming. Dit is geen academische discussie, dit is rechtspraak met directe gevolgen voor je compliance.

Wat dit concreet betekent voor jouw organisatie

De juridische gevolgen zijn niet abstract:

- Patiëntgegevens in de zorg kunnen zonder medeweten toegankelijk zijn voor buitenlandse autoriteiten, wat in strijd is met medisch beroepsgeheim
- Ontwerp-, onderzoeks- en productiedata kunnen inzichtelijk worden voor derden in andere jurisdicties
- Vertrouwelijke klantinformatie kan bij bepaalde verwerkingen buiten de bescherming van de AVG vallen
- Encryptie van data stelt de concrete toegang tot de niet ge-encrypte data alleen voor onbepaalde data uit door de toenemende capaciteit om encryptie-methoden te breken. Vandaar ook dat de AVG het verlies van op die manier beveiligde data ook als dataverlies beschouwd.

FINANCIËLE CONSEQUENTIES

De juridische verantwoordelijkheid voor naleving van de AVG ligt altijd bij de organisatie zelf, niet bij de cloudprovider. Bij ernstige overtredingen kunnen boetes oplopen tot €20 miljoen of **4%** van de wereldwijde jaaromzet. Een datalek als gevolg van ongewenste toegang via FISA 702 valt hier ook onder.

Belangrijk: geografische maatregelen alleen zijn onvoldoende. Dataopslag in een Europees datacenter van een Amerikaanse provider voorkomt niet dat FISA Section 702 van toepassing blijft.

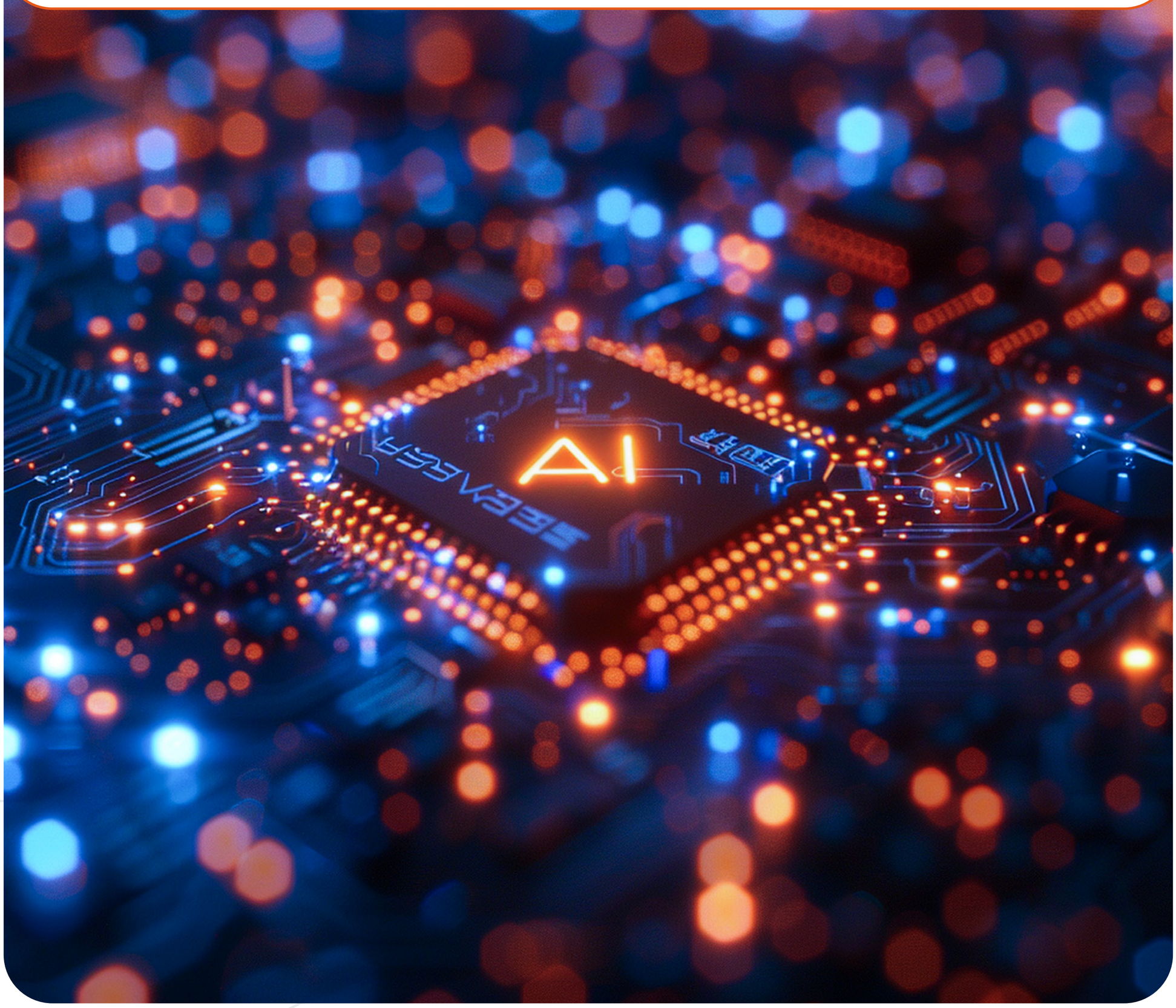
Een structurele manier om dit risico te beperken is kiezen voor cloudproviders die niet onder Amerikaanse jurisdictie vallen en data hosten in Nederlandse of Europese datacenters, onder Europees eigendom en beheer.

6. **AI-adoptie:** tussen ambitie en uitvoering

Organisaties erkennen het strategische belang van AI, maar de daadwerkelijke toepassing blijft achter. **62%** geeft aan dat AI nog te weinig wordt benut, terwijl **56%** AI ad-hoc gebruikt zonder duidelijke richtlijnen of structurele ondersteuning. Dit werkt shadow-IT en daarmee data-verlies in de hand.

DE AI-PARADOX

Medewerkers ontdekken generatieve AI-tools en ervaren directe productiviteitswinst. HR-processen versnellen, analyses gaan sneller, teksten zijn in seconden opgesteld. Maar tegelijkertijd ontstaat de onvermijdelijke vraag: waar zijn die gegevens verwerkt, wie heeft toegang, en onder welke voorwaarden? Tussen “geen AI gebruiken” en “onbegrensd AI gebruiken” ligt een smalle route van gecontroleerde inzet.



De grootste belemmeringen

83% maakt zich zorgen over datalekken of onvoldoende databeveiliging. De top-3 zorgen:

Zorgen over AI	Grootste zorg	Totaal
Datalekken of onvoldoende databeveiliging	34%	83%
Onbedoelde vooroordelen of fouten in uitkomsten	30%	78%
Gebrek aan interne kennis of vaardigheden	29%	78%

SECTORINZICHT: ZORG & AI

AI kan medische beelden sneller analyseren dan radiologen, maar wanneer die beelden worden verwerkt in publieke cloud-modellen ontstaat directe spanning met privacywetgeving en het medisch beroepsgeheim. Private AI binnen eigen infrastructuur biedt dezelfde technologische voordelen, maar patiëntbeelden verlaten nooit de zorgomgeving. Zo hoeven compliance en innovatie elkaar niet uit te sluiten, mits de juiste architectuurkeuzes worden gemaakt.

Bij strategische afwegingen rond AI blijkt dat **39%** eerst volledige grip op data en infrastructuur wil realiseren en daarna pas wil opschalen. Slechts **21%** kiest voor maximale snelheid, zelfs als dat ten koste gaat van controle. De meerderheid kiest daarmee expliciet voor controle en beheersbaarheid boven pure snelheid.

Private AI als logische vervolgstap

De combinatie van veiligheidszorgen, compliance-druk en behoefte aan controle wijst in één richting: private AI. Private AI betekent dat AI-systemen draaien binnen een gecontroleerde, soevereine omgeving, waarbij data de organisatie niet verlaat en niet wordt gebruikt voor training van publieke modellen.

Technieken zoals retrieval-augmented generation (RAG) versterken dit model. Het systeem haalt context op uit geselecteerde bronnen en gebruikt die uitsluitend voor het genereren van het antwoord. Zo blijven output en context controleerbaar, herleidbaar en organisatie-specifiek.

7. De druk van compliance: NIS2 en AI Act

TIJDLIJN COMPLIANCE 2026

NIS2: Implementatie verwacht Q2 2026 (geen overgangsperiode!) | AI Act: Gefaseerd ingegaan sinds 2025, hoog-risico AI-eisen vanaf 2026 | Sancties tot €40 miljoen of **7%** omzet bij AI-overtredingen | Tot €20 miljoen of **4%** omzet bij AVG-schendingen

NIS2: uitgesteld, maar onvermijdelijk

De NIS2-richtlijn had uiterlijk in oktober 2024 moeten zijn omgezet in nationale wetgeving. In Nederland is die implementatie vertraagd. De Cyberbeveiligingswet wordt nu verwacht in Q2 2026. Dat uitstel verandert niets aan de impact: zodra de wet van kracht is, moeten organisaties direct voldoen. Er is geen overgangsperiode.

De kernverplichtingen van NIS2:

- Structurele risicoanalyse en zorgplicht voor digitale risico's
- Technische en organisatorische beveiligingsmaatregelen op basis van die risico's
- Ingerichte incident response-processen, inclusief meldplicht binnen korte termijnen
- Aangescherpt toezicht en zwaardere sancties dan onder de oorspronkelijke NIS

NIS2 verschuift cyberbeveiliging daarmee van een operationeel IT-thema naar een expliciete bestuurlijke verantwoordelijkheid.

De AI Act: gefaseerd, maar met directe gevolgen

De AI Act treedt gefaseerd in werking. Vanaf 2025 gelden verboden op AI-toepassingen met onaanvaardbaar risico. Vanaf 2026 volgen aanvullende eisen voor hoog-risico AI-systemen, gericht op datakwaliteit, documentatie, governance, toezicht en aantoonbare risicobeheersing.

De sancties onder de AI Act zijn fors:

- Tot €40 miljoen of **7%** van de wereldwijde jaaromzet bij verboden AI-praktijken
- Tot €20 miljoen of **4%** bij overtredingen rond datagovernance en transparantie
- Tot €10 miljoen of **2%** bij overige overtredingen

Slechts **46%** van de organisaties voelt zich voldoende voorbereid op AI-wetgeving. Dit is risicovol, gezien de omvang van de sancties en het feit dat compliance niet meer vrijblijvend is.

8. Obstakels en uitdagingen

Ondanks de brede erkenning van het belang van digitale autonomie lopen organisaties in de praktijk tegen duidelijke belemmeringen aan. De grootste hindernissen zijn organisatorisch en bestuurlijk, niet alleen technologisch.

Top 5 obstakels

Obstakel	% Respondenten
Complexiteit van wet- en regelgeving	32%
Afhankelijkheid van bestaande leveranciers/platforms	27%
Onvoldoende technische kennis of capaciteit	26%
Beperkte interne kennis over datasoevereiniteit	24%
Onvoldoende budget of middelen	22%

VENDOR LOCK-IN RISICO

27% ervaart afhankelijkheid van leveranciers als concreet obstakel. Dit ontstaat wanneer kritieke IT-onderdelen sterk leunen op propriëtaire technologie. Het risico: minder onderhandelingsruimte, beperkte flexibiliteit om te migreren, en verhoogd operationeel risico bij storingen. Een organisatie met **80%** workloads in één cloud-ecosysteem heeft geen wendbare migratiestrategie meer, maar een meerjarig en kostbaar traject.

De combinatie van kennistekorten (**26%** technisch, **24%** soevereiniteit) maakt het lastig om strategische keuzes zelfstandig te maken en te onderbouwen richting bestuur. Dit onderstreept het belang van samenwerkingen met IT-partners die soevereiniteit, security en compliance niet als losse thema's benaderen, maar integraal meenemen.

9. IT-investeringen 2026: prioriteiten en budget

Organisaties blijven investeren in innovatie, maar de beschikbare ruimte is begrensd. **45%** van de organisaties verwacht in 2026 tussen **10 en 30%** van het IT-budget te besteden aan innovatie. Dat betekent dat ongeveer **70%** van het budget opgaat aan run en onderhoud.

De ruimte voor vernieuwing is daarmee beperkt. Tegelijk moeten juist uit dat innovatiebudget modernisering, AI-toepassingen, cloudmigraties én compliance-maatregelen worden gefinancierd. Dit dwingt organisaties tot scherpe prioritering.

IT-doel 2026	% Organisaties
Moderniseren van IT-infrastructuur	33%
Verbeteren van informatiebeveiliging en dataveiligheid	32%
Voldoen aan wet- en regelgeving (compliance)	30%
Implementatie of optimalisatie van AI-oplossingen	26%

Modernisering, beveiliging en compliance staan bovenaan de agenda. Die samenhang is logisch: verouderde IT-omgevingen zijn moeilijk te beveiligen, kostbaar in beheer en remmen innovatie. Investeren in modernisering is daarmee een randvoorwaarde voor veiligheid en wendbaarheid.

Concrete maatregelen voor meer datacontrole

29% van de organisaties onderzoekt expliciet hoe AI veiliger kan worden ingezet binnen eigen infrastructuur of een soevereine cloudomgeving. Soevereiniteit wordt steeds vaker vertaald naar concrete acties.

OPVALLEND

18% van de organisaties neemt GEEN specifieke maatregelen voor meer datacontrole.
Dit is een risico, zeker in het licht van NIS2 en de AI Act. Organisaties die nu niet handelen, lopen het risico straks in een ad-hoc compliance-race te belanden, met alle kosten en risico's van dien.

10. **Analyse:** vier strategische dilemma’s

De onderzoeksdata laten vier terugkerende dilemma’s zien waar veel organisaties tegenaan lopen. Deze spanningsvelden verklaren waarom keuzes rond cloud, AI en soevereiniteit zo complex zijn.

DILEMMA 1

INNOVATIESNELHEID VERSUS CONTROLE

De spanning: 62% vindt dat AI nog te weinig wordt benut, maar **75%** geeft aan dat veiligheids- en privacyrisico's doorslaggevend zijn bij AI-keuzes. **39%** kiest bewust voor eerst volledige grip op data, daarna pas opschalen met risico op shadow-it.

De uitweg: *Private AI in een soevereine omgeving waarbij organisaties de voordelen van AI benutten zonder data bloot te stellen aan externe jurisdicties.*

DILEMMA 2

VERTROUWEN IN CLOUD VERSUS JURIDISCHE REALITEIT

De spanning: Hoog vertrouwen in technische beveiliging van cloudproviders, maar tegelijk brede zorg (**68%**) over mogelijke juridische toegang door niet-Europese overheden.

De uitweg: *Bewuste keuze voor cloudproviders onder Europese jurisdictie, met data op Nederlandse of Europese bodem onder Europees eigendom en beheer.*

DILEMMA 3

COMPLIANCE-COMPLEXITEIT VERSUS CAPACITEIT

De spanning: Toenemende regelgeving complexiteit (32% ziet dit als obstakel) in combinatie met beperkte interne capaciteit en kennis.

De uitweg: *Samenwerking met strategische IT-partners die compliance-by-design hanteren en eisen uit NIS2, AVG en AI Act vertalen naar geïntegreerde platformkeuzes.*

DILEMMA 4

VENDOR LOCK-IN VERSUS SCHAALBAARHEID

De spanning: : Public cloud biedt snelle schaalbaarheid, maar vergroot tegelijk het risico op vendor lock-in en afhankelijkheid van één platform.

De uitweg: *Open standaarden, multi-cloud, cloud-native werken en private cloud met behoud van regie en mogelijkheid om te schakelen zonder schaalbaarheid te verliezen.*

11. **Aanbevelingen:** een routekaart voor IT-beslissers

90-DAGEN ACTIEPLAN

Week 1-2: Dataclassificatie en inventarisatie | Week 3-4: Cloudmodel per workload bepalen | Week 5-6: Compliance gap-analyse NIS2 & AI Act | Week 7-8: Provider-evaluatie en risico-assessment | Week 9-10: Pilot private AI voor kritieke use case | Week 11-12: Implementatieplan en roadmap 2026

1. Dataclassificatie als fundament

Een toekomstbestendige IT-strategie begint met helderheid over data. Door data te classificeren op vertrouwelijkheid, integriteit en beschikbaarheid ontstaat een praktisch kader voor infrastructuurkeuzes.

CHECKLIST: DATACLASSIFICATIE

- ☐ Alle datasets geïnventariseerd
- ☐ Classificatie per dataset (publiek/intern/vertrouwelijk/strikt vertrouwelijk)
- ☐ Wettelijke vereisten per categorie vastgesteld
- ☐ Eigenaar en verantwoordelijken per dataset benoemd
- ☐ Retentiebeleid gedocumenteerd
- ☐ Cloudmodel per categorie bepaald

2. Het juiste cloudmodel per workload

Bewuste keuze per applicatie of dataset:

- Niet-kritieke kantoorapplicaties → Public cloud
- ERP-, CRM- en HR-systemen → Private cloud
- Systemen welke IP van de organisatie bevatten → Private cloud
- Patiëntendossiers en financiële data → Private cloud op NL/EU bodem
- AI-workloads met gevoelige data → Private AI in soevereine omgeving
- Test- en ontwikkelomgevingen → Hybride opzet

3. Soevereine cloudproviders voor kritieke data

Voor bedrijfskritieke en privacygevoelige data verdienen deze aspecten structureel aandacht:

- Fysieke dataopslag in Nederland of Europa
- De provider valt onder Nederlandse of Europese jurisdictie
- Geen blootstelling aan CLOUD Act of FISA Section 702
- Relevante certificeringen: ISO 27001, NEN 7510, ISAE/SOC
- Aantoonbare voorbereiding op NIS2 en EUCS

4. Private AI voor gevoelige use cases

Voor AI-toepassingen met persoonsgegevens, medische informatie, financiële data of bedrijfsgeheimen ligt private AI voor de hand. Door AI binnen een gecontroleerde, soevereine omgeving te draaien, blijft data binnen de eigen infrastructuur en onder eigen governance. Actieve beveiliging tot voorkomen van data delen is ook essentieel, juist ook als de organisatie nog geen beleid heeft tot (toegestaan) gebruik van (AI-)tools om datalekken te voorkomen.

De inzet van retrieval-augmented generation (RAG) versterkt dit model: AI-antwoorden gebaseerd op geselecteerde interne bronnen, zonder dat data worden gebruikt voor training van externe modellen.

5. Tijdig starten met NIS2- en AI Act-compliance

Wachten tot wetgeving volledig van kracht is, vergroot het risico op ad-hocmaatregelen. Door tijdig te inventariseren welke systemen onder NIS2 en de AI Act kunnen vallen, ontstaat ruimte voor een gefaseerde aanpak.

COMPLIANCE CHECKLIST

NIS2:

- ☐ Scope-analyse (valt je organisatie eronder?)
- ☐ Gap-analyse huidige beveiliging
- ☐ Incident response-procedures
- ☐ Meldplicht-procedures ingericht

AI Act:

- ☐ AI-systemen geïnventariseerd
- ☐ Risicoclassificatie per systeem
- ☐ Documentatievereisten geïmplementeerd
- ☐ Governancestructuur opgezet

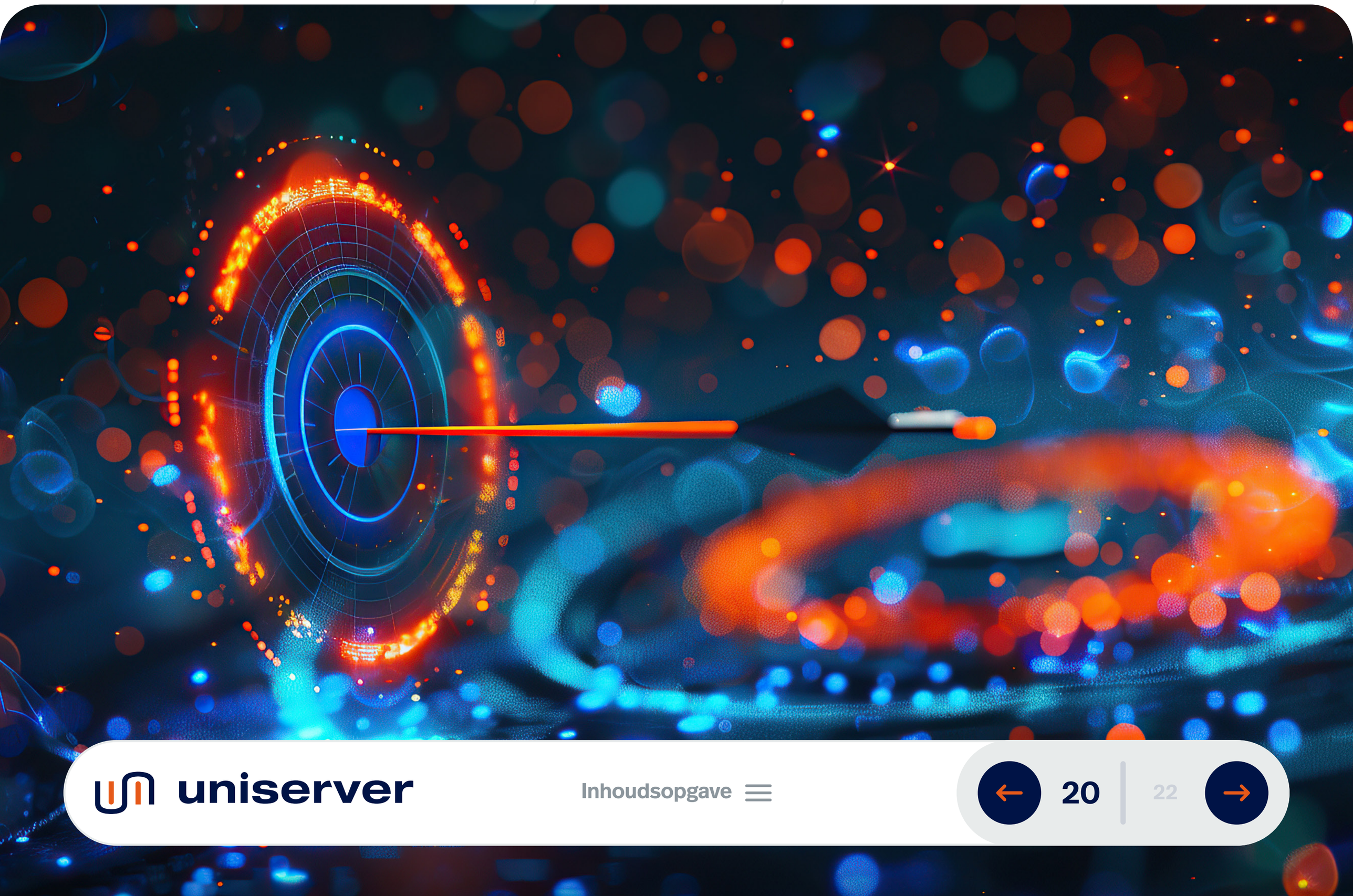
12. **Conclusie:** regie als voorwaarde voor digitale vooruitgang

De uitkomsten van dit onderzoek laten een helder beeld zien. Nederlandse organisaties willen versnellen met digitalisering en AI, maar doen dat niet ten koste van controle, veiligheid en compliance. Cloud, AI en geopolitiek zijn geen losse thema's meer, maar raken direct aan bestuur, risicomanagement en continuïteit.

Private cloud wint terrein, niet uit nostalgie voor eigen infrastructuur, maar vanuit een bewuste keuze voor regie. Digitale autonomie is voor een meerderheid expliciet onderdeel van de IT-strategie geworden. Tegelijkertijd blijft AI-innovatie achter door zorgen over dataveiligheid, juridische risico's en gebrek aan governance.

KERNBOODSCHAP

Wie digitale vooruitgang wil boeken, moet eerst zorgen dat de fundamenten kloppen.
Regie is geen rem op innovatie, maar de voorwaarde om deze verantwoord te laten groeien.
Organisaties die nu investeren in regie, transparantie en controle, bouwen niet alleen aan compliance, maar vooral aan toekomstbestendigheid.



13. Over Uniserver

Uniserver is een Nederlandse, soevereine private cloudpartner. Organisaties krijgen regie over data en infrastructuur, gehost in Nederlandse datacenters, beheerd door een Nederlands team en onder Nederlands recht.

Soeverein en compliant by design

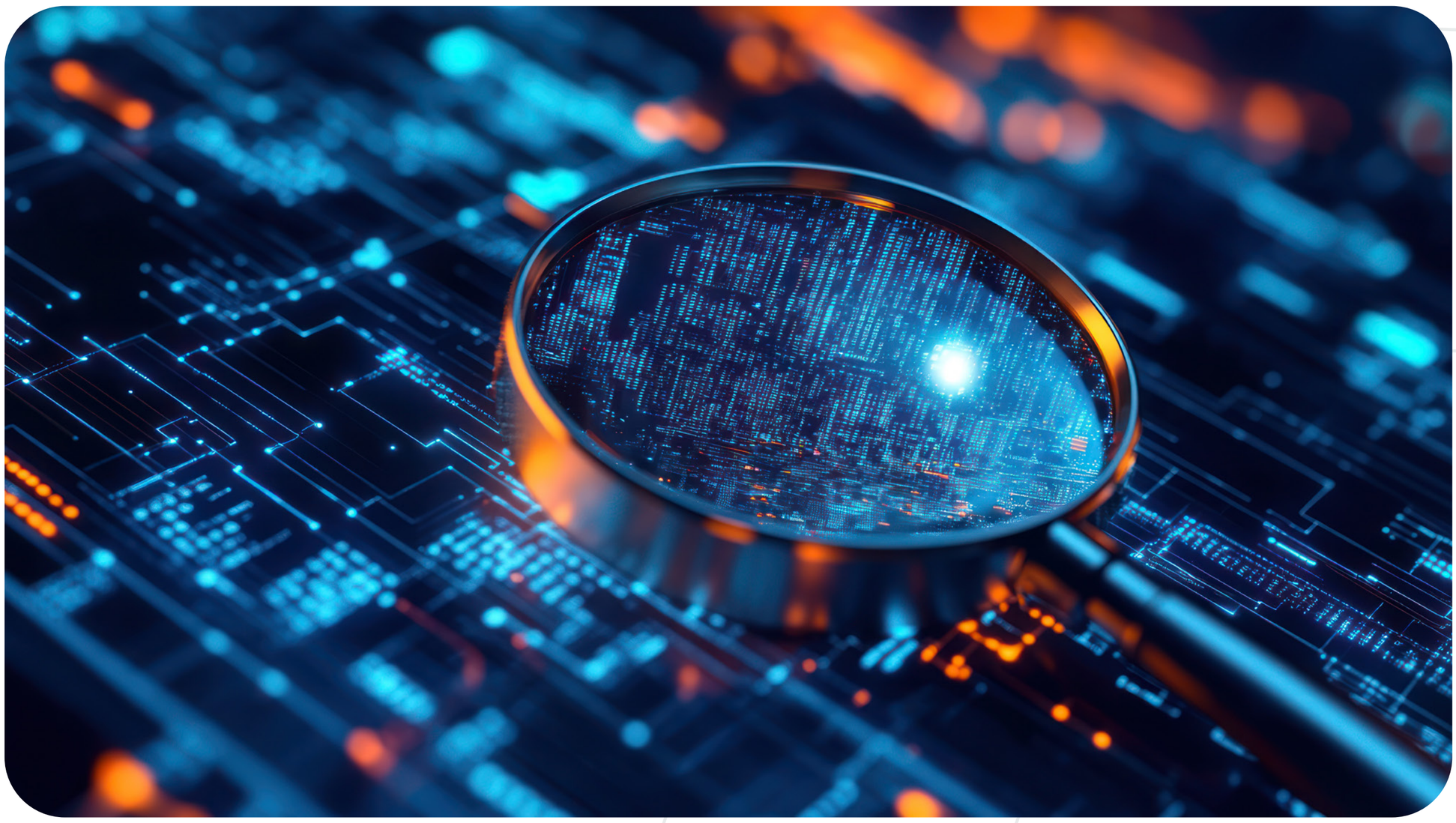
Data wordt gehost en beheerd in Nederlandse datacenters, binnen de Europese rechtsorde. De cloudomgeving is ingericht op datasoevereiniteit, security en compliance, met ISO 27001, NEN 7510 en ISAE/SOC-verklaringen als vaste basis.

In de praktijk betekent dit:

- → Zorgorganisaties draaien EPD-omgevingen en patiëntdata op soevereine cloudinfrastructuur, conform NEN 7510 en voorbereid op NIS2
- → Gemeenten moderniseren hun infrastructuur op Nederlandse bodem, audit-ready en in lijn met BIO en NIS2-verplichtingen
- → Softwareleveranciers en Managed service Providers gebruiken het Uniserver-platform om eigen oplossingen te leveren, met datasoevereiniteit als uitgangspunt

Fuse AI: AI, maar dan soeverein

Fuse AI draait volledig binnen de private, soevereine cloudomgeving van Uniserver. Data blijft onder Nederlands en Europees recht en integreert met bestaande IT-omgevingen. Door inzet van retrieval-augmented generation (RAG) koppelt Fuse AI veilig aan interne databronnen, zonder dat deze data worden gebruikt voor training van externe modellen.



14. Over het onderzoek

Dit onderzoek is uitgevoerd in opdracht van Uniserver en biedt inzicht in hoe Nederlandse organisaties omgaan met cloud, AI, datasoevereiniteit en compliance.

Onderzoeksjaar: 2025
Methode: kwantitatief onderzoek via online vragenlijst (16 vragen)
Doelgroep: IT-(mede)beslissers in Nederland (n = 1.023)
Sectorverdeling: 13% zorg en welzijn, 7,6% gemeenten en semioverheid, 79,4% overige sectoren

NEEM DE VOLGENDE STAP

Wil je weten hoe je organisatie scoort op digitale soevereiniteit en compliance-readiness?

- Plan een vrijblijvend strategiegesprek met onze experts

www.uniserver.nl

info@uniserver.nl