Kiteworks

OPLOSSINGSOVERZICHT

VOOR CISO'S, FG'S EN COMPLIANCE-VERANTWOORDELIJKEN – NEDERLAND EN DE PUBLIEKE SECTOR

Datasoevereiniteit in Nederland: Architectuur, Geen Contractclausule

Uw data. Uw jurisdictie. Uw controle.

De uitdaging: soevereiniteitshandhaving is realiteit geworden in Nederland

De meest gevoelige data van Nederlandse organisaties loopt in toenemende mate via multi-tenant cloudinfrastructuur waarover zij geen controle hebben, onderworpen aan buitenlandse rechtsmacht en extraterritoriale toegangswetten zoals de Amerikaanse CLOUD Act en FISA Section 702 – ongeacht of de data zich fysiek in Nederland bevindt. Contractuele toezeggingen kunnen wettelijke dwang niet opzij zetten, en de locatie van een datacenter alleen biedt geen bescherming zolang de aanbieder onder een buitenlandse jurisdictie valt.

Dit is voor de Nederlandse markt allang geen hypothetisch scenario meer. In mei 2026 blokkeerde de Nederlandse overheid de voorgenomen overname van Solvinity door Kyndryl – de Nederlandse hostingpartij achter DigiD (de nationale digitale identiteit), MijnOverheid, en de infrastructuur die toegang biedt tot belasting-, medische en pensioengegevens van vrijwel alle Nederlandse ingezetenen. Het Bureau Toetsing Investeringen (BTI) beoordeelde de deal onder de Wet ongewenste zeggenschap telecommunicatie (WOZT) en adviseerde een verbod – het enige verbod dat is uitgevaardigd sinds het BTI in 2020 operationeel werd. De onderbouwing verwees expliciet naar blootstelling aan de Amerikaanse CLOUD Act: functionarissen waarschuwden dat Amerikaans eigendom Amerikaanse autoriteiten toegang zou kunnen geven tot persoonsgegevens van Nederlandse burgers, ongeacht de Nederlandse wettelijke bescherming. De Tweede Kamer had eerder al met een motie gestemd om het DigiD-contract volledig te beëindigen als de overname zou doorgaan.

Deze ingreep volgde op een directe waarschuwing van de Autoriteit Persoonsgegevens, die de overheid in januari 2026 opriep om "zo snel mogelijk" te handelen ter bescherming van de digitale soevereiniteit – met kritiek op de versnipperde departementale besluitvorming en het ontbreken van exitstrategieën voor overheidsinstanties die afhankelijk zijn van in buitenlandse handen zijnde leveranciers. De toezichthouder stelde specifiek voor om soevereiniteitscriteria op te nemen in overheidscontracten, met verplichte ontbindingsclausules bij wijzigingen in buitenlandse zeggenschap.

Ondertussen stapelen de soevereiniteitsgerelateerde verplichtingen zich op voor organisaties die in Nederland actief zijn: de AVG en de nationale uitvoeringswet (UAVG), gehandhaafd door de Autoriteit Persoonsgegevens; de Cyberbeveiligingswet (de Nederlandse implementatie van NIS2), die op 15 augustus 2026 in werking treedt naast de Wet weerbaarheid kritieke entiteiten, en zorg- en meldplichten – inclusief expliciete ketenverantwoordelijkheid – uitbreidt naar meer dan 8.000 organisaties in 18 sectoren; toetsing onder de WOZT; en sectorspecifieke regelgeving zoals DORA, HIPAA, CMMC 2.0 en ITAR voor multinationals en defensiegerelateerde toeleveranciers. Een breed politiek draagvlak – van CDA, D66, VVD en BBB tot Progressief Nederland en JA21 – beschouwt controle over datacenters, onderzeese kabels en AI-infrastructuur inmiddels als een kwestie van nationale veiligheid, niet als een voetnoot in een aanbesteding.

De oplossing van Kiteworks

Kiteworks levert datasoevereiniteit als architectuur, niet als contractclausule – precies het soort aantoonbare controle waarvan de Autoriteit Persoonsgegevens zegt dat overheidsinstanties die nu missen. Implementeer op single-tenant infrastructuur: on-premises, in uw eigen Nederlandse of Europese cloud, of als door Kiteworks gehoste private single-tenant cloud, in de jurisdictie die u zelf kiest, versleuteld met sleutels die alleen u in bezit heeft. Met eigen encryptiesleutels en HSM-integratie kan noch Kiteworks, noch een derde partij – inclusief een overheid die een buitenlandse juridische vordering indient – uw data ontsleutelen.

Regel elke verzending, deling en download via de geofencing-regels van de Data Policy Engine, in realtime gehandhaafd over elk kanaal – precies de egress-controle en exitstrategie die de Autoriteit Persoonsgegevens publiekelijk zegt dat Nederlandse overheidsinstanties nodig hebben, maar momenteel missen. Onderbouw dit met een volledig, ongefilterd auditspoor dat live naar uw SIEM wordt gestuurd, ondersteund door FedRAMP- en IRAP-beoordeelde hostingopties die Nederlandse toezichthouders en inkopers een onafhankelijk getoetste maatstaf bieden voor soevereiniteit op overheidsniveau.

Waarom soevereiniteit nu een boardroomkwestie is in Nederland

- **Eerste verbod ooit.** In mei 2026 vaardigde de Nederlandse overheid het eerste – en tot nu toe enige – formele verbod uit sinds het Bureau Toetsing Investeringen (BTI) in 2020 operationeel werd, door een buitenlandse overname van de hostingpartij achter DigiD en MijnOverheid te blokkeren op gronden van datasoevereiniteit.
- **Ruim 8.000 organisaties nieuw binnen bereik.** De Cyberbeveiligingswet (de Nederlandse implementatie van NIS2), die op 15 augustus 2026 in werking treedt, breidt zorg- en meldplichten – inclusief ketenverantwoordelijkheid – uit naar meer dan 8.000 organisaties in 18 sectoren.
- **69 marktpartijen, één soevereine cloud.** Het NDS Cloud Implementatieprogramma van de Nederlandse overheid raadpleegde 69 marktpartijen, die bevestigden dat er voldoende Nederlandse expertise en capaciteit is om een staatseigen soevereine overheidscloud te bouwen – momenteel in de proof-of-concept-fase, met als doel dat er eind 2026 meerdere overheidsapplicaties op draaien.

Hoe Kiteworks aantoonbare soevereiniteit levert

Single-tenant by design

Toegewijde infrastructuur zonder gedeelde databases, bestandssystemen, applicatieomgevingen of besturingssystemen. Implementeer on-premises, in uw eigen cloud, of als door Kiteworks gehoste private single-tenant cloud, in de jurisdictie die u kiest – inclusief volledig binnen Nederland of de EU.

Eigen encryptiesleutels

Met HSM-integratie kunnen noch Kiteworks, noch een partij die Kiteworks daartoe dwingt, uw data ontsleutelen – ook niet bij geheime dagvaardingen of CLOUD Act-vorderingen.

Geofencing van egress

De Data Policy Engine blokkeert verzendingen en delingen of vereist hiervoor goedkeuring, en kan downloads volledig blokkeren, op basis van gebruikerslocatie, geblokkeerde landen en IP-reeksen – de egress-laag die op residency gebaseerde benaderingen missen.

Eén control plane, elk kanaal

E-mail, bestandsdeling, SFTP, MFT, API's en AI-agents vallen allemaal onder hetzelfde egress-beleid, zodat er geen gaten per kanaal ontstaan waar data doorheen kan glippen.

Volledig, ongefilterd auditspoor

Elke gebruikers-, beheerders- en systeemactie wordt in realtime gelogd en live naar uw SIEM gestuurd, zonder sampling en zonder vertraging onder belasting – precies het bewijsmateriaal waarvan de Autoriteit Persoonsgegevens zegt dat het nu ontbreekt bij soevereiniteitsbeslissingen van de overheid.

Getoetst aan overheidsnormen

FedRAMP High In Process, FedRAMP Moderate Authorized sinds 2017, en IRAP-beoordeelde hosting tonen aan dat de architectuur voldoet aan overheidseisen voor soevereiniteit – een onafhankelijk getoetste maatstaf waarnaar Nederlandse overheidsinkopers kunnen verwijzen zolang de nationale Soevereine Overheidscloud nog in de ontwerp- en pilotfase verkeert.

Waar soevereiniteit niet onderhandelbaar is in Nederland

Overheid en publieke sector

Burgergegevens op de schaal van DigiD/MijnOverheid, onder BTI/WOZT-toetsing van buitenlandse investeringen en de opkomende eisen van de Soevereine Overheidscloud, vereisen aantoonbare – geen contractuele – controle.

Digitale infrastructuur en kritieke entiteiten

Organisaties die nieuw onder de reikwijdte vallen van de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten (van kracht per 15 augustus 2026) krijgen te maken met zorg- en meldplichten die zich uitstrekken tot hun toeleveringsketen.

Defensie-industriële basis

CUI en exportgecontroleerde technische data onder CMMC 2.0, ITAR en doorwerkingseisen van hoofdaannemers.

Financiële sector

Klantgegevens onder DORA-gerelateerde operationele weerbaarheid en toezicht door De Nederlandsche Bank.

Zorg en life sciences

Patiëntgegevens onder HIPAA en de Nederlandse wetgeving voor gezondheidsgegevens, plus onderzoeksdata met residency-voorwaarden.

Bronnen

The Netherlands and the EU: Prioritising Cloud Sovereignty – Clingendael Institute.

Dutch Government Blocks U.S. Acquisition of Cloud Provider – Jones Day.

Netherlands weighs data sovereignty concerns with Solvinity digital identity contract – Biometric Update.

Netherlands faces rising digital sovereignty threat, data authority warns – dig.watch.

Dutch Cybersecurity Act final: NIS2 applies in the Netherlands from 15 August 2026 – ExposeNtry.

Dutch government designing own sovereign data cloud – NL Times.

State Secretary considers sovereignty requirements for IT procurement – Ziptone.

www.kiteworks.com

Juli 2026