



WHITEPAPER

Digitale autonomie voor de overheid

Inhoudsopgave

Digitale autonomie voor de overheid

Managementsamenvatting	4
Inleiding	7
1. Digitale autonomie en digitale soevereiniteit	8
2. Het debat en de context	8
3. De drie risicocategorieën	10
4. Het drielagenmodel voor de overheid	12
5. De NDS en wat die betekent voor jou	14
6. Aandachtspunten voor een functionerend Nederlands en Europees cloudlandschap	17
7. Aanbevelingen voor overheidsorganisaties	18
8. Conclusie	21
9. Bronverwijzingen	22

Managementsamenvatting

De digitale infrastructuur van jouw overheidsorganisatie maakt waarschijnlijk gebruik van Amerikaanse cloudtechnologie. Dat is geen vergissing. Het is het logische gevolg van jarenlange innovatie en de schaalvoordelen van deze providers. Maar het betekent wel dat er afhankelijkheden zijn geaccepteerd die mogelijk nooit bewust zijn afgewogen.

Het publieke debat over digitale autonomie wordt gedomineerd door alarmerende koppen en politieke stellingname. Dit whitepaper biedt wat daarin ontbreekt: een nuchter kader voor overheidsorganisaties, gebaseerd op feiten, actuele beleidsontwikkelingen en praktijkvoorbeelden.

Drie inzichten die je niet in de krant leest:

Je risico hangt af van je inrichting, niet van het label 'cloud'.

De CLOUD Act, het meest besproken risico, is alleen relevant wanneer een provider daadwerkelijk toegang heeft tot je data. Die nuance ontbreekt vrijwel volledig in het publieke debat en in de besluitvorming van te veel overheidsorganisaties.

Meer autonomie betekent meer verantwoordelijkheid.

Elke stap richting eigen beheer verlaagt je privacyrisico, maar verhoogt de eisen aan je eigen security en operationele capaciteit. Het is geen keuze tussen veilig en onveilig. Het is een keuze tussen verschillende soorten risico.

Volledige onafhankelijkheid bestaat niet.

De mondiale IT-keten zit vol wederzijdse afhankelijkheden: van Taiwanese chips tot Chinese zeldzame aardmetalen tot Nederlandse ASML-machines. De vraag is niet hoe je volledig onafhankelijk wordt, maar welke afhankelijkheden onaanvaardbaar zijn voor een functionerende democratische rechtsstaat.

Dit whitepaper sluit af met zeven concrete aanbevelingen. Drie daarvan kun je morgen al starten: breng je dienstenlandschap in kaart met het drielagenmodel, stel bij de eerstvolgende contractverlenging de juiste vragen over exit-clausules en dataportabiliteit, en zoek aansluiting bij de NDS-structuur om gezamenlijk sterker te staan.



Inleiding

Een overheidsorganisatie heeft in essentie één opdracht: de samenleving bedienen. Of het nu gaat om het innen van belastingen, het uitkeren van sociale zekerheid, het verlenen van vergunningen of het handhaven van de wet, de kern is overal dezelfde: betrouwbare, continue dienstverlening aan burgers en bedrijven. Altijd. Zonder onderscheid.

De dagelijkse uitdagingen om die opdracht waar te maken zijn al enorm. Bezuinigingen die de organisatie onder druk zetten. Verouderde IT-systemen die niet kunnen meegroeien met de ambities. Personeelstekorten in een arbeidsmarkt die vraagt om schaars digitaal talent. Een complexe juridische omgeving waarin AVG, BIO2, NIS2 en sectorale wetgeving samenkomen. Dát is waar de aandacht en het budget naartoe gaat, en terecht.

En dan staat er nog een thema op de agenda: digitale autonomie. Met de aanvaarding van de Nederlandse Digitaliseringsstrategie (NDS) door de ministerraad in juli 2025 is dit onderwerp verheven van beleidsdiscussie tot rijksbrede opdracht. De kernvragen zijn simpel: waar staat jouw data, wie kan erbij, welke regels gelden daar, en kun je er te allen tijde bij?

De verleiding is groot om digitale autonomie laag op de agenda te zetten. Maar autonomie is geen doel op zich; het is risicomanagement. En risicomanagement is iets wat overheidsorganisaties elke dag doen. Soevereiniteitsrisico's horen in diezelfde afweging thuis: niet bovenaan, niet onderaan, maar op de plek die past bij de waarschijnlijkheid en de impact.

Dit whitepaper helpt je daarbij. Het biedt bestuurders, CIO's, CISO's, CDO's, CTO's en inkoopverantwoordelijken bij gemeenten, provincies, uitvoeringsorganisaties en het Rijk een helder overzicht van wat digitale autonomie concreet betekent voor jouw organisatie, welke risico's reëel zijn en welke overdreven, en welke maatregelen verstandig zijn. Na het lezen beschik je over de kennis om gefundeerde keuzes te maken. Keuzes die passen bij een organisatie die haar schaarse middelen wil inzetten waar ze het meeste verschil maken: bij de burger.

1. Digitale autonomie en digitale soevereiniteit

Wat is digitale soevereiniteit?

Over het begrip digitale soevereiniteit bestaat brede consensus: het betreft het vermogen en de controle van een land, organisatie of individu om digitale infrastructuur, data en diensten te beheren en te beschermen volgens eigen wet- en regelgeving, zonder ongewenste afhankelijkheid of invloed van externe partijen.

Het verschil met digitale autonomie

Waar digitale soevereiniteit streeft naar volledige onafhankelijkheid en afdwingbare jurisdictie over het digitale domein, is digitale autonomie een meer haalbare stap. Het gaat om het vermogen zelfstandig keuzes te maken in het digitale domein, zonder per se totale controle na te streven. Concreet: weten waar je data staat, bepalen wie erbij kan, en de mogelijkheid hebben om van leverancier te wisselen als dat nodig is.

Digitale autonomie als beleidskeuze

Het kabinet kiest bewust voor de term 'digitale autonomie' boven 'digitale soevereiniteit'. Waar soevereiniteit een absoluut begrip is, erkent autonomie een spectrum: Nederland kan geleidelijk autonomer worden in het digitale domein. Het gaat om het 'doelgericht afbouwen' van strategische afhankelijkheden, niet om een radicale breuk met bestaande leveranciers.

Voor de overheid is dit geen abstracte beleidsoverweging. De NDS stelt expliciet dat beperkingen in digitale autonomie ook de digitale weerbaarheid beperken. En weerbaarheid is in publieke dienstverlening geen kwaliteitsaspect, het is een constitutionele randvoorwaarde.

De overheid die roept maar niet handelt

Er is een tegenstelling zichtbaar in het overheidsoptreden rond digitale autonomie. De overheid roept harder dan wie ook dat digitale autonomie noodzakelijk is en is tegelijk de organisatie die er het minst klaar voor lijkt te zijn.

Twee recente voorbeelden illustreren dit. In oktober 2025 maakte de Belastingdienst bekend over te stappen naar Microsoft 365 voor de kantoorautomatisering van 46.000 medewerkers, ondanks eerdere kritiek vanuit de Tweede Kamer. De staatssecretaris benadrukte dat de primaire belastingdata in het eigen datacenter in Apeldoorn blijft, en dat klopt: op die gegevens heeft Microsoft geen toegang, en dus heeft de CLOUD Act daar ook geen grip op.

Waar het risico wél ligt, is het e-mailverkeer van medewerkers. Microsoft 365 beheert die communicatie als Online Service Provider, wat betekent dat Microsoft technisch toegang heeft tot de inhoud. Onder de CLOUD Act kan de Amerikaanse overheid die data opvragen wanneer een medewerker van bijvoorbeeld de Belastingdienst in het vizier van de Amerikaanse justitie komt. Dat vereist in principe een concrete aanleiding, een vermoeden van strafbaar handelen. Maar de praktijk laat zien dat de grens tussen strafrechtelijke opsporing en politiek gemotiveerde informatieverzameling niet altijd scherp is. De wet vereist geen afstemming met Nederlandse of Europese autoriteiten, en biedt de Amerikaanse overheid ruimte om data op te vragen vanuit eigen rechts- of beleidsbelangen. Dat maakt het risicoprofiel moeilijker te beoordelen dan het op papier lijkt.

Begin 2026 laaide de discussie opnieuw op toen berichten circuleerden dat de Sociale Verzekeringsbank (SVB), die pensioenen, AOW, kinderbijslag en PGB uitbetaalt voor miljoenen Nederlanders, haar systemen naar Azure zou verhuizen. Na Kamervragen bleek dat er geen sprake was van een organisatiebrede migratie; de kritische uitbetalingsprocessen bleven buiten de publieke cloud. Maar de rel illustreerde hoe weinig grip politiek en samenleving ervaren op de cloudkeuzes van uitvoeringsorganisaties.

Tegelijkertijd tekent zich een patroon af van digitale monocultuur: als grote delen van de overheidskolom op dezelfde infrastructuur draaien, kan één storing, één juridische maatregel of één geopolitieke spanning

tegelijk tientallen organisaties raken. Dat is niet alleen een Rijksprobleem; het is een structureel probleem van de hele overheidskolom.

De Rekenkamer constateerde in 'Het Rijk in de Cloud' dat bij 67% van de belangrijkste public cloud-diensten geen risicoafweging was gemaakt. Dat is geen politiek statement, het is een feitelijke vaststelling over de kwaliteit van de besluitvorming.

De CLOUD Act: feiten en nuances

De CLOUD Act (Clarifying Lawful Overseas Use of Data Act) verplicht Amerikaanse bedrijven om data te verstrekken aan de Amerikaanse overheid wanneer die hierom verzoekt in het kader van een justitieel onderzoek, ongeacht waar de data fysiek is opgeslagen. Dit geldt voor Microsoft, Google, Amazon en alle andere Amerikaanse aanbieders. Dat Europese privacywetgeving dit volledig zou voorkomen is een veelgehoorde misvatting. Europese wetgeving is wel degelijk van kracht voor Europese organisaties en hun verwerkers, maar de CLOUD Act creëert een juridisch conflict: een Amerikaanse provider kan tegelijkertijd verplicht zijn data te verstrekken aan de VS én verplicht zijn die data te beschermen onder bijvoorbeeld de AVG. Welke wet in de praktijk de doorslag geeft, hangt af van waar de druk het grootst is.

De CLOUD Act is van toepassing wanneer data onder de possession, custody, or control van een Amerikaans bedrijf valt. Maar de CLOUD Act is alleen relevant wanneer een provider daadwerkelijk toegang heeft tot de data. Bij systemen die draaien op Europese infrastructuur met door de klant beheerde encryptiesleutels, ziet de provider (in de meeste scenario's) alleen versleutelde bestanden. Die nuance maakt een fundamenteel verschil voor het risicoprofiel en ontbreekt vrijwel volledig in het publieke debat.

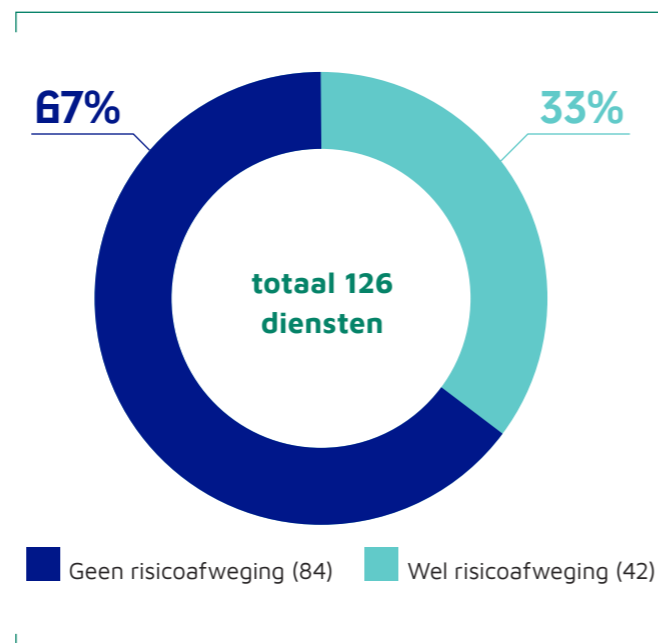
De kern blijft: jouw CLOUD Act-blootstelling is geen vast gegeven, maar het resultaat van bewuste technische keuzes. Die nuance ontbreekt vrijwel volledig in het publieke debat.

2. Het debat en de context

De achtergrond: Amerikaanse dominantie

De Nederlandse cloudmarkt wordt gedomineerd door Amerikaanse leveranciers. Microsoft Azure heeft in Nederland veruit het grootste marktaandeel, gevolgd door Amazon Web Services en Google Cloud Platform. De technologie, functionaliteit en schaal van hun dienstverlening is op dit moment ongeëvenaard; het resultaat van jarenlange miljarden-investeringen in datacenters, IT-infrastructuur en platformdiensten.

Die dominantie heeft geleid tot een stevig maatschappelijk debat. Het Draghi-rapport over Europese concurrentiekracht, de initiatiefnota 'Wolken aan de horizon' en het Rekenkamer-rapport 'Het Rijk in de Cloud' schetsen stuk voor stuk een beeld van te grote afhankelijkheid. De Rekenkamer constateerde dat bij 84 van de 126 belangrijkste public cloud-diensten van het Rijk (67%) geen risicoafweging was gemaakt.



3. De drie risicocategorieën

Digitale autonomie raakt drie fundamenteel verschillende risicocategorieën. Elk vraagt om een andere afweging en een andere aanpak.

Privacyrisico

Overheidsorganisaties verwerken de meest gevoelige persoonsgegevens die er zijn: belastingaangiften, uitkeringsgegevens, medische indicaties, verblijfsstatus, juridische dossiers. Dit zijn gegevens die burgers toevertrouwen aan de overheid in de verwachting dat ze worden beschermd.

Het privacyrisico zit niet alleen in hacks en datalekken. Het zit ook in de juridische kwetsbaarheid van data die onder buitenlandse jurisdictie valt. De CLOUD Act creëert een permanent potentieel inzagerecht voor de Amerikaanse overheid in data die door Amerikaanse providers wordt verwerkt.

De CLOUD Act is daarin niet het enige voorbeeld. In mei 2026 deelden Microsoft en andere techbedrijven namen van medewerkers van de Autoriteit Consument en Markt (ACM) en de Autoriteit Persoonsgegevens met een commissie van het Amerikaanse Huis van Afgevaardigden, die onderzoek doet naar de Europese handhaving van de Digital Services Act. De rechtsgrondslag was geen CLOUD Act-verzoek maar een parlementaire dagvaarding. Dat is een politiek onderzoeksinstrument waarmee het Congres bedrijven kan dwingen intern bewijsmateriaal te overhandigen. E-mails, notulen en uitnodigingen werden overhandigd met namen van Nederlandse ambtenaren die niet waren geanonimiseerd. Staatssecretaris Aerdts noemde de situatie "ontzettend onwenselijk".

Wat dit incident toevoegt aan het beeld: de gedeelde informatie zat in Microsofts eigen zakelijke systemen, niet in systemen die Microsoft namens de Nederlandse overheid beheert. De betrokken ambtenaren hadden zelf geen data bij Microsoft opgeslagen, ze hadden deelgenomen aan overleggen waar ook Microsoft bij was. Het laat zien dat de extraterritoriale bevoegdheden van de VS verder reiken dan cloudopslag alleen: wie in de dagelijkse uitvoering van zijn werk contact heeft met Amerikaanse bedrijven, laat

sporen na in hun systemen die via Amerikaanse juridische procedures kunnen worden opgevraagd, buiten het zicht van een Nederlandse rechter.

Continuïteitsrisico

Overheidsprocessen mogen niet stoppen. Uitkeringen moeten worden uitbetaald, vergunningen moeten worden verleend, de belasting moet worden geheven. Een overheidsorganisatie die haar primaire processen heeft uitbesteed aan een buitenlandse leverancier, is kwetsbaar voor storingen die buiten haar eigen invloedssfeer liggen.

De vraag is niet of een leverancier uitvalt, dat is statistisch zeker bij voldoende lange tijdshorizon, maar of je als organisatie een plan B hebt dat werkt voordat de schade onherstelbaar is. De Algemene Rekenkamer constateerde in januari 2025 in het rapport 'Het Rijk in de Cloud' dat bij 84 van de 126 belangrijkste public clouddiensten van het Rijk, twee derde dus, geen risicoafweging was gemaakt. De Rekenkamer waarschuwt expliciet dat dienstverlening aan burgers en bedrijven daardoor te veel risico loopt en dat de mogelijke schade de samenleving kan ontwrichten.

Maar technische storingen zijn niet het enige risico. Een cloudafhankelijkheid geeft een buitenlandse partij ook een potentieel drukmiddel. In mei 2025 blokkeerde Microsoft de toegang tot het officiële e-mailaccount van de hoofdaanklager van het Internationaal Strafhof in Den Haag, nadat de Amerikaanse overheid sancties had opgelegd. Microsoft was juridisch verplicht te voldoen, zonder tussenkomst van een Nederlandse rechter. Het ICC heeft naar aanleiding hiervan besloten Microsoft 365 volledig te verlaten.

De kans dat dit een gemiddelde gemeente of uitvoeringsorganisatie overkomt, is op dit moment klein. Maar het mechanisme bestaat: een Amerikaans bedrijf kan, onder druk van Amerikaanse wetgeving of politieke besluitvorming, diensten staken voor organisaties op Nederlands grondgebied. En wie afhankelijk is van diezelfde infrastructuur voor kritieke processen, heeft op dat moment geen alternatief.

Als laatste is er nog een continuïteitsrisico: de overname. In november 2025 kondigde het Amerikaanse IT-bedrijf Kyndryl een bod aan op het Nederlandse Solvinity, dat onder meer de infrastructuur achter DigiD beheert, goed voor 16,5 miljoen gebruikers. Het Bureau Toetsing Investerings (BTI) startte een onderzoek onder de Wet Vifo. In mei 2026 adviseerde het BTI de overname volledig te verbieden; staatssecretaris Aerdts nam dat advies over, "ter bescherming van het publieke belang."

De casus is illustratief op twee manieren. Ten eerste: een als Nederlands ervaren leverancier kan via een transactie binnen weken in een buitenlands eigendomsregime

terechtkomen, met alle juridische gevolgen van dien. Ten tweede: de Wet Vifo biedt de overheid een instrument om dat te blokkeren, maar dat instrument werkt alleen als er actief toezicht is en als soevereiniteitsrisico's tijdig worden gesignaleerd. Zonder change-of-control-clausules in contracten en zonder een actief investeringstoetsingsregime heeft een overheidsorganisatie bij zo'n transactie weinig inspraak.

Systeemrisico

Als grote delen van de overheidskolom op dezelfde infrastructuur draaien, wordt een kwetsbaarheid in één product een kwetsbaarheid van de hele overheid. Digitale monocultuur is geen hypothetisch gevaar: de aanval op Kaseya VSA in 2021 trof duizenden organisaties tegelijk. En in juli 2024 legde een foutieve update van beveiligingssoftware CrowdStrike luchthavens, ziekenhuizen en overheidsorganisaties wereldwijd plat. Niet door een aanval, maar door één gedeelde afhankelijkheid in de toeleveranciersketen.

Het concentratierisico heeft daarmee twee gezichten. Het eerste is direct: als één cloudleverancier uitvalt of wordt aangevallen, worden alle organisaties die daarvan afhankelijk zijn tegelijk geraakt. Het tweede is subtieler: zelfs organisaties die zelf niet worden aangevallen, kunnen worden meegesleurd via een gemeenschappelijke leverancier of component. Beide vormen vragen om actieve risicospreiding. Niet alleen in de keuze van cloudprovider, maar door de hele toeleveranciersketen heen.

Er is een derde verschijningsvorm van systeemrisico die minder technisch maar minstens zo reëel is: politieke druk als hefboom. Als grote delen van de overheidskolom afhankelijk zijn van dezelfde Amerikaanse leverancier, ontstaat een structurele kwetsbaarheid die verder gaat dan technisch falen. Een buitenlandse overheid of leverancier die weet dat uitval of afsluiting tientallen overheidsdiensten tegelijk treft, heeft daarmee in theorie een drukmiddel in handen. Dat hoeft zich niet te uiten in daadwerkelijk afsluiten, de dreiging alleen al kan de onderhandelingspositie van de Nederlandse overheid beïnvloeden.



4. Het drielagenmodel voor de overheid

Niet alle overheidssystemen zijn even gevoelig. Een systeem voor facilitair beheer vraagt om een andere soevereiniteitsborging dan DigiD of de basisregistraties. Het drielagenmodel biedt een ordeningsprincipe.

De drie lagen markeren drie fundamenteel verschillende posities op dat spectrum.

Laag 1: geen externe partij mag ooit de data kunnen lezen of het proces onderbreken. Niet op technische gronden, niet op juridische gronden, niet op politieke gronden.

Laag 2: een externe partij mag hosten, maar niet lezen, mits de juiste technische en contractuele waarborgen gelden.

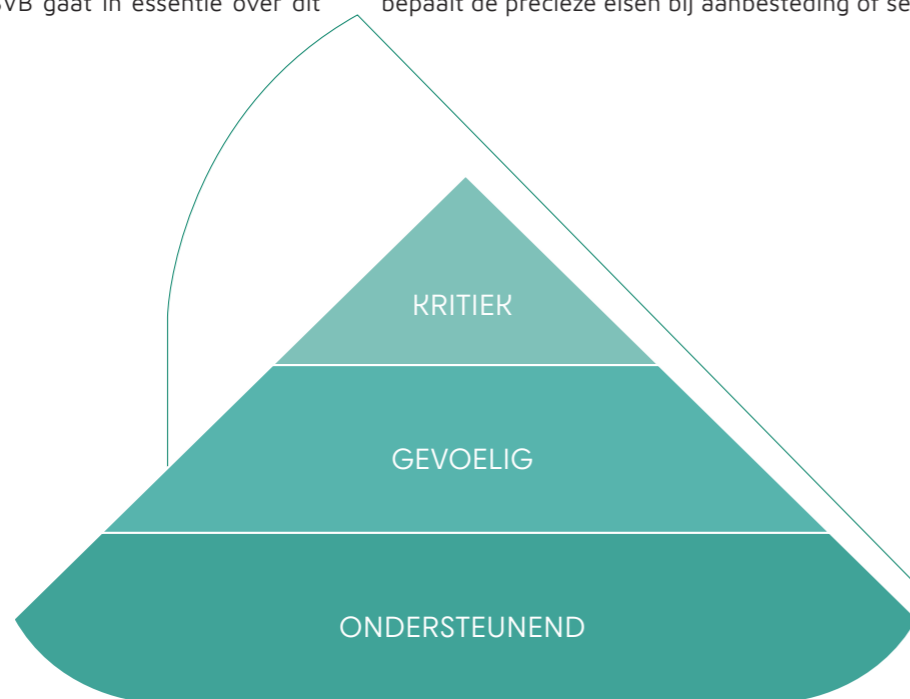
Laag 3: een externe partij mag ook verwerken, mits dit binnen Europese juridische kaders plaatsvindt.

Het drielagenmodel maakt zichtbaar dat volledige migratie naar soevereine infrastructuur niet nodig is. Maar dat voor laag-1-systemen geen compromis mag bestaan. De politieke discussie rond o.a. SVB gaat in essentie over dit

onderscheid: kritische uitbetalingsprocessen horen thuis in laag 1, kantoorautomatisering in laag 3. Voor laag-2-systemen geldt dat public cloud een verantwoorde keuze kán zijn, maar alleen wanneer de technische en contractuele waarborgen daadwerkelijk op orde zijn. Die combinatie van voorwaarden is geen vinkjeslijst; het is een functionele eis aan de inrichting.

De toepassing van dit model bij aanbestedingen is directe winst: wie een softwarecontract verlengt kan per systeem bepalen in welke laag het thuishoort, en op basis daarvan de inkoop-eisen formuleren.

Het drielagenmodel is een bestuurlijk ordeningsprincipe, geen technisch toetsingsinstrument. Voor organisaties die dieper willen gaan, biedt het DICTU Toetsingsinstrument Soevereiniteit Clouddiensten (januari 2026) een gedetailleerder kader met vijf dimensies; juridisch, data & AI, operationeel, technologisch en mens. Daarmee wordt per dienst een nauwkeurigere soevereiniteitsscore bepaald. De twee kaders vullen elkaar aan: het drielagenmodel bepaalt de urgentie en prioriteit, het DICTU-instrument bepaalt de precieze eisen bij aanbesteding of selectie.



Laag	Voorbeelden	Soevereiniteitseis
Laag 1 – Kritiek	DigiD, basisregistraties (BRP, BAG, BRK), belastingheffingssystemen, uitbetalingsprocessen (AOW, toeslagen), C2000-achtige systemen	Maximale soevereiniteit. Vereist: <ul style="list-style-type: none"> Eigen beheer in een privaat datacenter op Nederlandse of Europese bodem, óf uitbesteding aan een aanbieder waarvan het eigendom, de operatie en de juridische vestiging volledig binnen de EU liggen en die aantoonbaar voldoet en blijft voldoen aan Europese soevereiniteitscriteria, zoals het DICTU Toetsingsinstrument of het Europese EUCS-kader. Gebruik van public cloud is niet toegestaan, ook niet wanneer customer-managed encryptiesleutels worden ingezet. Customer-managed keys beperken het privacyrisico van een provider die technische toegang heeft, maar bieden geen bescherming tegen het continuïteitsrisico: een leverancier die onder juridische of politieke druk de dienst staakt, kan dat ongeacht de encryptieconfiguratie. Voor laag-1-systemen is dat risico onaanvaardbaar. Geen buitenlandse jurisdictie. Geen blootstelling aan politiek gemotiveerde continuïteitsdreigingen. Offline-bestendigheid vereist. Toeleveringsketen voor fysieke apparatuur zo min mogelijk blootgesteld aan geopolitieke uitdagingen.
Laag 2 – Gevoelig	Zaaksystemen, vergunningprocessen, minder kritische uitbetalingsprocessen (zoals Kinderbijslag), HR-administratie, dossierbeheersystemen, interne communicatieplatformen	Europese public cloud is acceptabel, mits de leverancier de data kan hosten maar niet in kan lezen. Vereist: <ul style="list-style-type: none"> customer-managed keys waarbij de encryptiesleutels buiten het beheer van de provider blijven, Europese hosting met eigendom en operatie binnen de EU, contractuele exit-clausules die uitvoerbaar zijn en een contractuele inspanningsverplichting voor de leverancier om de organisatie te informeren bij verzoeken van buitenlandse autoriteiten, voor zover wet- en regelgeving dat toestaat. Dit kader is gerechtvaardigd omdat een onderbreking van laag-2-systemen ernstig is, maar herstelbaar binnen een aanvaardbare termijn. Dat onderscheid met laag 1 is het fundament van de andere risicoafweging.
Laag 3 – Ondersteunend	Facilitair beheer, rapportagetools, intranet	Marktconforme cloudoplossingen zijn acceptabel, mits AVG-compliant, serviceverlening en hosting enkel op Europese bodem en met gedocumenteerde risicoafweging. Voor deze systemen is de economische logica van public cloud (lagere beheerlasten, schaalbaarheid, kortere time-to-market) een legitiem beslis criterium.

5. De NDS en wat die betekent voor jou

In juli 2025 stemde de ministerraad in met de Nederlandse Digitaliseringsstrategie (NDS), met als ondertitel 'Samen versnellen is de enige optie'. De NDS is een gezamenlijke strategie van gemeenten, provincies, waterschappen, uitvoeringsorganisaties en het Rijk een serieuze poging om als één overheid op te trekken in de digitale transitie.

De NDS heeft zes prioriteiten, waarvan twee direct relevant zijn voor het autonomievraagstuk: gezamenlijke cloudinfrastructuur (inclusief de verkenning van een soevereine overheidscloud) en het versterken van digitale weerbaarheid en autonomie.

Het NDS-uitvoeringsprogramma en de cloudprioriteit

Binnen het NDS-uitvoeringsprogramma is cloudinfrastructuur één van de zes prioriteiten. De inzet is het ontwikkelen van een soevereine cloudvoorziening voor de overheid. Geen fysiek gebouw met servers, maar een afsprakenstelsel, een marktplaats en een set van standaarden die samen de soevereiniteitsborging vormen. Nederlandse en Europese providers worden betrokken via open dialoogbijeentkomsten. De governance van dit programma is begin 2026 in beweging. Staatssecretaris Aerdts besloot de NDS-Raad, de beoogde onafhankelijke adviesraad, niet formeel in te stellen en koos voor een andere invulling van de advisering. Het uitvoeringsprogramma zelf loopt door.

Toetsingsinstrument Soevereiniteit Clouddiensten

In januari 2026 publiceerde DICTU (de ICT-uitvoeringsorganisatie van het Rijk) het Toetsingsinstrument Soevereiniteit Clouddiensten. Het instrument biedt overheidsorganisaties een gestructureerde methode om clouddiensten te beoordelen op soevereiniteit langs vijf dimensies: juridisch, data & AI, operationeel, technologisch en mens. De criteria zijn objectief, transparant en herhaalbaar, en zijn daarmee direct bruikbaar bij aanbestedingsprocedures.

Concreet beantwoordt het instrument vragen als:

- ▶ Onder welke jurisdictie vallen data en diensten?
- ▶ Wie heeft operationeel de mogelijkheid om de dienst te beïnvloeden of uit te schakelen?
- ▶ Hoe portabel is de technologie bij een leverancierswissel?

DICTU heeft op basis van het instrument ook een analyse gemaakt van de soevereiniteitsscore van een aantal hyperscalers.

Voor organisaties die hun cloudstrategie willen onderbouwen richting gemeenteraad, ministerie of toezichthouder, biedt het DICTU-framework een gezaghebbend vertrekpunt. Niet als vervanging van het drielagenmodel, maar als aanvulling die de beoordeling per dienst verder concretiseert.

Het DICTU-instrument staat niet alleen. In oktober 2025 publiceerde de Europese Commissie haar Cloud Sovereignty Framework (v1.2.1), met acht Sovereignty Objectives en SEAL-niveaus van 0 tot 4. De EC gebruikt het kader inmiddels zelf bij eigen aanbestedingen, waaronder een soeverein cloud-tender van €180 miljoen in april 2026 waarin drie aanbieders SEAL-3 haalden en geen enkele SEAL-4. Het EuroStack-initiatief gaat een stap verder en hanteert een pass-fail op jurisdictie en eigendom, een bewuste keuze om sovereignty-washing structureel te voorkomen. De drie kaders; DICTU, EC-Framework en EuroStack, verschillen in strengheid, maar wijzen in dezelfde richting: soevereiniteit is meetbaar, en zonder drempelwaarde op de juridische dimensie kan een hoge score op techniek of operatie een fundamenteel jurisdictieprobleem maskeren.

Wat de NDS niet regelt

De VNG (Vereniging van Nederlandse Gemeenten) constateert terecht dat het coalitieakkoord weliswaar aandacht heeft voor digitalisering, maar de gemeentelijke digitale opgave beperkt expliciet uitwerkt. Voor gemeenten, waterschappen en kleine uitvoeringsorganisaties betekent de NDS ambitie op papier, maar de uitvoering vraagt om capaciteit die veel van deze organisaties niet hebben.

Kleine gemeenten en provincies willen meedoen, maar weten niet hoe. Ze zoeken ontzorging, geen theorie. Ze willen weten: wat betekent dit voor onze aanbesteding volgende maand?

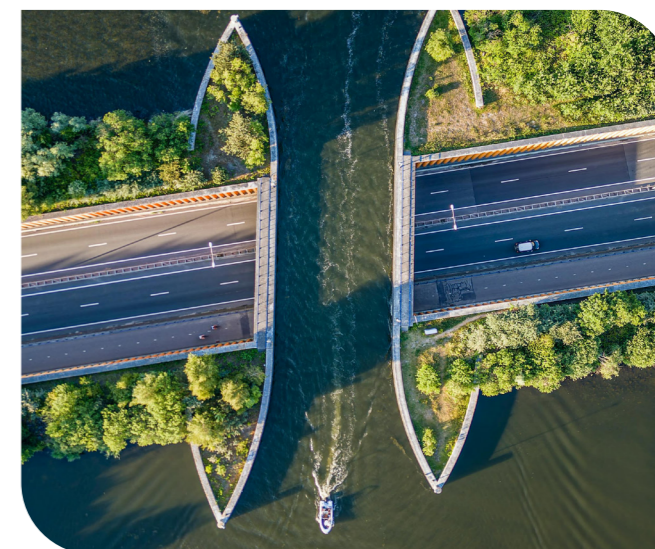
Op 24 april 2026 stuurden minister Herbert (EZK) en staatssecretaris Aerdts een beleidsbrief naar de Tweede Kamer met een apart hoofdstuk over digitale soevereiniteit. De brief erkent geopolitieke afhankelijkheidsrisico's en kondigt een verkenning aan van een soevereine clouddienst en een Nationale Digitale Dienst. Tegelijkertijd blijft de inzet voor een Europese digitale infrastructuur gebonden aan bestaande budgettaire kaders. Concrete financiering voor extra capaciteit ontbreekt. De brief stelt ook geen drempelwaarden voor soevereiniteit vast, en het DICTU-toetsingsinstrument (zoals eerder benoemd) wordt niet als toepassingskader benoemd. Voor overheidsorganisaties die nu keuzes moeten maken, biedt de brief daarmee beleidsmatige richting, maar nog geen operationele houvast.

Softwareleveranciers in een spagaat

Softwareleveranciers van de overheid zitten in een lastige positie. Ze willen aan de soevereiniteitseisen voldoen, maar draaien zelf vaak op Amerikaanse hyperscaler-infrastructuur. De beleidsrichting vanuit de NDS maakt soevereiniteit steeds explicieter een thema bij overheidsinkoop. Wie nu niet investeert in een Nederlands of Europees hostingmodel, loopt het risico straks buiten de boot te vallen bij aanbestedingen die op soevereiniteitscriteria toetsen.

Voor leveranciers die de soevereiniteitseis als kans zien in plaats van last, biedt de NDS een aanzienlijk voordeel in de markt. De overheid heeft immers honderden aanbestedingen per jaar en gaat die steeds explicieter toetsen op soevereiniteitscriteria.

De vraag die elke gemeente, provincie of uitvoeringsorganisatie nu zou moeten stellen: 'Welk systeem gaan we de komende twaalf maanden aanbesteden of verlengen en hoe nemen we daarin een adequate soevereiniteitseis mee?'





6. Aandachtspunten voor een functionerend Nederlands en Europees cloudlandschap

Voor overheidsorganisaties die willen werken aan digitale autonomie is het relevant om te weten wat Nederlandse en Europese cloudproviders vandaag de dag concreet kunnen bieden. Onderstaande aandachtspunten geven inzicht in de beleidsmatige randvoorwaarden die in het publieke debat worden aangedragen voor een goed functionerend Europees cloudlandschap.

Enkele aandachtspunten:

- ▶ **Prioriteer wat cruciaal is.** Begin met wat echt soeverein moet zijn voor het functioneren van de samenleving. Zorg dat die onderdelen weer soeverein worden of blijven. Maak het dus niet te groot en probeer geen Europese hyperscaler na te streven of te wachten totdat er een dergelijke aanbieder is. Het wachten op perfectie is de vijand van het goede.
- ▶ **Hervorm de aanbestedingsregels.** Maak 'strategische autonomie' een hard juridisch criterium bij inkoop van vitale infrastructuur. Geef gunningsvoordeel voor de mate waarin soevereiniteit wordt geleverd voor minder kritische onderdelen. Zo stimuleer je de Europese techindustrie zonder de standaard onhaalbaar te maken.
- ▶ **Geef de ACM een coördinerende taak.** Laat onderzoeken waar concentratierisico's zitten in de technologieketen en maak een strategische actieagenda om die risico's te reduceren. Geef de ACM bevoegdheden om in te grijpen als de markt strategisch verstoord is.
- ▶ **Maak een 'Buy European' wet.** Waarbij naast Europese spelers ook het MKB een reële kans krijgt. Een dergelijke wet zet de toon voor aanbestedingsbeleid en stimuleert de ontwikkeling van een competitieve Europese tech-industrie.
- ▶ **Stel data-doorgifteplichtig strafbaar.** Als Nederlandse entiteiten en hun bestuurders zich niet aan onze wetten houden omdat ze aan een wet van een buitenlandse mogendheid willen voldoen, moet dat serieuze consequenties hebben. De CLOUD Act mag geen vrijbrief zijn om de AVG te omzeilen.
- ▶ **Stimuleer de drie openen.** Open architectuur (geen vendor lock-in), open standaarden (data exporteerbaar), open source (transparantie). Overheidsorganisaties die nu al werken met open standaarden, bouwen flexibiliteit in die hen later enorme kosten bespaart.
- ▶ **Contractuele aanscherping.** Zorg voor exit-strategieën (plan B) en change-of-control-clausules zodat je bij ongewenste overnames het contract kunt beëindigen. Dit beschermt de overheid ook wanneer een leverancier wordt overgenomen door een partij uit een risicoland.

In Nederland en Europa bestaan voor een groot deel van de clouddiensten die nu bij hyperscalers worden afgenomen al volwaardige alternatieven. Het Aanjaagteam NDS Cloud en sectorpartijen als DCC en DINL brengen deze partijen actief in beeld voor overheidsorganisaties.

7. Aanbevelingen voor overheidsorganisaties

7.1 Voor gemeenten, provincies en uitvoeringsorganisaties

Stap 1: Breng je afhankelijkheden in kaart

Een Business Impact Analyse (BIA) is voor de meeste overheidsorganisaties al verplicht, vanuit de BIO2, NIS2 of interne continuïteitsnormen. Daarin breng je in kaart hoe erg het is als een systeem 24 uur, 72 uur of een week niet beschikbaar is, en welke processen prioriteit hebben bij herstel. Als je die analyse al hebt gedaan: goed. Maar er is één dimensie die in een standaard-BIA vrijwel altijd ontbreekt.

Een klassieke BIA gaat uit van technische verstoringen: storingen, aanvallen, menselijke fouten. Wat we met de afhankelijkheden bedoelen, is de geopolitieke risicolaag: wat als de dienst niet uitvalt door een technisch probleem, maar omdat een buitenlandse leverancier onder politieke of juridische druk staat? Wat als een Amerikaans bedrijf verplicht wordt dienstverlening te staken, of als escalerende spanning tussen landen leidt tot beperkingen in de digitale toeleveranciersketen?

Loop je bestaande BIA daarom opnieuw langs met deze aanvullende vraag per kritiek systeem: is de continuïteit van dit systeem afhankelijk van een partij die buiten Nederlandse of Europese jurisdictie valt, en wat is de impact als die partij wegvalt, niet door een storing, maar door een politieke beslissing?

Aandachtspunt: een volledige afhankelijkheidsanalyse vraagt capaciteit die bij kleinere gemeenten en uitvoeringsorganisaties niet altijd beschikbaar is. Organisaties die dit niet zelfstandig kunnen uitvoeren, kunnen aansluiten bij gezamenlijke VNG-trajecten of de BIO2-risicoklassificatie als startpunt gebruiken. Het doel is bewuste keuzes, niet een perfect register op dag één.

Stap 2: Classificeer op basis van het drielagenmodel

Gebruik bijvoorbeeld het drielagenmodel uit hoofdstuk 4 als ordeningsprincipe of kies een andere ordenings principe

zoals dat van DICTU. Maak een portfolio-overzicht van alle systemen, ingedeeld op laag. Dit overzicht vormt de basis voor de cloudstrategie én voor aanbestedingseisen.

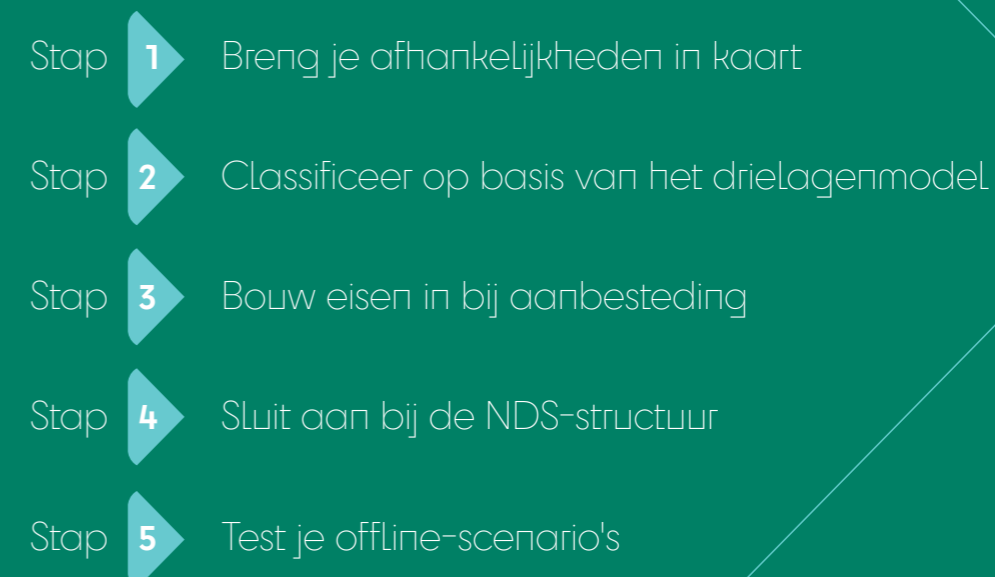
Stap 3: Bouw eisen in bij aanbesteding

Voorbeeldeisen bij aanbesteding:

- ▶ Data wordt opgeslagen op servers binnen de EER, contractueel vastgelegd
- ▶ Leverancier kan een actueel overzicht verstrekken van alle sub-processors
- ▶ Exit-strategie: data-export in open formaat bij beëindiging contract
- ▶ Notificatieplicht bij verzoeken van buitenlandse autoriteiten
- ▶ Change-of-control-clausule bij ongewenste overname
- ▶ NIS2-compliance aantoonbaar voor de gehele leveranciersketen

Voor gemeenten die verder willen gaan dan contractuele eisen, biedt Haven+ een concrete vertrekpunt. Haven+ is een referentiearchitectuur en set open-source componenten die is ontwikkeld binnen de Common Ground-beweging, met gemeente Utrecht als launching customer. Die inmiddels via Digilab (BZK) wordt uitgebouwd tot een landelijke standaard. Het bouwt voort op de Haven Kubernetes-standaard en voegt de services toe die je nodig hebt om applicaties volledig provider-onafhankelijk te draaien: monitoring, database-beheer, security en identity management. Nederlandse aanbieders zoals Previder zijn al Haven-compliant. Door Haven-conformiteit op te nemen als aanbestedingseis, verklein je vendor lock-in structureel. Niet als papieren clausule, maar als technische randvoorwaarde.

Aandachtspunt: strikte autonomie-eisen bij aanbesteding kunnen het aanbod van geschikte leveranciers verkleinen en de kosten verhogen. Een gedifferentieerde aanpak is verstandig: hanteer de zwaarste eisen voor laag-1-systemen (kritieke processen), en meer flexibele criteria voor laag-3-systemen (niet-kritieke bedrijfsvoering).





Stap 4: Sluit aan bij de NDS-structuur

Individueel sta je als gemeente of provincie niet sterk tegenover een techgigant met honderden miljarden omzet. Collectief wel. De NDS biedt een kader om gezamenlijk in te kopen en gezamenlijk soevereiniteitseisen te formuleren. Maak gebruik van de VNG-kanalen en de Thorbecketafel.

Aandachtspunt: collectieve trajecten via de NDS-structuur kennen langere doorlooptijden dan individuele beslissingen. Voor organisaties met een contract dat op korte termijn verloopt, is het praktischer om de NDS-standaarden als richtlijn mee te nemen in de eigen aanbesteding, zonder te wachten op volledige collectieve besluitvorming.

Stap 5: Test je offline-scenario's

Plan minimaal tweemaal per jaar een oefening waarbij kritieke systemen gesimuleerd worden uitgeschakeld. Hoe lang functioneert de organisatie zonder het primaire systeem? Oefening is de enige manier om papieren continuïteitsplannen te toetsen aan de werkelijkheid.

7.2 Voor softwareleveranciers van de overheid

Softwareleveranciers die toeleveren aan de overheid, worden via inkoopbeleid steeds harder afgerekend op soevereiniteitseisen. Wie nu niet investeert in een Nederlands of Europees hostingmodel, verliest straks de aanbesteding. De NDS maakt van soevereiniteit een selectie criterium, dat is een strategische kans voor leveranciers die het serieus nemen.

Concrete aanbevelingen:

- ▶ investeer in transparantie over je eigen sub-processors en hostingketen,
- ▶ documenteer de risico's die je daarin ziet en hoe je die mitigeert,
- ▶ positioneer digitale autonomie als onderdeel van je propositie,
- ▶ en zorg dat je data kunt exporteren in open standaarden.

8. Conclusie

Dit whitepaper begon met de paradox die de overheid zichzelf heeft gecreëerd: harder dan wie ook roepen dat digitale autonomie noodzakelijk is en tegelijk de organisatie zijn die er het minst klaar voor is. De cases van de Belastingdienst en de SVB zijn geen incidenten. Het zijn symptomen van een structureel patroon: strategische afhankelijkheden die nooit bewust zijn gekozen, maar organisch zijn gegroeid.

Dat hoeft geen probleem te zijn, mits je weet wat de risico's zijn en bewust hebt gekozen. De drie risicocategorieën uit dit whitepaper - privacy, continuïteit en systeemrisico - vragen elk om een andere afweging. Het drielagenmodel laat zien dat je blootstelling geen vast gegeven is, maar het resultaat van je eigen inrichtings- en inkoopkeuzes.

De NDS biedt de politieke en bestuurlijke rugdekking om nu te beginnen. De VNG en andere koepels werken aan gezamenlijke inkoopstandaarden. De bouwstenen liggen er. Drie dingen die je morgen al kunt doen:

- ▶ Loop je huidige dienstenlandschap langs met het drielagenmodel en bepaal per systeem waar het thuishoort.
- ▶ Stel bij de eerstvolgende contractverlenging de vraag of je exit-clausules, dataportabiliteit en notificatieplicht hebt vastgelegd.
- ▶ Zoek contact met de VNG of collega-organisaties om gezamenlijk soevereiniteitseisen te formuleren. Collectief sta je sterker.

De overheid hoeft niet in paniek te raken en hoeft niet alles morgen om te gooien. Maar bewust niets doen is ook een keuze, en dan wel eentje die je over vijf jaar moet verantwoorden: aan de Tweede Kamer, aan gemeenteraden, aan ministers, en aan de burgers die ervan uitgaan dat de overheid hun data beschermt en haar processen niet laat falen.

De organisaties die nu beginnen met een bewuste cloudstrategie, investeren niet in technologie maar in de toekomstbestendigheid van de democratische rechtsstaat.





Gebruikte bronnen

Alle bronnen zijn terug te vinden op de website van Intermax.
Bekijk de pagina door de QR-code te scannen.



ontdek.intermax.nl/bronvermeldingen-whitepaper-overheid

intermax 



ISAE 3402 TYPE II &
SOC2 ASSURANCE

Contact

Intermax

Schouwburgplein 30 – 34

3012 CL Rotterdam

+31(0) 10 – 710 4444

info@intermax.nl

2026 © Intermax Cloudsourcing B.V.

Over Intermax

Bij Intermax geloven we dat technologie pas waarde krijgt als ze bijdraagt aan iets groters. Aan overheidsdiensten die betrouwbaar functioneren. Aan infrastructuren die de samenleving dragen, en waarop iedereen blind moet kunnen vertrouwen, juist als het spannend wordt.

Intermax is één van de eerste Nederlandse IT-bedrijven die een eigen, soevereine cloud voor vitale organisaties bouwden, verdeeld over meerdere datacenters op Nederlandse bodem. Ook is onze Group CEO, Ludo Baauw, initiatief nemer van de 'Open Cloud Alliantie'.

Wij nemen actief deel aan het publieke debat over digitale autonomie: in de media, in de politiek en in de boardrooms van onze klanten. Onze experts waren te gast in de Tweede Kamer en delen regelmatig hun visie op LinkedIn en in vakbladen.

Kortom: waar IT nooit mag uitvallen, staan wij **altijd aan**.