

De gids naar een Soevereine Private Cloud aanbesteding



Introductie

Dit document is opgebouwd van context naar praktijk. Bent u al bekend met de urgentie van cloudsoevereiniteit? Sla dan hoofdstuk 1 en 2 over en begin bij hoofdstuk 3. Zoekt u direct bruikbare aanbestedingsvragen, ga dan naar de checklist in hoofdstuk 7. De hoofdstukken zijn zelfstandig leesbaar.

Inhoudsopgave

1. Waarom soevereiniteit nu urgenter is dan ooit	04
2. Wat is een soevereine cloud eigenlijk?	06
3. De 5 dimensies waarop u moet toetsen	08
4. Van criteria naar aanbesteding: zo pakt u het aan	14
5. Intern draagvlak organiseren	16
6. Veelgemaakte fouten bij soeverein aanbesteden	21
7. Checklist: 28 vragen voor uw aanbesteding	22
8. Hoe scoort Interconnect op de DICTU-criteria?	26

1. Waarom soevereiniteit nu urgenter is dan ooit

Tot voor kort leek het een hypothetisch risico. De meeste overheidsorganisaties wisten dat ze afhankelijk waren van Amerikaanse clouddaanbieders, maar de consequenties voelden abstract.

Dat veranderde begin 2025, toen Microsoft sancties uitvoerde namens de regering Trump tegen een hoofdaanklager van het Internationaal Strafhof (ICC). Een technologiebedrijf voerde een politiek besluit uit dat directe gevolgen had voor een internationale rechtsinstantie. Wat voorheen als een theoretisch scenario werd beschouwd, was realiteit geworden.

De wake-up call

“De rol van Microsoft bij Amerikaanse sancties tegen het ICC was een ernstige wake-up call. Voorheen als hypothetisch beschouwde risico’s zijn daarmee tastbaar en urgent geworden.” — DICTU Toetsingsinstrument Soevereiniteit Clouddiensten, januari 2026

De afhankelijkheid is ondertussen structureel. Meer dan 70% van de wereldwijde cloudmarkt is volgens een ACM-marktstudie in handen van drie Amerikaanse aanbieders: Microsoft, Google en Amazon. Voor overheidsorganisaties die gebruikmaken van deze platforms betekent dit dat cruciale data en processen vallen onder de jurisdictie van een land met andere belangen en wetgeving dan de EU.

De CLOUD Act: het juridische probleem

De Amerikaanse CLOUD Act (Clarifying Lawful Overseas Use of Data Act, 2018) geeft Amerikaanse opsporingsdiensten het recht om data op te eisen bij Amerikaanse technologiebedrijven, ongeacht waar die data fysiek is opgeslagen. Dat betekent: zelfs als uw data in een datacenter in Amsterdam staat, kunnen Amerikaanse autoriteiten die data opvragen bij de aanbieder zonder dat u daarvan op de hoogte hoeft te worden gesteld.

Dit botst fundamenteel met de AVG (Algemene Verordening Gegevensbescherming), die strikte eisen stelt aan de doorgifte van persoonsgegevens buiten de EU. Een Europese organisatie die gebruikmaakt van een Amerikaanse clouddaanbieder bevindt zich daarmee in een juridisch spagaat: de aanbieder kan verplicht worden te voldoen aan een Amerikaans verzoek, terwijl datzelfde verzoek een AVG-schending kan opleveren voor uw organisatie.

Kernpunt: Versleuteling biedt alleen bescherming als u zelf de encryptiesleutels beheert. Als de clouddaanbieder de sleutels beheert, kan hij verplicht worden deze over te dragen aan autoriteiten. Dit maakt sleutelbeheer een cruciaal onderdeel van elke soevereine cloudoplossing.

De Europese en Nederlandse beleidsreactie

De urgentie wordt inmiddels breed erkend. De Nederlandse Digitaliseringsstrategie (2025) benoemt digitale soevereiniteit als een van de zes kabinetsambities. De initiatiefnota ‘Wolken aan de Horizon’ roept op tot het terugdringen van afhankelijkheden van grote buitenlandse aanbieders.

Op Europees niveau werkt de Europese Commissie aan een Cloud Sovereignty Framework en een Tech Sovereignty Package, waarbij Nederland nadrukkelijk pleit voor een gemeenschappelijke gelaagde

definitie van ‘sovereine cloud’ om sovereigntywashing te voorkomen.

Dat laatste woord is veelzeggend. Veel clouddaanbieders, inclusief de grote hyperscalers, bieden inmiddels producten aan die zij ‘soverein’ noemen. Maar wat betekent dat precies? En wanneer is een claim over soevereiniteit meer dan een marketinglabel? Dat is precies de vraag die u moet kunnen beantwoorden.

2. Wat is een soevereine cloud eigenlijk?

Het begrip 'soevereine cloud' wordt breed gebruikt, maar zelden precies gedefinieerd. Dat is een probleem. U kunt alleen toetsen wat u kunt definiëren. De Nederlandse Rijksoverheid heeft daarvoor een werkdefinitie vastgesteld:

Rijksdefinitie soevereine cloud

"Soevereine Cloud moet worden beschouwd als een verzameling clouddiensten binnen een rechtsgebied die voldoet aan de eisen voor datalokalisatie en operationele autonomie. De soevereine Cloud moet ervoor zorgen dat de data, activiteiten, infrastructuurcomponenten en technologie niet kunnen worden beïnvloed door andere rechtsgebieden en beschermd moeten worden tegen directe invloed of toegang door overheden uit derde landen."

— Rijksdefinitie, DICTU 2026

Cruciaal in deze definitie is dat soevereiniteit niet gaat over de locatie van data alleen. Het gaat over controle en juridische bescherming over de volledige keten: wie is de eigenaar van het bedrijf dat de dienst levert, onder welk recht valt dat bedrijf, wie heeft er technische toegang tot uw data, en wie beheert de infrastructuur?

Soevereiniteit is geen binaire keuze

Zowel de Nederlandse 'Non-paper' aan de Europese Commissie (april 2026) als het EC Cloud Sovereignty Framework benadrukken dat soevereiniteit geen aan/uit-schakelaar is. Er zijn gradaties, van 'mid-autonoom' tot 'volledig soverein.' Dit heeft directe gevolgen voor hoe u aanbesteedt: u kunt een minimumdrempel instellen en leveranciers vervolgens op score rangschikken.

De valkuil: sovereigntywashing

Een leverancier die zijn Europese datacenter 'soverein' noemt, terwijl het moederbedrijf in de VS is gevestigd en de beheerders buiten Europa werken, levert geen soevereine dienst. Toch is deze claim gangbaar in de markt. Het DICTU-toetsingsinstrument en het EC-framework zijn er juist op ontworpen, zodat u dit soort claims kunt ontmaskeren met objectieve, herhaalbare criteria.

Praktijkvoorbeeld

Een Europese dochteronderneming van een Amerikaanse hyperscaler biedt een 'EU Sovereign Cloud' aan. Data staat in Europa. Maar: het moederbedrijf is Amerikaans, de CLOUD Act is van toepassing, de control plane wordt deels beheerd vanuit de VS en beheerders met privileged access zijn deels niet-Europees.

Op het DICTU-toetsingsinstrument scoort deze aanbieder hooguit een niveau 2 op juridische vestiging en een niveau 1 op toepasselijk recht. Dat is geen soevereine cloud.



3. De 5 dimensies waarop u moet toetsen

DICTU heeft een toetsingsinstrument ontwikkeld dat clouddiensten beoordeelt op vijf samenhangende dimensies. Elke dimensie heeft een hoofdvraag, concrete criteria en vijf soevereiniteitsniveaus (1 = geen soevereiniteit, 5 = volledig soeverein).

Hieronder vindt u per dimensie de essentie, de meest voorkomende risico's en de vragen die u direct kunt opnemen in uw aanbestedingsdocument.

3.1 Juridisch

Hoofdvraag: Aan welk juridisch en politiek systeem is de aanbieder uiteindelijk verantwoording schuldig?

Dit is de harde randvoorwaarde. Het maakt niet uit hoe goed de techniek is als het moederbedrijf uiteindelijk moet gehoorzamen aan niet-Europese wetgeving. De juridische dimensie kijkt naar drie criteria: de vestiging van het uiteindelijke moederbedrijf, het zeggenschap en eigenaarschap (formeel en feitelijk), en de bescherming tegen extraterritoriale wetgeving zoals de CLOUD Act.

Een lokale vestiging of een Europese dochteronderneming is onvoldoende als het zeggenschap feitelijk bij een niet-Europese entiteit ligt. Ook een minderheidsbelang met blokkerende rechten telt als niet-Europese invloed.

Vragen voor uw aanbesteding

1. Is de uiteindelijke moedermaatschappij juridisch gevestigd en heeft zij haar hoofdkantoor binnen de EU, EER of EFTA?
2. Is de aanbieder volledig vrij van directe of indirecte controle door niet-Europese entiteiten, zowel formeel (stemrechten) als feitelijk (invloed via belangen of bestuursmechanismen)?
3. Is de aanbieder juridisch en structureel beschermd tegen de extraterritoriale werking van niet-Europese wetgeving, zoals de Amerikaanse CLOUD Act of FISA 702?
4. Heeft de aanbieder ooit te maken gehad met een dataverzoek vanuit een niet-EU-overheid? Zo ja, hoe is daarmee omgegaan?
5. Onder welk recht valt het contract, en bij welke rechtbank worden geschillen beslecht?

3.2 Data & AI

Hoofdvraag: In welke mate zijn gegevens aantoonbaar beschermd, in zowel juridische als technische zin?

Data-soevereiniteit gaat verder dan ‘de data staat in Europa.’ Het gaat over wie technisch toegang heeft, wie de encryptiesleutels beheert, en of de aanbieder contractueel verplicht is om niet-Europese dataverzoeken te weigeren en u daarover te informeren. Met de opkomst van AI-diensten speelt ook de vraag waar en hoe AI-modellen worden getraind en welke data daarvoor wordt gebruikt.

Het hoogste niveau van technische bescherming is confidential computing, gecombineerd met klantbeheerde sleutels (HYOK: Hold Your Own Key). Daarmee is data cryptografisch geïsoleerd, ook tijdens verwerking, en heeft de aanbieder op geen enkel moment toegang tot ongecodeerde data.

Vragen voor uw aanbesteding

1. Worden alle klantdata, inclusief back-ups, metadata en logs, uitsluitend opgeslagen en verwerkt binnen het Europese grondgebied (EU, EER of EFTA)?
2. Zijn er aantoonbare technische maatregelen die ervoor zorgen dat ongecodeerde klantdata voor niemand toegankelijk is, inclusief de aanbieder zelf?
3. Wie beheert de encryptiesleutels, en biedt de aanbieder de mogelijkheid tot klantbeheerde sleutels (BYOK, CMK of HYOK)?
4. Is de aanbieder contractueel verplicht om niet-Europese dataverzoeken te melden en juridisch aan te vechten?
5. Worden AI-modellen of -diensten getraind op klantdata? Zo ja: waar, door wie en onder welke juridische voorwaarden?
6. Hoe wordt de naleving van dataresidency-vereisten aantoonbaar gemaakt, en wordt dit periodiek geaudit?

3.3 Technologie

Hoofdvraag: Biedt de technologie autonomie, inzichtelijkheid, weerbaarheid en portabiliteit voor de klant?

Technologische afhankelijkheid is de meest onderschatte dimensie van vendor lock-in. Proprietary technologie maakt overstappen technisch complex en financieel kostbaar. Open standaarden en opensource software zijn hierbij de sleutelbegrippen: ze maken data en workloads overdraagbaar en voorkomen dat u vastzit aan één leverancier.

Het EC-framework en de Nederlandse Non-paper benadrukken beide open source als een van de centrale enablers van digitale soevereiniteit. Dat betekent concreet: u kunt voorkeur geven aan leveranciers die kerncomponenten op opensource software bouwen én actief bijdragen aan de opensource gemeenschap.

Vragen voor uw aanbesteding

1. Is de dienst gebouwd op open standaarden, zodat overstap naar een andere aanbieder technisch en financieel haalbaar is?
2. Welke kerncomponenten zijn open source? Welke zijn proprietary?
3. Is de broncode van alle kerntechnologie beschikbaar voor inspectie, publiek of via een erkende derde partij (escrow)?
4. Kan een derde partij de dienst overnemen en zelfstandig exploiteren bij uitval of contractbeëindiging, op basis van de beschikbare documentatie?
5. Hoe worden data en workloads beschikbaar gesteld bij contractbeëindiging, en binnen welke termijn?
6. Draagt de aanbieder actief bij aan open source projecten die aan de dienst ten grondslag liggen?

3.4 Operationeel

Hoofdvraag: wie heeft de controle over de operationele omgeving van de dienst?

Het is onvoldoende dat data in Europa staat als de beheertaken worden uitgevoerd door personeel buiten Europa of via systemen die buiten de Europese jurisdictie vallen. De operationele dimensie kijkt naar drie zaken: de locatie van de fysieke infrastructuur en de control plane, de nationaliteit en verblijfplaats van beheerders met privileged access, en de weerbaarheid van de supply chain.

Privileged access is hierbij het kritieke begrip: medewerkers met toegang die het mogelijk maakt om systeemconfiguraties te wijzigen, auditlogs in te zien of data van andere gebruikers te benaderen. Zij moeten aantoonbaar burger en ingezetene zijn van de EU, in dienst zijn van een Europese entiteit, en hun werkzaamheden fysiek vanuit Europa uitvoeren.

Vragen voor uw aanbesteding

1. Bevinden de volledige technische infrastructuur (datacenters, netwerk) en de control plane zich fysiek binnen de EU, EER of EFTA?
2. Worden alle beheerwerkzaamheden met privileged access uitgevoerd door personeel dat burger en ingezetene is van de EU/EER/EFTA, in dienst is bij een Europese entiteit en fysiek vanuit Europa werkt?
3. Hoe wordt naleving van het Europees-personeel-vereiste aangetoond en geaudit?
4. Welke maatregelen zijn getroffen om continuïteit te waarborgen bij geopolitieke sancties of verstoringen in de toeleveringsketen?
5. Heeft de aanbieder een gedocumenteerde en geauditeerde strategie om afhankelijkheid van niet-Europese hardware en software te minimaliseren?
6. Wat zijn de garanties voor servicecontinuïteit bij een faillissement of overname van de aanbieder?

3.5 Mens

Hoofdvraag: In hoeverre is er zichtbaarheid en controle over wie toegang heeft tot systemen en data, en beschikt het personeel over de kennis en vaardigheden voor soevereine dienstverlening?

De menselijke dimensie wordt in bestaande raamwerken (zoals het Gartner-model) vaak niet apart benoemd, maar DICTU voegt deze bewust toe. Kennis over cloudjuridica, digitale autonomie en geopolitieke afhankelijkheden is schaars. Een aanbieder die zelf niet beschikt over interne EU-capaciteit om zijn eigen platform te bouwen, beheren en doorontwikkelen, is per definitie afhankelijk van partijen buiten zijn eigen jurisdictie.

Vragen voor uw aanbesteding

1. Is personeel met toegang tot kritieke systemen aantoonbaar gescreend, gecertificeerd en getraind?
2. Wordt screening periodiek herhaald en door een erkende, onafhankelijke Europese partij geaudit?
3. Beschikt de aanbieder over voldoende interne EU-capaciteit om soevereine cloud-diensten zelfstandig te bouwen, te beheren én door te ontwikkelen?
4. Is er lokale (Nederlandse) ondersteuningscapaciteit beschikbaar voor bouw en beheer?
5. Hoe borgt de aanbieder kennisbehoud bij vertrek van sleutelpersoneel?

4. Van criteria naar aanbesteding: zo pakt u het aan

De vijf dimensies en bijbehorende vragen geven u inhoudelijk houvast. Maar hoe vertaalt u dit naar een concreet aanbestedingsdocument? Hieronder vindt u een aanpak die aansluit bij gangbare aanbestedingspraktijk.

Gebruik de SEAL-niveaus als drempels

Het EC Cloud Sovereignty Framework werkt met Sovereignty Effectiveness Assurance Levels (SEALs), van SEAL-0 (geen soevereiniteit) tot SEAL-4 (volledige digitale soevereiniteit). U kunt een minimumdrempel instellen als knock-outcriterium: aanbieders die niet minimaal SEAL-2 halen, worden uitgesloten van verdere beoordeling. Boven die drempel bepaalt de Sovereignty Score de rangschikking.

SEAL-niveaus (EC Cloud Sovereignty Framework)

SEAL-0: Geen soevereiniteit SEAL-1: Beperkte soevereiniteitsmaatregelen SEAL-2: Substantiële soevereiniteitsmaatregelen SEAL-3: Hoge mate van soevereiniteit SEAL-4: Volledige digitale soevereiniteit. Het DICTU-toetsingsinstrument en het EC-framework hanteren sterk vergelijkbare dimensies en niveaus, waardoor u beiden kunt combineren.

Zet juridische vestiging als pass/fail

Het EuroStack-initiatief hanteert een strikt pass/fail-principe voor jurisdictie en eigendom. Dat is een verdedigbare keuze voor overheidsopdrachten met hoge gevoeligheidsclassificatie: een aanbieder waarvan het moederbedrijf buiten de EU is gevestigd, komt simpelweg niet in aanmerking voor het hoogste soevereiniteitsniveau. U kunt dit als minimumeis formuleren in uw Programma van Eisen.

Stel wegingsfactoren per dimensie

Niet elke dimensie weegt even zwaar voor elke opdracht. Pas deze weging aan op uw specifieke context: voor een opdracht met staatsgeheimen weegt juridisch zwaarder; voor een uitvoeringsdienst met veel burger-interactie weegt data & AI zwaarder.

Vereis aantoonbaarheid, geen zelfverklaring

Een cruciaal verschil tussen een sterke en een zwakke aanbesteding is de mate van aantoonbaarheid. Vraag niet alleen of een aanbieder aan een criterium voldoet, maar hoe hij dat aantoon (indien mogelijk). Certificering door een erkende Europese partij, periodieke audits en contractuele garanties zijn sterker dan zelfverklaringen. Bouw dit expliciet in uw beoordelingscriteria.

De GIBIT als juridisch fundament

Gemeenten die de Gemeentelijke Inkoop bij IT Toolbox (GIBIT 2025) hanteren, beschikken al over een contractuele basis voor een deel van de soevereiniteitsvereisten in dit whitepaper. Waar de GIBIT minimumvereisten stelt voor data-eigendom en exitrechten, vormen de soevereiniteitsdimensies in dit whitepaper een aanvullende laag op het gebied van jurisdictie, sleutelbeheer, Europees eigenaarschap en personele controle. Voor gemeenten die de GIBIT al hanteren, is soeverein aanbesteden dus geen breuk met bestaande praktijk, maar een bewuste verdieping ervan.*

*Ter referentie: relevante GIBIT 2025-artikelen voor nadere juridische duiding

Artikel 22 (Toegang tot Data en autorisaties): verplicht leveranciers om de opdrachtgever, gedurende de looptijd en bij beëindiging, toegang te geven tot data in een algemeen leesbaar elektronisch formaat. Het eigendom van de data berust op grond van artikel 21 bij de opdrachtgever. Sluit aan op dataportabiliteit en data residency (dimensies 2 en 3).

Artikel 25 (Software Bill of Materials): verplicht transparantie over alle softwarecomponenten, inclusief open source versus proprietary en de fysieke locatie van dataverwerking. Sluit aan op softwaretransparantie (dimensie 3).

Artikel 29 (Exit-plan): verplicht leveranciers actief mee te werken aan een ordentelijke overdracht bij contractbeëindiging. Sluit aan op operationele omkeerbaarheid (dimensie 3).

Artikel 27 (Opschorting, opzegging en ontbinding): bevat de gronden waarop de opdrachtgever de overeenkomst kan opschorten, opzeggen of ontbinden. Voor zover ontbinding mogelijk is wanneer voortzetting in strijd zou komen met wet- en regelgeving, kan dit relevant zijn voor het CLOUD Act-scenario (dimensie 1).

Raadpleeg voor de juridische toepasselijkheid van deze artikelen op uw specifieke aanbestedingssituatie uw juridisch adviseur of PIANOo (expertisecentrum aanbesteden, pianoo.nl).

5. Intern draagvlak organiseren

Soeverein aanbesteden begint zelden bij de inkoopafdeling. Het begint bij een bestuurder die vraagt waarom de vertrouwde hyperscaler plotseling niet meer voldoet, een IT-manager die zijn bestaande architectuur niet wil openbreken, of een budgethouder die ziet dat soevereine alternatieven duurder lijken. Bent u degene die dat gesprek moet voeren? Hieronder vindt u per stakeholder de argumenten die werken.



De bestuurder

Dit gesprek gaat niet over techniek, het gaat over risico en reputatie. De bestuurder wil weten wat er misgaat als u niets doet. Het antwoord is concreet: als uw clouddaanbieder onder de CLOUD Act valt, heeft u geen garantie dat gevoelige data van burgers of medewerkers buiten bereik blijft van buitenlandse autoriteiten. Dat is niet hypothetisch meer sinds het ICC-incident met Microsoft. Voeg daaraan toe dat de Rijks-overheid digitale soevereiniteit als kabinetsprioriteit heeft benoemd en dat de Autoriteit Persoonsgegevens hier actief op toeziet. Een bestuurder die dit negeert, neemt een bestuurlijk risico, geen technisch risico.

Kernargument: dit is een governance- en aansprakelijkheidsvraagstuk, geen IT-vraagstuk.

De CIO of IT-manager

Hier ligt de weerstand vaak bij continuïteit en vertrouwdheid. 'We draaien al jaren op Azure, onze mensen kennen het systeem, migreren is complex en kostbaar.' Dat is een legitiem argument, maar het veronderstelt dat de huidige situatie stabiel blijft. Wijs op het operationele risico van een enkele leverancier die eenzijdig voorwaarden kan wijzigen, diensten kan beëindigen of onderhevig kan zijn aan sancties. Multi-cloud en open standaarden zijn niet alleen een soevereiniteitskeuze, ze zijn ook een operationele risicobeheerstrategie. En: soeverein aanbesteden sluit niet uit dat bestaande systemen blijven draaien. Het gaat om nieuwe aanbestedingen, om bewuste keuzes bij contractverlenging.

Kernargument: soevereiniteit en operationele continuïteit zijn geen tegenstelling, ze versterken elkaar.

Budgethouder

De initiële kostenvergelijking valt vaak nadelig uit voor soevereine alternatieven. Maar die vergelijking is onvolledig. Wat zijn de overstapkosten als u over vijf jaar wil wisselen van aanbieder en uw data en workloads volledig proprietary zijn? Wat is de waarde van onderhandelingspositie als u niet afhankelijk bent van één leverancier? En wat zijn de potentiële boetes en reputatieschade als een datalek of ongeautoriseerde toegang via de CLOUD Act leidt tot een AVG-overtreding? Soeverein aanbesteden is een investering in keuzevrijheid en risicobeheersing, geen premie voor een ideologische voorkeur.

Kernargument: de werkelijke total cost of ownership inclusief lock-in, exitkosten en compliance-risico ligt bij soevereine oplossingen vaak lager op de middellange termijn.

Het VNG Model Inkoop- en Aanbestedingsbeleid 2025 benoemt rechtmatigheid, doelmatigheid en maatschappelijke verantwoording als centrale inkoopprincipes.

Soeverein aanbesteden sluit op alle drie aan:

- Het is rechtmatig omdat het voldoet aan de AVG en de GIBIT-vereisten;
- Het is doelmatig omdat het langetermijnafhankelijkheden en exitkosten beperkt;
- Het is maatschappelijk verantwoord omdat het publieke data onder publiek toezicht houdt.*

De juridische afdeling of CISO

Dit is doorgaans uw natuurlijke bondgenoot. Zij kennen de AVG-spanning met de CLOUD Act al, maar hebben vaak geen concreet toetsingsinstrument om leveranciers op te beoordelen. Geef hen het DICTU-toetsingsinstrument als werkdocument. De vijf dimensies en de bijbehorende vragen in dit whitepaper geven hen precies wat ze nodig hebben om een juridisch onderbouwd advies te schrijven aan de directie.

Kernargument: geef ze het instrument, niet alleen het probleem.

De vragen in hoofdstuk 7 zijn zo geformuleerd dat u ze ook intern kunt gebruiken om het gesprek te structureren, niet alleen in uw bestek.

*Extra toelichting

De koppeling aan soevereiniteitsvereisten is een inhoudelijke interpretatie; raadpleeg voor juridische toepasselijkheid uw adviseur of PIANOo.





6. Veelgemaakte fouten bij soeverein aanbesteden

Datalokalisatie verwarren met soevereiniteit

- 1 Data die in een Europees datacenter staat, is niet automatisch soeverein. Zolang het moederbedrijf van de aanbieder Amerikaans is, valt die data onder de CLOUD Act. Datalokalisatie is een noodzakelijke maar onvoldoende voorwaarde. Wees u bewust van sovereigntywashing.

Blindvaren op certificeringen

- 2 ISO 27001, SOC 2 en vergelijkbare certificeringen zeggen iets over informatiebeveiliging, maar niets over soevereiniteit. EUCS (European Cybersecurity Certification Scheme) is relevanter, maar bevindt zich momenteel in een politieke impasse; het striktste niveau (High+) met echte soevereiniteitsvereisten is voorlopig geschrapt. Laat u niet afschepen met certificaten die de kern van de vraag niet raken.

Eigendomsstructuur niet doorgronden

- 3 Een Europese naam of Europees hoofdkantoor zegt niets over de uiteindelijke zeggenschap. Controleer altijd de volledige eigendomsstructuur, inclusief indirecte aandeelhouders en eventuele blokkerende minderheidsbelangen van niet-Europese partijen.

Geen exitstrategie meenemen

- 4 Soevereiniteit betekent ook de vrijheid om van aanbieder te wisselen. Als uw data en workloads niet portabel zijn, bent u in feite gevangene van uw leverancier, ook al voldoet die op alle andere criteria. Neem exitprocedure, dataportabiliteit en overdrachtstermijnen expliciet op in uw contract.

Soevereiniteit als eenmalig vinkje behandelen

- 5 De geopolitieke situatie verandert. Een aanbieder die vandaag soeverein is, kan dat morgen niet meer zijn door een overname, een beleidswijziging of een nieuwe wet. Bouw periodieke hertoetsing en audit-verplichtingen in uw contracten.

7. Checklist: 28 vragen voor uw aanbesteding

Onderstaande vragen zijn gebaseerd op het DICTU Toetsingsinstrument Soevereiniteit Clouddiensten (januari 2026) en het EC Cloud Sovereignty Framework. U kunt deze vragen direct opnemen als uitvraag in uw aanbestedingsdocument of als toetsingskader bij de beoordeling van inschrijvingen.

Dimensie / Criterium	Aanbestedingsvraag
1.0 Juridisch	
1.1 Vestiging moederbedrijf	Is het uiteindelijke moederbedrijf juridisch gevestigd en hoofdkantoor gevestigd binnen de EU, EER of EFTA?
1.2 Zeggenschap	Is de aanbieder vrij van directe of indirecte controle door niet-Europese entiteiten (stemrechten en feitelijke invloed)?
1.3 Toepasselijk recht	Is de aanbieder structureel beschermd tegen extraterritoriale wetgeving zoals de CLOUD Act of FISA 702?
1.4 Contractueel recht	Onder welk recht valt het contract, en bij welke rechtbank worden geschillen beslecht?
1.5 Eerdere dataverzoeken	Heeft de aanbieder ooit een dataverzoek van een niet-EU-overheid ontvangen? Zo ja, wat was de respons?
1.6 Eigendomsstructuur	Kan de aanbieder de volledige eigendomsketen aantonen, inclusief indirecte aandeelhouders?

2. Data & AI	
2.1 Data residency	Worden alle klantdata, back-ups, meta-data en logs uitsluitend opgeslagen en verwerkt binnen de EU/EER/EFTA?
2.2 Sleutelbeheer	Wie beheert de encryptiesleutels? Biedt de aanbieder BYOK, CMK of HYOK?
2.3 Technische isolatie	Is confidential computing beschikbaar zodat data ook tijdens verwerking cryptografisch is geïsoleerd?
2.4 Juridische melding	Is de aanbieder contractueel verplicht niet-Europese dataverzoeken te melden en juridisch aan te vechten?
2.5 AI-training	Worden AI-modellen getraind op klantdata? Zo ja: waar, door wie en onder welke juridische voorwaarden?
2.6 Audit data residency	Hoe wordt naleving van dataresidency-vereisten aantoonbaar gemaakt en periodiek geaudit?

3. Technologie	
3.1 Open standaarden	Zijn alle kerncomponenten gebouwd op open standaarden? Welke zijn proprietary?
3.2 Open source	Welke kerncomponenten zijn open source? Draagt de aanbieder actief bij aan open source projecten?
3.3 Broncode-transparantie	Is de broncode beschikbaar voor inspectie, publiek of via erkende derde partij (escrow)?
3.4 Operationele omkeerbaarheid	Kan een derde partij de dienst overnemen en exploiteren op basis van bestaande documentatie?
3.5 Dataportabiliteit	Hoe worden data en workloads beschikbaar gesteld bij contractbeëindiging en binnen welke termijn?
4. Operationeel	
4.1 Infrastructuur locatie	Bevinden datacenters, netwerk en control plane zich volledig binnen de EU/EER/EFTA?
4.2 Control plane beheer	Wordt de control plane volledig beheerd door Europese entiteiten, zonder externe invloed vanuit buiten de EU?
4.3 Europees personeel	Zijn alle beheerders met privileged access EU-burger, EU-ingezetene en fysiek werkzaam in Europa?
4.4 Audit personeel	Wordt naleving van de personeelsvereiste periodiek geaudit door een erkende Europese partij?

4.5 Supply chain strategie	Heeft de aanbieder een gedocumenteerde strategie om afhankelijkheid van niet-Europese hardware/software te beperken?
4.6 Continuïteitsgarantie	Wat zijn de garanties voor servicecontinuïteit bij geopolitieke sancties, overname of faillissement?
5. Mens	
5.1 Screening	Is personeel met toegang tot kritieke systemen aantoonbaar gescreend, gecertificeerd en getraind?
5.2 Audit screening	Wordt screening periodiek geaudit door een erkende, onafhankelijke Europese partij?
5.3 EU-capaciteit	Beschikt de aanbieder over voldoende interne EU-capaciteit voor bouw, beheer en doorontwikkeling?
5.4 Lokale ondersteuning	Is er lokale (Nederlandse) capaciteit beschikbaar voor bouw en beheer?
5.5 Kennisborging	Hoe borgt de aanbieder kennisbehoud en continuïteit bij vertrek van sleutel-personeel?

8. Hoe scoort Interconnect op de DICTU-criteria?

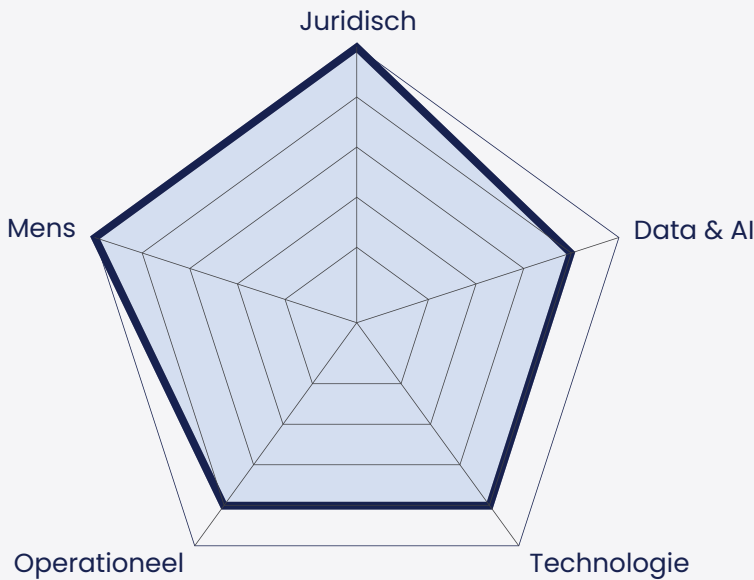
Interconnect is een Nederlandse Data & Cloud Center met 130 medewerkers, volledig in Nederlandse en dus Europese handen en operationeel vanuit Nederland. Als leverancier aan MKB+ en overheidsorganisaties kiezen wij bewust voor een positie als soevereine cloud- en datacenterpartner: geen doorverkoop van hyperscaler-diensten, maar een eigen multihypervisor cloudplatform gebouwd op Europese infrastructuur en open source technologie.

Aan de hand van het DICTU Toetsingsinstrument scoort Interconnect circa 76%, met ruimte voor verbetering op met name de technologiedimensie. Met de introductie van ons nieuwe, volledig op open source gebaseerde cloudplatform, gepland voor later dit jaar, loopt dit op naar circa 85%. We nodigen u uit dat samen met ons te toetsen, externe validatie volgt snel zodra dit beschikbaar komt.

Huidige score: 76%



Verwachte score na platformintroductie 2026: 85%



Wat betekent dit in de praktijk?

Interconnect scoort op de juridische dimensie het hoogste niveau: volledig EU-gevestigd met moederbedrijf en hoofdkantoor in Nederland, exclusief Nederlands eigenaarschap en geen blootstelling aan de CLOUD Act. Op technologie investeren wij actief in open source infrastructuur, wat dataportabiliteit en operationele omkeerbaarheid maximaliseert. De overgebleven 15-25% betreft voornamelijk onderdelen van de technologiestack waarvoor nog geen volledig Europese alternatieven beschikbaar zijn.

Contact

Wilt u weten hoe Interconnect scoort op een specifiek criterium dat relevant is voor uw aanbesteding, of wilt u doorpraten over hoe u soevereiniteitsvereisten het beste kunt formuleren in uw bestek?

Neem gerust contact met ons of lees eerst meer over hoe Interconnect digitale soevereiniteit in de praktijk brengt op interconnect.nl/datasoevereiniteit.



Bronnen en referenties

Autoriteit Consument & Markt (2023). Marktstudie Clouddiensten. Den Haag.

DICTU (januari 2026). Soevereiniteit clouddiensten: Toetsingsinstrument. Ministerie van Economische Zaken en Klimaat, Dienst ICT Uitvoering.

Europese Commissie (2025). Cloud Sovereignty Framework (EC-framework). Brussel.

EuroStack-initiatief (2025). EuroStack: A Proposal for European Digital Sovereignty. Ministerie van Economische Zaken en Klimaat (april 2026). Non-paper: An Integrated Approach for the EU Tech Sovereignty Package. Den Haag.

Rathenau Instituut (2024). Naar een nieuwe verhouding tot technologiebedrijven: Koers zetten richting digitale autonomie. Den Haag.

Rijksoverheid (2025). Initiatiefnota 'Wolken aan de horizon'. Kamerstuk, januari 2025.

Rijksoverheid (2025). Nederlandse Digitaliseringsstrategie 2025. Den Haag.

VNG (november 2025). VNG Model Inkoop- en Aanbestedingsbeleid 2025. Vereniging van Nederlandse Gemeenten, Den Haag.

VNG Realisatie (februari 2026). Gemeentelijke Inkoop bij IT Toolbox: GIBIT 2025 Artikelen. Vereniging van Nederlandse Gemeenten, Den Haag.

Interconnect Services B.V.
Interconnect.nl
solutions@interconnect.nl



