Dienst ICT Uitvoering
Ministerie van Economische Zaken en Klimaat

Soevereiniteit clouddiensten: Toetsingsinstrument

DICTU - januari 2026

Inhoud

1. Inleiding

1.1 Achtergrond en doel van het document

Publieke Cloud platformen bieden aanzienlijke voordelen op het gebied van schaalbaarheid, beveiliging en toegang tot geavanceerde diensten voor data-analyse en kunstmatige intelligentie. Deze mogelijkheden stellen DICTU, en daarmee het Rijk, in staat te innoveren en de nadruk te leggen op het leveren van maatschappelijke waarde.

Meer dan 70% van de wereldwijde Cloud markt is echter in handen van Amerikaanse aanbieders zoals Microsoft, Google en Amazon[1]; de zogenaamde *hyperscalers*. Daarmee groeit niet alleen de innovatiekracht, maar ook de afhankelijkheid van deze partijen. Dit brengt reële juridische, technologische en operationele risico's met zich mee, onder andere rond veiligheid, autonomie (zelfbeschikking en onafhankelijkheid) en onderhandelingspositie. De digitale soevereiniteit van het Rijk komt hierdoor onder druk te staan.

Tegelijkertijd ontwikkelt de markt nieuwe 'soevereine' Cloud varianten, vaak aangeboden door dezelfde hyperscalers. Dit roept fundamentele vragen op: wat betekent soevereiniteit voor DICTU? Wanneer voldoet een clouddienst aan die definitie? En in hoeverre kan een Amerikaanse aanbieder daadwerkelijk soevereine diensten leveren binnen Europa?
Het doel van dit document is als volgt:

1. Introductie van een toetsingsinstrument voor soevereine Cloud.
2. Inzicht bieden in het soevereiniteitsniveau van het aanbod van een aantal hyperscalers d.m.v. beoordelingen.
3. Een richtlijnen aanzet voor soevereiniteitscriteria vanuit het toetsingsinstrument en beoordelingen meegeven om te komen tot een toekomstbestendige soevereine overheidscloud.

DICTU heeft een inhoudelijke analyse gemaakt van de mate van soevereiniteit van geselecteerde hyperscalers, op basis van voorgestelde beoordelingscriteria, die inzetbaar zijn bij aanbestedings- of selectieprocedures. DICTU zal hiermee clouddienstverleners beoordelen op grond van objectieve, transparante en herhaalbare criteria voor digitale autonomie en soevereiniteit.

1.2 Strategische aanleiding

Het waarborgen van digitale soevereiniteit krijgt steeds meer aandacht en houvast in interne en publieke stukken van de overheid, zo is het benoemd als één van de zes prioriteiten in de Nederlandse Digitalisering Strategie (NDS). De afhankelijkheid van een klein aantal dominante

[1] Chart: The Big Three Stay Ahead in Ever-Growing Cloud Market | Statista

[1] https://www.rijksoverheid.nl/documenten/kamerstukken/2025/01/17/kamerbrief-initiatiefnota-wolken-aan-de-horizon

[1] https://www.rathenau.nl/nl/digitalisering/naar-een-nieuwe-verhouding-tot-technologiebedrijven/koers-zetten-richting-digitale-autonomie

buitenlandse clouddienstverleners beperkt de regie over data, technologie en continuïteit van de publieke dienstverlening. De initiatiefnota *"Wolken aan de horizon"*[2] en adviezen van onder meer het Rathenau Instituut[3] benadrukken dat deze afhankelijkheid risico's oplevert voor autonomie, veiligheid en de onderhandelingspositie.
In lijn met Europese initiatieven rond digitale autonomie (zoals EuroStack, EC-Framework) heeft DICTU nu een instrument in handen om clouddiensten systematisch te beoordelen op soevereiniteit. Daarmee ondersteunt DICTU het Rijk in het maken van bewuste, transparante en toekomstbestendige keuzes bij de inzet van cloudtechnologie.

[2] https://www.rijksoverheid.nl/documenten/kamerstukken/2025/01/17/kamerbrief-initiatiefnota-wolken-aan-de-horizon

[3] https://www.rathenau.nl/nl/digitalisering/naar-een-nieuwe-verhouding-tot-technologiebedrijven/koers-zetten-richting-digitale-autonomie

2. Soevereiniteit: Begrip en Uitgangspunten

2.1 Definitie van digitale soevereiniteit binnen cloudstrategieën

Digitale soevereiniteit binnen cloudstrategieën draait om de mate van controle en eigenaarschap (autonomie) over cloudinrichting en -diensten. Het is het vermogen van een organisatie of overheid om zelfstandig te beslissen en te handelen over essentiële digitale aspecten in economie, maatschappij en democratie. Soevereiniteit is daarmee een fundament voor publieke waarden, continuïteit en veiligheid.

Definitie vanuit het Rijk:
"*Digitale soevereiniteit is het vermogen om autonoom te kunnen beslissen en handelen over de essentiële digitale aspecten in economie, maatschappij en democratie*."

Daarnaast geldt voor het begrip 'soevereine Cloud' de volgende definitie, zoals vastgesteld door het Rijk:
"*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*."

2.2 Perspectieven en dimensies van cloudsoevereiniteit

Deze autonomie kan worden bekeken vanuit vier hoofdperspectieven:

1. **Juridisch:** De mate waarin wet- en regelgeving, databescherming en aansprakelijkheid binnen het eigen rechtsgebied geborgd zijn.
2. **Economisch:** Invloed op de lokale economie, technologische onafhankelijkheid en het stimuleren van Europese innovatie.
3. **Geopolitiek:** Vermindering van afhankelijkheid van andere landen en waarborging van nationale veiligheid.
4. **Organisatie:** Flexibiliteit, onafhankelijkheid en aansluiting op de eigen behoeften en processen.

Voor DICTU en het Rijk is vooral het organisatieperspectief leidend: het gaat om praktische autonomie, grip op processen en het kunnen waarborgen van publieke belangen in de digitale infrastructuur.

Vanuit het organisatieperspectief wordt digitale soevereiniteit verder uitgewerkt langs vijf samenhangende dimensies:

- **Juridisch:** Onder welke jurisdictie vallen data en diensten? Geldt uitsluitend Europese wetgeving, of is er ook sprake van Amerikaanse invloed (zoals de CLOUD Act)?
- **Data & AI:** Controle over data-encryptie, locatie en toegang. Voldoet de dienst aan privacywetgeving (GDPR, AVG)? Wie kan bij de data en waar wordt deze fysiek opgeslagen?
- **Operationeel:** In hoeverre heeft DICTU controle over operationele partijen? Kunnen derden de dienstverlening beïnvloeden of uitschakelen?

- **Technologisch:** Hoe inzichtelijk, aanpasbaar en portabel is de gebruikte technologie? Zijn open standaarden en interoperabiliteit geborgd?
- **Mens:** Wie heeft toegang tot systemen en data? Is er voldoende zichtbaarheid en controle over de mensen die aan de digitale infrastructuur werken?

2.3 Reflecties op digitale soevereiniteit

De term digitale soevereiniteit kent verschillende interpretaties en wordt steeds vaker gebruikt in beleidsstukken, media en wetenschappelijke publicaties. De hierboven geciteerde definities vormen het uitgangspunt voor het toetsingsinstrument van DICTU.

Voor het Rijk betekent dit:

- Eigenaarschap over eigen data, inclusief die van burgers en bedrijven.
- Volledige controle op dataverwerkende systemen en inzicht in wie toegang heeft tot data en hoe deze wordt gebruikt.
- Het vermogen om publieke waarden, continuïteit van dienstverlening en gegevensbescherming structureel te waarborgen.

Het realiseren van digitale soevereiniteit vraagt om een integrale benadering, waarbij juridische, technologische, operationele en menselijke factoren in samenhang worden beschouwd. Alleen zo kan DICTU een robuust en toekomstbestendig kader ontwikkelen voor het beoordelen en selecteren van clouddiensten.

3. Risico's

Naast de eerdergenoemde voordelen die Cloud met zich meebrengt, zijn er ook risico's die de digitale soevereiniteit onder druk zetten. De rol van Microsoft in sancties namens de regering-Trump tegenover een hoofdaanklager van het ICC, was een ernstige *wake-up call*[4]. Voorheen als hypothetisch beschouwde risico's zijn daarmee tastbaar en urgent geworden.
Deze risico's ontstaan enerzijds door de agressieve tactieken van clouddienstverleners om marktaandeel te veroveren en te behouden, en anderzijds door toenemende geopolitieke spanningen en veranderingen in internationale wet- en regelgeving.
Volgens de Autoriteit Consument & Markt (ACM)[5] is sprake van een toenemende consolidatie in de markt voor clouddiensten, gedreven door schaalvoordelen en netwerkeffecten en gaat gepaard met vendor lock-in, en gelimiteerde dataportabiliteit en cloudinteroperabiliteit. Hierdoor wordt het voor kleinere, ook Europese aanbieders steeds moeilijker om effectief te concurreren. Nederlandse overheidsorganisaties raken daardoor in toenemende mate afhankelijk van een beperkt aantal grote technologiebedrijven van buiten de EU. Deze afhankelijkheid kan leiden tot een ongelijke machtsbalans, met gevolgen voor zeggenschap, continuïteit en publieke waarden.

Figuur 1 De drie pilaren van Digitale Soevereiniteitsrisico's voor overheden volgens Gartner.

De drie aandachtsgebieden worden in de literatuur vaak ondergebracht in drie pilaren: data, operationeel en technologie (zie Fig. 1). Ter aanvulling voegen wij juridisch, AI (naast data) en mens toe als dimensies, zoals gedefinieerd in 3.2. In de volgende paragrafen worden de belangrijkste risico's beschreven langs vijf dimensies: juridische, data- en AI-, operationele, technologische en menselijke risico's.

[4] https://ibestuur.nl/artikel/rol-microsoft-bij-amerikaanse-sancties-icc-ernstige-wake-up-call/

[5] https://www.acm.nl/nl/publicaties/marktstudie-clouddiensten

3.1 Juridische risico's

Juridische risico's hebben betrekking op de mate waarin DICTU en haar opdrachtgevers zeggenschap behouden over data en digitale diensten binnen de Europese rechtsorde.

- Extraterritoriale wetgeving**:** Clouddienstverleners buiten de EU kunnen verplicht worden data te delen met hun nationale autoriteiten. De *U.S. CLOUD Act* blijft hierbij het bekendste voorbeeld. Volgens cybersecurityexperts (zoals prof. Bart Jacobs) bestaat het risico dat toekomstige beleidswijzigingen in de VS de toegang tot Europese data verder verruimen.
- Jurisdictieconflicten**:** Digitale diensten vallen regelmatig onder meerdere rechtsgebieden, waardoor onzekerheid ontstaat over eigendom, toegang en toezicht.
- Beperkte rechtsbescherming**:** Contractuele afspraken bieden beperkte afdwingbaarheid buiten de EU-jurisdictie.

Bij de beoordeling van leveranciers dient structureel te worden vastgesteld onder welke jurisdictie data en diensten vallen, hoe toegang door derden is geregeld, en in welke mate dit binnen de Europese rechtsorde blijft.

3.2 Data- en AI-risico's

Data en algoritmen vormen de kern van digitale dienstverlening. Beheersing van dataopslag, -verwerking en -toegang is essentieel voor het behoud van digitale autonomie.

- Beperkte controle over data buiten EU-jurisdictie**:** Data die wordt beheerd door niet-Europese aanbieders kan onderhevig zijn aan buitenlandse toegangseisen.
- Onvoldoende datalokaalheid**:** Niet altijd is inzichtelijk waar data fysiek wordt opgeslagen, verwerkt of gerepliceerd.
- Afhankelijkheid van gesloten AI-modellen**:** Niet-transparante algoritmen maken het lastig om uitlegbaarheid en controle te borgen, wat de publieke legitimiteit kan ondermijnen.

DICTU zal kaders hanteren die datalokaalheid en transparantie afdwingbaar maken, en daarbij aandacht te besteden aan dataopslag, AI-trainingsdata en algoritmische uitlegbaarheid.

3.3 Operationele risico's

Operationele risico's hebben betrekking op de continuïteit, beschikbaarheid en beheersbaarheid van Cloud- en datadiensten.

- Leveringszekerheid en geopolitieke risico's**:** Internationale spanningen of sancties kunnen leiden tot abrupte onderbrekingen in dienstverlening.
- Onzekerheid over servicelevels**:** Buitenlandse leveranciers kunnen eenzijdig voorwaarden wijzigen, wat risico's oplevert voor continuïteit en begrotingszekerheid.

DICTU zal sturen op technische en contractuele mogelijkheden tot portabiliteit, en bij aanbesteding nadrukkelijk de mate van afhankelijkheid en overstapkosten te betrekken.

3.4 Technologische risico's

Technologische risico's ontstaan door afhankelijkheid van buitenlandse infrastructuur, gesloten ecosystemen en beperkte Europese controle over kritieke technologieën.

- Vendor lock-in en beperkte portabiliteit: Overstappen naar andere aanbieders is vaak technisch en financieel complex door proprietary technologie en gebrekkige interoperabiliteit.
- Beperkte controle over infrastructuur en standaarden: De meeste clouddiensten, hardware en AI-platforms zijn van niet-Europese makelij, waardoor technologische keuzes buiten de Europese invloedssfeer vallen.
- Kwetsbaarheid in de toeleveringsketen: Storingen in chipproductie of exportrestricties kunnen directe impact hebben op beschikbaarheid.
- Cybersecurityafhankelijkheden: Buitenlandse technologie kan kwetsbaarheden introduceren die moeilijk te auditen zijn.
- Sluiting van ecosystemen: Proprietary technologieën beperken interoperabiliteit en vergroten migratiekosten.

Het is van belang om in architectuurontwerpen prioriteit te geven aan open standaarden, transparante softwarecomponenten en multi-cloudstrategieën die overstapbaarheid bevorderen.

3.5 Menselijke risico's

Menselijke risico's hebben betrekking op kennis, governance en de bestuurlijke grip op digitale afhankelijkheden.

- Beperkte kennispositie: Zowel binnen de overheid als bij leveranciers ontbreekt soms specifieke kennis over cloudjuridica, datalokaalheid en geopolitieke afhankelijkheden.
- Versnipperde governance: Beleidsvorming, inkoop en uitvoering zijn vaak onvoldoende op elkaar afgestemd.
- Onvoldoende bewustzijn van afhankelijkheden: Niet altijd is inzichtelijk welke delen van de cloudstack buiten Europese controle vallen.
- Reputatierisico's: Incidenten met datatoegang of serviceonderbrekingen kunnen publieke legitimiteit schaden.

DICTU draagt bij aan kennisversterking door expertise op te bouwen over digitale autonomie, leveranciersafhankelijkheden en Europese regelgeving, en deze kennis actief te delen binnen het Rijk.

3.6 Samenvatting en handelingsperspectief

De risico's die samenhangen met cloudgebruik en digitale soevereiniteit zijn onderling verweven: juridische beperkingen versterken operationele afhankelijkheden, terwijl technologische keuzes directe gevolgen hebben voor controle.

Het Rathenau Instituut[3] benadrukt dat digitale autonomie niet bereikt wordt door enkel afhankelijkheden te benoemen, maar door actief alternatieven te ontwikkelen en af te nemen. Voor publieke organisaties ligt de nadruk op drie complementaire strategieën:

1. Beperk de machtsconcentratie van grote aanbieders door kritisch inkoopbeleid en open standaarden te stimuleren.
2. Vergroot de onderhandelings- en kennispositie van publieke domeinen, zodat zij regie behouden over data, contracten en technologie.

3. Ontwikkel alternatieven en versterk onafhankelijkheid, door bewuste keuzes in architectuur, aanbesteding en samenwerking met Europese en open-source-ecosystemen.

Voor DICTU betekent dit een structurele koers richting meer grip, kennis en diversificatie, zodat digitale soevereiniteit niet enkel een compliancevraagstuk is, maar een integraal onderdeel van de strategische rijksbrede digitale infrastructuur. Om deze strategieën meer handvaten te geven heeft het Rathenau Instituut vier handelingsopties geformuleerd[3] (zie figuur 2):

1. Koop anders in;
2. Creëer een gelijk speelveld;
3. Breng de kennispositie over digitale autonomie op orde;
4. Kies een route voor digitale autonomie.

Figuur 2- Om koers te zetten op het opbouwen van digitale autonomie heeft het Rathenau Instituut vier handelingsopties opgesteld.

Met name 1) Koop anders in, is een relevante handelingsoptie die wordt omarmd in deze analyse, waarin we invulling geven aan het maken van bewustere keuzes bij de inkoop van digitale diensten die de afhankelijkheden verminderen.

4. Juridische context cloudsoevereiniteit

Het doel van dit hoofdstuk is om inzicht te bieden in de relevante wet- en regelgeving, beleidsstukken, richtlijnen en kaders die van belang zijn voor het opstellen van een afgestemde (EU-, Rijk- en DICTU) analyse voor clouddiensten op digitale soevereiniteit. De inhoud vormt het fundament voor het toetsingsinstrument, dat is gebaseerd op het EuroStack initiatief en het European Commission Cloud Sovereignty Framework, maar is aangepast om aan te sluiten bij DICTU's eigen definitie van cloudsoevereiniteit en de specifieke context van haar dienstverlening aan het Rijk. Ook zijn de belangrijkste juridische en beleidsmatige raakvlakken verkend om de belangrijkste juridische implicaties aan het licht te brengen. Het is nadrukkelijk niet volledig; voor een diepgaande en context-specifieke analyse van juridische implicaties is aanvullend onderzoek vereist. De hier opgenomen informatie dient als vertrekpunt voor strategische reflectie en het ontwikkelen van een toetsingsinstrument, en moet worden aangevuld met organisatie-specifieke inzichten en gespecialiseerde juridische beoordeling.

4.1 Overzicht relevante wet- en regelgeving

Het beoordelen van cloudsoevereiniteit vereist inzicht in een complex samenspel van nationale en Europese beleid, kaders, wet- en regelgeving. Belangrijke regelingen zijn onder meer:

- CLOUD Act (VS, 2018) – Verleent Amerikaanse autoriteiten extraterritoriale bevoegdheden om data op te vragen bij Amerikaanse cloudaanbieders voor internationale opsporingsactiviteiten, ongeacht fysieke opslaglocatie.
- AVG/GDPR (EU, 2018) – Legt verplichtingen vast rond bescherming en verwerking van persoonsgegevens binnen en buiten de EU.
- NIS2 & DORA – Versterken de digitale weerbaarheid van vitale sectoren en financiële instellingen.
- EU Data Act en AI Act – Beogen controle over data, interoperabiliteit en verantwoord gebruik van kunstmatige intelligentie.
- EUCS (European Cybersecurity Certification Scheme) – Een (vrijwillig) Europees certificeringsschema voor clouddiensten met beveiligingsniveaus (Basic, Substantial, High).

4.1.1 De CLOUD Act: Impact op Europese organisaties

De Clarifying Lawful Overseas Use of Data (CLOUD) Act is een Amerikaanse federale wet uit 2018 die Amerikaanse opsporingsdiensten het recht geeft om toegang te eisen tot data, ongeacht waar deze fysiek is opgeslagen, zolang de dienstverlener een Amerikaans bedrijf is. Dit heeft ingrijpende gevolgen voor Europese organisaties die gebruikmaken van Amerikaanse clouddienstverleners zoals Microsoft, Amazon of Google.

Belangrijkste kenmerken van de CLOUD Act:

- Extraterritoriale werking: De wet geldt ook voor data die buiten de VS is opgeslagen, bijvoorbeeld in Europese datacenters.
- Jurisdictie volgt eigendom: Niet de locatie van de data, maar het moederbedrijf bepaalt onder welke wetgeving de data valt.

- Conflict met Europese privacywetgeving: De CLOUD Act kan botsen met de AVG (GDPR), die strikte eisen stelt aan datadoorgifte buiten de EU.

Praktische gevolgen:

- Europese organisaties kunnen geconfronteerd worden met verzoeken van Amerikaanse autoriteiten om data te overhandigen, zelfs als deze data in Europa staat.
- Versleuteling biedt alleen bescherming als de organisatie zelf de encryptiesleutels beheert; anders kan de clouddienstverlener verplicht worden deze te overhandigen.
- Synchronisatie en back-ups over meerdere locaties maken het lastig om te bepalen wie toegang heeft tot data.

4.1.2 Botsing CLOUD Act met de AVG (GDPR)

De AVG stelt dat persoonsgegevens van Europese burgers niet zomaar buiten de EU mogen worden verwerkt, tenzij er passende waarborgen zijn. De CLOUD Act plaatst Amerikaanse bedrijven in een juridische spagaat: zij moeten voldoen aan verzoeken van de Amerikaanse overheid, terwijl de AVG het overdragen van persoonsgegevens aan derde landen beperkt.
Juridische dilemma's:

- Voldoen aan een Amerikaans verzoek kan leiden tot overtreding van de AVG, met hoge boetes tot gevolg.
- Privacy Shield, het eerdere verdrag tussen de VS en EU, werd in 2020 ongeldig verklaard vanwege onvoldoende bescherming tegen staatsinmenging.
- De Europese Data Protection Board stelt dat overdracht van data op basis van de CLOUD Act niet is toegestaan zonder internationale overeenkomst (MLAT).

4.1.3 Status van EUCS

De besluitvorming over EUCS bevindt zich momenteel in een politieke impasse. In eerdere versies bevatte het schema een vierde niveau, High+, waarin juist de strikte soevereiniteitscriteria (zoals Europees eigendom, beheer en rechtsbescherming) waren opgenomen. Onder druk van enkele lidstaten en industriepartijen is dit niveau voorlopig geschrapt.
Echter staat de wereld van Europese cloudsoevereiniteit niet stil, en zijn er initiatieven vanuit de industrie (EuroStack) en Europese Commissie (Cloud Sovereignty Framework). Deze worden verder in dit hoofdstuk behandeld.

4.2 Relevante beleidsstukken vanuit het Rijk

Het Rijksbrede beleid vormt het nationale referentiekader waarbinnen DICTU haar cloudstrategie operationaliseert:

- Het Rijk in de Cloud – Donkere Wolken Pakken Samen (2025) – Analyse van kansen, risico's en beleid rond cloudgebruik binnen de Rijksoverheid, met nadruk op afhankelijkheden, soevereiniteit en risicobeheersing.
- Nederlandse Digitaliseringsstrategie (2025) – Stelt digitale soevereiniteit als een van de zes prioriteiten van het kabinet, gericht op verantwoord datagebruik en versterking van Europese technologische autonomie.
- DICTU Cloudstrategie (2025) – Bepaalt de koers naar een hybride multicloudomgeving met nadruk op regie, open standaarden en onafhankelijkheid van niet-Europese leveranciers.

- Wolken aan de Horizon (2023-2024) – Kamerbrief en initiatiefnota die oproepen tot het terugdringen van afhankelijkheden van grote buitenlandse aanbieders en het stimuleren van Europese alternatieven.
- I-Strategie Rijksoverheid (2021-2025) – Richt zich op digitale autonomie, interoperabiliteit en duurzaamheid, en roept op tot meer grip op cruciale IT-leveranciers.
- Implementatiekader Risicoafweging Cloudgebruik (2022) – Biedt concrete richtlijnen voor risicobeoordeling, selectiecriteria, exitstrategieën en DPIA's.
- Baseline Informatiebeveiliging Overheid (BIO, 2025) – Stelt uniforme beveiligingseisen aan overheidsorganisaties, ook bij cloudgebruik.
- Strategisch Leveranciersmanagement Rijk (SLM, 2023) – Coördineert de strategische relatie met grote IT-leveranciers en onderhandelt rijksbreed over voorwaarden en datasecurity.

Gezamenlijk vormen deze documenten het beleidsmatige fundament waarop DICTU haar toetsingsinstrument voor soevereine clouddiensten bouwt.

4.3 Europese referentiekaders: EuroStack en het EC-Sovereignty Framework

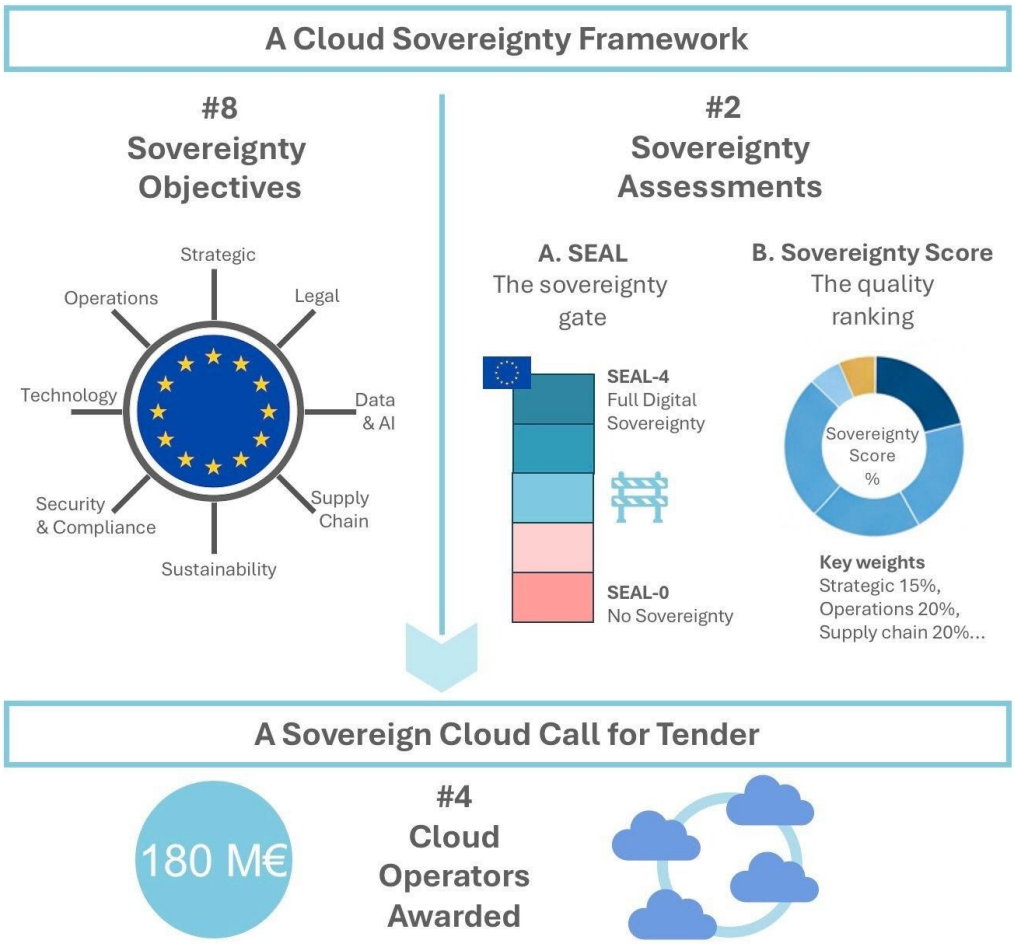
Het EuroStack-voorstel en het European Commission Cloud Sovereignty Framework vormen de Europese maatstaf voor digitale soevereiniteit clouddiensten(verleners). Beide identificeren dezelfde structurele risico's; buiten-Europese jurisdictie, technologische lock-in en beperkte operationele controle, en hanteren grotendeels overlappende beoordelingsdimensies: juridisch, technisch, operationeel, data en economisch.

Het verschil zit in de toepassing en drempelwaarden:

- Het EuroStack-model hanteert een strikt pass-fail-principe voor jurisdictie en eigendom, waarmee niet-Europese aanbieders direct worden uitgesloten van het hoogste soevereiniteitsniveau.
- Het EC-framework werkt met flexibele Sovereignty Effectiveness Assurance Levels (SEALs) als minimumtoegangseis en een weging via Sovereignty Scores (SOV).

Het DICTU-toetsingsinstrument combineert elementen uit zowel het EuroStack-initiatief als het EC-Sovereignty Framework. De indeling in vijf dimensies (risicogebieden) is grotendeels gebaseerd op EuroStack, waarbij het DICTU-toetsingsinstrument de vijfde dimensie 'Mens' toevoegt in plaats van 'Economisch'. Een andere gelijkenis tussen het DICTU-toetsingsinstrument en EuroStack zijn de scherp en concreet geformuleerde criteria; deze zijn echter aangepast aan de DICTU-specifieke context en het Nederlandse recht. Opvallend is dat de SEALs en Sovereignty Scores uit het EC-framework pas zijn geïntroduceerd nadat wij onze soevereiniteit niveaus hadden ontwikkeld. De komst van deze concepten en de sterke gelijkenissen met onze aanpak bevestigen de juistheid en relevantie van het DICTU-toetsingsinstrument. Deze aanpak zorgt voor een gestructureerde, maar flexibele beoordeling

van de mate van soevereiniteit.



Figuur 3 Visualisatie van het EC-framework gepubliceerd op LinkedIn

5. Toetsingsinstrument Soevereiniteit

Het doel van het toetsingsinstrument is het structureel kunnen beoordelen van clouddiensten en haar leveranciers op de mate van soevereiniteit. Het toetsingsinstrument soevereiniteit bestaat uit vijf dimensies, elk met een hoofdvraag, criteria, leidende vragen, toelichtingen en soevereiniteitsniveaus. Deze structuur zorgt voor een precieze, objectieve en toch flexibel middel voor beoordeling. De dimensies, criteria en hoogste soevereiniteitsniveaus samen vormen de definitie van een soevereine clouddienst(verlener) voor Europa.

Dimensies en Criteria

5.1 Juridisch

Hoofdvraag: "*Aan welk juridisch en politiek systeem is de aanbieder uiteindelijk verantwoording schuldig?*"
Door het beantwoorden van deze vraag kom je tot het fundamentele inzicht aan welke rechtsmacht de clouddienstverlener uiteindelijk verantwoording moet afleggen. Dit is een harde randvoorwaarde, wat betekent dat er geen ruimte is voor grijs gebied of mate van verantwoording. Het waarborgt dat de nalevingsverplichtingen van een aanbieder niet worden ondermijnd door conflicterende wettelijke eisen van een niet-EU-land.

5.1.1 Vestiging

Leidende vraag: "*Is de uiteindelijke moedermaatschappij van de aanbieder juridisch gevestigd en heeft zij haar hoofdkantoor binnen de EU, EER of EFTA?*"

Een lokale vestiging is niet voldoende; het hoogste moederbedrijf moet juridisch zijn opgericht in de EU en het hoofdkantoor moet zich in de EU bevinden.

Soevereiniteitsniveaus:

1. **Geen EU-vestiging** – Geen juridische vestiging of hoofdkantoor binnen de EU.
2. **EU-filiaalvestiging** – Alleen een filiaal of dochteronderneming in de EU, moederbedrijf en hoofdkantoor buiten de EU.
3. **EU-moederbedrijf** vestiging – Moederbedrijf juridisch gevestigd in de EU, hoofdkantoor buiten de EU.
4. **Volledig EU gevestigd** – Moederbedrijf juridisch gevestigd in EU, hoofdkantoor binnen de EU.
5. **Volledig EU gevestigd en lokaal (NL)** – Moederbedrijf juridisch gevestigd in EU, en hoofdkantoor binnen de EU. Ook een filiaal of dochteronderneming in NL.

5.1.2 Zeggen- en eigenaarschap

Leidende vraag: *"Is de aanbieder volledig vrij van directe of indirecte controle door niet-Europese entiteiten, zowel formeel (stemrechten) als feitelijk (invloed via belangen of mechanismen)?"*

Formele vestiging is onvoldoende als een niet-EU partij beslissende invloed kan uitoefenen. Een soevereine aanbieder moet vrij zijn van niet-EU controle, zowel juridisch (de jure: meerderheid stemrechten in Europese handen) als feitelijk (de facto: geen blokkerende minderheidsbelangen of andere mechanismen van dwang). Optioneel zou het hoogste niveau van soevereiniteit kunnen worden aangevuld met het toepassen van een (juridisch) beschermingsmechanisme dat een toekomstige non-EU overname voorkomt. Momenteel is deze niet meegenomen, wegens een mogelijk conflict met internationale handelsverdragen/concurrentieregels.

Soevereiniteitsniveaus:

1. **Volledige non-EU zeggenschap** – Niet-EU entiteit heeft doorslaggevende controle.
2. **Blokkerende non-EU invloed** – Niet-EU partij bezit blokkerend minderheidsbelang of vergelijkbare rechten.
3. **Gedeelde zeggenschap EU/non-EU** – Controle gedeeld tussen EU en niet-EU entiteiten.
4. **Overwegend EU-zeggenschap** – Meerderheid stemrechten in EU-handen, beperkte externe invloed.
5. **Volledige EU-zeggenschap** – Alle stemrechten en feitelijke invloed exclusief Europees.

5.1.3 Toepasselijk recht

Leidende vraag: "*Is de aanbieder juridisch en structureel beschermd tegen de extraterritoriale werking van niet-Europese wetgeving, zoals de Amerikaanse CLOUD Act of FISA 702?*"

De aanbieder moet juridisch en structureel geïsoleerd zijn van extraterritoriale wetgeving en exportrestricties van niet-EU landen. Dit voorkomt dat buitenlandse wetgeving toegang kan afdwingen tot Europese data of technologie, wat cruciaal is voor autonomie en vertrouwelijkheid.

Soevereiniteitsniveaus

1. **Non-EU rechtsmacht**
5. **EU rechtsmacht**

5.2 Data & AI

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

Deze dimensie richt zich op de mate waarin data en algoritmen juridisch en technisch beschermd zijn, met aandacht voor opslag, verwerking, toegang en transparantie binnen het Europese rechtsgebied.

5.2.1 Data residency

Leidende vraag: "*Worden alle klantdata (incl. back-ups), uitsluitend opgeslagen en verwerkt binnen het Europese grondgebied (EU, EER, EFTA)?*"

Alle data moeten fysiek en logisch binnen Europa blijven. Geen enkele vorm van verwerking of overdracht naar buiten de EU is toegestaan. Onder verwerking wordt ook de wijze waarop AI-modellen worden getraind en ingezet meegenomen.

Soevereiniteitsniveaus:

1. **Geen garantie EU-opslag** - Geen enkele garantie dat data, back-ups, metadata of logs binnen de EU worden opgeslagen of verwerkt.
2. **Gedeeltelijke EU-opslag** - Hoofddata wordt in de EU opgeslagen, maar back-ups, metadata of logs kunnen buiten de EU staan of verwerkt worden. Overdracht van data is mogelijk buiten de EU.
3. **EU-opslag met uitzonderingen** - Hoofddata en back-ups worden binnen de EU opgeslagen, maar systeemgegenereerde data (zoals metadata en logs) kan buiten de EU worden opgeslagen of verwerkt. Overdracht van data voor analytics/training is mogelijk buiten de EU voor deze systeemdata.
4. **EU-opslag en verwerking** - Alle data, inclusief back-ups, metadata en logs, wordt fysiek en logisch binnen de EU opgeslagen en verwerkt. Geen enkele vorm van data transfer buiten de EU, ook niet voor analytics of training.
5. **Lokaal/EU-opslag en verwerking** - Alle data, inclusief back-ups, metadata en logs, wordt fysiek en logisch binnen de EU opgeslagen en verwerkt. Geen enkele vorm van data transfer buiten de EU, ook niet voor analytics of training. Ook zijn er opties om data naar keuze lokaal (bv. landelijk of on-premise) op te slaan.

5.2.2 Technische Toegangsbeveiliging

Leidende vraag: *"Zijn er aantoonbare technische maatregelen die ervoor zorgen dat ongecodeerde klantdata voor niemand toegankelijk is, inclusief de aanbieder zelf?"*

Juridische beloftes zijn niet voldoende. Er moeten verifieerbare technische garanties zijn, zoals confidential computing of klant-exclusief sleutelbeheer, die het cryptografisch onmogelijk maken voor derden – inclusief de clouddienstverlener – om ongecodeerde data te benaderen.

Soevereiniteitsniveaus:

1. **Geen technische bescherming -** Clouddienstverlener heeft volledige toegang tot data; geen encryptie of sleutelbeheer door klant.
2. **Basisversleuteling (Platform Managed Keys)** - Data is versleuteld, maar clouddienstverlener beheert alle sleutels en kan toegang verkrijgen.
3. **Gedeeld sleutelbeheer (BYOK/CMK)** - Klant levert of beheert sleutels (Bring Your Own Key/Customer Managed Key), maar clouddienstverlener kan rechten aanpassen of toegang verkrijgen via het cloudplatform.
4. **Klantdominantie sleutelbeheer (External Key Management/Managed HSM)** - Sleutelbeheer volledig onder controle van klant via externe HSM of Cloud HSM; clouddienstverlener heeft geen of zeer beperkte toegang tot sleutelbeheer.
5. **Volledige cryptografische isolatie (HYOK + Confidential Computing)** - Klant houdt eigen sleutels (Hold Your Own Key) en data blijft cryptografisch geïsoleerd, zelfs tijdens verwerking; clouddienstverlener heeft op geen enkel moment toegang tot ongecodeerde data.

5.2.3 Juridische Toegangsbeveiliging

Leidende vraag: *"Is de aanbieder contractueel verplicht om niet-Europese verzoeken tot datatoegang juridisch aan te vechten en de klant hierover te informeren?"*

De aanbieder moet optreden als juridisch beschermingsmechanisme voor de klant en actief verzet bieden tegen niet-EU dataverzoeken, inclusief verplichte melding.

Soevereiniteitsniveaus:

1. **Geen verplichting** - Clouddienstverlener voldoet aan buitenlandse verzoeken zonder verzet.
2. **Vrijwillige melding** - Clouddienstverlener informeert klant vrijwillig en/of op aanvraag, maar vecht verzoeken niet aan.
3. **Contractuele melding** - Clouddienstverlener meldt verplicht verzoeken, maar vecht verzoeken niet aan.
4. **Actief juridisch verzet** - Clouddienstverlener is verplicht verzoeken te melden en voldoet niet aan verzoek; probeert altijd door te verwijzen naar de klant.
5. **Volledige juridische bescherming** - Clouddienstverlener verplicht verzoeken te melden, voldoet niet aan verzoek en verwijst de zaak naar internationale juridische mechanismen zoals het MLAT (overeenkomst wederzijdse juridische bijstand).

5.3 Technologie

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

Technologie heeft enerzijds de kracht om de afnemer compleet afhankelijk te maken wanneer de werking ervan als een "black-box" werkt; in essentie een *soevereine gevangenis*. Anderzijds kan het de afnemer onafhankelijk maken en juist vrijheid geven als de technologie compleet op open standaarden en/of open-source gebouwd is.

5.3.1 Interoperabiliteit & Portabiliteit

Leidende vraag: *"Is de dienst gebouwd op open standaarden zodat het mogelijk is om van aanbieders te wisselen en/of gebruik te maken van meerdere aanbieders tegelijkertijd?"*
Dit voorkomt vendor lock-in en biedt vrijheid om van aanbieder te wisselen en/of gebruik te maken van meerdere aanbieders tegelijkertijd.

Soevereiniteitsniveaus:

1. **Volledige lock-in** - Diensten zijn volledig proprietary; migratie van data en workloads is niet mogelijk zonder aanzienlijke inspanning of kosten. Geen portabiliteit en interoperabiliteit.
2. **Gedeeltelijke openheid** - Open standaarden worden toegepast, maar kerncomponenten zijn proprietary; migratie is beperkt mogelijk en vereist vaak extra inspanning; portabiliteit en interoperabiliteit zijn laag.
3. **Open standaarden met beperkingen** - Open standaarden worden veelvuldig gebruikt, maar niet alle componenten voldoen eraan of maken gebruik van weinig gangbare standaarden; portabiliteit en interoperabiliteit zijn deels beperkt.

4. **Alle diensten gebaseerd op open standaarden** - Alle componenten gebruiken open standaarden, maar niet altijd de meest gangbare varianten. Portabiliteit en interoperabiliteit zijn hoog, maar niet volledig geoptimaliseerd.
5. **Alle diensten gebaseerd op meest gebruikte open standaarden** - Alle componenten gebruiken de meest gangbare en breed geaccepteerde open standaarden. Portabiliteit en interoperabiliteit zijn gemaximaliseerd; migratie en integratie zijn eenvoudig en kostenefficiënt.

5.3.2 Open-source

Leidende vraag: *"Maakt de dienst gebruik van opensource software voor de kerncomponenten?"*

Het gebruik van opensource maakt een dienst in mindere mate afhankelijk van derde partijen. Het draagt bij aan data en workload portabiliteit, en voorkomt vendor lock-in door keuzevrijheid in clouddienstverleners.

Soevereiniteitsniveaus:

1. **Proprietary** - Onduidelijk of en waar opensource gebruikt wordt; migratie van workloads is niet mogelijk zonder aanzienlijke inspanning of Kosten.
2. **Proprietary met opensource componenten** - De dienst is hoofdzakelijk proprietary, maar bevat enkele opensource componenten; migratie van workloads blijft complex door afhankelijkheid proprietary kern componenten.
3. **Opensource met beperkingen** - Kerncomponenten van de dienst zijn deels gebouwd op opensource software, maar hebben unieke aanpassingen, enige in soort en/of gelinkt aan proprietary integraties. Workloads migreren zijn niet triviaal en kosten kunnen oplopen.
4. **Volledig opensource** - De dienst is volledig open source; workloads zijn eenvoudig te migreren. De gekozen opensource software heeft grote en actieve support communities.
5. **Opensource evangelist** - De dienst is volledig open source; data en workloads zijn eenvoudig te migreren. De opensource gekozen software heeft grote en actieve support communities. Clouddienstverlener is tevens grote bijdrager aan de ontwikkeling van (eigen in gebruik genomen) opensource software.

5.3.3 Software transparantie

Leidende vraag: *"Is de broncode van alle kerntechnologie beschikbaar voor inspectie, bijvoorbeeld publiek of via een erkende derde partij (escrow)?"*
Transparantie verlaagt kans op verborgen kwetsbaarheden en biedt verifieerbare zekerheid over de werking en veiligheid van de software. Daarnaast is uitlegbaarheid van algoritmen belangrijk: de clouddienstverlener moet kunnen aantonen dat AI-modellen geen ongewenste bias bevatten en dat beslissingen reproduceerbaar en controleerbaar zijn.

Soevereiniteitsniveaus:

1. **Geen transparantie** - Kerntechnologie is volledig gesloten; geen inzage in design of broncode, werking en veiligheid zijn een "black box".
2. **Beperkte transparantie** - Kerntechnologie is deels inzichtelijk via beperkte documentatie. Enige toelichting broncode op werking en beveiliging. Verifieerbaarheid is beperkt.

3. **Contractuele transparantie** - Broncode is beschikbaar voor de klant of erkende Europese partij ter inspectie. Broncode verifieerbaar, maar software supply chain is beperkt verifieerbaar en traceerbaar.
4. **Volledig transparant** - Broncode is beschikbaar voor de klant of erkende Europese partij ter inspectie. Broncode en gehele software supply chain (zoals AI/algoritmen) is traceerbaar en verifieerbaar.
5. **Volledig transparant en geaudit** - Broncode is beschikbaar voor de klant of erkende Europese partij ter inspectie. Gehele software supply chain (zoals AI/algoritmen) is traceerbaar en verifieerbaar; alle software is reproduceerbaar en periodiek geaudit door onafhankelijke partijen.

5.3.4 Operationele omkeerbaarheid

Leidende vraag: *"Kan een derde partij de dienst overnemen bij uitval van de aanbieder of beëindiging van het contract, op basis van de beschikbare documentatie en ontwerp?"*

De dienst moet zo zijn ontworpen en gedocumenteerd dat een derde partij deze kan herdeployen en exploiteren. Dit verlaagt vendor lock-in, en faciliteert een exit.

Soevereiniteitsniveaus:

1. **Geen omkeerbaarheid** - De dienst is niet overdraagbaar; continuïteit bij uitval van de aanbieder is niet gegarandeerd.
2. **Beperkte omkeerbaarheid** - Documentatie is beperkt aanwezig, maar overdracht aan een derde partij is complex en niet volledig mogelijk.
3. **Contractuele omkeerbaarheid** - De dienst is grotendeels overdraagbaar; documentatie en ontwerp zijn hoogover beschikbaar, om een derde partij in staat te stellen de dienst op termijn zelfstandig te exploiteren.
4. **Actieve omkeerbaarheid** - De dienst is volledig overdraagbaar; documentatie en ontwerp zijn voldoende gedetailleerd om een derde partij in staat te stellen de dienst zelfstandig te exploiteren.
5. **Volledige operationele omkeerbaarheid** - De dienst is volledig overdraagbaar; documentatie en ontwerp zijn voldoende gedetailleerd en getest om een derde partij in staat te stellen de dienst zelfstandig te exploiteren.

5.4 Operationeel

Hoofdvraag: *"Wie heeft de controle over de operationele omgeving van de dienst?"*

Vanuit waar de operatie wordt uitgevoerd en door wie de infrastructuur wordt beheerd is van groot belang voor de mate van soevereiniteit die je behaalt. Naast technisch en juridisch, kan ook personeel onder druk worden gezet of worden beïnvloed.

5.4.1 EU-Infrastructuur en Control Plane

Leidende vraag: Bevindt de volledige technische infrastructuur (datacenters, netwerk) en operatie ervan (control plane) zich fysiek binnen de EU/EER/EFTA?
De gehele fysieke infrastructuur (datacenters, netwerken), en de control plane om de Cloud services mee te managen en orkestreren, moeten zich bevinden en uitgevoerd worden binnen de EU/EER/EFTA.

Soevereiniteitsniveaus:

1. **Volledige non-EU operatie** - De fysieke infrastructuur (datacenters, netwerk) en control plane bevinden zich volledig buiten de EU en worden volledig beheerd door niet-Europese partijen.
2. **EU-infra en non-EU control plane** - De fysieke infrastructuur (datacenters, netwerk) zijn in de EU, maar de control plane wordt extern beheerd en bevindt zich buiten de EU.
3. **EU-infra en control plane** - De fysieke infrastructuur (datacenters, netwerk) en control plane zijn in de EU, maar de control plane wordt (deels) extern beheerd.
4. **Volledige EU-operatie** - De fysieke infrastructuur (datacenters, netwerk) en de control plane zijn gegarandeerd volledig in de EU.
5. **Volledige EU-operatie gegarandeerd** - De fysieke infrastructuur (datacenters, netwerk) en de control plane zijn gegarandeerd volledig in de EU. Wordt periodiek geaudit door een erkende EU-partner.

5.4.2 Exclusief Europees Personeel

Leidende vraag: *"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 zijn werkzaamheden fysiek vanuit Europa verricht?"*

Alle medewerkers met privileged access moeten burger en ingezetenen zijn van de EU/EER/EFTA, in dienst zijn bij een Europese entiteit, en hun werkzaamheden fysiek vanuit Europa uitvoeren. Alle operationele, administratieve en beheersmatige activiteiten met betrekking tot de dienstverlening en gegevensverwerking worden uitsluitend uitgevoerd door natuurlijke of rechtspersonen die exclusief onder de jurisdictie van een lidstaat van de Europese Unie vallen, en die niet onderworpen zijn aan enige extraterritoriale wetgeving of rechtsmacht van een derde land (non-EU).

In uitzonderlijke gevallen, zoals kritieke storingen of specialistisch onderhoud waarvoor unieke expertise vereist is, kan tijdelijk een non-EU engineer met een specifiek securitylevel worden ingezet. Dit gebeurt uitsluitend na voorafgaande goedkeuring, met minimale en gecontroleerde toegang, volledige documentatie en een verplichte audit achteraf om de soevereiniteit en veiligheid te waarborgen. Deze afbakening voorkomt dat beheerders onder niet-Europees recht kunnen worden verplicht om toegang tot data of systemen te verlenen. Zo blijft zowel de operationele controle als de rechtsmacht volledig Europees gewaarborgd.

Privileged Access wordt gedefinieerd als toegang die de gebruiker de mogelijkheid kan geven om belangrijke systeemconfiguraties te wijzigen, toegang te hebben tot audit- of gerelateerde informatie, of toegang te hebben tot datastromen, bestanden en accounts die eigendom zijn van andere gebruikers.[6]

[6] Wright, C. S. (2008). The IT regulatory and standards compliance handbook: How to survive information systems audit and assessments. Elsevier.

Een burger is een natuurlijke persoon die in juridische zin het burgerschap of staatsburgerschap bezit van een bepaalde staat (door geboorte, afstamming of naturalisatie), en daardoor onder de bescherming én de rechtsmacht van die staat valt.[7]

Ingezetene betekent een natuurlijke persoon die duurzaam in Nederland verblijft en is ingeschreven in de Basisregistratie Personen (BRP), ongeacht nationaliteit. Het begrip verwijst naar feitelijk verblijf binnen de Nederlandse jurisdictie, niet naar staatsburgerschap.[8]

Soevereiniteitsniveaus:

1. **Geen controle personeel** - Beheerwerkzaamheden met privileged access worden volledig uitgevoerd door non-EU personeel, buiten Europa uitgevoerd, en zijn in dienst van een non-EU organisatie.
2. **Beperkte controle personeel** - Beheerwerkzaamheden met privileged access worden deels uitgevoerd door non-EU personeel, buiten Europa uitgevoerd, maar zijn in dienst van een EU entiteit.
3. **Controle personeel soevereine diensten** - Voor soevereine diensten is 100% van het personeel met privileged acces tot service-infrastructuur en klantdata, ingezetenen en burger van de EU en fysiek werkzaam in Europa onder Europees entiteit. Voor hoge uitzondering zoals kritieke specialistische ondersteuning kan een non-EU persoon worden ingeschakeld.
4. **Volledige personele soevereiniteit beheer** - 100% van het personeel met privileged acces tot service-infrastructuur en klantdata zijn ingezetenen en burger van de EU en fysiek werkzaam in Europa, onder Europees entiteit. Voor hoge uitzondering zoals kritieke specialistische ondersteuning kan een non-EU persoon worden ingeschakeld.
5. **Volledige personele soevereiniteit beheer gegarandeerd** - 100% van het personeel met privileged acces tot service-infrastructuur en klantdata zijn ingezetenen van de EU en fysiek werkzaam in Europa, onder Europees entiteit. Wordt periodiek geaudit door erkende EU-partner, daarmee gegarandeerd.

5.4.3 Supply Chain Resilience

Leidende vraag: *"Heeft de aanbieder een aantoonbare strategie om afhankelijkheid van niet-Europese hardware en software te minimaliseren?"*

De aanbieder moet servicecontinuïteit waarborgen bij geopolitieke sancties of supply chain verstoringen.

Soevereiniteitsniveaus:

1. **Afwezig** - Geen strategie beschreven hoe om te gaan met supply chain disruptie.
2. **Ad-hoc** - De clouddienstverlener beschikt over een initiële of gedeeltelijke strategie (datacenters/infrastructuur of diensten) om de afhankelijkheid van non-EU hardware en kritieke software te beperken en zo continuïteit van de dienstverlening te waarborgen in het geval van geopolitieke sancties of verstoringen in de supply chain.
3. **Herhaalbaar gedocumenteerd** - De clouddienstverlener moet over een complete (datacenters, infrastructuur en diensten) gedocumenteerde strategie beschikken die herhaalbaar en auditeerbaar is om de afhankelijkheid van non-EU hardware en kritieke

[7] Art. 2(d) of Regulation (EC) No 862/2007 (Migration Statistics Regulation)

[8] Artikel 1.2 Wet basisregistratie personen

software te beperken en zo de continuïteit van de dienstverlening te waarborgen in het geval van geopolitieke sancties of verstoringen in de supply chain.

4. **Systematisch** - De clouddienstverlener moet over een complete (datacenters, infrastructuur en diensten) gedocumenteerde strategie beschikken die regelmatig geaudit wordt door erkende Europese partij om de afhankelijkheid van non-EU hardware en kritieke software te beperken en zo de continuïteit van de dienstverlening te waarborgen in het geval van geopolitieke sancties of verstoringen in de supply chain.
5. **Leidend** - De clouddienstverlener moet over een complete (datacenters, infra en diensten) gedocumenteerde strategie beschikken die geaudit is om de afhankelijkheid van non-EU hardware en kritieke software te beperken en zo de continuïteit van de dienstverlening aantoonbaar te waarborgen voor een minimaal afgesproken termijn in het geval van geopolitieke sancties of verstoringen in de supply chain.

5.5 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 om soevereine, duurzame, veilige en innovatieve clouddiensten te ontwikkelen en te beheren?"*

De kennis, kunde en beschikbaarheid van personeel binnen de clouddienstverlener zijn cruciaal voor soevereiniteit en veiligheid. Medewerkers moeten aantoonbaar betrouwbaar, deskundig en Europees gebonden zijn. De leverancier dient bovendien te beschikken over voldoende interne capaciteit en expertise om soevereine diensten zelfstandig te ontwikkelen, te beheren en door te ontwikkelen.

5.5.1 Training, certificering en screening

Leidende vraag: *Is personeel met toegang tot kritieke systemen aantoonbaar gescreend, gecertificeerd en getraind?*

Waarborgt dat personeel met toegang tot kritieke systemen aantoonbaar betrouwbaar en gekwalificeerd is.

Soevereiniteitsniveaus:

1. **Geen screening en training** - Onbekend opleidingsniveau; geen screening.
2. **Beperkte screening en training** - Medewerkers zijn gescreend en getraind op eigen initiatief clouddienstverlener, maar niet gedocumenteerd of gepubliceerd.
3. **Gedocumenteerde screening en training** - Medewerkers zijn gescreend en getraind op eigen initiatief clouddienstverlener, gedocumenteerd en eventueel gepubliceerd.
4. **Controleerbare screening en training** - Medewerkers zijn gescreend en getraind op eigen initiatief clouddienstverlener, gedocumenteerd, gepubliceerd, en auditeerbaar door erkende Europese partij.
5. **Gecontroleerde screening en training** - Medewerkers zijn gescreend en getraind op eigen initiatief clouddienstverlener, gedocumenteerd, gepubliceerd, en wordt periodiek geaudit door erkende Europese partij.

5.5.2 Capaciteit en vaardigheden

Leidende vraag: *"Beschikt de clouddienstverlener over voldoende capaciteit en de juiste vaardigheden om autonoom een soevereine cloudomgeving te bouwen, te beheren en door te ontwikkelen?"*

De clouddienstverlener moet intern beschikken over voldoende capaciteit en de juiste technische en organisatorische vaardigheden om zelfstandig soevereine clouddiensten te onderhouden, bouwen en door te ontwikkelen.

Soevereiniteitsniveaus:

1. **Volledig afhankelijk non-EU** - De clouddienstverlener beschikt enkel over interne non-EU capaciteit of is compleet afhankelijk van externe non-EU capaciteit voor het bouwen, beheren en door ontwikkelen van een (soevereine) cloudomgeving.
2. **Beperkt EU-capaciteit, sterk afhankelijk non-EU** - De clouddienstverlener beschikt beperkt over interne EU-capaciteit voor kritieke beheer. Structurele (externe) non-EU ondersteuning is nodig voor bouw en doorontwikkeling.
3. **Basis EU-capaciteit, deels afhankelijk non-EU** - De clouddienstverlener beschikt over voldoende interne EU-capaciteit voor bouw en beheer. Structurele (externe) non-EU ondersteuning is nodig voor doorontwikkeling.
4. **Volwaardig EU cloudteam** - De clouddienstverlener beschikt over voldoende interne EU-capaciteit voor bouw, beheer en doorontwikkeling.
5. **Soevereine Cloud innovator EU met lokale (NL) ondersteuning** - De clouddienstverlener beschikt over vooroplopende interne EU-capaciteit voor bouw, beheer en doorontwikkeling, met lokale (NL) capaciteit voor de bouw en het beheer.

6. Bijlagen

TOETSINGSINSTRUMENT; DIMENSIES, CRITERIA, LEIDENDE VRAGEN EN TOELICHTINGEN

Dimensie	Hoofdvraag	Criterium	Leidende vraag	Toelichting
1. Juridisch	**Aan welk juridisch en politiek systeem is de aanbieder uiteindelijk verantwoording schuldig?**	**1.1 Vestiging**	Is de uiteindelijke moedermaatschappij van de aanbieder juridisch gevestigd en heeft zij haar hoofdkantoor binnen de EU, EER of EFTA?	Een lokale vestiging is niet voldoende; het hoogste moederbedrijf moet juridisch zijn opgericht in de EU en het hoofdkantoor moet zich in de EU bevinden.
		1.2 Zeggen- en eigenaarschap	Is de aanbieder volledig vrij van directe of indirecte controle door niet-Europese entiteiten, zowel formeel (stemrechten) als feitelijk (invloed via belangen of mechanismen)?	Formele vestiging is onvoldoende als een niet-EU partij beslissende invloed kan uitoefenen. Een soevereine aanbieder moet vrij zijn van niet-EU controle, zowel juridisch (*de jure*: meerderheid stemrechten in Europese handen) als feitelijk (*de facto*: geen blokkerende minderheidsbelangen of andere mechanismen van dwang).
		1.3 Toepasselijk recht	Is de aanbieder juridisch en structureel beschermd tegen de extraterritoriale werking van niet-Europese wetgeving, zoals de Amerikaanse CLOUD Act of FISA 702?	De aanbieder moet juridisch en structureel geïsoleerd zijn van extraterritoriale wetgeving en exportrestricties van niet-EU landen. Dit voorkomt dat buitenlandse wetgeving toegang kan afdwingen tot Europese data of technologie, wat cruciaal is voor autonomie en vertrouwelijkheid.
2. Data & AI	**In welke mate zijn gegevens aantoonbaar beschermd, in zowel juridische als technische zin?**	**2.1 Data residency**	Worden alle klantdata (incl. back-ups), uitsluitend opgeslagen en verwerkt binnen het Europese grondgebied (EU, EER, EFTA)?	Alle data moeten fysiek en logisch binnen Europa blijven. Geen enkele vorm van overdracht buiten EU is toegestaan.
		2.2 Technische Toegangsbeveiliging	Zijn er aantoonbare technische maatregelen die ervoor zorgen dat ongecodeerde klantdata voor niemand toegankelijk is, inclusief de aanbieder zelf?	Juridische beloftes zijn niet voldoende. Er moeten verifieerbare technische garanties zijn, zoals confidential computing of klant-exclusief sleutelbeheer, die het cryptografisch onmogelijk maken voor derden - inclusief de clouddienstverlener - om ongecodeerde data te benaderen.
		2.3 Juridische Toegangsbeveiliging	Is de aanbieder contractueel verplicht om niet-Europese verzoeken tot datatoegang juridisch aan te vechten en de klant hierover te informeren?	De aanbieder moet optreden als juridisch beschermingsmechanisme voor de klant en actief verzet bieden tegen niet-EU dataverzoeken, inclusief verplichte melding.

3. Technologie	**Biedt de technologie autonomie, inzichtelijkheid, weerbaarheid en portabiliteit voor de klant?**	**3.1 Interoperabiliteit & Portabiliteit**	Is de dienst gebouwd op open standaarden zodat het mogelijk is om van aanbieders te wisselen en / of gebruik te maken van meerdere aanbieders tegelijkertijd?	Dit voorkomt vendor lock-in en biedt vrijheid om van aanbieder te wisselen en /of gebruik te maken van meerdere aanbieders tegelijkertijd.
		3.2 Opensource	Maakt de dienst gebruik van opensource software voor de kerncomponenten?	Het gebruik van opensource maakt een dienst in mindere mate afhankelijk van derde partijen. Het draagt bij aan data en workload portabiliteit, en voorkomt vendor lock-in door keuzevrijheid in clouddienstverleners.
		3.3 Software Transparantie	Is de broncode van alle kerntechnologie beschikbaar voor inspectie, bijvoorbeeld publiek of via een erkende derde partij (escrow)?	Transparantie verlaagt kans op verborgen kwetsbaarheden en biedt verifieerbare zekerheid over de werking en veiligheid van de software.
		3.4 Operationele omkeerbaarheid	Kan een derde partij de dienst overnemen bij uitval van de aanbieder of beëindiging van het contract, op basis van de beschikbare documentatie en ontwerp?	De dienst moet zo zijn ontworpen en gedocumenteerd dat een derde partij deze kan herdeployen en exploiteren. Dit verlaagt vendor lock-in, en faciliteert een exit.
4. Operationeel	**Wie heeft de controle over de operationele omgeving van de dienst?**	**4.1 EU-Infrastructuur en Control Plane**	Bevindt de volledige technische infrastructuur (datacenters, netwerk) en operatie ervan (control plane) zich fysiek binnen de EU/EER/EFTA?	De gehele fysieke infrastructuur (datacenters, netwerken), en de control plane om de Cloud services mee te managen en orkestreren, moeten zich bevinden en uitgevoerd worden binnen de EU/EER/EFTA. Dit voorkomt dat data in de EU wordt opgeslagen, maar extern wordt beheerd of beïnvloed.
		4.2 Exclusief Europees Personeel	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 zijn werkzaamheden fysiek vanuit Europa verricht?	Alle medewerkers met privileged access moeten burger en ingezetenen zijn van de EU/EER/EFTA, in dienst zijn bij een Europese entiteit, en hun werkzaamheden fysiek vanuit Europa uitvoeren.
		4.3 Supply Chain Resilience	Heeft de aanbieder een aantoonbare strategie om afhankelijkheid van niet-Europese hardware en software te minimaliseren?	De aanbieder moet servicecontinuïteit waarborgen bij geopolitieke sancties of supply chain verstoringen.

5. Mens	**In hoeverre is er zichtbaarheid en controle over wie toegang heeft tot systemen en data, en beschikt het personeel over de kennis en vaardigheden om soevereine, duurzame, veilige en innovatieve clouddiensten te ontwikkelen en te beheren?**	**5.1 Training, Certificering en Screening**	Is personeel met toegang tot kritieke systemen aantoonbaar gescreend, gecertificeerd en getraind?	Waarborgt kwaliteit en betrouwbaarheid van personeel.
		5.2 Capaciteit en vaardigheden	Beschikt de clouddienstverlener over voldoende capaciteit en de juiste vaardigheden om autonoom een soevereine cloudomgeving te bouwen, beheren en door te ontwikkelen?	De clouddienstverlener moet intern beschikken over voldoende capaciteit en de juiste technische en organisatorische vaardigheden om zelfstandig soevereine clouddiensten te ontwerpen, bouwen en onderhouden.

TOETSINGSINSTRUMENT; NIVEAUS VAN SOEVEREINITEIT PER CRITERIA

Criterium	Niveau Soevereiniteit	1	2	3	4	5
1.1 Vestiging		**1. Geen EU-vestiging** - Geen juridische vestiging of hoofdkantoor binnen de EU	**2. EU filiaalvestiging** - Alleen een filiaal of dochteronderneming in de EU; moederbedrijf en hoofdkantoor buiten de EU	**3. EU moederbedrijf vestiging** - Moederbedrijf juridisch gevestigd in de EU, hoofdkantoor buiten de EU	**4. Volledig EU gevestigd** - Moederbedrijf juridisch gevestigd in EU, hoofdkantoor binnen de EU	**5. Volledig EU gevestigd en lokaal (NL)** - Moederbedrijf juridisch gevestigd in EU, en hoofdkantoor binnen de EU. Ook een filiaal of dochteronderneming in NL
1.2 Zeggen- en eigenaarschap		**1. Volledige non-EU zeggenschap** - Niet-EU entiteit heeft doorslaggevende controle	**2. Blokkerende non-EU invloed** - Niet-EU partij bezit blokkerend minderheidsbelang of vergelijkbare rechten	**3. Gedeelde zeggenschap EU/non-EU** - Controle gedeeld tussen EU en niet-EU entiteiten	**4. Overwegend EU-zeggenschap** - Meerderheid stemrechten in EU-handen, beperkte externe invloed	**5. Volledige EU-zeggenschap** - Alle stemrechten en feitelijke invloed exclusief Europees
1.3 Toepasselijk recht		**1. Non-EU rechtsmacht**				**5. EU rechtsmacht**
2.1 Data residency		**1. Geen garantie EU-opslag** - Geen enkele garantie dat data, back-ups, metadata of logs binnen de EU worden opgeslagen of verwerkt	**2. Gedeeltelijke EU-opslag** - Hoofddata wordt in de EU opgeslagen, maar back-ups, metadata of logs kunnen buiten de EU staan of verwerkt worden. Overdracht van data is mogelijk buiten de EU	**3. EU-opslag met uitzonderingen** - Hoofddata en back-ups worden binnen de EU opgeslagen, maar systeemgegenereerde data (zoals metadata en logs) kan buiten de EU worden opgeslagen of verwerkt. Overdracht van data voor analytics/training is mogelijk buiten de EU voor deze systeemdata	**4. EU-opslag en verwerking** - Alle data, inclusief back-ups, metadata en logs, wordt fysiek en logisch binnen de EU opgeslagen en verwerkt. Geen enkele vorm van data transfer buiten de EU, ook niet voor analytics of training	**5. Lokaal/EU-opslag en verwerking** - Alle data, inclusief back-ups, metadata en logs, wordt fysiek en logisch binnen de EU opgeslagen en verwerkt. Geen enkele vorm van data transfer buiten de EU, ook niet voor analytics of training. Ook zijn er opties om data naar keuze lokaal (bv. landelijk of on-premise) op te slaan
2.2 Technische Toegangsbeveiliging		**1. Geen technische bescherming -** Clouddienstverlener heeft volledige toegang tot data; geen encryptie of sleutelbeheer door klant	**2. Basisversleuteling (Platform Managed Keys) -** Data is versleuteld, maar clouddienstverlener beheert alle sleutels en kan toegang verkrijgen	**3. Gedeeld sleutelbeheer (BYOK/CMK) -** Klant levert of beheert sleutels (Bring Your Own Key/Customer Managed Key), maar clouddienstverlener kan rechten aanpassen of toegang verkrijgen via het cloudplatform	**4. Klantdominantie sleutelbeheer (External Key Management/Managed HSM) -** Sleutelbeheer volledig onder controle van klant via externe HSM of Cloud HSM; clouddienstverlener heeft geen of zeer beperkte toegang tot sleutelbeheer	**5. Volledige cryptografische isolatie (HYOK + Confidential Computing) -** Klant houdt eigen sleutels (Hold Your Own Key) en data blijft cryptografisch geïsoleerd, zelfs tijdens verwerking; clouddienstverlener heeft op geen enkel moment toegang tot ongecodeerde data

2.3 Juridische Toegangsbeveiliging		**1. Geen verplichting** - Clouddienstverlener voldoet aan buitenlandse verzoeken zonder verzet	**2. Vrijwillige melding** - Clouddienstverlener informeert klant vrijwillig en/of op aanvraag, maar vecht verzoeken niet aan	**3. Contractuele melding** - Clouddienstverlener meldt verplicht verzoeken, maar vecht verzoeken niet aan	**4. Actief juridisch verzet** - Clouddienstverlener is verplicht verzoeken te melden en voldoet niet aan verzoek; probeert altijd door te verwijzen naar de klant	**5. Volledige juridische bescherming** - Clouddienstverlener verplicht verzoeken te melden, voldoet niet aan verzoek en verwijst de zaak naar internationale juridische mechanismen zoals het MLAT (overeenkomst wederzijdse juridische bijstand)
3.1 Interoperabiliteit & Portabiliteit		**1. Volledige lock-in** - Diensten zijn volledig proprietary; migratie van data en workloads is niet mogelijk zonder aanzienlijke inspanning of kosten. Geen portabiliteit en interoperabiliteit	**2. Gedeeltelijke openheid** - Open standaarden worden toegepast, maar kerncomponenten zijn proprietary; migratie is beperkt mogelijk en vereist vaak extra inspanning; portabiliteit en interoperabiliteit zijn laag	**3. Open standaarden met beperkingen** - Open standaarden worden veelvuldig gebruikt, maar niet alle componenten voldoen eraan of maken gebruik van weinig gangbare standaarden; portabiliteit en interoperabiliteit zijn deels beperkt	**4. Alle diensten gebaseerd op open standaarden -** Alle componenten gebruiken open standaarden, maar niet altijd de meest gangbare varianten. Portabiliteit en interoperabiliteit zijn hoog, maar niet volledig geoptimaliseerd	**5. Alle diensten gebaseerd op meest gebruikte open standaarden** - Alle componenten gebruiken de meest gangbare en breed geaccepteerde open standaarden. Portabiliteit en interoperabiliteit zijn gemaximaliseerd; migratie en integratie zijn eenvoudig en kostenefficiënt
3.2 Opensource		**1. Proprietary** - Onduidelijk of en waar opensource gebruikt wordt; migratie van workloads is niet mogelijk zonder aanzienlijke inspanning of kosten	**2. Proprietary met opensource componenten** - De dienst is hoofdzakelijk proprietary, maar bevat enkele opensource componenten; migratie van workloads blijft complex door afhankelijkheid proprietary kern componenten	**3. Opensource met beperkingen** - Kerncomponenten van de dienst zijn deels gebouwd op opensource software, maar hebben unieke aanpassingen, enige in soort en/of gelinkt aan proprietary integraties. Workloads migreren zijn niet triviaal en kosten kunnen oplopen	**4. Volledig opensource** - De dienst is volledig opensource; workloads zijn eenvoudig te migreren. De gekozen opensource software heeft grote en actieve support communities	**5. Opensource evangelist -** De dienst is volledig opensource; data en workloads zijn eenvoudig te migreren. De opensource gekozen software heeft grote en actieve support communities. Clouddienstverlener is tevens grote bijdrager aan de ontwikkeling van (eigen in gebruik genomen) opensource software
3.3 Software Transparantie		**1. Geen transparantie** - Kerntechnologie is volledig gesloten; geen inzage in design of broncode, werking en veiligheid zijn een "black box"	**2. Beperkte transparantie** - Kerntechnologie is deels inzichtelijk via beperkte documentatie. Enige toelichting broncode op werking en beveiliging. Verifieerbaarheid is beperkt	**3. Contractuele transparantie** - Broncode is beschikbaar voor de klant of erkende Europese partij ter inspectie. Broncode verifieerbaar, maar software supply chain is beperkt verifieerbaar en traceerbaar	**4. Volledige transparant** - Broncode is beschikbaar voor de klant of erkende Europese partij ter inspectie. Broncode en gehele software supply chain is traceerbaar en verifieerbaar	**5. Volledige transparant en geaudit** - Broncode is beschikbaar voor de klant of erkende Europese partij ter inspectie. Gehele software supply chain is traceerbaar en verifieerbaar; alle software is reproduceerbaar en periodiek geaudit door onafhankelijke partijen

3.4 Operationele omkeerbaarheid		**1. Geen omkeerbaarheid** - De dienst is niet overdraagbaar; continuïteit bij uitval van de aanbieder is niet gegarandeerd	**2. Beperkte omkeerbaarheid** - Documentatie is beperkt aanwezig, maar overdracht aan een derde partij is complex en niet volledig mogelijk	**3. Contractuele omkeerbaarheid** - De dienst is grotendeels overdraagbaar; documentatie en ontwerp zijn hoog over beschikbaar, om een derde partij in staat te stellen de dienst op termijn zelfstandig te exploiteren	**4. Actieve omkeerbaarheid** - De dienst is volledig overdraagbaar; documentatie en ontwerp zijn voldoende gedetailleerd om een derde partij in staat te stellen de dienst zelfstandig te exploiteren	**5. Volledige operationele omkeerbaarheid** - De dienst is volledig overdraagbaar; documentatie en ontwerp zijn voldoende gedetailleerd en getest om een derde partij in staat te stellen de dienst zelfstandig te exploiteren
4.1 EU-Infrastructuur en Control Plane		**1. Volledige non-EU operatie** - De fysieke infrastructuur (datacenters, netwerk) en control plane bevinden zich volledig buiten de EU en worden volledig beheerd door niet-Europese partijen	**2. EU-infra en non-EU control plane** - De fysieke infrastructuur (datacenters, netwerk) zijn in de EU, maar de control plane wordt extern beheerd en bevindt zich buiten de EU	**3. EU-infra en control plane** - De fysieke infrastructuur (datacenters, netwerk) en control plane zijn in de EU, maar de control plane wordt (deels) extern beheerd	**4. Volledige EU-operatie** - De fysieke infrastructuur (datacenters, netwerk) en de control plane zijn gegarandeerd volledig in de EU	**5. Volledige EU-operatie gegarandeerd** - De fysieke infrastructuur (datacenters, netwerk) en de control plane zijn gegarandeerd volledig in de EU. Wordt periodiek geaudit door een erkende EU partner
4.2 Exclusief Europees Personeel		**1. Geen controle personeel** - Beheerwerkzaamheden met privileged access worden volledig uitgevoerd door non-EU personeel, buiten Europa uitgevoerd, en zijn in dienst van een non-EU organisatie	**2. Beperkte controle personeel** - Beheerwerkzaamheden met privileged access worden deels uitgevoerd door non-EU personeel, buiten Europa uitgevoerd, maar zijn in dienst van een EU entiteit	**3. Controle personeel soevereine diensten -** Voor soevereine diensten is 100% van het personeel met privileged acces tot service infrastructuur en klantdata zijn ingezetenen en burger van de EU, fysiek werkzaam in Europa, onder Europees entiteit. Voor hoge uitzondering zoals kritieke specialistische ondersteuning kan een non-EU persoon worden ingeschakeld	**4. Volledige personele soevereiniteit beheer -** 100% van het personeel met privileged acces tot service infrastructuur en klantdata zijn ingezetenen en burger van de EU, fysiek werkzaam in Europa, onder Europees entiteit. Voor hoge uitzondering zoals kritieke specialistische ondersteuning kan een non-EU persoon worden ingeschakeld	**5. Volledige personele soevereiniteit beheer gegarandeerd -** 100% van het personeel met privileged acces tot service infrastructuur en klantdata zijn ingezetenen van de EU, fysiek werkzaam in Europa, onder Europees entiteit. Wordt periodiek geaudit door erkende EU-partner, daarmee gegarandeerd
4.3 Supply Chain Resilience		**1. Afwezig** - Geen strategie beschreven hoe om te gaan met supply chain disruptie	**2. Ad-hoc -** De clouddienstverlener beschikt over een initiële of gedeeltelijke strategie (data centers/ infrastructuur of diensten) om de afhankelijkheid van non-EU hardware en kritieke software te beperken en zo continuïteit van de dienstverlening te waarborgen in het geval van geopolitieke sancties of verstoringen in de supply chain	**3. Herhaalbaar gedocumenteerd -** De clouddienstverlener moet over een complete (datacenters, infrastructuur en diensten) gedocumenteerde strategie beschikken die herhaalbaar en auditeerbaar is om de afhankelijkheid van non-EU hardware en kritieke software te beperken en zo de continuïteit van de dienstverlening te waarborgen in het geval van geopolitieke sancties of verstoringen in de supply chain	**4. Systematisch -** De clouddienstverlener moet over een complete (datacenters, infrastructuur en diensten) gedocumenteerde strategie beschikken die regelmatig geaudit wordt door erkende Europese partij om de afhankelijkheid van non-EU hardware en kritieke software te beperken en zo de continuïteit van de dienstverlening te waarborgen in het geval van geopolitieke sancties of verstoringen in de supply chain	**5. Leidend -** De clouddienstverlener moet over een complete (datacenters, infra en diensten) gedocumenteerde strategie beschikken die geaudit is om de afhankelijkheid van non-EU hardware en kritieke software te beperken en zo de continuïteit van de dienstverlening aantoonbaar te waarborgen voor een minimaal afgesproken termijn in het geval van geopolitieke sancties of verstoringen in de supply chain

5.1 Training, Certificering en Screening		**1. Geen screening en training** - Onbekend opleidingsniveau; geen screening	**2. Beperkte screening en training -** Medewerkers zijn gescreend en getraind op eigen initiatief clouddienstverlener, maar niet gedocumenteerd of gepubliceerd	**3. Gedocumenteerde screening en training -** Medewerkers zijn gescreend en getraind op eigen initiatief clouddienstverlener, gedocumenteerd en eventueel gepubliceerd	**4. Controleerbare screening en training -** Medewerkers zijn gescreend en getraind op eigen initiatief clouddienstverlener, gedocumenteerd, gepubliceerd, en auditeerbaar door erkende Europese partij	**5. Gecontroleerde screening en training -** Medewerkers zijn gescreend en getraind op eigen initiatief clouddienstverlener, gedocumenteerd, gepubliceerd, en wordt periodiek geaudit door erkende Europese partij
5.2 Capaciteit en vaardigheden		**1. Volledig afhankelijk non-EU -** De clouddienstverlener beschikt enkel over interne non-EU capaciteit of is compleet afhankelijk van externe non-EU capaciteit voor het bouwen, beheren en doorontwikkelen van een (soevereine) cloudomgeving	**2. Beperkt EU capaciteit, sterk afhankelijk non-EU -** De clouddienstverlener beschikt beperkt over interne EU capaciteit voor kritieke beheer. Structurele (externe) non-EU ondersteuning is nodig voor bouw en doorontwikkeling	**3. Basis EU capaciteit, deels afhankelijk non-EU -** De clouddienstverlener beschikt over voldoende interne EU capaciteit voor bouw en beheer. Structurele (externe) non-EU ondersteuning is nodig voor doorontwikkeling	**4. Volwaardig EU cloudteam -** De clouddienstverlener beschikt over voldoende interne EU capaciteit voor bouw, beheer en doorontwikkeling	**5. Soevereine Cloud innovator EU met lokale (NL) ondersteuning -** De clouddienstverlener beschikt over vooroplopende interne EU capaciteit voor bouw, beheer en doorontwikkeling, met lokale (NL) capaciteit voor de bouw en het beheer

DEZE PAGINA IS OPZETTELIJK LEEG