

## WHITEPAPER AI & Soevereine Cloud. Juridische, Strategische & Technologische Criteria voor Nederland

### Introductie

Er is veel discussie over de afhankelijkheid van Amerikaanse Big Tech en de noodzaak van een soevereine cloud. Opmerkingen van wereldleiders tijdens het WEF (Davos, Feb 2026) zoals “*de wereldorde die wij kennen bestaat niet meer*” zetten veel bedrijven en overheidsinstanties aan het denken. En in mei 2025 verloor de hoofdprocureur van het Internationaal Strafhof (ICC), Karim Khan, toegang tot zijn officiële Microsoft-emailaccount nadat de VS sancties oplegden aan het ICC. Als gevolg van die sancties werd zijn e-mailaccount afgesloten. Veel Europese beleidsmakers en experts noemden de gebeurtenis een “wake-up call” voor digitale soevereiniteit omdat het laat zien dat de Amerikaanse wetgeving en geopolitieke besluiten direct invloed kunnen hebben op vitale Europese instellingen die op de Amerikaanse clouddiensten vertrouwen. Maar wat is nou eigenlijk ‘soevereine cloud’ precies?

### 1. “Soevereine cloud”: Definities & betekenis

#### Definitie

Een *soevereine cloud* is een cloudinfrastructuur en -dienst die zodanig georganiseerd is dat:

- **Data, verwerking en controle** binnen een specifieke jurisdictie blijven;
- De cloud **niet vatbaar is voor directe invloed of toegang door regeringen van derde landen (bijvoorbeeld de ‘Kill Switch’)**;
- De juridische, operationele en technische controle onder de controle valt van de overheid of entiteit binnen die jurisdictie.

In Europese context omvat dit doorgaans:

- **Datageografische soevereiniteit** — data wordt uitsluitend lokaal of binnen de EU opgeslagen en verwerkt;
- **Operationele autonomie en transparantie** — beheer, logging en sleutelbeheer zijn exclusief onder lokale of EU-jurisdictie;
- **Juridische bescherming** — de cloud is niet onderworpen aan buitenlandse wetten zoals de Amerikaanse *Cloud Act* of *Patriot Act*.

Deze definitie wordt ook veel gebruikt door overheidsinstellingen als uitgangspunt in beleidsdocumenten en tenderkaders.

### 2. Criteria voor een soevereine cloud — vanuit overheid & experts

De discussie over cloudsoevereiniteit richt zich op een combinatie van juridische, technische en operationele eisen.

#### 2.1 Juridische criteria

Een soevereine cloud moet:

- Vallen onder **EU- of nationale wetgeving** zonder extraterritoriale afdwingbaarheid van derde landen;
- Zich houden aan Europese rechten zoals de **AVG (GDPR)**;
- Bescherming bieden tegen bijvoorbeeld de *Cloud Act* of soortgelijke Amerikaanse wetgeving;
- Uitgesloten zijn van enige **buitenlandse overheidsinmenging** in data-toegang of operationele controle.

## 2.2 Data & locatie

- Data moet fysiek binnen Nederland/EU verblijven;
- Back-ups en disaster recovery moeten dezelfde data-lokaliteit garanderen;
- Geen replicatie naar landen buiten de EU zonder expliciete controle.

## 2.3 Operationele autonomie

- Lokale of EU-personeel met formele beheersrechten;
- Administratieve en technische controle over encryptie en sleutelbeheer (bijvoorbeeld BYOK : ‘Bring Your Own Key’);
- Realtime monitoring en auditing die onder Europese/juridische grenzen blijft;
- Geen operationele afhankelijkheden van buitenlandse infrastructuurcomponenten.

## 2.4 Technologische onafhankelijkheid

- Open standaarden en interoperabiliteit om *vendor lock-in* te vermijden;
- Transparante supply chains voor hardware en software;
- Mogelijkheid tot vrije inspectie van code en infrastructuurcomponenten;
- Een architectuur die *vendor neutrality* ondersteunt.

## 2.5 Governance & compliance

- Certificeringen onder EU-standaarden;
- Transparante compliance frameworks met toezicht door lokale toezichthouders;
- Bescherming tegen toegang op basis van buitenlandse gerechtelijke bevelen.

### **Kerncriteria samengevat:**

*Jurisdiction, Data Residency, Operational Control, Technological Transparency & Legal Immunity.*

## 3. Amerikaanse Big Tech & Soevereine Cloud: Voldoet het?

### 3.1 ESG-juridische zorgen: Patriot Act & Cloud Act

Nederland en EU-experts zijn bezorgd over de Amerikaanse wetten zoals de *Cloud Act* of de *Patriot Act* die de Amerikaanse overheid onder bepaalde omstandigheden toegang kan geven tot data van Amerikaanse bedrijven, ook als die data fysiek buiten de VS staat. Dit wordt vaak gezien als **juridische exposure voor EU-data**.

### 3.2 Hyperscalers proberen soevereiniteit te bieden

Ondanks beleidskritiek hebben Amerikaanse hyperscalers **souvereine cloud-varianten gelanceerd**:

- Amazon Web Services biedt een “European Sovereign Cloud” die volledig door EU-burgers wordt bediend onder EU-wetgeving.
- Daarbij beloven deze initiatieven dat operationele controle volledig aan EU-wetgeving wordt onderworpen en toegankelijk is door EU-bedrijven/werkers.

### 3.3 Kritische evaluatie

Hoewel deze initiatieven **verhoogde lokale governance** kunnen bieden, is er kritiek:

- Nog steeds blijft de onderliggende corporate & juridische structuur van Amerikaanse techgiganten afkomstig uit de VS, wat mogelijk juridische blootstelling inhoudt;
- Transparantie en onafhankelijke audits zijn vaak beperkter dan vereist door strikte soevereiniteitscriteria;
- Sommige experts betwijfelen of deze cloud aanbieders werkelijk onafhankelijk zijn van de moederorganisatie of Amerikaanse wetgeving.

**Conclusie:** Amerikaanse hyperscalers kunnen tegemoetkomen aan sommige criteria, vooral technisch en operationeel, maar blijven juridisch en structureel kwetsbaar voor beleidsrisico's vanuit de VS, wat door veel burgers, experts en beleidsmakers als problematisch wordt gezien.

## 4. Europese & Nederlandse markt: echte soevereine cloudproviders

Er zijn verschillende Europese/ Nederlandse partijen en initiatieven die inspelen op cloudsoevereiniteit:

### 4.1 Europees Cloud Sovereignty Framework

De Europese Commissie werkt aan een **Cloud Sovereignty Framework** dat 8 concrete doelen definieert voor soevereiniteitsmeting en inzet binnen EU-instellingen.

### 4.2 Europese/cloud-native initiatieven

- Diverse **EU-cloud oplossingen** worden ontwikkeld met volledige data residency en operationele autonomie;
- Europese samenwerkingsverbanden zoals het CISPE *Sovereign Cloud Manifesto* stimuleren onafhankelijke cloudinfrastructuur zonder buitenlandse invloed.

### 4.3 Nederlandse initiatieven

- Rijksoverheid pleit voor een uniforme definitie en instrumenten om soevereiniteit te operationaliseren.

- Kamerdebatten in de Tweede Kamer richten zich op het verminderen van afhankelijkheid van Amerikaanse Big Tech.

## 5. Conclusie. Kansen en risico's voor Nederland en Europa

Aspect	Status / Interpretatie
Definitie van soevereine cloud	Nog in ontwikkeling binnen EU en NL beleid; politieke consensus groeit. Proces duurt lang maar zal belangrijke basis vormen voor groei.
Juridische risico's	Amerikaanse wetten geven aanleiding tot bezorgdheid; onafhankelijkheid blijft politiek aandachtspunt.
Hyperscaler initiatieven	Proactieve bewegingen naar "EU sovereign cloud" maar met gemengde beoordelingen.
Europese markt	Actieve ontwikkeling van volledig Europese cloudalternatieven en frameworks.
Nederlandse context	Beleidsdruk om de afhankelijkheid van grote Amerikaanse Tech te verminderen groeit significant.

### Samenvatting

De beweging naar soevereine cloud is zowel een **juridisch als strategisch verschuivingspunt** voor Nederland en Europa. Hoewel Amerikaanse hyperscalers stappen zetten naar Europese soevereine oplossingen, blijft er discussie over of deze voldoen aan alle soevereiniteitscriteria. Europese en Nederlandse initiatieven blijven cruciaal om echte autonomie te bereiken zonder blootstelling aan Amerikaanse wet- en regelgeving.

### Kan AI in een soevereine cloud?

Nederlandse burgers, bedrijven en overheden *kunnen* AI gebruiken binnen een soevereine cloud, maar het is op dit moment **nog niet volledig realiseerbaar voor alle lagen van de AI-stack**. Sommige lagen worden sterk gedomineerd door Amerikaanse Big Tech; andere zijn beter te *sovereïnisieren* met Europese of open oplossingen.

### AI Technology Stack & Soevereiniteit. Een 'Level-by-Level' analyse

Voor een fundamentele analyse gebruiken we 6 lagen in de AI Technology Stack:

1. Compute (GPU / Accelerators)
2. Model Usage (Tokens / API Calls)
3. Data & Vector Storage
4. Network & Data Egress
5. Orchestration & Agent Frameworks

## 6. Governance, Monitoring & Tooling

### Layer 1 'Compute' (GPU / Accelerators)

#### Omschrijving:

Fysieke rekenkracht (CPU/GPU/TPU), data-centers, hardware.

#### Is er soevereine optie?

Ja, maar wel beperkt.

#### Europese/sovereign alternatieven:

- **European HPC/AI clusters:** Sommige EU initiatieven bouwen & financieren high-performance AI-clusters binnen EU-jurisdictie.
- **Nederlandse onderzoeksinfrastructuur:** SURF, NL-e-Science centraal, Netherlands eInfrastructure for HPC.

#### Beperkingen

- High-end GPU-accelerators (zoals NVIDIA / AMD) worden *wereldwijd verkocht* maar de supply chain en hardware zijn niet volledig EU-onder controle. Kortom, geen volledige technologische onafhankelijkheid van Amerikaanse hardware.

**Conclusie t.a.v. sovereign check:** Het is *gedeeltelijk mogelijk*. We kunnen AI compute *binnen EU* draaien, maar de afhankelijkheid van externe hardware leveranciers blijft groot.

### Layer 2 'Model Usage' (Tokens / API Calls)

#### Omschrijving:

Het draaien van AI-modellen, inferentie, prompts, API-calls.

#### Big Tech dominantie is significant:

- OpenAI (GPT)
- Anthropic
- Google Cloud
- Microsoft Azure

Deze zijn *wereldwijd leidend* en zeer sterk gepositioneerd in de AI inference-markt.

#### EU Soevereine alternatieven

- **Open Source LLMs** ("GPT-like") draaien volledig binnen de eigen cloud-omgeving (bijv. LLaMA-achtige modellen)
- **EU/European modelinitiatieven**
  - Voorbeelden: Duitse/Franse nationale AI-modellen, EU-gefinancierde taalmodellen
  - Doel: *Model training & inference binnen EU jurisdictie, met opensourced control*

## **Beperkingen**

- Open modellen missen soms schaal en performance van de Big Tech-modellen.
- Veel bedrijven gebruiken Big Tech API's omdat ze "state-of-the-art" zijn wat de afhankelijkheid verder vergroot.

### **Conclusie:**

*Soeverein gebruik van AI-modellen is mogelijk met open source en EU-modellen maar er is een prestatiekloof met Big Tech.*

## **Layer 3 'Data & Vector Storage'**

### **Omschrijving:**

Opslag van embeddings, databases, kennisrepliatie.

### **EU/sovereign opties**

- EU-cloud providers met vector database ondersteuning
- Eigen implementatie van vector stores (bijv. Milvus, Weaviate) binnen de EU-regio
- Data Encryptie & Key Management kan volledig lokaal

### **Beperkingen**

- De technologie zelf kan open en EU-hosted zijn, *maar* connecties met AI-modellen buiten EU moeten beveiligd/gescheiden worden.

### **Conclusie:**

Volledig soeverein mogelijk, vector opslag hoeft niet afhankelijk te zijn van Big Tech.

## **Layer 4 'Network & Data Egress'**

**Omschrijving:** Communicatie, dataverkeer, egress fees, latency-routing.

### **EU opties:**

- Lokale Europese connectivity
- Geen datatransfer buiten EU-regio's
- Eigen interconnects

### **Beperkingen:**

- Als AI-services buiten EU lopen → data-kopieën of inference-calls kunnen extern verkeer veroorzaken.

### **Conclusie:**

Netwerk & Data Egress kan soeverein *mits* alle bijbehorende services binnen de EU blijven.

## **Layer 5 'Orchestration & Agent Frameworks'**

**Omschrijving:**

Tools die AI-workflows orkestreren.

**EU/Souvereine alternatieven:**

- Open source workflow engines beschikbaar (Apache Airflow, Kubeflow, Argo, etc.)
- EU-gehoste AI orchestration platforms
- Zelf ontwikkelde frameworks

**Conclusie:**

*Volledig soeverein te implementeren met bijvoorbeeld open source tools.*

**Layer 6 ‘Governance, Monitoring & Tooling’****Omschrijving:**

Security, observability, cost analytics, compliance dashboards.

**EU/sovereign tools:**

- Open source monitoring (Prometheus, Grafana, ELK stack)
- Eigen policy, logging, SIEM tools
- EU certificerings- en audit-frameworks

**Conclusie:**

*Dit is volledig soeverein mogelijk.*

**Korte samenvatting per laag in de AI-Technology Stack**

Laag	Souverein mogelijk?	Opmerkingen
1. Compute	Beperkt/Partial	Hardware supply chain blijft (te) afhankelijk
2. Models	Mogelijk via open/EU modellen	Big Tech domineert commerciële AI
3. Data/Vector	Ja	EU-gehost en controleerbaar
4. Network	Ja	EU-only routing mogelijk
5. Orchestration	Ja	Open solutions bestaan (maar niet altijd gewenst)
6. Governance	Ja	Open/EU tooling beschikbaar

## Zijn er serieuze alternatieven voor Big Tech per laag in de AI Stack?

AI Stack Layer	Alternatieven (EU/souverein)
1 – Compute	→ EU-HPC clusters, nationale GPU pools; maar nog hardware afhankelijk
2 – Models	→ Open-source LLM's (Meta, EleutherAI, Mistral, BLOOM, etc), EU-modelleringen
3 – Data/Vector	→ Milvus, Weaviate, Qdrant binnen EU Cloud
4 – Network	→ EU-only egress, private networks
5 – Orchestration	→ Airflow, Kubeflow, Argo
6 – Governance/Monitoring	→ Grafana, ELK, OpenPolicyAgent, native EU tools

## Waar liggen de belangrijkste uitdagingen voor Europa en NL?

### 1. Modelprestaties versus Soevereiniteit

- Big Tech levert momenteel betere prestaties en schaal dan open/EU modellen.
- Nederlandse bedrijven moeten prioriteren: *performance versus soevereiniteit*.

### 2. Hardware Ketens

- Hardware (GPU/accelerators) komt overwegend uit de VS/Asia Tech-chain. Dit heeft juridisch en supply chain-risico's.

### 3. Integratie & Governance

- Soevereine setup vereist eigen governance, certificering en onderhoud (meer personele inspanning).

## Conclusies

Er *bestaan* soevereine alternatieven voor de meeste lagen van de AI-stack. Maar **Layer 1 ('Compute')** en **Layer 2 ('Models')** zijn momenteel het meest afhankelijk van Amerikaanse Big Tech of opkomende externe innovatie.

De andere lagen in de AI Stack, zoals Data, Network, Orchestration en Governance *kan volledig en goed binnen EU worden gehouden*.

Aanbevelingen voor Nederlandse burgers & bedrijven t.a.v. strategische roadmap:

1. **Inventariseer data die soeverein moet blijven** (niet alle data hoeft soeverein, classificeer en segmenteer).
2. **Use case selectie**. Waarvoor is performance essentieel versus waar volstaat open source/EU modellen?

3. **Eigen of EU-Compute pools.** Bouw/ Participeer in een gezamenlijke GPU-infrastructuur.
4. **Open model adoptie.** Train & draai modellen binnen de EU.
5. **Governance & compliance first.** “EU-only” logging, observability & SIEM.
6. **Certificering en audit.** Voldoen aan de EU cloud sovereignty compliance.

Afsluitend kunnen Nederlandse burgers, bedrijven en overheidsinstanties in principe AI binnen een soevereine cloud stack realiseren maar alleen als ze kritisch zijn op architectuur, modellen en infrastructuur.

T.a.v. 2 lagen in de AI Stack (kernmodellen, Compute/HW) zijn de services van Amerikaanse Big Tech nog steeds zeer dominant, maar er bestaan serieuze EU-alternatieven die nu snel volwassen worden.