



Ministerie van Sociale Zaken en
Werkgelegenheid

Soevereiniteitsscore SZW|DSU

Versienummer 1.1

Datum	15 oktober 2026
Status	Definitief

Inhoud

1	Soevereiniteitsscore SZW DSU—1
2	SOV-1: Strategische Soevereiniteit—2
2.1	Locatie van beslissingsbevoegdheden—2
2.2	Waarborgen tegen wijziging van controle—2
2.3	Afhankelijkheid van EU-financiering—3
2.4	Investerings, banen en waardecreatie binnen de EU—3
2.5	Betrokkenheid bij EU-initiatieven—3
2.6	Vermogen om veilige bedrijfsvoering te handhaven—4
3	SOV-2: Juridische en Jurisdictionele Soevereiniteit—5
3.1	Toepasselijk nationaal rechtssysteem—5
3.2	Blootstelling aan niet-EU wetten met grensoverschrijdende reikwijdte—5
3.3	Bestaande kanalen voor gedwongen toegang door niet-EU autoriteiten—6
3.4	Toepasbaarheid van internationale regimes—6
3.5	Locatie van intellectueel eigendom—7
4	SOV-3: Soevereiniteit over Gegevens en AI—8
4.1	Controle over cryptografische toegang—8
4.2	Zichtbaarheid en controleerbaarheid van gegevenstoegang—8
4.3	Geografische beperking van opslag en verwerking—9
4.4	EU-controle over AI-modellen en datapijplijnen—9
5	SOV-4: Operationele Soevereiniteit—10
5.1	Migratie van workloads—10
5.2	Capaciteit voor EU-operators—10
5.3	EU-gebaseerd talentpool—11
5.4	Locatie en juridisch kader van operationele ondersteuning—11
5.5	Beschikbaarheid van documentatie en broncode—11
6	SOV-5: Soevereiniteit van de Toeleveringsketen—13
6.1	Locatie en juridische controle van kritische leveranciers—13
6.2	Geografische oorsprong van hardware—13
6.3	Jurisdictie en herkomst van embedded code/firmware—14
6.4	Oorsprong van software—14
6.5	Afhankelijkheid van niet-EU leveranciers—15
6.6	Zichtbaarheid in de toeleveringsketen—15
7	SOV-6: Technologische Soevereiniteit—16
7.1	Interoperabiliteit via open standaarden—16
7.2	Open licentiemodel—16
7.3	Zichtbaarheid in ontwerp en werking—17
7.4	EU-onafhankelijkheid in high-performance computing—17
8	SOV-7: Soevereiniteit op het gebied van Veiligheid en Compliance—18
8.1	Certificeringen—18
8.2	Naleving van EU-regelgeving—18
8.3	Locatie van Security Operations Centers (SOCs)—19
8.4	Transparante rapportage van inbreuken op veiligheid—19
8.5	Onafhankelijke veiligheids- en nalevingsaudits—19

9	SOV-8: Milieuduurzaamheid—21
9.1	Adoptie van energie-efficiënte infrastructuur—21
9.2	Circulaire economie-praktijken—21
9.3	Transparante meting en openbaarmaking—22
9.4	Inkoop van hernieuwbare energie—22

1 Soevereiniteitsscore SZW|DSU

Vanuit het [Cloud Sovereignty Framework](#) van de Europese Commissie is er een rekenmethode beschreven om te komen tot een soevereiniteitsscore, die daarmee te vertalen is naar het desbetreffende SEAL-niveau. Met behulp van een externe partner van SZW|DSU zijn de 'contributing factors' vertaald naar concrete vragen en antwoorden om de score te bepalen (zie hoofdstuk 2). Elk soevereiniteitsonderwerp heeft een specifieke weging, hierin is de weging vanuit het Cloud Sovereignty Framework aangehouden. In onderstaande tabel is de totale score weergegeven per onderwerp, met het bijbehorende soevereiniteitsniveau.

Omschrijving	Weging	Score	SEAL-niveau
SOV-1: Strategische Soevereiniteit	15%	2,67	SEAL-3
SOV-2: Juridische en jurisdictionele Soevereiniteit	10%	2,60	SEAL-3
SOV-3: Soevereiniteit over Gegevens en AI	10%	3,00	SEAL-3
SOV-4: Operationele Soevereiniteit	15%	2,60	SEAL-3
SOV-5: Soevereiniteit van de Toeleveringsketen	20%	2,33	SEAL-2
SOV-6: Technologische Soevereiniteit	15%	2,50	SEAL-3
SOV-7: Soevereiniteit op het gebied van Veiligheid en Compliance	10%	2,80	SEAL-3
SOV-8: Milieuduurzaamheid	5%	2,75	SEAL-3
Totaal	100%	2,61	SEAL-3

Met behulp van deze berekening komt SZW|DSU uit op niveau SEAL-3. In hoofdstuk 2 wordt dieper ingegaan op de antwoorden van SZW|DSU en daarmee op de onderbouwing. Het antwoord van SZW|DSU op de vraagstelling is **oranje** gemarkeerd.

De score is tot stand gekomen door verschillende experts afzonderlijk antwoord te geven op de vragen en vervolgens gezamenlijk tot consensus te komen. Hierbij is onderstaande tabel gebruikt, waarbij het SEAL-niveau gelijk staat aan een score.

SEAL-niveau	Score
SEAL-0	0
SEAL-1	1
SEAL-2	2
SEAL-3	3
SEAL-4	4

2 SOV-1: Strategische Soevereiniteit

Beschrijving: Strategische soevereiniteit meet in hoeverre de diensten van een cloudprovider (of technologische actor) verankerd zijn binnen het juridische, financiële en industriële ecosysteem van de Europese Unie. Het beoordeelt de stabiliteit van eigendom, invloedsmogelijkheden op governance en afstemming met EU-strategische prioriteiten.

2.1 Locatie van beslissingsbevoegdheden

Vraag: Waar zijn de uiteindelijke beslissingsorganen (bijv. Raad van Bestuur, Directie) met beslissende bevoegdheid over de cloudservice primair gevestigd?

SEAL-niveau	Antwoord
SEAL-0	Exclusief buiten de EU gevestigd.
SEAL-1	Primair buiten de EU gevestigd, met een symbolische, niet-uitvoerende EU-adviserende raad.
SEAL-2	De cloudservice-entiteit heeft een geregistreerde EU-dochteronderneming, maar finale strategische beslissingen berusten bij de niet-EU moedermaatschappij.
SEAL-3	Belangrijke operationele en managementbeslissingen worden gecontroleerd door een in de EU gevestigde entiteit, waarbij strategische beslissingen EU-juridische naleving vereisen.
SEAL-4	Alle organen met beslissende juridische en operationele bevoegdheid zijn exclusief gevestigd binnen een EU-lidstaat.

2.2 Waarborgen tegen wijziging van controle

Vraag: Welke juridische en contractuele waarborgen zijn er om een wijziging van controle (bijv. overname) die de EU-soevereiniteit in gevaar zou brengen, te voorkomen of te mitigeren?

SEAL-niveau	Antwoord
SEAL-0	Geen specifieke juridische/contractuele beschermingen; wijziging van controle kan doorgaan zonder EU-goedkeuring.
SEAL-1	Contractuele clausules vereisen melding van een wijziging van controle, maar de klant heeft geen recht om bezwaar te maken of het contract te beëindigen.
SEAL-2	Contractuele rechten stellen onmiddellijke beëindiging en gegevensoverdracht mogelijk in geval van een overname door een niet-EU entiteit.
SEAL-3	Governance-afspraken geven EU-klanten/autoriteiten een voorkeursrecht of vetorecht op elke wijziging van controle die beslissende bevoegdheid buiten de EU verplaatst.
SEAL-4	De service is zodanig gestructureerd (bijv. als stichting of publiek-private entiteit) dat het juridisch onmogelijk is voor elke niet-EU entiteit om beslissende controle te verkrijgen.

2.3 Afhankelijkheid van EU-financiering

Vraag: Wat is de primaire geografische herkomst van de eigen vermogens-, schuld- en belangrijkste investeringsfinanciering van de cloudprovider?

SEAL-niveau	Antwoord
SEAL-0	Exclusief afhankelijk van niet-EU financieringsbronnen (bijv. buitenlandse staatsfondsen, niet-EU banken).
SEAL-1	Overwegend niet-EU financiering, met minimale startfinanciering of schulden afkomstig van EU-gevestigde instellingen.
SEAL-2	Een aanzienlijk deel (bijv. 30-50%) van de financiering komt van institutionele of private EU-investeerders.
SEAL-3	Meerderheid (bijv. meer dan 50%) van de financiering is afkomstig van EU-kapitaalmarkten, financiële instellingen of EU-gevestigde entiteiten.
SEAL-4	Exclusief gefinancierd en gekapitaliseerd door EU-entiteiten, wat financiële en politieke onafhankelijkheid waarborgt.

2.4 Investerings, banen en waardecreatie binnen de EU

Vraag: Welk percentage van de totale O&O-investeringen, hoogwaardige banen en algehele economische waardecreatie van de cloudservice blijft binnen de EU?

SEAL-niveau	Antwoord
SEAL-0	Minder dan 5% van O&O en hoogwaardige creatie/banen zijn gevestigd binnen de EU.
SEAL-1	Minder dan 20% van O&O en banen zijn in de EU, voornamelijk in niet-kritische verkoop- of basis ondersteuningsfuncties.
SEAL-2	Tussen 20% en 50% van de waardeketen, inclusief enige O&O, is gebaseerd in de EU, wat betekenisvolle EU-werkgelegenheid creëert.
SEAL-3	Meer dan 50% van O&O, kernplatformontwikkeling en hoogwaardige banen zijn verankerd in de EU.
SEAL-4	Bijna 100% van alle O&O, software-architectuur en hoogwaardige banencreatie zijn gevestigd en gehandhaafd binnen de EU.

2.5 Betrokkenheid bij EU-initiatieven

Vraag: Hoe is de provider actief betrokken bij en afgestemd op sleutelinitiatieven van de EU (bijv. Gaia-X, EU Chip Act, Green Deal-doelstellingen)?

SEAL-niveau	Antwoord
SEAL-0	Geen deelneming of uitgesproken afstemming met EU-strategische digitale of industriële doelen.
SEAL-1	Minimale deelneming (bijv. incidentele aanwezigheid bij EU-evenementen), met afstemming die wel wordt verkondigd maar niet aantoonbaar is geïmplementeerd.

SEAL-2	Actief lidmaatschap en toewijding aan kern-EU-initiatieven (bijv. Gaia-X), met eerste stappen naar afstemming.
SEAL-3	Diepgaande, structurele betrokkenheid bij en toewijding aan EU-strategische programma's, met bewezen toewijding via concrete investeringen en implementatieplannen.
SEAL-4	Leidende rol in het vaststellen van normen en doelstellingen voor EU-soevereiniteitsinitiatieven, met volledige, onafhankelijk controleerbare afstemming.

2.6 Vermogen om veilige bedrijfsvoering te handhaven

Vraag: Welke mechanismen zijn er om de continuïteit van de service te waarborgen als de niet-EU moedermaatschappij of externe autoriteit eist dat de service wordt opgeschort of de ondersteuning wordt ingetrokken?

SEAL-niveau	Antwoord
SEAL-0	Geen mechanisme; de niet-EU moedermaatschappij kan de service onmiddellijk beëindigen.
SEAL-1	Een juridisch kader (bijv. escrow-overeenkomst) voorziet in een korte wachttijd (bijv. 90 dagen) voor beëindiging.
SEAL-2	Volledige technische documentatie en operationele procedures worden in escrow gehouden door een EU-entiteit, waardoor een overname door een EU-operator in een crisis mogelijk is.
SEAL-3	De EU-exploitatie-entiteit beschikt over de nodige licenties, broncode en autonome operationele capaciteit om de service onbepaald door te laten gaan zonder ondersteuning van de niet-EU leverancier.
SEAL-4	Het in de EU gevestigde operationele team behoudt volledige, onafhankelijke controle over alle code, infrastructuur en licenties, waardoor het inherent veerkrachtig is tegen niet-EU-bemoeienis.

3 SOV-2: Juridische en Jurisdictionele Soevereiniteit

Beschrijving: Juridische en jurisdictionele soevereiniteit evalueert de juridische omgeving, blootstelling aan buitenlandse autoriteiten en afdwingbaarheid van rechten die de diensten van een technologische aanbieder regelen. Het bepaalt in hoeverre de diensten verankerd zijn in de Europese jurisdictie en afgeschermd zijn tegen externe juridische claims.

3.1 Toepasselijk nationaal rechtssysteem

Vraag: Welk nationaal rechtssysteem regelt het kern-dienstverleningscontract en de bedrijfsvoering van de aanbieder binnen de EU?

SEAL-niveau	Antwoord
SEAL-0	Het contract en de bedrijfsvoering vallen onder niet-EU recht (bijv. VS, China).
SEAL-1	Het contract valt onder EU-recht, maar de uiteindelijke bedrijfsvoering van de aanbieder valt onder niet-EU recht.
SEAL-2	Zowel het contract als de directe exploitatie-entiteit vallen onder EU-recht, maar de upstream leverancier/moedermaatschappij is niet-EU.
SEAL-3	De contracterende entiteit en alle kritische bedrijfsvoering vallen onder het recht van een EU-lidstaat, met beperkte niet-EU juridische invloed.
SEAL-4	Alle contracten en bedrijfsvoering vallen exclusief onder het recht van een EU-lidstaat, zonder concurrerende juridische claims.

3.2 Blootstelling aan niet-EU wetten met grensoverschrijdende reikwijdte

Vraag: Wat is de blootstelling van de gegevens en systemen aan verplichte toegang tot gegevensverzoeken krachtens niet-EU wetgeving met extraterritoriale reikwijdte (bijv. Amerikaanse CLOUD Act, Chinese Cybersecurity Law)?

SEAL-niveau	Antwoord
SEAL-0	Hoge blootstelling, omdat de aanbieder direct onder niet-EU recht valt en klantgegevens worden opgeslagen/verwerkt door een niet-EU entiteit.
SEAL-1	Matige blootstelling; hoewel gegevens in de EU worden opgeslagen, betekent de eigenaarsstructuur van de aanbieder dat deze moet voldoen aan niet-EU juridische verzoeken.
SEAL-2	Lage blootstelling; de aanbieder heeft juridische en technische waarborgen geïmplementeerd om niet-EU verzoeken aan te vechten, maar naleving is nog steeds mogelijk in specifieke scenario's.
SEAL-3	Minimale blootstelling; de service wordt uitgevoerd door een onafhankelijke EU-entiteit die juridisch is gestructureerd om niet-EU verzoeken af te wijzen en te bestrijden, met een publieke toezegging tot niet-naleving.

SEAL-4	Nul blootstelling; de service is juridisch en technisch afgeschermd van alle grensoverschrijdende niet-EU juridische regimes, waardoor naleving onmogelijk is zonder een EU-rechterlijk bevel.
---------------	--

3.3 Bestaande kanalen voor gedwongen toegang door niet-EU autoriteiten

Vraag: Welke bestaande kanalen (juridisch, contractueel of technisch) zijn er waarlangs niet-EU autoriteiten gedwongen toegang tot klantgegevens kunnen afdwingen?

SEAL-niveau	Antwoord
SEAL-0	Meerdere, directe juridische en technische kanalen bestaan, inclusief verplichte verstrekking van decoderingssleutels aan de niet-EU moedermaatschappij.
SEAL-1	Indirecte juridische kanalen bestaan via de niet-EU moedermaatschappij, maar contractuele/technische controles vereisen dat de moedermaatschappij formele procedures gebruikt.
SEAL-2	Geen contractuele achterdeuren; toegang vereist formele juridische procedures en de EU-exploitatie-entiteit beheert de versleutelingssleutels.
SEAL-3	Technisch ontwerp gebruikt "Zero-Knowledge"-principes, waardoor alleen de klant de cryptografische sleutel bezit en toegang onmogelijk is, zelfs bij een niet-EU juridisch verzoek.
SEAL-4	Volledige digitale soevereiniteit: dergelijke kanalen bestaan niet en het systeem is ontworpen om alle gedwongen toegang door niet-EU partijen te voorkomen, gegarandeerd door een vertrouwde EU-derde partij.

3.4 Toepasbaarheid van internationale regimes

Vraag: Hoe worden internationale regimes (bijv. exportcontrole, handelsbeperkingen) aangepakt met betrekking tot de overdracht en het gebruik van de onderliggende technologie van de service?

SEAL-niveau	Antwoord
SEAL-0	De technologie valt onder verplichte niet-EU exportcontroles, die het gebruik door EU-klanten kunnen beperken.
SEAL-1	De aanbieder beheert de naleving van exportcontrole, maar de mogelijkheid dat een niet-EU autoriteit het gebruik beperkt, blijft bestaan.
SEAL-2	Contractuele voorwaarden garanderen voortgezet servicegebruik ondanks niet-EU exportcontroles, met gebruik van EU-gebaseerde technologie waar mogelijk.
SEAL-3	De technologiестack is grotendeels gebaseerd op door de EU ontwikkelde componenten die aantoonbaar buiten de reikwijdte van beperkende niet-EU regimes vallen.
SEAL-4	Alle onderliggende technologie, inclusief kritische componenten, is vrij van niet-EU internationale beperkingen en wordt volledig gecontroleerd en overgedragen binnen de EU.

3.5 Locatie van intellectueel eigendom

Vraag: Waar wordt het kritieke intellectuele eigendom (IE) voor de cloudservicetechnologie gecreëerd, juridisch geregistreerd en ontwikkeld?

SEAL-niveau	Antwoord
SEAL-0	Het IE wordt volledig buiten de EU gecreëerd, geregistreerd en ontwikkeld.
SEAL-1	Het IE wordt buiten de EU gecreëerd en ontwikkeld, maar een licentie om het te gebruiken wordt gehouden door de EU-exploitatie-entiteit.
SEAL-2	Belangrijke ontwikkeling vindt plaats in de EU, maar het juridische eigendom en de registratie van het IE blijven bij de niet-EU moedermaatschappij.
SEAL-3	De EU-exploitatie-entiteit bezit de IE-rechten voor de serviceversie die in de EU wordt aangeboden, en de kernontwikkeling vindt plaats in de EU.
SEAL-4	Het kritieke IE wordt voor 100% gecreëerd, juridisch geregistreerd en ontwikkeld binnen de EU-jurisdictie.

4 SOV-3: Soevereiniteit over Gegevens en AI

Beschrijving: Soevereiniteit over gegevens en AI richt zich op de bescherming, controle en onafhankelijkheid van data-assets en AI-diensten binnen de EU. Het behandelt hoe gegevens worden beveiligd, waar ze worden verwerkt, en de mate van autonomie die klanten behouden over AI-mogelijkheden.

4.1 Controle over cryptografische toegang

Vraag: Wie heeft de effectieve controle over de cryptografische sleutels die nodig zijn om toegang tot en ontcijfering van klantgegevens mogelijk te maken?

SEAL-niveau	Antwoord
SEAL-0	De aanbieder of zijn niet-EU moedermaatschappij bezit alle hoofdsleutels voor versleuteling en kan toegang tot gegevens verkrijgen zonder actie van de klant.
SEAL-1	De aanbieder beheert de sleutels maar verbindt zich ertoe deze alleen te gebruiken bij een geldig juridisch verzoek; de controle van de klant is beperkt tot versleuteling op applicatieniveau.
SEAL-2	De klant kan eigen sleutels meenemen en beheren (BYOK), maar de aanbieder behoudt indirecte controle over het sleutelbeheersysteem (KMS) of de hoofdsleutel.
SEAL-3	De klant heeft volledige controle over de hoofdsleutels (KMS) en cryptografische toegang, waardoor toegang door de aanbieder technisch onmogelijk is zonder toestemming van de klant.
SEAL-4	Het systeem handhaaft "Confidential Computing", waarbij gegevens ook tijdens verwerking versleuteld zijn en alleen de klant de sleutel beheert, gecertificeerd door een onafhankelijke EU-auditor.

4.2 Zichtbaarheid en controleerbaarheid van gegevenstoegang

Vraag: Wat is het niveau van klantenzichtbaarheid en controleerbare verzekering met betrekking tot gegevenstoegang, AI-modelgebruik en onomkeerbare gegevensverwijdering?

SEAL-niveau	Antwoord
SEAL-0	Geen zichtbaarheid of auditlogs worden aan de klant verstrekt; bevestiging van gegevensverwijdering is een eenvoudige verklaring.
SEAL-1	Basis auditlogs tonen interne toegang door de aanbieder, maar gedetailleerde informatie over "wie, wanneer, waar" is beperkt; bevestiging van gegevensverwijdering is niet controleerbaar.
SEAL-2	Uitgebreide auditlogs worden verstrekt voor alle toegang (klant/aanbieder) en gegevensverwijdering wordt contractueel gegarandeerd, maar verificatie is nog steeds door de aanbieder bevestigd.
SEAL-3	Volledige, realtime controleerbaarheid van alle gegevens- en AI-modelgebruik door klant/EU-autoriteit, met controleerbaar,

	cryptografisch verzekerd bewijs van onomkeerbare gegevensvernietiging.
SEAL-4	Volledige transparantie via open-source logging tools en onafhankelijke verificatie door een EU-derde partij, wat onveranderlijke auditsporen en aantoonbaar onomkeerbare gegevensvernietiging waarborgt.

4.3 Geografische beperking van opslag en verwerking

Vraag: Waar wordt gegarandeerd dat de gegevens van de klant worden opgeslagen en verwerkt, inclusief alle back-ups en rampherstel-failovers?

SEAL-niveau	Antwoord
SEAL-0	Gegevens worden opgeslagen en verwerkt buiten de EU, of kunnen naar een niet-EU regio worden verplaatst zonder kennisgeving.
SEAL-1	Gegevens worden primair opgeslagen in de EU, maar back-ups of rampherstel-failovers kunnen in niet-EU jurisdicties plaatsvinden.
SEAL-2	Opslag en verwerking van gegevens zijn strikt beperkt tot de EU, maar niet-EU-medewerkers kunnen op afstand toegang krijgen tot gegevens voor ondersteuning.
SEAL-3	Alle gegevensopslag en -verwerking, inclusief alle back-up- en rampherstelsites, zijn exclusief beperkt tot jurisdicties van EU-lidstaten.
SEAL-4	Alle gegevensopslag en -verwerking is juridisch en technisch beperkt tot EU-eigendom en EU-geëxploiteerde faciliteiten binnen de EU, met de mogelijkheid om de geografische locatie te verifiëren.

4.4 EU-controle over AI-modellen en datapijplijnen

Vraag: Wat is het niveau van EU-controle over de gehele levenscyclus van AI-modellen (ontwikkeling, training, hosting, governance) die binnen de service worden gebruikt?

SEAL-niveau	Antwoord
SEAL-0	AI-modellen en pijplijnen worden volledig ontwikkeld, getraind en beheerd door niet-EU entiteiten op niet-EU stacks.
SEAL-1	AI-modellen worden getraind op EU-gegevens binnen de EU, maar de kern AI-framework/technologiestack is niet-EU eigendom.
SEAL-2	AI-modellen worden ontwikkeld, getraind en gehost in de EU, maar ze zijn afhankelijk van niet-EU-gecontroleerde fundamentele modellen of softwareafhankelijkheden.
SEAL-3	De volledige AI-levenscyclus (ontwikkeling, training, hosting en governance) staat onder controle van een EU-entiteit, met overwegend door de EU ontwikkelde open-sourcetechnologie.
SEAL-4	AI-modellen en datapijplijnen worden exclusief ontwikkeld, getraind, gehost en beheerd door EU-entiteiten op een door de EU gecontroleerde, volledig controleerbare technologiestack.

5 SOV-4: Operationele Soevereiniteit

Beschrijving: Operationele soevereiniteit meet het praktische vermogen van EU-actoren om een technologie onafhankelijk van buitenlandse controle te runnen, te ondersteunen en te laten evolueren. Het richt zich op continuïteit van bedrijfsvoering, beschikbaarheid van vaardigheden en veerkracht tegen externe afhankelijkheden.

5.1 Migratie van workloads

Vraag: In hoeverre vergemakkelijkt de cloudservice-architectuur de migratie van workloads naar alternatieve door de EU gecontroleerde cloudoplossingen of de integratie daarmee?

SEAL-niveau	Antwoord
SEAL-0	Migratie/integratie is onmogelijk door eigen formaten, ongedocumenteerde API's en strikte contractuele barrières.
SEAL-1	Migratie is technisch uitdagend en vereist aanzienlijke herontwikkeling, gespecialiseerde tools en ondersteuning van niet-EU leveranciers.
SEAL-2	Migratie is mogelijk, maar complex, afhankelijk van open standaarden voor gegevens en basis-API's, maar kerncomponenten zijn nog steeds eigen.
SEAL-3	De service gebruikt breed geaccepteerde open standaarden en gedocumenteerde API's, wat de migratie naar een andere door de EU gecontroleerde platform aanzienlijk vereenvoudigt.
SEAL-4	De service is gebaseerd op open-sourcetechnologie met gedocumenteerde, niet-eigen standaarden, wat naadloze en autonome migratie en interoperabiliteit met elke door de EU gecontroleerde oplossing waarborgt.

5.2 Capaciteit voor EU-operators

Vraag: Wat is de afhankelijkheid van betrokkenheid van niet-EU leveranciers voor het continue beheer, onderhoud en ondersteuning van de onderliggende cloudtechnologie?

SEAL-niveau	Antwoord
SEAL-0	Alle kritische beheer-, onderhouds- en L3-ondersteuningsfuncties worden exclusief uitgevoerd door niet-EU personeel van derden.
SEAL-1	Routinematige ondersteuning wordt binnen de EU afgewikkeld, maar kritische technische escalaties en updates vereisen directe, verplichte toegang door niet-EU personeel van de leverancier.
SEAL-2	Beheer en L1/L2-ondersteuning zijn primair EU-gebaseerd, maar grote software-updates, patches en kern architectuurondersteuning worden exclusief gecontroleerd door de niet-EU moedermaatschappij.
SEAL-3	EU-gebaseerd personeel kan de technologie beheren, onderhouden en ondersteunen, met een complete operationele

	kennisbank, hoewel toegang van niet-EU leveranciers af en toe nodig is voor diepgaande componentproblemen.
SEAL-4	De service wordt volledig beheerd, onderhouden en ondersteund door personeel binnen de EU, met volledige, onafhankelijke operationele controle en geen verplichte afhankelijkheid van niet-EU personeel van de leverancier voor kritische functies.

5.3 EU-gebaseerd talentpool

Vraag: Hoe wordt de expertise en talentpool die nodig zijn om de service te runnen en te handhaven, gegarandeerd EU-gebaseerd te zijn?

SEAL-niveau	Antwoord
SEAL-0	Kritische vaardigheden zijn geconcentreerd buiten de EU, met geen lokale EU-trainings- of ontwikkelingsprogramma's.
SEAL-1	Er bestaat een minimale EU-talentpool, maar deze is sterk afhankelijk van constante training en documentatie van niet-EU hoofdkantoren.
SEAL-2	De aanbieder ontwikkelt actief een EU-gebaseerde talentpool en kan EU-personeel werven/opleiden voor de meeste operationele rollen.
SEAL-3	De aanbieder heeft een robuuste, zelfstandige EU-gebaseerde talentpool opgebouwd met de capaciteit om de service onafhankelijk te runnen en te laten evolueren.
SEAL-4	De aanbieder leidt EU-brede initiatieven voor vaardigheidsontwikkeling en technologietransfer, wat waarborgt dat de talentpool volledig autonoom en EU-gecontroleerd is.

5.4 Locatie en juridisch kader van operationele ondersteuning

Vraag: Waar wordt de technische en operationele ondersteuning voor de cloudservice geleverd en onder welk juridisch kader?

SEAL-niveau	Antwoord
SEAL-0	Alle hoogwaardige technische ondersteuning wordt geleverd vanaf buiten de EU en valt onder niet-EU recht.
SEAL-1	Tier 1 (basis) ondersteuning wordt verstrekt vanaf binnen de EU, maar Tier 2/3 (kritische) ondersteuning wordt geleverd vanaf niet-EU locaties onder niet-EU recht.
SEAL-2	Alle ondersteunend personeel is fysiek gevestigd in de EU, maar de juridische structuur van de aanbieder onderwerpt hun handelen nog steeds aan een niet-EU juridisch kader.
SEAL-3	Alle niveaus van technische en operationele ondersteuning worden geleverd vanaf binnen de EU door EU-personeel, en hun activiteiten vallen exclusief onder EU-recht.
SEAL-4	Operationele ondersteuning wordt geleverd door een EU-entiteit, exclusief onder EU-recht, en gebruikt alleen EU-communicatie- en monitoringtools om nul externe juridische blootstelling te waarborgen.

5.5 Beschikbaarheid van documentatie en broncode

Vraag: In hoeverre zijn volledige technische documentatie, broncode en operationele knowhow beschikbaar voor een EU-entiteit voor langdurige autonomie?

SEAL-niveau	Antwoord
SEAL-0	Geen documentatie of broncode wordt verstrekt; alle knowhow is eigendom van en wordt vastgehouden door de niet-EU moedermaatschappij.
SEAL-1	Basis gebruikershandleidingen worden verstrekt, maar de broncode en kritische operationele knowhow zijn niet beschikbaar.
SEAL-2	Kritische technische documentatie en objectcode worden in escrow gegeven aan een vertrouwde EU-derde partij, en wordt vrijgegeven alleen in geval van leveranciers falen.
SEAL-3	Volledige, up-to-date broncode, ontwerpspecificaties en complete operationele knowhow zijn toegankelijk voor een EU-entiteit voor audit- en onderhoudsdoeleinden.
SEAL-4	Volledige broncode, documentatie en operationele knowhow worden verstrekt onder een open licentie (bijv. EUPL), wat volledige, blijvende EU-autonomie en evolutiecapaciteit waarborgt.

6 SOV-5: Soevereiniteit van de Toeleveringsketen

Beschrijving: Soevereiniteit van de toeleveringsketen evalueert de geografische oorsprong, transparantie en veerkracht van de technologische toeleveringsketen, met focus op de mate waarin kritische componenten en processen onder EU-controle blijven of blootgesteld zijn aan niet-EU afhankelijkheden.

6.1 Locatie en juridische controle van kritische leveranciers

Vraag: Waar zijn de kritische leveranciers en onderaannemers voor de dienstverlening gevestigd en onder wiens juridische controle opereren zij?

SEAL-niveau	Antwoord
SEAL-0	Kritische leveranciers/onderaannemers zijn gevestigd en gecontroleerd volledig buiten de EU.
SEAL-1	Leveranciers zijn buiten de EU, maar de hoofdcontractuele relatie is met een in de EU geregistreerde entiteit.
SEAL-2	Belangrijke onderaannemers opereren binnen de EU, maar de hoogst risico leveranciers (bijv. chipfabrikanten) zijn niet-EU en niet-controleerbaar.
SEAL-3	Het merendeel van de kritische leveranciers en onderaannemers zijn gevestigd binnen de EU en opereren onder EU-juridische kaders.
SEAL-4	Alle kritische leveranciers en onderaannemers voor de dienstverlening zijn gevestigd in de EU en staan onder de volledige juridische en contractuele controle van de EU-aanbieder entiteit.

6.2 Geografische oorsprong van hardware

Vraag: Wat is de geografische oorsprong van de sleutel fysieke hardware-onderdelen en de locatie waar de hardware wordt gefabriceerd of gemonteerd?

SEAL-niveau	Antwoord
SEAL-0	Sleutel fysieke onderdelen zijn exclusief afkomstig uit niet-EU landen met hoog geopolitiek risico, en montage vindt buiten de EU plaats.
SEAL-1	Hardware wordt in de EU gemonteerd, maar alle belangrijkste fysieke onderdelen (processoren, geheugen) zijn afkomstig van niet-EU partijen.
SEAL-2	Sleutel fysieke componenten en de belangrijkste fabricage/montage komen uit een diverse set van EU- en bondgenootlanden.
SEAL-3	Het merendeel van de sleutel fysieke onderdelen en de definitieve montage van kritische hardwarecomponenten vinden plaats binnen de EU.
SEAL-4	Alle sleutel fysieke onderdelen (inclusief kritische micro-elektronica) zijn afkomstig en gefabriceerd/gemonteerd volledig

	binnen de EU of vertrouwde bondgenootlanden onder een controleerbare EU-toeleveringsketencontrole.
--	--

6.3 Jurisdictie en herkomst van embedded code/firmware

Vraag: Wat is de jurisdictie en herkomst (oorsprong) van de embedded code en firmware die de kritische hardwarecomponenten aanstuurt?

SEAL-niveau	Antwoord
SEAL-0	Alle embedded code/firmware wordt ontwikkeld en gecontroleerd door een niet-EU entiteit onder niet-EU jurisdictie.
SEAL-1	De firmware wordt buiten de EU ontwikkeld, maar een ondertekend EU-certificaat garandeert dat deze niet is gemanipuleerd sinds de levering.
SEAL-2	De aanbieder werkt met niet-EU leveranciers om de firmware te auditen en aan te passen, maar de broncode is niet volledig beschikbaar.
SEAL-3	Kritische firmware wordt aangepast en gecontroleerd door de EU-entiteit, en de ontwikkeling en updates vinden plaats onder EU-jurisdictie.
SEAL-4	De hele embedded code/firmware-stack wordt ontwikkeld, onderhouden en bijgewerkt door de EU-exploitatie-entiteit met volledige toegang tot de broncode en onder EU-recht.

6.4 Oorsprong van software

Vraag: Waar en door wie wordt de kern cloudplatform-software ontworpen, geprogrammeerd, verpakt en bijgewerkt, en welke jurisdictie regelt deze processen?

SEAL-niveau	Antwoord
SEAL-0	Alle software-architectuur, programmering en updates worden exclusief buiten de EU uitgevoerd onder niet-EU jurisdictie.
SEAL-1	Kernarchitectuur is niet-EU, maar dienstverlening en -distributie voor de EU worden afgewikkeld door een niet-EU team dat in de EU is gevestigd.
SEAL-2	Een aanzienlijk deel van de programmering wordt gedaan door EU-teams, maar de kernarchitectuur en de definitieve update-release worden gecontroleerd door de niet-EU moedermaatschappij.
SEAL-3	De gehele software-levenscyclus—architectuur, programmering, verpakken en updates—wordt gecontroleerd en geregeld door een EU-entiteit onder EU-recht.
SEAL-4	De software is open-source (of vergelijkbaar), met architectuur en programmering volledig uitgevoerd binnen de EU, wat controleerbare, autonome updates onder EU-jurisdictie waarborgt.

6.5 Afhankelijkheid van niet-EU leveranciers

Vraag: Wat is de algemene mate van afhankelijkheid van niet-EU leveranciers, faciliteiten of eigendomstechnologieën voor de kernfunctionaliteit van de service?

SEAL-niveau	Antwoord
SEAL-0	Bijna 100% afhankelijkheid van niet-EU eigendomstechnologie, faciliteiten en leveranciers voor kernfunctionaliteit.
SEAL-1	Hoge afhankelijkheid (70-90%) van niet-EU elementen, met alleen niet-kritische componenten of basisinfrastructuur die EU-gebaseerd zijn.
SEAL-2	Matige afhankelijkheid (30-70%); kerncomponenten zijn dubbel geleverd of gebruiken open standaarden, waardoor overschakeling naar EU-alternatieven met inspanning mogelijk is.
SEAL-3	Lage afhankelijkheid (minder dan 30%); alleen niet-kritische afhankelijkheden of commerciële standaardproducten zijn niet-EU; de kern is EU-gecentreerd.
SEAL-4	Nul tot bijna nul afhankelijkheid van niet-EU leveranciers, faciliteiten of eigendomstechnologieën; de gehele service draait op door de EU gecontroleerde open source en infrastructuur.

6.6 Zichtbaarheid in de toeleveringsketen

Vraag: Welk niveau van zichtbaarheid en auditrechten heeft de klant/EU-autoriteit over de gehele leveranciers- en onder leveranciersketen?

SEAL-niveau	Antwoord
SEAL-0	Geen zichtbaarheid voorbij de eerstelijns leverancier; geen auditrechten bestaan.
SEAL-1	Beperkte zichtbaarheid tot de tweede lijn van leveranciers, en auditrechten zijn beperkt door vertrouwelijkheidsclausules.
SEAL-2	Volledige zichtbaarheid in alle kritische leveranciers en onder leveranciers, met contractuele rechten voor de EU-entiteit om audits uit te voeren.
SEAL-3	Volledige, transparante mapping van de gehele kritische toeleveringsketen wordt verstrekt, en directe, onvoorwaardelijke auditrechten worden gegarandeerd aan de contracterende EU-autoriteit.
SEAL-4	Volledige, realtime zichtbaarheid in de gehele toeleveringsketen via een gedeelde, onveranderlijke grootboekadministratie, met onafhankelijke EU-lichamen die verplichte, controleerbare en diepgaande toeleveringsketenbeoordelingen uitvoeren.

7 SOV-6: Technologische Soevereiniteit

Beschrijving: Technologische soevereiniteit evalueert de mate van openheid, transparantie en onafhankelijkheid in de onderliggende technologiystack, wat ervoor zorgt dat EU-actoren kunnen interopereren, auditen en oplossingen kunnen laten evolueren zonder lock-in bij buitenlandse eigendomssystemen.

7.1 Interoperabiliteit via open standaarden

Vraag: In hoeverre houdt de service zich aan open, niet-eigen, openbaar bestuurd standaarden voor API's en protocollen om interoperabiliteit te waarborgen?

SEAL-niveau	Antwoord
SEAL-0	Integratie is alleen mogelijk via eigendom, ongedocumenteerde API's, wat leidt tot maximale vendor lock-in.
SEAL-1	Sommige branche-standaardprotocollen worden ondersteund (bijv. HTTP), maar kernintegratie is afhankelijk van eigendom extensies en API's.
SEAL-2	De service gebruikt goed gedocumenteerde, niet-eigen API's voor de meeste kernfuncties, wat matige interoperabiliteit mogelijk maakt.
SEAL-3	De service houdt zich strikt aan openbaar bestuurd, breed geaccepteerde open standaarden en protocollen (bijv. ISO, OASIS) voor alle kritische functies.
SEAL-4	De service is gebaseerd op volledig open, goed gedocumenteerde en door de EU bestuurd standaarden, wat volledige interoperabiliteit met elke conforme EU-technologiystack waarborgt.

7.2 Open licentiemodel

Vraag: Wat is het licentiemodel voor de kritische softwarecomponenten van de cloudservice, en welke rechten verleent het?

SEAL-niveau	Antwoord
SEAL-0	De software is volledig closed source en eigendom; toegang tot de code is niet toegestaan.
SEAL-1	Objectcode wordt verstrekt, maar de broncode is gesloten; wijziging is verboden.
SEAL-2	De broncode wordt in escrow gehouden en wordt vrijgegeven onder specifieke niet-operationele omstandigheden (bijv. faillissement).
SEAL-3	De broncode voor kritische servicecomponenten is toegankelijk onder een restrictieve licentie, die rechten verleent voor audit en interne wijziging, maar niet voor her distributie.
SEAL-4	De gehele service draait op software die onder een door de EU erkende open licentie (bijv. EUPL) is uitgebracht, wat volledige rechten verleent voor audit, wijziging en her distributie.

7.3 Zichtbaarheid in ontwerp en werking

Vraag: Welk niveau van zichtbaarheid wordt geboden in het interne ontwerp, de architectuur, gegevensstromen en externe afhankelijkheden van de service?

SEAL-niveau	Antwoord
SEAL-0	Geen zichtbaarheid; alle architectonische details en afhankelijkheden worden als bedrijfsgeheimen beschouwd.
SEAL-1	Hoogwaardige architectuurschema's worden verstrekt, maar gedetailleerde documentatie over gegevensstromen en afhankelijkheden is beperkt.
SEAL-2	Uitgebreide architectuur- en gegevensstroomdocumentatie is beschikbaar voor de klant onder NDA voor veiligheids- en compliance-audits.
SEAL-3	Volledige, up-to-date documentatie over het hele systeemontwerp, inclusief alle gegevensstromen en afhankelijkheden, is permanent beschikbaar voor de EU-autoriteit voor governance en audit.
SEAL-4	Volledige transparantie, met een volledig gedocumenteerde en controleerbare open architectuur, die EU-autoriteiten in staat stelt om alle servicefuncties en afhankelijkheden onafhankelijk te verifiëren.

7.4 EU-onafhankelijkheid in high-performance computing

Vraag: Wat is de afhankelijkheid van de service van niet-EU gecontroleerde processors, versnellers en high-performance computing (HPC) software-ecosystemen?

SEAL-niveau	Antwoord
SEAL-0	Exclusieve afhankelijkheid van gesloten (proprietary) hardware- en softwarestacks die beheerst worden door niet-EU-partijen, voor HPC-mogelijkheden.
SEAL-1	De service gebruikt in de EU geassembleerde hardware, maar de kernprocessors/versnellers zijn niet-EU en hun intellectueel eigendom is niet-EU.
SEAL-2	De service heeft een aantoonbare strategie om door de EU ontwikkelde HPC-hardware/processoren te integreren naarmate deze beschikbaar komen.
SEAL-3	De service gebruikt en prioriteert actief door de EU ontworpen en gefabriceerde HPC-hardware, waarbij een aanzienlijk deel van het software-ecosysteem door de EU is ontwikkeld.
SEAL-4	De service draait op HPC-mogelijkheden die volledig zijn gebaseerd op door de EU ontwikkelde, gefabriceerde processors, versnellers en open-source software-ecosystemen.

8 SOV-7: Soevereiniteit op het gebied van Veiligheid en Compliance

Beschrijving: Soevereiniteit op het gebied van veiligheid en compliance meet in hoeverre veiligheidsoperaties, compliance-verplichtingen en veerkrachtmaatregelen binnen de EU worden gecontroleerd, wat onafhankelijkheid van buitenlandse jurisdicties en langdurige operationele zekerheid waarborgt.

8.1 Certificeringen

Vraag: Welke veiligheids- en compliance-certificeringen worden door de service aangehouden, en wat is hun relevantie voor EU-soevereiniteit?

SEAL-niveau	Antwoord
SEAL-0	Alleen basis niet-EU veiligheidscertificeringen worden aangehouden, zonder specifieke afstemming op EU-kaders.
SEAL-1	Internationaal erkende certificeringen (bijv. ISO 27001) worden aangehouden, maar geen specifieke EU-certificeringen (bijv. ENISA-schema's).
SEAL-2	De service is conform en streeft actief naar EU-specifieke certificeringen (bijv. een specifiek ENISA Cybersecurity Certification Scheme).
SEAL-3	De service houdt erkende EU-certificeringen aan (bijv. ENISA of nationale soevereiniteitsschema's) die alle kritische servicecomponenten dekken.
SEAL-4	De service houdt het hoogste niveau van relevante EU-veiligheidscertificering aan, geauditeerd en onderhouden door een onafhankelijke EU-autoriteit.

8.2 Naleving van EU-regelgeving

Vraag: Wat is het niveau van naleving van de provider van grote EU-regelgevende kaders zoals GDPR, NIS2 en DORA?

SEAL-niveau	Antwoord
SEAL-0	Geen aantoonbare naleving of conformiteit met sleutel EU-regelgeving; naleving is zelf gecertificeerd.
SEAL-1	Contractuele toezegging tot GDPR, maar naleving van NIS2/DORA is gedeeltelijk of in afwachting.
SEAL-2	De service is formeel conform met GDPR, NIS2 en DORA, ondersteund door interne audits en documentatie.
SEAL-3	Naleving van alle grote EU-kaders is onafhankelijk geverifieerd door een gekwalificeerde EU-auditor, en de provider is actief betrokken bij toekomstige compliance-planning.
SEAL-4	Volledige, aantoonbare en onafhankelijk gecertificeerde naleving van alle huidige en toekomstige grote EU-regelgevende kaders (GDPR, NIS2, DORA).

8.3 Locatie van Security Operations Centers (SOCs)

Vraag: Waar zijn de Security Operations Centers (SOCs) en incidentresponsteams gevestigd, en wie heeft directe toezicht op monitoring en logging?

SEAL-niveau	Antwoord
SEAL-0	SOCs en responsteams zijn gevestigd buiten de EU, en de klant heeft geen toegang tot raw logs.
SEAL-1	SOCs zijn nominaal in de EU, maar alle sleutelanalyses en incidentafhandeling worden geëscaleerd naar niet-EU teams onder niet-EU jurisdictie.
SEAL-2	De SOC en responsteams zijn volledig in de EU gevestigd en vallen onder EU-recht, en de klant heeft toegang tot samengevatte logs en alerts.
SEAL-3	De SOC en responsteams zijn exclusief in de EU gevestigd, en de klant/EU-autoriteit heeft directe, realtime toegang en controle over alle raw security logs en monitoringfuncties.
SEAL-4	Alle veiligheidsoperaties (monitoring, logging, incidentresponse) worden uitgevoerd door een onafhankelijke EU-entiteit, met volledige, controleerbare en exclusieve controle door de EU-contracterende autoriteit.

8.4 Transparante rapportage van inbreuken op veiligheid

Vraag: Hoe wordt de transparante, tijdige en EU-conforme rapportage van inbreuken op veiligheid gewaarborgd?

SEAL-niveau	Antwoord
SEAL-0	Rapportage gebeurt alleen op verzoek van de klant, zonder verplichting tot openbaarmaking aan EU-autoriteiten.
SEAL-1	Inbreuken worden gerapporteerd volgens contractuele afspraken, maar niet noodzakelijk in overeenstemming met EU-wetgeving.
SEAL-2	Inbreuken worden gerapporteerd aan de klant en relevante EU-autoriteiten in overeenstemming met EU-wetgeving, maar zonder onafhankelijke verificatie.
SEAL-3	Inbreuken worden tijdig gerapporteerd aan EU-autoriteiten, met onafhankelijke verificatie van de omvang en impact.
SEAL-4	Real-time, transparante rapportage van inbreuken aan EU-autoriteiten, met onafhankelijke verificatie en volledige samenwerking met EU-onderzoeken.

8.5 Onafhankelijke veiligheids- en nalevingsaudits

Vraag: Wat is de mogelijkheid voor de klant of een EU-autoriteit om onafhankelijke veiligheids- en nalevingsaudits uit te voeren?

SEAL-niveau	Antwoord
SEAL-0	Geen rechten voor onafhankelijke audits; alleen door de leverancier verstrekte rapporten zijn toegestaan.

SEAL-1	Audits zijn alleen toegestaan door vooraf goedgekeurde derde partijen en zijn sterk beperkt in omvang en toegang.
SEAL-2	Audits kunnen worden uitgevoerd door elke gecertificeerde EU-auditor, met volledige toegang tot systemen en documentatie, onder voorbehoud van langdurige voorafgaande goedkeuringsprocedures.
SEAL-3	Onvoorwaardelijk recht voor de klant of EU-autoriteit om onafhankelijke, op aanvraag uit te voeren veiligheids- en nalevingsaudits met volledige, realtime toegang tot alle systemen en gegevens
SEAL-4	Onafhankelijke audits zijn verplicht, routineus en worden uitgevoerd door een door de EU aangewezen, vertrouwde derde partij-auditor, met volledige, juridisch gegarandeerde toegang tot alle faciliteiten, broncode en personeel.

9 SOV-8: Milieuduurzaamheid

Beschrijving: Milieuduurzaamheid beoordeelt de autonomie en veerkracht van cloudservices op de lange termijn in relatie tot energiegebruik, afhankelijkheid en schaarste aan grondstoffen.

9.1 Adoptie van energie-efficiënte infrastructuur

Vraag: Wat is de Power Usage Effectiveness (PUE) van de datacenters en zijn er meetbare doelstellingen voor verbetering?

SEAL-niveau	Antwoord
SEAL-0	PUE wordt niet gemeten of openbaar gemaakt; er bestaan geen energie-efficiëntiedoelstellingen.
SEAL-1	PUE wordt gemeten maar ligt boven het branchegemiddelde (bijv. >1,7); doelstellingen zijn vaag of niet-bestaand.
SEAL-2	PUE ligt op of nabij de beste branchepraktijk (bijv. 1,4-1,5), en er zijn specifieke, tijdgebonden doelstellingen voor PUE-verlaging.
SEAL-3	PUE ligt aanzienlijk onder het branchegemiddelde (bijv. <1,3), ondersteund door controleerbare metriekeken en een langetermijn-, openbaar plan voor continue PUE-optimalisatie.
SEAL-4	De aanbieder gebruikt innovatieve, in de EU ontwikkelde technologie om beste-in-klasse PUE (bijv. <1,1) te bereiken en draagt bij aan EU-onderzoek naar energie-efficiëntienormen.

9.2 Circulaire economie-praktijken

Vraag: Welke circulaire economie-praktijken zijn van toepassing voor de cloudservice-hardware, van hergebruik tot end-of-life-behandeling?

SEAL-niveau	Antwoord
SEAL-0	Hardware wordt aan het einde van de levensduur afgedankt zonder gedocumenteerd hergebruiks- of opknappingsprogramma.
SEAL-1	Er vindt enige basisrecycling plaats, maar er is geen formeel programma voor hergebruik of opknapping van componenten.
SEAL-2	Er is een formeel programma voor hardware-opknapping en intern hergebruik, wat de consumptie van nieuwe middelen vermindert.
SEAL-3	Er wordt een robuust, controleerbaar model voor circulaire economie afgedwongen, met prioriteit voor componenthergebruik

	en verlenging van de levensduur van hardware voordat gecertificeerde, verantwoorde EU-recycling plaatsvindt.
SEAL-4	De aanbieder houdt zich aan een gecertificeerd gesloten-kringloopsysteem, met in de EU gemaakte, herbruikbare componenten, en garandeert dat 100% van de end-of-life-hardware binnen de EU wordt verwerkt met duurzame praktijken.

9.3 Transparante meting en openbaarmaking

Vraag: Welk niveau van transparantie en openbaarmaking wordt geboden voor CO₂-uitstoot, watergebruik en andere milieukundige indicatoren?

SEAL-niveau	Antwoord
SEAL-0	Er worden geen milieukundige indicatoren gemeten of openbaar gemaakt.
SEAL-1	CO ₂ -uitstoot wordt berekend en gerapporteerd, maar watergebruik en andere sleutelmetriecken worden niet openbaar gemaakt.
SEAL-2	Volledige meting en openbare openbaarmaking van alle sleutelmilieukundige indicatoren (koolstof, water, afval) voor EU-operaties, geverifieerd door een intern EU-team.
SEAL-3	Alle milieukundige metriecken worden gemeten en openbaar gemaakt volgens EU-normen (bijv. CSRD), en de gegevens worden geverifieerd door een onafhankelijke EU-derde partij.
SEAL-4	Real-time, gedetailleerde meting en openbare openbaarmaking van alle milieueffecten, met de gegevens beschikbaar gesteld aan de EU-autoriteit voor onafhankelijke verificatie tegen EU Green Deal-doelstellingen.

9.4 Inkoop van hernieuwbare energie

Vraag: Welk percentage van de energie die wordt gebruikt om de cloud-infrastructuur en -operaties van stroom te voorzien, is afkomstig uit verifieerbare hernieuwbare of koolstofarme bronnen?

SEAL-niveau	Antwoord
SEAL-0	Minder dan 10% van de energie is afkomstig uit verifieerbare hernieuwbare of koolstofarme bronnen.
SEAL-1	Tussen 10% en 50% van de energie is gedekt door een mix van hernieuwbare energiecertificaten en PPAs.

SEAL-2	Meer dan 50% van de energie is aantoonbaar ingekocht via langetermijn, verifieerbare Power Purchase Agreements (PPA's) van nieuwe, lokale EU-hernieuwbare projecten.
SEAL-3	100% van de energie die in de EU wordt verbruikt, wordt gekoppeld aan verifieerbare, nieuw geproduceerde hernieuwbare of koolstofarme energie uit EU-bronnen.
SEAL-4	De aanbieder investeert in en bezit lokale EU-hernieuwbare energieproductieassets, waardoor de service volledig koolstofnegatief is voor zijn EU-operaties.