WHITEPAPER

Wendbaar en weerbaar

Architectuurprincipes voor een open overheidscloud

Een adviesstuk voor architecten over portabiliteit, interoperabiliteit, open standaarden en digitale soevereiniteit

OPEN CLOUD ALLIANTIE

Over deze whitepaper

Deze whitepaper is geschreven door architecten van de deelnemende organisaties, vanuit hun eigen ervaring met de architectuurvraagstukken waar Nederlandse overheidsorganisaties dagelijks tegenaan lopen: hoe voorkom je dat een praktische, korte-termijnkeuze uitgroeit tot een structurele afhankelijkheid; hoe toon je soevereiniteit aan in plaats van te beloven; hoe weeg je wendbaarheid, weerbaarheid en kosten tegen elkaar af zonder in dogma te vervallen. De principes in deze whitepaper zijn dan ook niet vanuit een verkoopdoel geformuleerd, maar vanuit de vraag welke architectuurkeuzes een organisatie daadwerkelijk helpen om deze uitdagingen het hoofd te bieden.

De leden van de Open Cloud Alliantie zijn tegelijk commerciële cloudaanbieders met een eigen belang bij de architectuurrichting die deze whitepaper bepleit. Dat belang benoemen wij liever expliciet dan onbenoemd te laten. De principes zelf zijn grotendeels afgeleid van onafhankelijk vastgestelde kaders (BIO2, het EU Cloud Sovereignty Framework, NIS2) en onze eigen ervaring bij het leveren van vitale diensten, en wij nodigen lezers uitdrukkelijk uit deze op hun eigen technische merites te beoordelen, niet op basis van wie ze heeft opgesteld.

Versie 1.0

Inhoudsopgave

Managementsamenvatting

Deze whitepaper werkt de architectuurvisie van de Open Cloud Alliantie uit tot concrete, toetsbare principes voor architecten. Zij is primair voor architecten geschreven, maar bewust op een niveau gehouden dat ook voor beleidsmakers, bestuurders en andere niet-architecten te volgen is. Dat is geen toeval: het doel van deze whitepaper is niet alleen om architecten houvast te geven, maar ook om de kloof tussen beleid en architectuur te helpen dichten. In de praktijk ervaren wij die kloof regelmatig: beleidsdoelen rond digitale soevereiniteit en weerbaarheid worden op bestuurlijk niveau vastgesteld, maar landen niet vanzelfsprekend in concrete architectuurkeuzes, en architectuurkeuzes worden niet altijd herkend als iets waar bestuurders verantwoordelijkheid voor dragen.

Die verantwoordelijkheid is niet vrijblijvend. De NIS2-richtlijn, in Nederland omgezet via de Cyberbeveiligingswet, spreekt bestuurders nadrukkelijk aan op de inrichting en uitvoering van beveiligingsmaatregelen, niet alleen op de vaststelling van beleid. Digitale soevereiniteit, weerbaarheid en compliance zijn daarmee net zo goed een bestuurlijk onderwerp als een technisch onderwerp, en deze whitepaper is bedoeld om beide werelden dichter bij elkaar te brengen.

Voor het bestuurlijke, politieke verhaal achter deze whitepaper, waarom digitale soevereiniteit voor Nederland en Europa urgent is, en wat de Open Cloud Alliantie de overheid concreet aanbiedt, verwijzen wij naar het manifest Een Open Cloud voor Nederland (april 2026). Deze whitepaper herhaalt dat verhaal niet, maar bouwt erop voort: zij vertaalt de drie uitgangspunten uit het manifest (open architectuur, open standaarden, open source) naar een samenhangend architectuurkader van wendbaarheid, weerbaarheid en compliance (hoofdstuk 3), met een uitgewerkte catalogus van architectuurprincipes (bijlage A).

Kernboodschappen van deze whitepaper:

- Wendbaarheid, weerbaarheid en compliance zijn de drie kapstokken waarlangs een architectuur bijdraagt aan digitale soevereiniteit en autonomie; soevereiniteit is daarbij het resultaat, niet een op zichzelf staand ontwerpprincipe.
- Een exit-strategie zonder een daadwerkelijk getest migratiepad biedt weinig houvast: portabiliteit moet vanaf de eerste architectuurbeslissing worden meegewogen, niet pas op het moment dat een exit onvermijdelijk wordt.
- Open source is een krachtig instrument voor wendbaarheid en, in mindere mate, weerbaarheid, maar geen synoniem voor soevereiniteit en geen doel op zich.
- Compliance is meer dan techniek: het vraagt om aantoonbaarheid, governance en contractuele waarborgen, niet alleen om certificering.

Lezers die vooral het bestuurlijke verhaal zoeken, kunnen volstaan met het manifest en deze samenvatting. Lezers die de architectuurkeuzes willen doorgronden of toepassen, architecten voorop, vinden vanaf hoofdstuk 3 de volledige uitwerking.

1. Voorwoord

Dit is geen herhaling van het manifest *Een Open Cloud voor Nederland*. Dat manifest richtte zich tot bestuurders en politiek: het beschreef wáárom Nederland nu moet bewegen naar een soevereine overheidscloud, en wát de Open Cloud Alliantie (OCA) daarvoor aanbiedt. Dit document is de vertaalslag naar de werkvloer van de architect.

Architecten die vandaag ontwerpbeslissingen nemen over overheidsapplicaties, dataplatformen en cloudinfrastructuur hebben geen behoefte aan nog een politiek statement. Zij hebben behoefte aan bruikbare principes: waar moet een architectuur aan voldoen om wendbaar te blijven, weerbaar te zijn tegen uitval en druk van buitenaf, en tegelijk aantoonbaar te voldoen aan de eisen die de Nederlandse en Europese overheid aan digitale soevereiniteit stelt?

Deze whitepaper beantwoordt die vraag langs drie kapstokken, wendbaarheid, weerbaarheid en compliance, en werkt de onderliggende bouwstenen uit tot een fijnmazige catalogus van architectuurprincipes in de bijlage. Elk principe krijgt een heldere beschrijving en een expliciete rationale, zodat architecten niet alleen weten wát het principe voorschrijft, maar ook waaróm, en dus zelf kunnen beoordelen wanneer en hoe het toepasbaar is in hun eigen context.

We nemen daarbij bewust een genuanceerd standpunt in over open source, over de verhouding tussen exit- en migratiestrategieën, en over de manier waarop soevereiniteit zich verhoudt tot security en tot commerciële realiteit. Digitale autonomie is geen doel dat losstaat van goede architectuur, het is een eigenschap die voortvloeit uit goede architectuurkeuzes, consequent toegepast.

De leden van de Open Cloud Alliantie passen de principes uit deze whitepaper toe in hun eigen dienstverlening. Voor de beoordeling van het soevereiniteitsniveau van een clouddienst geldt op dit moment nog dat deze via zelfevaluatie plaatsvindt, aangezien er in Nederland nog geen onafhankelijke autoriteit is die dit objectief kan vaststellen. De Alliantie werkt aan een manier om die toepassing van de principes ook onafhankelijk te laten valideren, zodat opdrachtgevers hier op termijn niet alleen op hoeven te vertrouwen, maar het ook kunnen verifiëren.

Open Cloud Alliantie

2. Inleiding: waarom architecten dit nodig hebben

Een marktcontext die om architectuurkeuzes vraagt

Nederland en Europa zijn in korte tijd sterk afhankelijk geworden van een klein aantal niet-Europese hyperscalers. Deze afhankelijkheid is geen abstract beleidsvraagstuk: zij manifesteert zich concreet op het bord van de architect, in elke keuze voor een cloudplatform, een dataformaat, een identity-provider of een API-standaard. De Algemene Rekenkamer concludeerde in het onderzoek *Het Rijk in de cloud: donkere wolken pakken samen* (januari 2025) dat 67 procent van de onderzochte rijksorganisaties de verplichte risicoanalyse bij materieel cloudgebruik niet uitvoerde. Dat is geen bestuurlijk falen alleen, het is ook een signaal dat architecten onvoldoende instrumentarium hadden om afhankelijkheden zichtbaar en beheersbaar te maken.

Sindsdien is het beleidslandschap snel veranderd. De herziening van het Rijksbreed cloudbeleid (vastgesteld in de ministerraad op 3 juli 2026) scherpt aan: rijksorganisaties moeten minder afhankelijk worden van met name Amerikaanse techbedrijven en altijd een achtervang hebben voor het geval een leverancier uitvalt. Op Europees niveau introduceert de Europese Commissie met het vastgestelde Cloud Sovereignty Framework (oktober 2025) een scoringssystematiek voor soevereiniteit, en met de voorgestelde Cloud and AI Development Act (juni 2026), op het moment van schrijven nog in behandeling bij Europees Parlement en Raad, een mogelijke EU-brede verplichting daarvan voor de publieke sector.

Voor architecten betekent dit dat soevereiniteit, portabiliteit en open standaarden niet langer optionele kwaliteitsattributen zijn die je toevoegt als de tijd het toelaat. Het zijn randvoorwaarden die vanaf de eerste ontwerpbeslissing moeten meewegen, net zoals beveiliging, performance en beheerbaarheid dat al zijn.

De bouwstenen uit deze whitepaper zijn daarmee niet alleen relevant bij het maken van ontwerpbeslissingen. Ze spelen ook een belangrijke rol bij het opstellen van inkoopeisen: wie soevereiniteit, portabiliteit en open standaarden pas bij de start van een implementatie meeneemt, komt structureel te laat. Deze eisen horen thuis in de aanbestedingsdocumenten en de gunningscriteria, naast de gebruikelijke eisen op het gebied van functionaliteit, prijs en beveiliging.

De blinde vlek: exit zonder migratie

Vrijwel elk overheidsdocument dat over cloudafhankelijkheid gaat, spreekt over de noodzaak van een exit-strategie. Dat is terecht, maar onvolledig: een exit-strategie zegt niets over de vraag of, en hoe, een workload vervolgens daadwerkelijk ergens anders kan draaien. Hoofdstuk 5 werkt dit verder uit en behandelt exit- en migratiestrategie daarom nadrukkelijk als één samenhangend geheel.

Voor wie is dit document

Deze whitepaper is geschreven voor enterprise-, informatie- en oplossingsarchitecten binnen overheidsorganisaties en hun toeleveranciers, die concrete richting zoeken bij het ontwerpen van cloudarchitecturen die tegelijk wendbaar (aanpasbaar, portabel, innovatief) en weerbaar (continu, controleerbaar, soeverein) zijn. Het document veronderstelt bekendheid met cloudarchitectuurconcepten (IaaS/PaaS/SaaS, API's, IAM) en met de hoofdlijnen van het Nederlandse en Europese cloudbeleid; waar nodig wordt dat beleid kort samengevat, met verwijzing naar de onderliggende bronnen.

Bestuurders, beleidsmakers en andere lezers die vooral het bestuurlijke en politieke verhaal zoeken, verwijzen wij naar de managementsamenvatting aan het begin van dit document en naar het manifest Een Open Cloud voor Nederland. De hoofdstukken hierna gaan de architectuurdiepte in en veronderstellen de bekendheid genoemd hierboven.

Leeswijzer

- Hoofdstuk 3 introduceert de drie kapstokken wendbaarheid, weerbaarheid en compliance, en de onderliggende bouwstenen die samen leiden tot digitale soevereiniteit en autonomie.
- Hoofdstuk 4 plaatst open source in perspectief: een belangrijk maar geen exclusief onderdeel van de visie.
- Hoofdstuk 5 werkt portabiliteit uit tot een praktisch classificatiemodel, inclusief migratiepaden en exportformaten.
- Hoofdstuk 6 beschrijft de normenkaders waarmee architectuurkeuzes aantoonbaar en toetsbaar worden gemaakt.
- Hoofdstuk 7 vertaalt dit alles naar een concreet afwegingskader voor architectuurbeslissingen.
- Hoofdstuk 8 schetst het implementatieperspectief voor architecten die vandaag willen beginnen.
- Bijlage A bevat de volledige, fijnmazige catalogus van architectuurprincipes, elk met beschrijving en rationale.

3. Wendbaarheid, weerbaarheid en compliance

Het manifest Een Open Cloud voor Nederland formuleert drie uitgangspunten: open architectuur, open standaarden en open source software. Voor de architectuurpraktijk is dat een goed vertrekpunt, maar geen volledig beeld. Deze whitepaper ordent de onderliggende bouwstenen daarom langs drie kapstokken die samen bepalen of een organisatie werkelijk controle heeft over haar eigen digitale fundament: wendbaarheid, weerbaarheid en compliance.

Digitale soevereiniteit en autonomie zijn in dit document geen bouwsteen naast de andere, maar het resultaat waartoe deze drie kapstokken gezamenlijk leiden. We hanteren daarbij een bewust onderscheid tussen beide begrippen. Digitale autonomie is het bredere, politiek-economische doel: het vermogen van Nederland en Europa om onafhankelijk strategische keuzes te maken over de eigen digitale infrastructuur. Digitale soevereiniteit is de concrete, meetbare en aantoonbare invulling daarvan op organisatie- en architectuurniveau, bijvoorbeeld uitgedrukt in een Sovereignty Effective Assurance Level (SEAL)-score. Een architect draagt aan autonomie bij door soevereiniteit aantoonbaar te maken, niet door autonomie rechtstreeks te "ontwerpen".

Wendbaarheid gaat over het vermogen om te veranderen: van platform te wisselen, componenten te vervangen, en applicaties en data overdraagbaar te houden. Weerbaarheid gaat over het vermogen om stand te houden: dienstverlening te laten doorlopen bij uitval, aanvallen of druk van buitenaf, en gevoelige gegevens te beschermen tegen ongewenste toegang. Compliance ten slotte gaat over aantoonbaarheid: kunnen bewijzen, met erkende normenkaders en jurisdictionele en contractuele waarborgen, dat wendbaarheid en weerbaarheid niet alleen intenties zijn maar geverifieerde feiten.

Wendbaarheid

Onder wendbaarheid vallen de bouwstenen die een organisatie in staat stellen om, wanneer dat nodig is, te veranderen van leverancier, platform of technologie zonder daarbij vast te lopen.

Portabiliteit

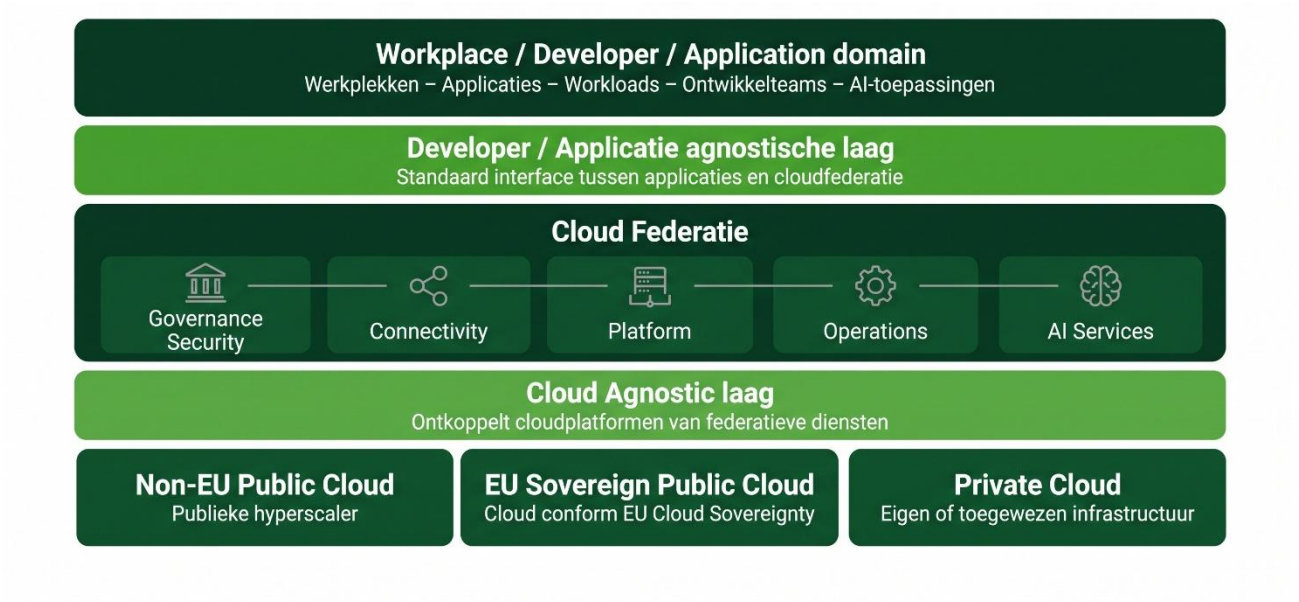
Portabiliteit is het vermogen om data, applicaties en configuraties over te zetten van het ene platform naar het andere, met behoud van functionaliteit en zonder onevenredige kosten of vertraging. Portabiliteit is de technische voorwaarde die een exit-strategie daadwerkelijk uitvoerbaar maakt. Hoofdstuk 5 werkt deze bouwsteen verder uit tot een classificatiemodel (data-, applicatie- en operationele portabiliteit) en bespreekt concrete standaarden, migratiepaden en formaten.

Open architectuur

Een open architectuur is modulair opgebouwd, met componenten die uitwisselbaar zijn en waarin geen enkele leverancier, hoe goed ook, een structurele, onvervangbare positie inneemt. Dit is niet hetzelfde als "geen leveranciers gebruiken": het betekent dat de architectuur zodanig is ontworpen dat een leverancier vervangen kán worden zonder het gehele fundament opnieuw te hoeven bouwen. Een open architectuur kent bewust technologische diversiteit, wat behalve voor wendbaarheid ook bijdraagt aan weerbaarheid, zoals hierna wordt toegelicht. Diversiteit verhoogt de weerbaarheid, maar kan de beheersbaarheid verlagen: meer variëteit in de technologiestack betekent doorgaans ook meer verschillende vaardigheden, beheerprocessen en securitymaatregelen die een organisatie moet beheersen. Dit is een bewuste afweging per workload, geen absolute regel.

Drie servicelagen en twee ontkoppellagen

Om open architectuur concreet te maken, is het behulpzaam onderscheid te maken tussen drie servicelagen, met daartussen twee expliciete ontkoppellagen. Dit model staat los van de fysieke netwerkconnectiviteit (WAN, mobiele diensten), die als randvoorwaardelijke infrastructuur buiten dit model valt.



Figuur 1. Cloud referentiemodel

De onderste servicelaag omvat drie naast elkaar bestaande platformcategorieën, geen opeenvolgende stappen: een publieke hyperscaler zonder EU-soevereiniteitsstatus, een publieke cloud die wel voldoet aan het EU Cloud Sovereignty Framework (hoofdstuk 6), en een private cloud (eigen of toegewezen infrastructuur). Runtime placement, containers en virtuele machines zijn de manier waarop een organisatie elk van deze platformen benut, geen aparte laag ernaast. De Cloud Agnostic Layer ontkoppelt de keuze tussen deze drie platformcategorieën van de federatieve functies erboven, zodat een organisatie van cloudplatform, of van categorie, kan wisselen zonder de federatieve laag opnieuw te hoeven inrichten.

De middelste servicelaag, Cloud Federation, bundelt functies die per definitie platformoverstijgend zijn. Voor de leesbaarheid clusteren wij deze in vijf groepen: Governance (identity, identity federation), Security, Connectivity (intercloud connectivity, netwerk als federatieve dienst, te onderscheiden van de fysieke WAN- en mobiele connectiviteit die buiten dit model valt), Platform Operations (observability, cost management) en AI Services. Deze indeling is zelf een referentiepatroon (zie principe A8 in bijlage A) en kan per organisatie worden aangepast. Dit is de laag waar de in dit hoofdstuk genoemde risicospreiding over meerdere, federatief samenwerkende platformen (zie categorie E, continuïteit) concreet vorm krijgt.

De Developer/Application Agnostic Layer ontkoppelt vervolgens het applicatie-ecosysteem van de federatieve cloudlaag, zodat ontwikkelaars en applicaties niet direct afhankelijk zijn van de specifieke inrichting van de federatie eronder. De Haven-standaard van VNG Realisatie, met Haven+ als bijbehorende referentie-implementatie, is een operationeel Nederlands voorbeeld van precies deze ontkoppeling: gemeentelijke applicaties worden hosting-onafhankelijk gemaakt via een gestandaardiseerde, containerbased interface, wat in de praktijk al laat zien dat dit model niet alleen theoretisch is. Hoofdstuk 5 gaat hier verder op in.

De "uniforme stekker" is een concept in ontwikkeling

De Open Referentie Cloud Architectuur (ORCA) en de bijbehorende "uniforme stekker" van de Open Cloud Alliantie, die in hoofdstuk 5 wordt toegelicht, vullen de Cloud Agnostic Layer en de Developer/Application Agnostic Layer verder in. Op het moment van schrijven is dit een concept in ontwikkeling, nog niet bewezen op schaal. Architecten doen er goed aan hierop te anticiperen zonder er nu al op te bouwen alsof het een vastgestelde standaard betreft.

Open standaarden

Open standaarden zijn de taal waarin componenten van verschillende leveranciers met elkaar communiceren. Zonder open standaarden is een open architectuur een lege belofte: componenten kunnen dan wel in theorie uitwisselbaar zijn, maar in de praktijk niet, omdat zij niet met elkaar kunnen samenwerken. De Nederlandse overheid hanteert hiervoor het "pas toe of leg uit"-principe van het Forum Standaardisatie, met wettelijke verankering via de Wet digitale overheid, en op Europees niveau bepaalt de Interoperable Europe Act verplichte interoperabiliteitstoetsen voor nieuwe of ingrijpend gewijzigde digitale overheidsdiensten.

Open source, met een wendbaarheidsdoel

Open source software draagt in de eerste plaats bij aan wendbaarheid, doordat de broncode van platformcomponenten publiek controleerbaar en niet aan één leverancier gebonden is. Vendor lock-in wordt daarbij primair voorkomen via open, gestandaardiseerde interfaces (zie de Cloud Agnostic Layer eerder in dit hoofdstuk, en principe B3); open source voegt daar een eigen, aanvullende bijdrage aan toe doordat het beheer van een component bij uitval van de leverancier ook daadwerkelijk door een andere partij kan worden overgenomen. Hoofdstuk 4 werkt dit standpunt genuanceerd uit, inclusief het onderscheid tussen het platform, waarvoor open source wordt nagestreefd, en de vrije keuze van workloads, die ook commerciële, closed-source software kunnen omvatten.

Weerbaarheid

Onder weerbaarheid vallen de bouwstenen die een organisatie in staat stellen om stand te houden bij uitval, aanvallen, overname van een leverancier of ongewenste toegang tot gevoelige gegevens.

Continuïteit

Continuïteit is het vermogen van een organisatie om haar digitale dienstverlening te laten doorlopen, ook wanneer een leverancier uitvalt, wordt overgenomen, of onder ongewenste buitenlandse zeggenschap komt. Continuïteit wordt in de architectuur gerealiseerd door risicospreiding, door technologische diversiteit, en door een uitgewerkte combinatie van exit- en migratiestrategie. Continuïteit is niet gratis: de architect maakt hier een bewuste afweging, gebaseerd op de kriticiteit[1] van de betreffende workload, niet elke applicatie heeft hetzelfde continuïteitsniveau nodig.

[1] “Kriticiteit” is geen woordenboekwoord in deze betekenis, maar een in risicomanagement en IT-governance ingeburgerde term voor de mate waarin een systeem of workload kritiek is. De term wordt in vergelijkbare zin gebruikt in Europese risicobeoordelingen van kritieke infrastructuur.

Databescherming, inclusief privacy

Databescherming gaat over het beschermen van gegevens tegen ongeautoriseerde toegang, verlies of misbruik, met persoonsgegevens als een belangrijke, wettelijk verankerde deelverzameling. Voor persoonsgegevens geldt de Algemene verordening gegevensbescherming (AVG) als generieke basis, met de data protection impact assessment (DPIA) als het belangrijkste instrument om privacyrisico's vooraf in kaart te brengen. Voor clouddiensten specifiek biedt ISO/IEC 27018 aanvullende richtlijnen voor de bescherming van persoonlijk identificeerbare informatie. Databescherming is nauw verbonden met soevereiniteit, maar valt er niet mee samen: een leverancier kan onder Europese jurisdictie vallen en toch onvoldoende waarborgen bieden voor de verwerking van persoonsgegevens, en omgekeerd.

Security

Security, of informatiebeveiliging, betreft de bescherming van netwerken, datacenters, software, databases en clouddiensten tegen digitale dreigingen. Security en soevereiniteit zijn complementaire, niet inwisselbare eigenschappen: een platform kan volledig soeverein zijn en toch onvoldoende beveiligd, en omgekeerd. Hoofdstuk 6 werkt dit onderscheid verder uit aan de hand van het EU Cloud Sovereignty Framework, dat soevereiniteit beoordeelt, en het separate EUCS-certificeringsschema van ENISA, dat cybersecurity-assurance beoordeelt.

Open source, met een weerbaarheidsnuance

Open source draagt daarnaast, in mindere maar reële mate, ook bij aan weerbaarheid, via operationele ontvlechtbaarheid: omdat de broncode niet gebonden is aan één leverancier, kan het beheer, de doorontwikkeling of de ondersteuning van een component bij uitval, overname of geopolitieke druk op de oorspronkelijke leverancier worden overgenomen door een andere partij, of desnoods door de organisatie zelf. Deze weerbaarheidsbijdrage is voorwaardelijk: zij vereist dat de organisatie of een alternatieve partij daadwerkelijk over de kennis en capaciteit beschikt om dat beheer over te nemen, zoals hoofdstuk 4 nader toelicht.

Compliance

Onder compliance vallen de bouwstenen die wendbaarheid en weerbaarheid aantoonbaar maken: niet als intentie of belofte, maar als geverifieerd feit, getoetst aan erkende normenkaders.

Aantoonbaarheid en jurisdictie

Soevereiniteitsclaims moeten aantoonbaar zijn, niet zelfverklaard. Het EU Cloud Sovereignty Framework operationaliseert dit in acht meetbare objectieven en een bijbehorende SEAL-score, waaronder de eigendomsstructuur van een leverancier, de geldende jurisdictie, en de mogelijkheid om data en technologie onafhankelijk van niet-Europese controle te beheren.

Contractuele borging

Aantoonbaarheid op papier is onvoldoende zonder contractuele waarborgen die dit afdwingbaar maken: ontbindingsmogelijkheden bij een ongewenste wijziging van zeggenschap bij een leverancier (change of control), consortiumconstructies met exit-clausules, en heldere afspraken over dataoverdracht bij beëindiging van een contract.

Normenkaders

Hoofdstuk 6 beschrijft de belangrijkste normenkaders waarmee compliance wordt getoetst: BIO2 en ABRO als Nederlandse beveiligingsbaselines, EUCS als Europees cybersecurity-certificeringsschema, en het EU Cloud Sovereignty Framework als soevereiniteitskader. Deze kaders zijn niet optioneel naast de architectuur, zij zijn het instrument waarmee wendbaarheid en weerbaarheid worden geverifieerd.

Soevereiniteit en autonomie als resultaat

Soevereiniteit is een resultaat, geen ontwerpprincipe op zichzelf

Een architect kan niet rechtstreeks "soevereiniteit ontwerpen". Soevereiniteit is de optelsom van wendbaarheid en weerbaarheid, aantoonbaar gemaakt via compliance: expliciete transparantie over jurisdictie, en contractuele waarborgen zoals ontbindingsmogelijkheden bij een ongewenste wijziging van zeggenschap. Zonder heldere afspraken over de geldende jurisdictie en zonder afdwingbare ontbindingsmogelijkheden in het contract blijft soevereiniteit een intentie in plaats van een aantoonbaar feit. Digitale autonomie is vervolgens het resultaat op stelselniveau van vele organisaties die deze soevereiniteit consequent en aantoonbaar realiseren.

Een belangrijke nuance, ontleend aan zowel het manifest van de Open Cloud Alliantie als aan de kabinetsreactie op de initiatiefnota Wolken aan de horizon: soevereiniteit gaat niet over protectionisme of digitaal isolement. Wendbaarheid, weerbaarheid en compliance zijn geen keuzemenu waaruit een organisatie naar smaak kan putten, maar drie elkaar versterkende kapstokken. Een architectuur die bijvoorbeeld wél open standaarden gebruikt maar geen daadwerkelijk geteste migratiepaden heeft, claimt wendbaarheid zonder deze waar te maken. Een architectuur die wél soeverein is maar onvoldoende beveiligd, claimt weerbaarheid zonder deze waar te maken. Pas de combinatie van alle drie, aantoonbaar en getoetst, levert digitale soevereiniteit op, en daarmee een bijdrage aan digitale autonomie.

4. Position paper: open source genuanceerd

Open source software speelt een belangrijke rol in de architectuurvisie van de Open Cloud Alliantie. Tegelijk is het belangrijk om precies te zijn over wélke rol dat is, en vooral over welke rol het niet is. Deze positiebepaling is bedoeld om architecten, inkopers en bestuurders een eenduidig en genuanceerd uitgangspunt te geven, zodat discussies over open source niet verzanden in een schijntegenstelling tussen "open source" en "soeverein".

In hoofdstuk 3 is open source geplaatst onder zowel wendbaarheid als weerbaarheid: primair als wendbaarheidsinstrument, omdat het vendor lock-in vermindert en overdraagbaarheid vergroot, en in aanvulling daarop als weerbaarheidsinstrument, omdat het beheer van een open source component bij uitval of geopolitieke druk op de oorspronkelijke leverancier kan worden overgenomen door een andere partij. Dit hoofdstuk werkt beide invalshoeken verder uit.

Open source is geen synoniem voor soevereiniteit

Een veelgemaakte aanname is dat open source software per definitie bijdraagt aan digitale soevereiniteit. Dat is onjuist, of op zijn best onvolledig. Soevereiniteit gaat over jurisdictie, zeggenschap, controle over data en aantoonbaarheid, niet over de licentievorm van de broncode. Open source software die wordt beheerd, gehost en ondersteund door een partij onder niet-Europese jurisdictie levert geen soevereiniteitswinst op. Omgekeerd kan closed-source software van een Europese, onder Nederlandse jurisdictie vallende leverancier, met transparante contractvoorwaarden en een uitgewerkte exit-strategie, in de praktijk een hogere mate van aantoonbare soevereiniteit bieden dan een slecht beheerde open source-implementatie.

Open source is dus een instrument dat soevereiniteit kán ondersteunen, met name doordat het vendor lock-in vermindert, transparantie vergroot (de broncode is controleerbaar) en overdraagbaarheid vereenvoudigt, maar het is niet de enige, en niet automatisch de doorslaggevende factor.

Waar open source wél het verschil maakt: het platform, niet de applicatie

Deze whitepaper, en het onderliggende manifest, richt zich op de cloudinfrastructuur: het platform waarop applicaties draaien. Niet op de talloze applicaties die op dat platform kunnen worden ingezet. Voor het platform streeft de Open Cloud Alliantie zoveel mogelijk naar open source software, binnen de voorwaarden en afwegingen die de principes in bijlage A daaraan stellen. De redenen daarvoor zijn architectuurtechnisch van aard:

- Controleerbaarheid: de broncode van platformcomponenten kan door onafhankelijke partijen worden geïnspecteerd, wat vertrouwen vergroot en de kans op verborgen functionaliteit ("backdoors") verkleint.
- Aanvullende bescherming tegen vendor lock-in: waar open, gestandaardiseerde interfaces (zie hoofdstuk 3 en principe B3) een component al vervangbaar maken, voegt open source daar een eigen laag aan toe, namelijk dat de organisatie niet afhankelijk hoeft te zijn van het voortbestaan of de bereidwilligheid van één specifieke leverancier voor onderhoud en doorontwikkeling zelf.
- Gedeelde ontwikkelkosten: meerdere partijen investeren gezamenlijk in dezelfde componenten, wat de kosten per organisatie verlaagt en de kwaliteit door bredere review verhoogt.
- Aansluiting bij internationale en Europese ontwikkeling: initiatieven als IPCEI-CIS zetten expliciet in op open source voor de cloud-edge-continuum-laag.

Klanten behouden vrijheid van workload-keuze

Het is essentieel dat dit uitgangspunt niet wordt verward met een verplichting voor eindgebruikers. Organisaties die gebruikmaken van een cloudplatform van een OCA-lid blijven volledig vrij in de keuze van de applicaties en workloads die zij op dat platform inzetten, inclusief commerciële, closed-source bedrijfs- en kantoorsoftware, of andere leveranciersspecifieke toepassingen. Het manifest is expliciet: het gaat over het fundament, niet over de applicaties die daarop draaien, en de intellectuele-eigendomsbescherming van commerciële softwareleveranciers wordt gerespecteerd, zonder die bescherming zouden deze bedrijven immers snel van de markt verdwijnen.

Deze scheiding is bewust een afbakening van de reikwijdte van dit document, geen inhoudelijk oordeel over de applicatielaag. Deze whitepaper, en het onderliggende manifest, richten zich uitdrukkelijk op de cloudlaag: het platform waarop applicaties draaien. Of, en hoe, een vergelijkbare beweging richting open source wenselijk is op applicatieniveau, is een aparte discussie die hier bewust buiten beschouwing blijft; dit document neemt daar geen standpunt over in.

> **Wat dit concreet betekent voor een architect**
>
> Een cloudplatform dat voor 90% uit open source componenten bestaat, kan zonder problemen closed-source workloads hosten. Andersom: een organisatie die om functionele of contractuele redenen kiest voor overwegend commerciële software op een soeverein platform, verliest daarmee niet automatisch haar soevereiniteitswinst op het niveau van jurisdictie, databeheer en exit-mogelijkheden. De keuze voor open source op platformniveau en de keuze voor bepaalde workloads zijn twee onafhankelijke architectuurbeslissingen.

Voor- en nadelen van open source in de architectuur

Voordelen

- Transparantie en controleerbaarheid van de broncode.
- Geen contractuele lock-in door licentiemodellen van één leverancier.
- Mogelijkheid tot aanpassing en doorontwikkeling naar eigen behoefte.
- Kostendeling door gemeenschappelijke ontwikkeling binnen een bredere gebruikersgroep.
- Aansluiting bij Europese en internationale open source-initiatieven (bijvoorbeeld in het kader van IPCEI-CIS en het Nederlandse programma Beter Samen Werken).

Nadelen en aandachtspunten

- Niet voor alle noodzakelijke datacentersoftware bestaan (nog) volwassen open source-alternatieven; een dogmatische "alleen open source"-eis kan de architectuur onnodig beperken of vertragen.
- Open source vereist eigen beheercapaciteit en expertise; "gratis" in licentiekosten betekent niet "gratis" in totale kosten van eigendom (TCO), support, patchmanagement en doorontwikkeling moeten worden georganiseerd.
- De kwaliteit en onderhoudsstatus van open source-projecten verschilt sterk; een principe-toepassing vereist due diligence per component, niet een generieke aanname van kwaliteit.
- Zonder actieve bijdrage aan de onderliggende gemeenschap (in plaats van alleen consumptie) ontstaat op termijn alsnog een vorm van afhankelijkheid, nu van de bereidheid van een externe gemeenschap om het component te onderhouden.

- Veel open source platformimplementaties leunen in de praktijk op commerciële supportcontracten van de aanbieder; deze support introduceert een eigen afhankelijkheid, en de partij die deze support levert kan zelf weer buiten de EU-jurisdictie vallen, wat de soevereiniteitswinst van open source teniet kan doen.
- De invloed van een individuele organisatie op de roadmap en ondersteuning van een open source project is doorgaans beperkt: de gemeenschap kan besluiten onderdelen te “deprecaten” (buiten gebruik te stellen), met mogelijke gevolgen voor functionaliteit en, bij uitblijvend onderhoud, ook voor veiligheid.

Verantwoordelijkheden: leverancier en klant

Een verantwoorde inzet van open source vereist een heldere rolverdeling tussen leverancier (in dit geval het OCA-lid dat het platform aanbiedt) en klant (de overheidsorganisatie die het platform gebruikt).

Verantwoordelijkheid van de leverancier

- Transparant zijn over welke onderdelen van het platform open source zijn, welke closed source, en waarom.
- Zorgdragen voor tijdig patch- en kwetsbaarhedenbeheer van gebruikte open source-componenten (vulnerability management, conform bijvoorbeeld ISO/IEC 29147 en 30111).
- Actief bijdragen aan de gemeenschappen achter kritieke open source-componenten, in plaats van uitsluitend te consumeren.
- Documenteren van de licentievoorwaarden en eventuele copyleft-verplichtingen die relevant zijn voor de klant.

Verantwoordelijkheid van de klant (overheidsorganisatie)

- Zelf een weloverwogen afweging maken over welke workloads op welk soevereiniteits- en beveiligingsniveau moeten draaien, ongeacht of het onderliggende platform open of closed source is.
- Bij de keuze voor closed-source workloads op een open platform, zelf de bijbehorende contractuele en exit-risico's beoordelen (zie hoofdstuk 5).
- Niet uitgaan van de vooronderstelling dat "open source" automatisch "veilig" of "soeverein" betekent, maar dit toetsen aan de concrete criteria uit hoofdstuk 6.

Conclusie van deze positiebepaling

De Open Cloud Alliantie presenteert zich niet als een uitsluitend open source-initiatief, en architecten doen er goed aan hetzelfde onderscheid te hanteren in hun eigen ontwerpbeslissingen. Open source is een krachtig en op platformniveau sterk aan te bevelen middel om vendor lock-in te verminderen en transparantie te vergroten, maar het is een middel ten dienste van de bouwstenen continuïteit, portabiliteit en soevereiniteit, geen doel op zich, en geen vervanging voor expliciete architectuurkeuzes op het gebied van jurisdictie, exit-mogelijkheden en aantoonbaarheid.

5. Portabiliteit in de praktijk

Portabiliteit wordt in beleidsstukken vaak behandeld als sluitstuk van een exit-strategie: iets waar je over nadenkt op het moment dat een leverancierswissel onvermijdelijk wordt. Deze whitepaper keert die volgorde om. Portabiliteit is een ontwerpeis die vanaf de eerste architectuurbeslissing meeweegt, niet omdat een exit waarschijnlijk is, maar omdat de mogelijkheid tot exit alleen waarde heeft als zij ook daadwerkelijk uitvoerbaar is.

Exit-strategie versus migratiestrategie: een noodzakelijk onderscheid

Een exit-strategie beschrijft de contractuele, juridische en organisatorische voorwaarden waaronder een overheidsorganisatie een leveranciersrelatie kan beëindigen: opzegtermijnen, dataoverdrachtsverplichtingen, escrow-regelingen, en bepalingen voor het geval een leverancier wordt overgenomen door een partij van buiten de EU ("change of control"-clausules). Vrijwel alle relevante beleidsdocumenten, het herziene Rijksbreed cloudbeleid, de Data Act, het NCSC-advies over ketenafhankelijkheden, benoemen het belang van zo'n strategie.

Een migratiestrategie gaat een stap verder en beschrijft hóe een workload, inclusief de bijbehorende data en configuraties, daadwerkelijk kan worden overgezet naar een ander platform: welke exportformaten worden gebruikt, welke gestandaardiseerde interfaces beschikbaar zijn, welk testregime wordt gevolgd, en welke hersteltijd (RTO) en gegevensverlies (RPO) bij een migratie realistisch zijn.

> **Het verschil in één zin**
>
> Een exit-strategie regelt of je mag vertrekken; een migratiestrategie regelt of je ook daadwerkelijk kunt aankomen. Zonder migratiestrategie is een exit-strategie een papieren recht.

Voor architecten volgt hieruit een concrete eis: elke architectuurbeslissing die (mede) op basis van een exit-strategie wordt gemotiveerd, moet vergezeld gaan van een aantoonbaar geteste migratieprocedure voor de betreffende workloadcategorie. "Aantoonbaar getest" betekent hier: er is minimaal één keer een representatieve migratie daadwerkelijk uitgevoerd of gesimuleerd, niet alleen op papier beschreven.

Een getest migratiepad en een financiële raming (zie principe D6, exit-kosten in de Total Cost of Ownership) zijn niet voldoende zonder een derde, organisatorisch onderdeel: een concreet exitplan. Waar D1 vaststelt dát een migratie technisch mogelijk is en D6 vaststelt wat die ongeveer kost, legt het exitplan vast wíe de exit uitvoert, in welke volgorde, en binnen welke termijn. Zonder dit vooraf uitgewerkte draaiboek moeten rolverdeling en planning bij een daadwerkelijke exit voor het eerst worden bedacht, precies op het moment dat daar de minste tijd voor is. Principe D8 in bijlage A werkt dit verder uit.

Classificatie van portabiliteit

Portabiliteit is geen binaire eigenschap die simpelweg wel of niet aanwezig is; zij kent verschillende dimensies die elk apart beoordeeld moeten worden. Deze whitepaper hanteert de volgende classificatie:

Type portabiliteit	Wat het betreft	Belangrijkste risico bij afwezigheid
Dataportabiliteit	Het exporteren van ruwe en verwerkte data in een bruikbaar, gedocumenteerd formaat	Data kan technisch niet of alleen met groot kwaliteitsverlies worden overgezet

Type portabiliteit	Wat het betreft	Belangrijkste risico bij afwezigheid
Applicatieportabiliteit	Het overzetten van de applicatielogica zelf (containers, code, configuraties)	Applicatie moet grotendeels opnieuw gebouwd worden bij een overstap
Operationele portabiliteit	Beheerprocessen, monitoring, IAM-koppelingen, security-baselines	Werkende applicatie draait wel, maar kan niet beheerd/bewaakt worden op de nieuwe omgeving
Operationele omkeerbaarheid	Het vermogen om, bij samenwerking tussen meerdere aanbieders (consortia), taken tijdelijk of blijvend over te dragen	Consortiumpartner kan bij problemen niet inspringen of overnemen

Dit classificatiemodel sluit aan bij de criteria uit het EU Cloud Sovereignty Framework, waarin "de mogelijkheid om meerdere aanbieders gezamenlijk opdrachten te laten verstrekken, waardoor interoperabiliteit en portabiliteit geborgd zijn" expliciet wordt aangeduid als operationele omkeerbaarheid, een aparte beoordelingscategorie naast de meer technische vormen van portabiliteit.

Migratiepaden: van intentie naar uitvoering

Een migratiepad beschrijft de concrete route waarlangs een workload van platform A naar platform B kan worden overgezet. In de architectuurpraktijk onderscheiden we vier generieke migratiepaden, drie gericht op de applicatiekant en één op de datakant van een migratie, elk met een eigen complexiteit en risicoprofiel. Deze paden sluiten elkaar niet uit en worden in de praktijk vrijwel altijd gecombineerd, zoals hierna wordt toegelicht.

1. Lift-and-shift via gestandaardiseerde infrastructuur-templates

Toepasbaar wanneer infrastructuur is beschreven met open, declaratieve standaarden zoals TOSCA (Topology and Orchestration Specification for Cloud Applications) voor topologie en orkestratie. Deze aanpak heeft de laagste applicatie-impact, maar vereist dat de onderliggende platformen vergelijkbare abstractieniveaus ondersteunen.

2. Applicatie-herbouw op basis van open API's en containerstandaarden

Toepasbaar bij cloud-native applicaties die zijn opgebouwd rond gecontaineriseerde diensten met gestandaardiseerde interfaces. Vereist meer inspanning dan lift-and-shift, maar levert doorgaans een robuustere, beter onderhoudbare uitkomst op de nieuwe omgeving.

3. Rehosting van klassieke, niet-cloud-native applicaties

Veel overheidsapplicaties zijn niet cloud-native en lenen zich niet, of niet op korte termijn, voor herbouw. Voor dit type applicaties is rehosting het meest realistische pad: het overzetten van bestaande virtuele machines of images naar het doelplatform, eventueel gecombineerd met een beperkte modernisering van de meest kritieke koppelvlakken ("wrap-and-modernize"). Dit pad levert doorgaans niet dezelfde mate van portabiliteit op als de eerste twee paden, maar voorkomt dat legacy-applicaties de facto onoverdraagbaar blijven totdat een volledige herbouw haalbaar is.

4. Datamigratie met behoud van semantiek

Het overzetten van datasets vereist niet alleen een technisch exportformaat, maar ook behoud van betekenis (semantiek): metadata, classificaties en relaties tussen gegevens moeten intact blijven. Dit is vaak het meest onderschatte onderdeel van een migratie.

In de praktijk zijn applicatie en data bij een migratie vrijwel altijd gelijktijdig in beweging: een applicatie zonder haar data heeft weinig waarde, en data zonder de applicatie die haar oorspronkelijk beheerde, verliest vaak een deel van haar context. De paden 1, 2 en 3 beschrijven daarom niet een keuze naast de datamigratie uit pad 4, maar de applicatiekant van een migratie die altijd samen met de datakant wordt gepland en getest. Voor de architect betekent dit dat een migratieoefening nooit alleen de applicatie of alleen de data test, maar beide in combinatie, inclusief de onderlinge afhankelijkheden tussen applicatielogica en dataconsistentie tijdens de overgangsperiode.

Haven en Haven+: een bestaand Nederlands voorbeeld

De Haven-standaard van VNG Realisatie is een operationeel, in de praktijk toegepast voorbeeld van de Developer/Application Agnostic Layer die in hoofdstuk 3 is geïntroduceerd. Haven maakt gemeentelijke websites en applicaties hosting-onafhankelijk door ze te ontwerpen als gecontaineriseerde diensten met een gestandaardiseerde interface, zodat zij op verschillende, onderling vervangbare hostingomgevingen kunnen draaien. Haven+ is de bijbehorende referentie-implementatie: een concrete, openbare uitwerking waarmee aanbieders kunnen aantonen dat hun platform daadwerkelijk aan de Haven-standaard voldoet. Gebruik van de referentie-implementatie is raadzaam, maar niet verplicht; verplicht is naleving van de standaard zelf, te toetsen met de Haven Compliancy Checker.

Voor de architectuurpraktijk laat Haven zien dat de ontkoppeling van applicatie-ecosysteem en onderliggende cloudlaag geen theoretisch concept is, maar op gemeentelijk niveau al werkt. Rijksorganisaties en andere overheidslagen die de Developer/Application Agnostic Layer willen inrichten, kunnen de Haven-standaard en de Haven+ referentie-implementatie raadplegen, ook wanneer de eigen context (schaal, kriticiteit, soevereiniteitseisen) uiteindelijk om een eigen invulling vraagt. Beide zijn recent aangewezen als bouwsteen binnen de Generieke Digitale Infrastructuur (GDI), wat de status van Haven verstevigt van een gemeentelijk initiatief naar structureel onderdeel van de landelijke digitale infrastructuur.

Infrastructure-as-code en GitOps als operationeel mechanisme

Portabiliteit blijft een papieren belofte zolang een migratiepad niet daadwerkelijk en herhaalbaar is getest, zoals principe D1 vereist. Infrastructure-as-code, het declaratief beschrijven van infrastructuur in versiebeheerde configuratiebestanden in plaats van handmatige inrichting, maakt dat testen operationeel haalbaar: dezelfde configuratie kan in beginsel op elk platform dat de gebruikte standaarden ondersteunt, opnieuw worden toegepast.

GitOps bouwt hierop voort door versiebeheer (doorgaans Git) als centrale bron van waarheid te hanteren voor zowel infrastructuur als applicatieconfiguratie, met geautomatiseerde, controleerbare uitrol op basis van wijzigingen in die configuratie. Voor portabiliteit is dit relevant omdat een GitOps-aanpak een migratieoefening kan reduceren tot het toepassen van dezelfde, reeds geteste configuratie op een nieuw platform, in plaats van een handmatige, foutgevoelige exercitie.

Het specifieke gereedschap waarmee infrastructure-as-code wordt toegepast (op het moment van schrijven bijvoorbeeld Terraform of OpenTofu) is zelf een referentiepatroon, geen tijdloos onderdeel van het principe: over vijf jaar kan een ander gereedschap dominant zijn. Toch is een korte illustratie leerzaam. Toen HashiCorp in 2023 de licentie van Terraform wijzigde van een open source-licentie naar de restrictievere Business Source License, forkte de gemeenschap het project tot het onder de Linux Foundation ondergebrachte OpenTofu, een vrijwel schoolvoorbeeld van het lock-in-risico dat hoofdstuk 4 bij ogenschijnlijk open gereedschap bespreekt, en van de operationele ontvlechtbaarheid uit principe C6.

Relevante open standaarden en specificaties

De "Study on Interoperability of Data Processing Services", uitgevoerd in opdracht van de Europese Commissie (resultaten gepubliceerd 23 februari 2026) ter voorbereiding van de Unie-repository van open specificaties onder artikel 35 van de Data Act, beveelt een concrete set standaarden aan voor generieke (niet-sectorspecifieke) interoperabiliteit, met nadruk op de PaaS-laag. Voor architecten relevant zijn onder meer:

- TOSCA: voor het beschrijven van topologie en orkestratie van cloud-workloads op een platformonafhankelijke manier.
- OIDC (OpenID Connect), OAuth 2.0 en SAML: open specificaties voor identiteit, authenticatie en autorisatie, essentieel voor operationele portabiliteit van IAM-koppelingen.
- Gestandaardiseerde exportformaten voor data (bijvoorbeeld op basis van breed gedragen open bestandsformaten in plaats van proprietary databaseformaten).

De Data Act zelf verplicht aanbieders van dataverwerkingsdiensten sinds 12 september 2025 om overstapbelemmeringen weg te nemen: technische medewerking aan een overstap, geen contractuele blokkades, en, na een overgangsperiode, geen kosten meer voor het exporteren van data ("egress fees"). Deze wettelijke basis versterkt, maar vervangt niet, de architectuurverantwoordelijkheid om portabiliteit daadwerkelijk te ontwerpen en te testen.

De "uniforme stekker": een gestandaardiseerde interface-laag

De Open Cloud Alliantie ontwikkelt het concept van een "uniforme stekker": een open source component (API) waarmee uiteenlopende applicaties op verschillende, door OCA-leden aangeboden platformen kunnen "landen", ongeacht of de onderliggende voorziening centraal of gedistribueerd is georganiseerd. Het concept is vergelijkbaar met de invoering van de uniforme Eurostekker in 1990: geen technologiekeuze op zich, maar een afspraak over de interface waarmee uiteenlopende technologieën met elkaar kunnen samenwerken.

De nadere technische uitwerking van deze interface-laag volgt in de Open Referentie Cloud Architectuur (ORCA), die de Alliantie op het moment van schrijven ontwikkelt. Architecten die nu al willen anticiperen op deze uitwerking, doen er goed aan hun platformkeuzes te toetsen aan de principes uit bijlage A onder de categorie portabiliteit, in het bijzonder de principes over vermijden van niet-standaard exportformaten en het ontwerpen van gestandaardiseerde interfaces.

Praktische aanbeveling: portabiliteit als terugkerend architectuurproces

Portabiliteit is geen eenmalige exercitie bij de bouw van een systeem, maar een terugkerend aandachtspunt gedurende de gehele levenscyclus van een architectuur. Concreet betekent dit:

- Neem portabiliteitseisen op als expliciet, toetsbaar kwaliteitsattribuut in architectuurbeoordelingen (naast beveiliging, performance en beheerbaarheid).
- Voer periodiek, bijvoorbeeld jaarlijks voor kritieke workloads, een migratie-oefening ("game day") uit, waarbij een representatieve dataset en workload daadwerkelijk naar een alternatieve omgeving wordt overgezet.
- Documenteer bij elke nieuwe architectuurbeslissing expliciet welke exportformaten en interfaces worden gebruikt, en waarom deze als voldoende gestandaardiseerd worden beoordeeld.

- Betrek portabiliteit als criterium bij leveranciersselectie en -beoordeling, in aanvulling op de reeds gangbare beveiligings- en continuïteitscriteria.

6. Architectuurcontroles & normenkaders

Dit hoofdstuk werkt de compliance-kapstok uit hoofdstuk 3 verder uit. Architectuurprincipes voor wendbaarheid en weerbaarheid zijn pas bruikbaar wanneer zij kunnen worden getoetst. Dit hoofdstuk beschrijft de belangrijkste normenkaders waarmee dat gebeurt: het onderscheid tussen security-assurance en soevereiniteits-assurance, de Nederlandse beveiligingsbaselines, en de manier waarop deze kaders samen een gelaagd toetsingsmodel vormen.

Twee complementaire assurance-lagen: security en soevereiniteit

Een terugkerend misverstand in de architectuurpraktijk is het door elkaar gebruiken van cybersecurity-assurance en soevereiniteits-assurance, terwijl dit twee aparte, complementaire beoordelingslagen zijn met ieder een eigen normenkader en een eigen doel.

	EUCS (ENISA)	EU Cloud Sovereignty Framework
Beoordeelt	Cybersecurity van de clouddienst	Soevereiniteit: jurisdictie, zeggenschap, controle
Schaal	Drie assurance-niveaus: Basic, Substantial, High	Acht objectieven, gescoord via Sovereignty Effective Assurance Levels (SEAL 0–4)
Kernvraag	Is deze dienst voldoende beveiligd tegen het relevante dreigingsniveau?	Kan deze dienst onder ongewenste buitenlandse invloed komen te staan?
Typisch gebruik	Certificeringsschema, gebaseerd op ISO/IEC 27001/27002/27017	Aanbestedingscriterium en scoringsmethodiek, o.a. toegepast bij de EU-cloudaanbesteding van april 2026

Het manifest van de Open Cloud Alliantie benoemt dit onderscheid expliciet: de focus op soevereiniteit mag niet leiden tot verminderde aandacht voor security, want beide zijn nodig en complementair. Voor architecten volgt hieruit een concrete toetsingsregel: een architectuurbeoordeling is pas compleet wanneer zij zowel een security-assurance-niveau (bijvoorbeeld conform EUCS) áls een soevereiniteitsniveau (bijvoorbeeld conform het EU Cloud Sovereignty Framework) expliciet vaststelt. Eén hoge score op de ene as compenseert geen lage score op de andere.

Nederlandse beveiligingsbaselines: BIO2 en ABRO

De Baseline Informatiebeveiliging Overheid 2 (BIO2, definitieve versie 9 januari 2026, gepubliceerd in de Staatscourant op 5 maart 2026) is het normenkader voor informatiebeveiliging binnen alle Nederlandse overheidslagen, Rijk, gemeenten, provincies en waterschappen, en wordt via de Cyberbeveiligingswet (de Nederlandse implementatie van NIS2) wettelijk verankerd. BIO2 is gebaseerd op NEN-EN-ISO/IEC 27001:2022 en 27002:2022, en bevat sinds de doorontwikkeling naar aanleiding van de kabinetsreactie op de initiatiefnota Wolken aan de horizon specifieke beheersmaatregelen voor cloudgebruik:

- Een verplichte inventaris van bedrijfsmiddelen die van belang zijn voor informatieverwerking, waarin cloudomgevingen expliciet zijn opgenomen.
- Een beheersmaatregel voor het inventariseren, classificeren, selecteren, beoordelen en managen van clouddienstaanbieders, inclusief het beëindigen van dienstverlening, een directe koppeling naar de exit- en migratie-eisen uit hoofdstuk 5.

De Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO 2026) stellen aanvullende eisen aan leveranciers op contracten die de nationale veiligheid raken, en vervangen in dat domein de eerdere Algemene Beveiligingseisen Defensieopdrachten (ABDO). Voor architecten die met dergelijke contracten te maken hebben, is ABRO het aanvullende, strengere kader boven op de generieke BIO2-baseline.

Het EU Cloud Sovereignty Framework: acht objectieven

Het door de Europese Commissie op 20 oktober 2025 gepubliceerde Cloud Sovereignty Framework (versie 1.2.1) operationaliseert soevereiniteit in acht objectieven: strategisch, juridisch/jurisdictioneel, data & AI, operationeel, supply chain, technologisch, security & compliance, en milieu. Elk objectief wordt gescoord op een Sovereignty Effective Assurance Level (SEAL) van 0 tot 4, en gezamenlijk vormen deze scores een totale soevereiniteitsscore op basis van 48 criteria.

Architecten die een leverancier of platform beoordelen, doen er goed aan minimaal de volgende criteria uit het framework expliciet te toetsen:

- De eigendomsstructuur: is het hoofdkantoor van het moederbedrijf juridisch gevestigd in de EU?
- Is de cloudprovider blootgesteld aan niet-Europese wetgeving met extraterritoriale werking (zoals de Amerikaanse CLOUD Act)?
- Kunnen data en technologie onafhankelijk van niet-Europese controle worden beheerd, ondersteund en onderhouden?
- Is er transparantie over de herkomst van kritieke hardware- en softwarecomponenten?
- Zijn medewerkers met geprivilegieerde toegangsrechten in dienst van een Europese entiteit, ingezetene van de EU/EER/EFTA, en voeren zij hun werk fysiek vanuit Europa uit?

Waarborgen tegen "sovereignty washing"

Een reëel risico bij de toepassing van deze kaders is "sovereignty washing": een aanbieder die soevereiniteit claimt zonder dat harde, verifieerbare controles dit ondersteunen. Het EU Cloud Sovereignty Framework is nadrukkelijk bedoeld om dit tegen te gaan door soevereiniteit aantoonbaar en niet zelfverklaard te maken. Voor architecten betekent dit dat leverancierclaims over soevereiniteit altijd getoetst moeten worden aan de onderliggende SEAL-scores, en niet worden aangenomen op basis van marketingmateriaal.

De voorgestelde Cloud and AI Development Act (CADA)

De door de Europese Commissie op 3 juni 2026 voorgestelde Cloud and AI Development Act introduceert een gegradeerd systeem van vier "Union assurance levels", waarbij niveau 3 vereist dat een aanbieder EU-eigendom en -zeggenschap heeft (met aanvullende eisen aan personeel), en niveau 4 volledige transparantie en controle over de softwaretoeleveringsketen vereist, zonder inmenging van een derde land. Op het moment van schrijven is CADA een wetgevingsvoorstel dat de reguliere EU-wetgevingsprocedure (behandeling door Europees Parlement en Raad) nog moet doorlopen; de uiteindelijke inhoud, het tijdpad en zelfs de vraag óf het wordt aangenomen, staan nog niet vast. Mocht het voorstel in de huidige of vergelijkbare vorm worden aangenomen, dan zou dit de aanpak van het Cloud Sovereignty Framework EU-breed verplicht kunnen maken voor de publieke sector. Architecten die nu al aanbestedingen en architectuurbeoordelingen baseren op het Cloud Sovereignty Framework, bouwen in dat scenario een voorsprong op, maar dit is geen zekerheid waarop de architectuur volledig mag worden gebaseerd.

De AI Act: architectuurrelevante verplichtingen

Naast CADA en de EU Open Source Strategy is er een derde Europese regelgeving die architectuurkeuzes raakt zodra een organisatie AI-toepassingen ontwikkelt of inzet: de AI Act (Verordening (EU) 2024/1689), sinds 1 augustus 2024 in werking, met een gefaseerde inwerkingtreding. Verplichtingen voor aanbieders van general-purpose AI-modellen (GPAI) gelden sinds augustus 2025; de handhavingsbevoegdheid van het AI-Office en de transparantieverplichtingen zijn sinds 2 augustus 2026 actief.

Recente vertraging voor hoogrisico AI-systemen

Via het zogeheten "Digital Omnibus"-pakket, eind juni 2026 door de Raad goedgekeurd, is de verplichting voor hoogrisico AI-systemen (Annex III, onder meer werving, kredietbeoordeling en kritieke infrastructuur) uitgesteld van 2 augustus 2026 naar 2 december 2027, vanwege het ontbreken van geharmoniseerde normen. Dit is een zeer recente wijziging; architecten doen er goed aan de actuele stand bij het AI Office van de Europese Commissie te verifiëren voordat hierop wordt gebouwd.

Voor architecten zijn met name de volgende verplichtingen relevant, ongeacht de precieze datum waarop ze onverkort van toepassing worden:

- Risicoclassificatie: AI-toepassingen die onder een hoogrisicocategorie vallen (bijvoorbeeld werving, kredietbeoordeling, kritieke infrastructuur, rechtshandhaving) kennen aanvullende verplichtingen op het gebied van risicomanagement, gegevensgovernance en documentatie (zie principe H10).
- Menselijk toezicht: voor hoogrisicotoepassingen moet de architectuur daadwerkelijke interventie mogelijk maken, niet alleen op papier (zie principe G7).
- Logging en bewaartermijn: hoogrisico AI-systemen vereisen automatische logging met een bewaartermijn van ten minste zes maanden, een eis die direct op de observability-laag van het platform landt (zie principe G3).
- Doorwerking van modeldocumentatie: aanbieders van GPAI-modellen zijn verplicht technische documentatie te leveren; een organisatie die op zo'n model voortbouwt, moet deze documentatie overnemen en het eigen gebruik binnen het gedocumenteerde toepassingsgebied houden (zie principe H11).

De AI Act raakt zo dezelfde drie kapstokken als de rest van deze whitepaper: wendbaarheid (uitwisselbaarheid van modellen, principe A9), weerbaarheid (continuïteit bij modeldeprecatie en menselijk toezicht, principes E8 en G7) en compliance (risicoclassificatie en documentatie-doorwerking, principes H10 en H11). Bijlage A werkt dit verder uit.

De EU Open Source Strategy

Naast CADA presenteerde de Europese Commissie op 3 juni 2026, als onderdeel van hetzelfde European Technological Sovereignty Package, ook de EU Open Source Strategy. Dit betreft een Communication, geen wetsvoorstel, en is daarmee anders dan CADA niet juridisch bindend; het geeft wel een richting aan waarop toekomstig beleid en toekomstige regelgeving kunnen voortbouwen.

De strategie kondigt gemeenschappelijke security baselines aan voor de eigen open source repositories van de Commissie, met vier elementen: security monitoring, vulnerability management, licence compliance en dependency risk detection. Dat komt inhoudelijk vrijwel overeen met wat de in principe C4 genoemde

referentiekaders (CHAOSS, OpenSSF Scorecard) en Software Composition Analysis-tooling (zie principe G6) al beogen te ondersteunen, nu ook als EU-beleidsinstrument. Op het moment van schrijven gelden deze baselines voor de eigen repositories van de Commissie, niet als verplicht kader voor marktpartijen of aanbestedingen in het algemeen.

Daarnaast kondigt de strategie een Open Source Maintenance Instrument aan, een financieringsmechanisme voor het onderhoud van kritieke open source projecten, vergelijkbaar in opzet met het Duitse Sovereign Tech Fund. Dit sluit aan bij principe C3 (actief bijdragen aan open source-gemeenschappen): de strategie erkent op EU-niveau dat onderhoud van open source een investering vereist, niet iets dat vanzelf gebeurt.

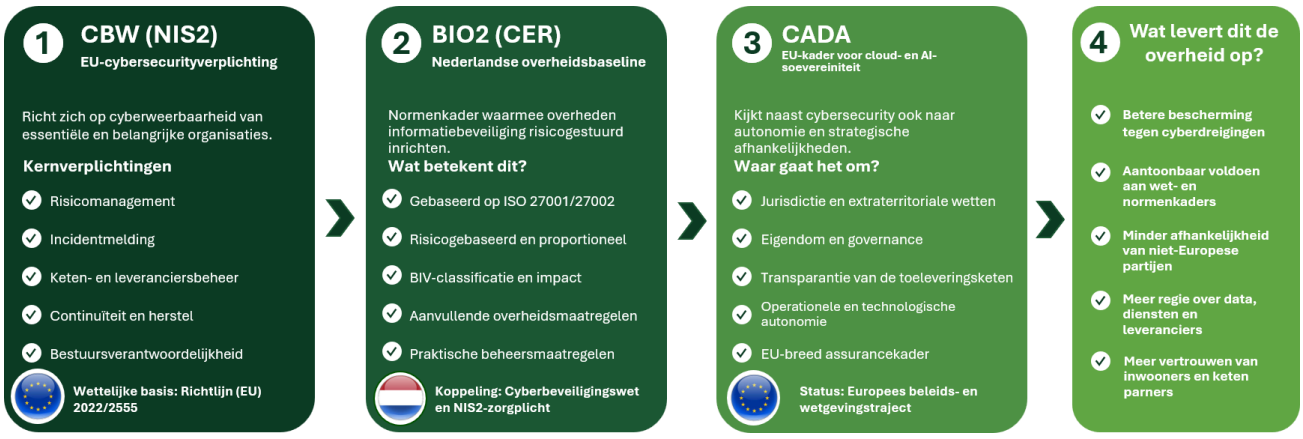
Samenvattend toetsingsmodel

Voor een architectuurbeoordeling die recht doet aan alle relevante normenkaders, adviseert deze whitepaper de volgende gelaagde toetsing:

Laag	Normenkader	Toetst
1. Basisbeveiliging	BIO2 (+ ABRO waar van toepassing)	Generieke informatiebeveiliging, verplicht voor alle overheidslagen
2. Cybersecurity-assurance	EUCS (ENISA), ISO 27018	Specifiek beveiligingsniveau van de clouddienst zelf
3. Soevereiniteit	EU Cloud Sovereignty Framework (de CADA vervangt dit op termijn)	Jurisdictie, zeggenschap, controle, transparantie
4. Portabiliteit	Data Act art. 35 + interoperabiliteitsstudie + principes uit bijlage A	Daadwerkelijke overdraagbaarheid van data en applicaties

Samenhang met NIS2/Cbw, Wwke/CER en soevereiniteit

Naast de gelaagde toetsing hierboven, die uitgaat van het type assurance (basisbeveiliging, cybersecurity, soevereiniteit, portabiliteit), is het behulpzaam dezelfde normenkaders ook te bezien vanuit de bestuurlijke volgorde waarin een organisatie ze doorloopt: van wettelijke weerbaarheidsverplichting, via de praktische baseline, naar de soevereiniteitsafweging.



Figuur 2. Van wetgeving en kaders naar weloverwogen keuzes

Cbw en Wwke zijn geen opeenvolgende stappen, maar zusterrichtlijnen die op dezelfde datum van kracht zijn geworden: Cbw (NIS2) adresseert digitale weerbaarheid, Wwke (CER) adresseert fysieke en hybride weerbaarheid (sabotage, natuurrampen, insider-dreigingen). Zodra een organisatie als kritieke entiteit onder Wwke wordt aangewezen, valt de bijbehorende IT-omgeving automatisch ook onder Cbw. Voor workloads met een OT-component werkt principe E6 (bijlage A) dit verder uit.

Dit vertaalt zich naar een praktisch, viertraps proces dat een architect of informatiebeveiliger kan doorlopen bij het beoordelen van een clouddienst of AI-toepassing, waarbij de eerste stap uitgaat van de bekende BIV-classificatie (Beschikbaarheid, Integriteit, Vertrouwelijkheid):

7. Wat dit betekent voor architecten

De voorgaande hoofdstukken beschrijven een samenhangende visie. Dit hoofdstuk vertaalt die visie naar een praktisch afwegingskader dat architecten kunnen gebruiken bij concrete platform- en leveranciersbeslissingen.

Kernvragen bij een architectuurbeslissing

Bij elke significante architectuurbeslissing, een nieuw platform, een nieuwe leverancier, een nieuwe workload, adviseren wij de volgende vragen expliciet te beantwoorden en te documenteren, gegroepeerd langs de drie kapstokken uit hoofdstuk 3:

Wendbaarheid

- Portabiliteit: is er een getest migratiepad naar minimaal één alternatief platform? In welk exportformaat kan de data worden overgezet, en welke informatie (semantiek, metadata) gaat daarbij mogelijk verloren?
- Open architectuur: is deze component vervangbaar zonder de gehele architectuur te moeten herbouwen? Zijn er technische afhankelijkheden die verdergaan dan functioneel noodzakelijk is?
- Open standaarden: welke standaarden worden gebruikt voor API's, IAM en dataformaten, en zijn dit erkende (Forum Standaardisatie, Europese of internationale) standaarden?
- Open source: welke platformcomponenten zijn open source, en is de workload-keuze van de klant daarmee onbeperkt?

Weerbaarheid

- Continuïteit: wat gebeurt er met deze workload als de leverancier uitvalt, wordt overgenomen door een partij buiten de EU, of anderszins niet meer kan leveren? Is er een reële achtervang?
- Databescherming en privacy: is een DPIA uitgevoerd voor deze workload, en welke aanvullende waarborgen gelden er als de cloudprovider optreedt als verwerker van persoonsgegevens?
- Security: welk assurance-niveau (bijvoorbeeld EUCS Basic/Substantial/High) is vastgesteld voor deze workload?

Compliance

- Soevereiniteit en jurisdictie: onder welke jurisdictie valt de leverancier, waar wordt de data verwerkt en opgeslagen, en welk SEAL-niveau of gelijkwaardige score is aantoonbaar?
- Contractuele borging: welke ontbindingsmogelijkheden gelden bij een ongewenste wijziging van zeggenschap bij de leverancier, en is dit onafhankelijk geverifieerd of alleen zelfverklaard?

Een gedifferentieerde aanpak per workload

Niet elke workload vereist hetzelfde niveau van soevereiniteit, portabiliteit of continuïteit. Een dogmatische, uniforme toepassing van alle principes uit bijlage A op elke applicatie leidt tot onnodige kosten en vertraging. In lijn met de kabinetsreactie op de initiatiefnota Wolken aan de horizon en het herziene Rijksbreed cloudbeleid adviseren wij een risico- en kriticiteitsafhankelijke toepassing:

- Voor niet-kritieke, niet-gevoelige workloads (bijvoorbeeld publieke informatievoorziening) is gebruik van grote, niet-Europese clouddiensten in beginsel geen probleem, mits een reële exit-mogelijkheid bestaat en er een getest migratiepad is.
- Voor bedrijfskritieke en gevoelige workloads (persoonsgegevens, kritieke bedrijfsvoering) gelden aanvullende eisen op het gebied van jurisdictie en soevereiniteit, conform BIO2 en het Cloud Sovereignty Framework.
- Voor workloads met een nationale-veiligheidsdimensie geldt het uitgangspunt dat staatsgeheim-gerubriceerde informatie nooit in de public cloud wordt verwerkt, en gelden de aanvullende ABRO-eisen.

De gewichtsclassificatie uit bijlage A (kernprincipe, aanbevolen principe, contextafhankelijk principe) sluit hierop aan: kernprincipes gelden voor vrijwel elke workload uit bovenstaande indeling, aanbevolen principes wegen zwaarder naarmate een workload kritieker is, en contextafhankelijke principes komen pas in beeld wanneer de specifieke situatie (OT-component, consortium, nationale veiligheid) daadwerkelijk van toepassing is. Dit voorkomt dat een architect bij elke workload alle bijna zestig principes gelijkwaardig moet doorlopen.

Met "kritieke bedrijfsvoering" doelen wij op systemen die mede bepalend zijn voor het functioneren van de fysieke leefomgeving, zoals systemen die vallen onder de noemer operationele technologie (OT): aansturing van waterkeringen en waterzuivering, energievoorziening, industriële processen en logistiek. Voor dit type systemen gaat het niet primair om vertrouwelijkheid van gegevens, maar om de beschikbaarheid en integriteit ervan: onbevoegde overname of stillegging door derden kan direct maatschappelijk ontwrichtend zijn. De Wet weerbaarheid kritieke entiteiten (Wwke, sinds augustus 2026 van kracht, de Nederlandse vertaling van de Europese Critical Entities Resilience-richtlijn) verplicht organisaties die essentiële diensten leveren tot weerbaarheid tegen zowel fysieke als digitale dreigingen. Cloudproviders die kritieke overheidsapplicaties met een OT-component hosten, kunnen op grond hiervan zelf worden aangewezen als kritieke entiteit, met bijbehorende aanvullende verplichtingen.

De financiële dimensie van architectuurkeuzes

Deze whitepaper richt zich op architectuurprincipes, niet op een volledige business case of financieringsstrategie, dat blijft de verantwoordelijkheid van de opdrachtgevende organisatie. Toch heeft elke keuze op het gebied van wendbaarheid, weerbaarheid en compliance een kostenkant die een architect zichtbaar moet maken, ook als de uiteindelijke afweging bij bestuurders ligt. Principe D6 (bijlage A) vereist al dat exit-kosten expliciet worden meegewogen in de Total Cost of Ownership. Diezelfde discipline geldt breder: een architectuur die aanzienlijk soeverein of weerbaar is, maar tegen een veelvoud van de kosten van een alternatief, zal in de praktijk moeilijk op brede adoptie kunnen rekenen. Een architect documenteert daarom bij belangrijke architectuurbeslissingen niet alleen de bijdrage aan wendbaarheid, weerbaarheid en compliance, maar ook de verwachte impact op CAPEX, OPEX en beheerkosten, zodat bestuurders een volledige afweging kunnen maken.

Praktisch stappenplan voor architecten

- 1. Breng de bestaande cloudportfolio in kaart en classificeer elke workload naar kriticiteit en gevoeligheid van data.
- 2. Toets voor elke workload of een reëel getest migratiepad bestaat; documenteer waar dit ontbreekt als architectuurschuld.

- 3. Beoordeel leveranciers expliciet op zowel het EUCS-assurance-niveau als het Cloud Sovereignty Framework-niveau, niet op basis van marketingclaims, maar op basis van de onderliggende scores en criteria.
- 4. Neem portabiliteit op als vast, terugkerend agendapunt in architectuurreviews, niet als eenmalige exercitie.
- 5. Prioriteer open standaarden en gestandaardiseerde API's bij nieuwe ontwikkeling, ook wanneer dit op korte termijn meer inspanning vraagt dan een leverancierssspecifieke oplossing.
- 6. Volg de ontwikkeling van de Open Referentie Cloud Architectuur (ORCA) en de "uniforme stekker" van de Open Cloud Alliantie, en anticipeer hierop in nieuwe architectuurkeuzes.

8. Implementatieperspectief

Het manifest Een Open Cloud voor Nederland schetst drie actielijnen op bestuurlijk niveau: starten en leveren, opschalen, en Europese samenwerking. Voor architecten vertalen deze actielijnen zich naar een concreet, direct te starten werkprogramma.

Actielijn 1: starten met wat er al is

Architecten hoeven niet te wachten op de volledige uitwerking van de Open Referentie Cloud Architectuur om te beginnen. De principes uit bijlage A zijn vandaag toepasbaar op nieuwe architectuurbeslissingen, en de classificatie van portabiliteit uit hoofdstuk 5 kan direct worden gebruikt om bestaande workloads te beoordelen. Begin bij applicaties die al cloud-native zijn opgebouwd, daar is de transitie naar een portabele, gestandaardiseerde architectuur het eenvoudigst, en bij workloads met overzichtelijke impact, zodat er ervaring wordt opgebouwd zonder dat fouten direct grote gebruikersgroepen raken.

Actielijn 2: opschalen via herbruikbare architectuurpatronen

Naarmate meer workloads volgens dezelfde principes worden beoordeeld en ingericht, ontstaan herbruikbare architectuurpatronen: referentie-implementaties voor IAM-koppelingen op basis van OIDC/OAuth, gestandaardiseerde datamigratieprocedures, en getoetste leveranciersprofielen op basis van het EUCS- en Sovereignty Framework-toetsingsmodel uit hoofdstuk 6. Het vastleggen en delen van deze patronen, binnen de eigen organisatie en, waar relevant, tussen overheidsorganisaties, versnelt de toepassing aanzienlijk ten opzichte van het steeds opnieuw doordenken van dezelfde vraagstukken.

Actielijn 3: aansluiten bij de Europese ontwikkeling

De architectuurprincipes in deze whitepaper staan niet op zichzelf, maar sluiten aan bij een bredere Europese beweging: de Interoperable Europe Act, de Data Act en het EU Cloud Sovereignty Framework zijn reeds vastgesteld, terwijl de Cloud and AI Development Act nog een wetgevingsvoorstel is dat de reguliere EU-procedure moet doorlopen. Architecten die hun eigen architectuurbeslissingen nu al baseren op de vastgestelde kaders, en anticiperen op het CADA-voorstel zonder er volledig op te bouwen, verkleinen het risico op een architectuur die later alsnog moet worden aangepast.

Verandermanagement: de andere helft van het werk

Een soevereine, portabele architectuur draait op een andere stack dan waar veel overheidsorganisaties aan gewend zijn. Dat raakt niet primair de eindgebruiker, maar wél de architecten die de stack moeten ontwerpen, de beheerders die 24/7 beschikbaarheid moeten leveren, en de bestuurders die de investeringsbeslissing moeten nemen en dragen. Zonder draagvlak bij deze groepen komt geen enkele architectuurtransitie werkelijk van de grond, ongeacht de kwaliteit van de onderliggende techniek. Investeer daarom evenredig in kennisoverdracht, opleiding en interbestuurlijke samenwerking als in de technische implementatie zelf.

9. Ten slotte

Digitale soevereiniteit wordt op bestuurlijk niveau vastgesteld als beleidsdoel, maar wordt in de praktijk gerealiseerd door duizenden individuele ontwerpbeslissingen van architecten: de keuze voor een exportformaat, voor een IAM-standaard, voor het daadwerkelijk testen van een migratiepad in plaats van alleen documenteren ervan.

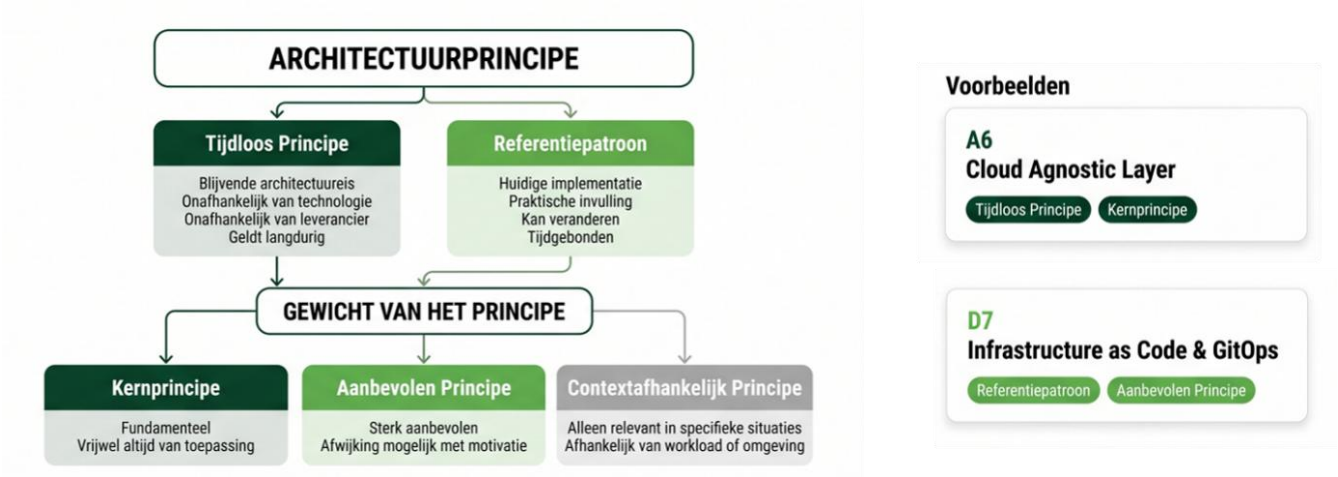
Deze whitepaper heeft geprobeerd die verbinding te leggen: van de bestuurlijke urgentie uit het manifest Een Open Cloud voor Nederland, naar een samenhangend architectuurkader, naar een fijnmazige catalogus van toetsbare principes. Dit is geen uitputtend of definitief kader. De Open Referentie Cloud Architectuur, die de Open Cloud Alliantie ontwikkelt, zal op onderdelen verdere verdieping bieden. Voor architecten die vandaag al beslissingen moeten nemen, biedt deze whitepaper in de tussentijd een bruikbaar startpunt.

Het manifest stelt terecht dat techniek niet de grootste belemmering is voor digitale soevereiniteit. De benodigde bouwstenen zijn beschikbaar. Wat op architectuurniveau resteert, is deze consequent toe te passen: in aanbestedingen, in ontwerpbeslissingen, en in de dagelijkse afweging tussen wat praktisch is en wat op termijn wendbaarheid, weerbaarheid en compliance oplevert.

Bijlage A: Architectuurprincipes

Deze bijlage bevat de volledige, fijnmazige catalogus van architectuurprincipes die aan deze whitepaper ten grondslag ligt. De principes zijn geordend langs dezelfde drie kapstokken als hoofdstuk 3: wendbaarheid (categorieën A tot en met D), weerbaarheid (categorieën E tot en met G) en compliance (categorie H). Elk principe kent een vast format: een kernstatement, een beschrijving van wat het principe in de praktijk inhoudt, de rationale (waarom dit principe nodig is) en de implicaties voor concrete ontwerpbeslissingen. Principes zijn generiek geformuleerd en per organisatie en workload te wegen, zie hoofdstuk 7 voor het bijbehorende afwegingskader.

Elk principe is bovendien gelabeld naar aard: **tijdloos principe** betreft een blijvende architectuureis die onafhankelijk is van een specifieke technologie, standaard of leverancier, terwijl **referentiepatroon (tijdelijk van aard)** een huidige, concrete implementatiekeuze, technologie of referentie-implementatie aanduidt die de onderliggende eis illustreert, maar die in de toekomst door een andere invulling kan worden vervangen. Waar een referentiepatroon wordt genoemd, blijft het onderliggende, tijdloze principe (doorgaans elders in deze bijlage terug te vinden) het uitgangspunt; het patroon is een van de manieren waarop dat principe vandaag wordt gerealiseerd.



Figuur 3. Principemodel

Daarnaast is elk principe gewaardeerd naar gewicht, om bij deze omvangrijke catalogus onderscheid te maken tussen principes die vrijwel altijd gelden en principes die alleen in specifieke situaties relevant zijn: **kernprincipe** is fundamenteel voor de architectuurvisie, raakt doorgaans meerdere bouwstenen tegelijk, en geldt vrijwel ongeacht workload of context; **aanbevolen principe** is in de meeste situaties van toepassing, met meer ruimte voor een afgewogen uitzondering; **contextafhankelijk principe** is waardevol maar alleen relevant onder specifieke omstandigheden, bijvoorbeeld bij OT-systemen, consortiumconstructies of overheidsarchivering, en vraagt geen universele toepassing. Dit gewicht is een aanvulling op, en volledig onafhankelijk van, het onderscheid tussen tijdloos principe en referentiepatroon hierboven.

DEEL I Wendbaarheid

De principes in dit deel borgen dat een organisatie kan veranderen van leverancier, platform of technologie zonder daarbij vast te lopen.

A. Open architectuur en open ecosystemen

Principes die borgen dat een architectuur modulair, uitwisselbaar en niet structureel afhankelijk van één leverancier is.

A1 Ontwerp modulair, niet monolithisch

Aard: Tijdloos principe **Gewicht: Kernprincipe**

> ***Bouw architecturen op uit losstaande, onafhankelijk vervangbare modules in plaats van als één ondeelbaar geheel.***

Beschrijving: Een modulaire architectuur verdeelt functionaliteit over afzonderlijke componenten met heldere, gedocumenteerde interfaces tussen die componenten. Elk component kan in beginsel worden vervangen zonder dat de overige componenten daarvoor opnieuw ontworpen hoeven te worden.

Rationale: Monolithische architecturen creëren impliciete afhankelijkheden tussen onderdelen die geen functionele relatie met elkaar hebben. Bij een leverancierswissel of technologie-update moet dan het geheel worden aangepast, wat kosten, risico en doorlooptijd van elke verandering onnodig vergroot.

Implicaties: Vereist bij ontwerp expliciete aandacht voor interfacedefinities en scheiding van verantwoordelijkheden (separation of concerns). Kan op korte termijn meer ontwerpinspanning vragen dan een geïntegreerde, leveranciersspecifieke oplossing.

A2 Voorkom structurele vendor lock-in

Aard: Tijdloos principe **Gewicht: Kernprincipe**

> ***Geen enkele architectuurbeslissing mag een organisatie onomkeerbaar aan één leverancier binden zonder dat dit een expliciete, gemotiveerde keuze is.***

Beschrijving: Vendor lock-in ontstaat wanneer overstapkosten (technisch, organisatorisch of financieel) zo hoog worden dat een overstap in de praktijk onmogelijk is, ongeacht de contractuele mogelijkheid daartoe. Dit principe vraagt om actieve monitoring van cumulatieve afhankelijkheid, niet alleen beoordeling per individuele beslissing.

Rationale: Uit de kabinetsreactie op de initiatiefnota Wolken aan de horizon en de ACM-marktstudie naar clouddiensten blijkt dat vendor lock-in in de praktijk vaak sluipend ontstaat: geen enkele afzonderlijke beslissing is doorslaggevend, maar de optelsom van kleine keuzes leidt tot feitelijke onvervangbaarheid.

Implicaties: Vraagt om een periodieke "lock-in-audit": een expliciete beoordeling van de cumulatieve overstapkosten van een workload, los van individuele architectuurbeslissingen.

A3 Streef naar technologische diversiteit

Aard: Tijdloos principe **Gewicht: Aanbevolen principe**

> ***Voorkom ongewenste concentratie- en afhankelijkheidsrisico's; kies bewust waar standaardisatie en waar spreiding de voorkeur verdient, in plaats van diversiteit als doel op zich na te streven.***

Beschrijving: Technologische diversiteit is geen doel op zich, maar een middel om concentratierisico te beperken. Binnen één samenhangend platform kan sterke standaardisatie juist bijdragen aan hogere betrouwbaarheid, beveiliging en operationele kwaliteit. Diversiteit is vooral waardevol tussen onafhankelijke failure domains, locaties of providers, niet noodzakelijk binnen elk platform afzonderlijk.

Rationale: Homogeniteit binnen een onafhankelijk failure domain hoeft geen probleem te zijn en kan zelfs bijdragen aan betrouwbaarheid en beheersbaarheid. Het risico ontstaat wanneer meerdere, in theorie onafhankelijke failure domains dezelfde kwetsbaarheid delen: dan kan één kwetsbaarheid, aanval of storing alsnog alle systemen tegelijk treffen. Het manifest van de Open Cloud Alliantie benadrukt daarom een gezonde variëteit tussen platformen en aanbieders, niet noodzakelijk binnen elk platform afzonderlijk.

Implicaties: Moet worden afgewogen tegen de extra beheerlast van meerdere technologieën. Beoordeel diversiteit primair op het niveau van failure domains, locaties en providers, niet als eis binnen elk individueel platform. Voor workloads die baat hebben bij schaal en sterk geïntegreerde infrastructuur, bijvoorbeeld grootschalige AI- of HPC-toepassingen, kan standaardisatie binnen het platform de voorkeur verdienen, mits dat platform zelf onderdeel is van een breder, gespreid geheel.

A4 Ontwerp voor losse koppeling (loose coupling)

Aard: Tijdloos principe **Gewicht:** Aanbevolen principe

Componenten communiceren via gedefinieerde interfaces en kennen elkaars interne werking niet.

Beschrijving: Losse koppeling betekent dat een component kan worden aangepast, vervangen of vernieuwd zonder dat de componenten die ermee samenwerken daarvan iets hoeven te weten, zolang de interface ongewijzigd blijft.

Rationale: Strak gekoppelde ("tightly coupled") systemen maken elke wijziging risicovol en duur, omdat een aanpassing in het ene onderdeel onvoorspelbare effecten kan hebben op andere onderdelen. Dit ondermijnt zowel wendbaarheid als portabiliteit.

Implicaties: Vereist API-first ontwerp en het expliciet versiebeheer van interfaces, zodat wijzigingen aan de ene kant van een koppeling niet ongecontroleerd doorwerken aan de andere kant.

A5 Maak bouwstenen herbruikbaar

Aard: Tijdloos principe **Gewicht:** Aanbevolen principe

Ontwikkel en documenteer architectuurcomponenten zodanig dat zij door andere teams en organisaties kunnen worden hergebruikt.

Beschrijving: Herbruikbaarheid betekent dat een oplossing voor een specifiek probleem (bijvoorbeeld een IAM-koppeling of een migratieprocedure) wordt vastgelegd als generiek toepasbaar patroon, in plaats van als eenmalige, projectgebonden oplossing.

Rationale: Dit sluit aan bij het reusability-principe uit het European Interoperability Framework: publieke organisaties dienen bereid te zijn hun oplossingen, concepten en componenten met andere publieke organisaties te delen. Herbruikbaarheid versnelt bovendien de opschaling van soevereine architectuurpatronen binnen de overheid.

Implicaties: Vraagt om documentatie- en beheerinspanning die verder gaat dan wat voor een enkel project strikt noodzakelijk is, maar die zich terugverdient over meerdere implementaties.

A6 Ontkoppel de platformkeuze via een Cloud Agnostic Layer

Aard: Tijdloos principe **Gewicht: Kernprincipe**

Richt een expliciete ontkoppellaag in tussen de gekozen cloudplatformen (servicelaag 1) en de federatieve functies erboven (servicelaag 2), zodat een platform vervangen kan worden zonder de federatieve laag opnieuw in te richten.

Beschrijving: Zonder deze expliciete laag verweven organisaties platformspecifieke eigenschappen ongemerkt door hun federatieve functies (identity, observability, cost management), waardoor een platformwissel alsnog een herontwerp van de federatie vereist.

Rationale: Deze laag operationaliseert de portabiliteitseis uit categorie D op architectuurniveau: zij maakt zichtbaar en toetsbaar of platformonafhankelijkheid daadwerkelijk is ingebouwd, in plaats van een intentie te blijven.

Implicaties: Vereist dat federatieve functies (zie A8) worden ontworpen tegen een geabstraheerde interface, niet tegen de API's van één specifiek cloudplatform. Deze ontkoppeling werkt overigens ongeacht of het onderliggende platform open source of closed source is: substitueerbaarheid ontstaat hier door de interface, niet door de licentie (zie ook principe C1).

A7 Ontkoppel het applicatie-ecosysteem via een Developer/Application Agnostic Layer

Aard: Tijdloos principe **Gewicht: Kernprincipe**

Richt een expliciete ontkoppellaag in tussen de federatieve cloudlaag (servicelaag 2) en het applicatie-ecosysteem (servicelaag 3), zodat ontwikkelaars en applicaties niet direct afhankelijk zijn van de specifieke inrichting van de federatie eronder.

Beschrijving: Deze laag is waar ontwikkelaars, applicaties en workloads mee werken. Zonder ontkoppeling van de federatieve laag eronder ontstaat alsnog een indirecte, moeilijk zichtbare afhankelijkheid van de gekozen platformen en federatieve inrichting.

Rationale: De Haven-standaard van VNG Realisatie, met Haven+ als bijbehorende referentie-implementatie, is het huidige Nederlandse referentievoorbeeld van deze laag in de praktijk (zie hoofdstuk 5): gemeentelijke applicaties worden hosting-onafhankelijk gemaakt via een gestandaardiseerde, containerbased interface. Haven/Haven+ is zelf een referentiepatroon dat kan evolueren; de onderliggende eis, ontkoppeling via een gestandaardiseerde interface, is het tijdloze principe dat blijft gelden.

Implicaties: Vereist dat applicaties worden ontworpen tegen gestandaardiseerde interfaces (containers, gestandaardiseerde API's) in plaats van tegen federatie-specifieke of platformspecifieke voorzieningen.

A8 Richt de Cloud Federation-laag in met expliciet benoemde, gedeelde functies

Aard: Referentiepatroon (tijdelijk van aard) **Gewicht:** Contextafhankelijk principe

Benoem welke functies onderdeel zijn van de federatieve laag, geclusterd naar vijf herkenbare groepen: Governance (identity, identity federation), Security, Connectivity (intercloud connectivity, netwerk als federatieve dienst), Platform Operations (observability, cost management) en AI Services.

Beschrijving: Deze functies zijn per definitie platformoverstijgend: zij horen niet thuis in één specifiek cloudplatform (servicelaag 1), maar vormen de gedeelde voorzieningen waarmee meerdere platformen federatief samenwerken. Het clusteren naar deze vijf groepen, in plaats van een ongeordende opsomming, maakt de federatieve laag herkenbaar en overzichtelijk te ontwerpen en te beoordelen. Fysieke netwerkconnectiviteit (WAN, mobiele diensten) valt hier nadrukkelijk buiten: dat is randvoorwaardelijke infrastructuur, geen federatieve functie. AI Services binnen deze laag betreft platformoverstijgende voorzieningen zoals gedeelde modellencatalogi en AI-governance; specifieke AI-infrastructuur zoals accelerated compute, gespecialiseerde AI-opslag, high-performance networking, runtimes en de onderliggende trainingsdata laat zich niet volledig als federatieve dienst abstraheren en vraagt om een eigen, platformspecifieke afweging, zie categorie D voor de portabiliteitsafweging die dit met zich meebrengt.

Rationale: Zonder expliciete benoeming van deze functies en clustering ontstaat het risico dat federatieve voorzieningen alsnog impliciet aan één platform worden gekoppeld, bijvoorbeeld door gebruik van de platform-eigen identity-dienst zonder federatielaag ertussen, of dat de indeling van de federatieve laag per project willekeurig verschilt.

Implicaties: Vereist een architectuurbeslissing per federatieve functiegroep: welke gestandaardiseerde interface of welk protocol (bijvoorbeeld OIDC voor identity federation) wordt gebruikt, onafhankelijk van het onderliggende platform. De precieze indeling in vijf groepen is zelf een referentiepatroon en kan per organisatie worden aangepast, zolang de onderliggende eis (platformoverstijgende, expliciet ontworpen federatieve functies) overeind blijft.

A9 Standaardiseer de aanroep-interface van AI-modellen

Aard: Tijdloos principe **Gewicht:** Aanbevolen principe

Standaardiseer de interface waarmee applicaties AI-modellen aanroepen, zodat een onderliggend model vervangen kan worden zonder de applicatie te herbouwen.

Beschrijving: Net als bij cloudplatformen (zie principe A2) ontstaat afhankelijkheid van één AI-modelaanbieder wanneer applicaties rechtstreeks tegen de specifieke API van dat model worden gebouwd, in plaats van tegen een geabstraheerde interface. Een modelgateway of vergelijkbare abstractielaag maakt het mogelijk om onderliggende modellen te vervangen, te vergelijken of te combineren zonder de applicatiecode aan te passen.

Rationale: Modellen ontwikkelen zich sneller dan cloudplatformen, en aanbieders wijzigen regelmatig hun dienstenaanbod, prijsmodel of beschikbaarheid. Zonder ontkoppeling wordt elke modelwissel een applicatie-herbouw in plaats van een configuratiewijziging.

Implicaties: Vereist een architectuurbeslissing voor een modelgateway of vergelijkbare abstractielaag, met gestandaardiseerde in- en uitvoerformaten, voordat een AI-toepassing in productie wordt genomen.

B. Open standaarden

Principes die de interoperabiliteit tussen componenten en platformen technisch mogelijk maken.

B1 Pas toe of leg uit

Aard: Tijdloos principe **Gewicht: Kernprincipe**

Gebruik de open standaarden op de lijst van het Forum Standaardisatie; wijk hiervan alleen gemotiveerd af.

Beschrijving: Het "pas toe of leg uit"-beleid is wettelijk verankerd via de Wet digitale overheid voor ICT-aanschaffingen vanaf € 50.000. Een architect die van een aanbevolen standaard afwijkt, documenteert expliciet waarom en welke risico's dit met zich meebrengt.

Rationale: Zonder een gedeeld, verplicht uitgangspunt ontstaat versnippering: elke organisatie kiest eigen standaarden, waardoor interoperabiliteit tussen overheidsorganisaties in de praktijk verdwijnt, ook al is elke individuele keuze op zichzelf verdedigbaar.

Implicaties: Vereist een structureel proces om nieuwe architectuurkeuzes te toetsen aan de actuele Forum Standaardisatie-lijst, en een vastgelegde escalatieroute voor gemotiveerde afwijkingen.

B2 Geef voorrang aan internationale en Europese standaarden boven proprietary alternatieven

Aard: Tijdloos principe **Gewicht:** Aanbevolen principe

Bij een keuze tussen een open, breed gedragen standaard en een leveranciersspecifiek alternatief, heeft de open standaard de voorkeur. Afwijking is mogelijk wanneer het alternatief aantoonbaar strategische waarde biedt,

mits dit gezamenlijk wordt afgewogen door business-, architectuur- en security & continuity-stakeholders, en expliciet gedocumenteerd wordt vastgelegd.

Beschrijving: Internationale en Europese standaardisatieorganisaties (zoals ISO, ETSI en de instanties achter TOSCA, OIDC en OAuth) ontwikkelen specificaties in een open, consensusgedreven proces, wat de kans op langdurige beschikbaarheid en brede ondersteuning vergroot ten opzichte van eigendomsspecificaties van één leverancier. Voor de Nederlandse overheidscontext geldt daarnaast de aanbevolen en deels verplichte standaardenlijst van het Forum Standaardisatie als praktisch vertrekpunt: zie principe B1 voor het bijbehorende "pas toe of leg uit"-beleid.

Rationale: Proprietary standaarden kunnen op korte termijn functioneel superieur zijn, maar creëren op middellange termijn afhankelijkheid van de voortzetting en het onderhoud door één specifieke leverancier.

Implicaties: Vraagt om een gestructureerd afwegingsmoment tussen business, architectuur en security & continuity, waarin de strategische waarde van het alternatief expliciet wordt gewogen tegen de resulterende lock-in-risico's (zie principe A2) en exit-kosten (zie principe D6). Een eenzijdige business- of architectuurbeslissing is onvoldoende: alle drie de perspectieven moeten aantoonbaar zijn betrokken, en de uitkomst wordt gedocumenteerd (zie ook principe H7 voor de bijbehorende governance-rol).

B3 Standaardiseer API's over platformgrenzen heen

Aard: Tijdloos principe **Gewicht: Kernprincipe**

Ontwerp en documenteer API's zodanig dat zij consistent zijn, ongeacht of de onderliggende voorziening centraal of gedistribueerd is georganiseerd. Voor de Nederlandse overheidscontext betekent dit concreet: aansluiten bij de standaarden van het Forum Standaardisatie, de REST-API Design Rules en de API-standaarden van Logius, en het kennisplatform developer.overheid.nl (Kennisplatform API's) raadplegen voor actuele richtlijnen en voorbeelden.

Beschrijving: Eén werkmodel voor API's, onafhankelijk van de fysieke of organisatorische locatie van de dienst, voorkomt dat elke nieuwe leverancier of platform een eigen integratie-inspanning vergt. Een component achter een gestandaardiseerde API is in beginsel vervangbaar, ook wanneer de onderliggende software zelf closed source is (zie principe C1 voor de aanvullende afweging die open source daarnaast biedt).

Rationale: Het manifest van de Open Cloud Alliantie benoemt gestandaardiseerde API's expliciet als kernvoorwaarde voor het "landen" van applicaties op uiteenlopende platformen, de kern van de beoogde "uniforme stekker".

Implicaties: Vereist bij multi-platform-architecturen een centraal beheerde API-gateway of -catalogus, met versiebeheer en duidelijke contractdefinities (bijvoorbeeld via OpenAPI-specificaties), en het periodiek toetsen van nieuwe API's aan de REST-API Design Rules van Logius.

B4 Standaardiseer identity- en accessmanagement (IAM)

Aard: Tijdloos principe **Gewicht: Aanbevolen principe**

Gebruik open IAM-standaarden zoals OIDC, OAuth 2.0 en SAML voor authenticatie en autorisatie, ongeacht het onderliggende platform.

Beschrijving: Een gestandaardiseerde IAM-laag zorgt ervoor dat gebruikersidentiteiten en autorisaties overdraagbaar zijn tussen platformen, zonder dat bij elke migratie een volledig nieuw toegangsbeheer moet worden opgebouwd. De drie genoemde standaarden dekken elk een andere praktijksituatie, en zijn niet onderling inwisselbaar: SAML blijft dominant bij bestaande, vaak langlopende enterprise-koppelingen (denk aan ADFS- of Shibboleth-achtige voorzieningen) en verdwijnt naar verwachting niet op korte termijn, terwijl OIDC inmiddels het standaardadvies is voor nieuwe ontwikkeling, met name voor mobiele en API-toepassingen waarvoor SAML technisch ongeschikt is. OAuth 2.0

vormt in beide gevallen de onderliggende autorisatiestandaard, waarbij de praktijk inmiddels convergeert rond OAuth 2.1 (met Authorization Code plus PKCE als aanbevolen uitwisselingsflow) als de bijgewerkte best practice.

Rationale: IAM is doorgaans de meest onderschatte bron van operationele lock-in: zelfs wanneer applicatie en data goed overdraagbaar zijn, kan een leverancierssspecifieke IAM-implementatie een migratie alsnog vertragen of blokkeren.

Implicaties: Vereist ontkoppeling van de IAM-laag van specifieke platformfunctionaliteit, en periodieke toetsing of IAM-koppelingen daadwerkelijk overdraagbaar zijn (niet alleen in theorie, maar getest). Houd bij nieuwe ontwikkeling rekening met de keuze tussen SAML en OIDC als een bewuste, situatieafhankelijke afweging, niet als vrije keuze tussen gelijkwaardige alternatieven, en volg de ontwikkeling van opkomende standaarden voor niet-menselijke identiteiten (workload-identiteit, bijvoorbeeld SPIFFE), die met de opkomst van machine-to-machine- en AI-toepassingen aan relevantie winnen.

B5 Documenteer en publiceer gebruikte standaarden en versies

Aard: Tijdloos principe **Gewicht:** Aanbevolen principe

Leg voor elk systeem expliciet vast welke standaarden en welke versies daarvan worden gebruikt.

Beschrijving: Documentatie van gebruikte standaarden, inclusief versienummers en eventuele afwijkingen van de standaard, is een randvoorwaarde om interoperabiliteit en portabiliteit op enig moment daadwerkelijk te kunnen beoordelen en testen.

Rationale: Zonder deze documentatie is niet vast te stellen of twee systemen die beide beweren een bepaalde standaard te gebruiken, ook daadwerkelijk met elkaar kunnen samenwerken; standaarden kennen vaak varianten en optionele onderdelen.

Implicaties: Vraagt om opname van standaardendocumentatie als vast onderdeel van architectuurdossiers en leveranciersdocumentatie, niet als losstaand of optioneel document.

C. Open source software

Principes over de rol van open source op platformniveau. Primair een wendbaarheidsinstrument, met een aanvullende weerbaarheidsnuance in C6, en met behoud van vrijheid van workload-keuze (zie hoofdstuk 4).

C1 Maximaliseer open source op platformniveau

Aard: Tijdloos principe **Gewicht: Kernprincipe**

Gebruik voor het cloudplatform, het fundament waarop applicaties draaien, zoveel mogelijk open source software, binnen de voorwaarden en afwegingen die dit principe daaraan stelt.

Beschrijving: Dit principe betreft uitdrukkelijk de infrastructuurlaag (compute, storage, netwerk, orkestratie), niet de applicaties die op die infrastructuur worden ingezet. Waar volwassen open source-alternatieven ontbreken, is closed-source platformsoftware een tijdelijk aanvaardbare keuze, mits transparant gedocumenteerd.

Rationale: Open source op platformniveau vergroot controleerbaarheid en sluit aan bij Europese initiatieven zoals IPCEI-CIS, dat expliciet inzet op open source voor de cloud-edge-continuum-laag. Substitueerbaarheid van een bouwblok ontstaat overigens primair via een open, gestandaardiseerde interface (zie principe B3 en de Cloud Agnostic Layer, principe A6): een closed-source component achter een open standaard is in beginsel al vervangbaar. Open source voegt daar een eigen, aanvullende waarde aan toe die een open standaard niet biedt: de mogelijkheid om het beheer zelf over te nemen wanneer een leverancier wegvalt (zie principe C6). Dit zijn twee afzonderlijke afwegingen; een architect kan bewust kiezen voor een closed-source oplossing achter een open standaard wanneer vervangbaarheid voldoende is geborgd, ook zonder dat de onderliggende code open is.

Implicaties: Vereist een periodieke inventarisatie van welke platformcomponenten (nog) geen volwassen open source-alternatief kennen, zodat dit bewust en zichtbaar wordt beheerd in plaats van stilzwijgend te blijven bestaan.

C2 Laat klanten vrij in de keuze van workloads

Aard: Tijdloos principe **Gewicht: Kernprincipe**

> ***De keuze voor open source op platformniveau legt geen beperking op aan de applicaties en workloads die klanten op dat platform draaien.***

Beschrijving: Commerciële, closed-source applicatiesoftware blijft volledig inzetbaar op een overwegend open source platform. Dit principe voorkomt dat "open source" wordt verward met een verplichting voor eindgebruikers.

Rationale: Zonder deze expliciete scheiding ontstaat het risico dat een soevereine architectuurvisie wordt afgewezen als onpraktisch of ideologisch, terwijl de kern van de visie, controle over het fundament, losstaat van de keuze voor specifieke applicatiesoftware.

Implicaties: Vereist heldere communicatie naar klanten en gebruikers over waar het principe van open source wel en niet van toepassing is, om verwarring te voorkomen.

C3 Draag actief bij aan open source-gemeenschappen

Aard: Tijdloos principe **Gewicht: Aanbevolen principe**

> ***Consumeer open source-componenten niet alleen, investeer ook in het onderhoud en de doorontwikkeling ervan.***

Beschrijving: Actieve bijdrage kan bestaan uit het melden en oplossen van kwetsbaarheden, het financieel ondersteunen van kernontwikkelaars, of het beschikbaar stellen van eigen personeelscapaciteit aan een gemeenschapsproject.

Rationale: Een organisatie die uitsluitend consumeert zonder bij te dragen, bouwt een nieuwe, subtielere vorm van afhankelijkheid op: die van de bereidheid van een externe gemeenschap om het component te blijven onderhouden. Bij onvoldoende bijdrage door de bredere gebruikersgroep kan een kritiek component zonder waarschuwing onderhoudsloos raken.

Implicaties: Vraagt om een expliciete afweging in de begroting: bijdragen aan open source-onderhoud als investering in continuïteit, niet als vrijblijvende geste.

C4 Beoordeel elk open source-component op onderhoudsstatus en kwaliteit

Aard: Tijdloos principe **Gewicht: Kernprincipe**

> ***Neem geen open source-component in gebruik zonder due diligence op actief onderhoud, kwetsbaarhedenbeleid en gemeenschapsomvang.***

Beschrijving: De kwaliteit en onderhoudsstatus van open source-projecten loopt sterk uiteen: van professioneel beheerde, breed gedragen projecten tot projecten die door één vrijwilliger in de vrije tijd worden onderhouden. Voor deze beoordeling bestaan inmiddels gevestigde, breed erkende referentiekaders: CHAOSS (Linux Foundation) voor community- en gezondheidsmetrics, en OpenSSF Scorecard (eveneens Linux Foundation, ook aanbevolen door de Amerikaanse CISA) voor beveiligingspraktijken van een project. Beide zijn publiek raadpleegbaar en vormen een concreet startpunt, in aanvulling op de eigen beoordeling van een organisatie.

Rationale: Een generieke aanname dat "open source" gelijk staat aan "veilig" of "betrouwbaar" is onjuist en kan tot onverwachte risico's leiden, met name bij kritieke platformcomponenten diep in de afhankelijkheidsketen. Bestaande frameworks dekken overigens niet elk risico: voor de geografische herkomst van bijdragen aan een project (welke

landen of organisaties leveren de code) bestaat op dit moment geen breed erkend meetinstrument. Dit blijft een open leemte, ook binnen het EU Cloud Sovereignty Framework.

Implicaties: Vereist een vast beoordelingsproces (bijvoorbeeld op basis van commit-frequentie, aantal actieve onderhouders, en het bestaan van een verantwoord-openbaarmakingsbeleid) voordat een component in productie wordt genomen.

C5 Respecteer de commerciële basis van applicatiesoftware

Aard: Tijdloos principe **Gewicht:** Aanbevolen principe

> ***Deze whitepaper en de bijbehorende architectuurprincipes gaan over het platform, niet over de intellectuele-eigendomsbescherming van applicaties die private bedrijven hebben ontwikkeld.***

Beschrijving: Veel toepassingssoftware is ontwikkeld door private partijen die hun investering terugverdienen via licentie- of abonnementsmodellen. Dit principe erkent expliciet dat deze commerciële basis legitiem en noodzakelijk is voor een gezonde softwaremarkt.

Rationale: Zonder deze erkenning zou een te dogmatische toepassing van open source-principes de markt voor applicatiesoftware kunnen ondermijnen, met als gevolg minder keuze en minder innovatie voor overheidsorganisaties.

Implicaties: Vraagt om een architectuur die closed-source applicaties even goed kan hosten als open source applicaties, zolang het platform zelf aan de overige principes uit deze bijlage voldoet.

C6 Benut de operationele ontvlechtbaarheid van open source voor weerbaarheid

Aard: Tijdloos principe **Gewicht:** Contextafhankelijk principe

> ***Beoordeel bij kritieke platformcomponenten expliciet of het beheer, bij uitval of geopolitieke druk op de oorspronkelijke leverancier, door een andere partij of door de organisatie zelf kan worden overgenomen.***

Beschrijving: Omdat de broncode van open source componenten niet aan één leverancier gebonden is, kan de operationele verantwoordelijkheid in theorie worden overgedragen zonder dat de software zelf vervangen hoeft te worden. Dit is een aanvullende bijdrage aan weerbaarheid, naast de wendbaarheidsbijdrage die in C1 tot en met C5 centraal staat, en een andere bijdrage dan de substitueerbaarheid die een open standaard biedt (zie principe B3): een open standaard maakt een component vervangbaar, open source maakt het bovendien mogelijk om het beheer ervan zelf over te nemen.

Rationale: Deze weerbaarheidsbijdrage is voorwaardelijk en geen automatisme: zonder voldoende kennis, documentatie en een reëel alternatief beheerteam blijft de theoretische overdraagbaarheid van de broncode zonder praktische waarde, zoals hoofdstuk 4 toelicht.

Implicaties: Vereist dat voor kritieke open source componenten expliciet wordt vastgelegd welke partijen (intern of extern) in staat zijn het beheer over te nemen, en dat dit periodiek wordt getoetst, vergelijkbaar met de continuïteitsprincipes in categorie E.

D. Portabiliteit

Principes die de daadwerkelijke, geteste overdraagbaarheid van data, applicaties en beheer waarborgen (zie hoofdstuk 5).

Portabiliteit is een afweging, geen universeel optimum: niet elke workload hoeft volledig platformonafhankelijk te zijn. Een organisatie kan bewust kiezen voor platformspecifieke mogelijkheden, bijvoorbeeld gespecialiseerde AI-hardware of high-performance infrastructuur, wanneer de voordelen daarvan opwegen tegen de extra

afhankelijkheid, mits dit een expliciete, gemotiveerde keuze is met een realistische exit-mogelijkheid (zie principe A2) en een getest migratiepad zodra dat wordt ingezet (zie principe D1).

D1 Combineer exit-strategie altijd met een getest migratiepad

Aard: Tijdloos principe **Gewicht: Kernprincipe**

> ***Een exit-strategie zonder aantoonbaar getest migratiepad wordt beschouwd als onvolledig.***

Beschrijving: Voor elke workload waarvoor een exit-strategie is vastgelegd, wordt minimaal één keer een representatieve migratie uitgevoerd of gesimuleerd, met documentatie van de resultaten, doorlooptijd en eventuele functionaliteitsverliezen.

Rationale: Een exit-strategie die alleen op papier bestaat, geeft schijnzekerheid: op het moment dat een daadwerkelijke exit nodig is (bijvoorbeeld door een overname van de leverancier door een partij buiten de EU), blijkt vaak pas dan dat de praktische uitvoering onvoldoende is voorbereid.

Implicaties: Vereist capaciteit en budget voor periodieke migratieoefeningen, ook wanneer een daadwerkelijke exit op korte termijn niet wordt verwacht.

D2 Vermijd niet-standaard exportformaten en verborgen datamodellen

Aard: Tijdloos principe **Gewicht: Aanbevolen principe**

> ***Data wordt opgeslagen en beschikbaar gesteld in gedocumenteerde, bij voorkeur open formaten, niet in leveranciersspecifieke, ongedocumenteerde structuren.***

Beschrijving: Een exportformaat is pas bruikbaar als de structuur en semantiek ervan volledig gedocumenteerd zijn, zodat een ontvangend systeem de data correct kan interpreteren zonder reverse engineering.

Rationale: Veel praktische migratieproblemen ontstaan niet doordat export technisch onmogelijk is, maar doordat het exportformaat onvoldoende gedocumenteerd is om de data elders correct te kunnen laden, met verlies van metadata, classificaties en onderlinge relaties tot gevolg.

Implicaties: Vereist bij elke nieuwe dataopslag-beslissing een expliciete toets: is er een gedocumenteerd exportpad, en is dit ooit daadwerkelijk gebruikt?

D3 Classificeer portabiliteit per workload langs vier dimensies

Aard: Tijdloos principe **Gewicht: Aanbevolen principe**

> ***Beoordeel voor elke workload afzonderlijk de dataportabiliteit, applicatieportabiliteit, operationele portabiliteit en operationele omkeerbaarheid.***

Beschrijving: Portabiliteit is geen binaire eigenschap. Een workload kan bijvoorbeeld goed overdraagbare data hebben, maar een applicatielogica die vrijwel volledig herbouwd moet worden, of omgekeerd. Zie de classificatietabel in hoofdstuk 5.

Rationale: Zonder deze differentiatie ontstaat een vals gevoel van portabiliteit: een organisatie die alleen dataportabiliteit heeft getoetst, kan ten onrechte concluderen dat een workload volledig overdraagbaar is.

Implicaties: Vereist het vastleggen van vier aparte scores per workload in het architectuurdossier, in plaats van één samengevat "portabiliteitsoordeel".

D4 Test operationele omkeerbaarheid bij consortiumconstructies

Aard: Tijdloos principe **Gewicht: Contextafhankelijk principe**

Wanneer meerdere aanbieders gezamenlijk een dienst leveren (consortium), wordt getest of taken tijdelijk of blijvend kunnen worden overgedragen tussen consortiumpartners.

Beschrijving: Operationele omkeerbaarheid is een aparte beoordelingscategorie uit het EU Cloud Sovereignty Framework: de mogelijkheid om bij problemen bij één aanbieder het beheer over te dragen aan een andere, vooraf gekwalificeerde partij binnen hetzelfde consortium.

Rationale: Consortiumconstructies worden vaak opgezet met de aanname dat overdracht bij calamiteiten "vanzelf" mogelijk is, terwijl dit in de praktijk aanzienlijke voorbereiding vergt: gedeelde toegang, gedeelde documentatie en geoefende overdrachtsprocedures.

Implicaties: Vereist contractuele en technische afspraken over overdracht als vast onderdeel van elke consortiumovereenkomst, inclusief een periodieke oefening.

D5 Ontwikkel en onderhoud een uniforme interface-laag ("stekker")

Aard: Referentiepatroon (tijdelijk van aard) **Gewicht:** Contextafhankelijk principe

Werk toe naar een gestandaardiseerde, platformonafhankelijke interface waarmee applicaties kunnen "landen" op verschillende onderliggende platformen.

Beschrijving: Naar analogie van de invoering van de uniforme Eurostekker in 1990: geen keuze voor één technologie, maar een afspraak over de interface waarmee uiteenlopende technologieën met elkaar kunnen samenwerken. Dit principe loopt vooruit op de door de Open Cloud Alliantie ontwikkelde Open Referentie Cloud Architectuur (ORCA).

Rationale: Zonder een dergelijke gedeelde interface-laag blijft portabiliteit afhankelijk van ad-hoc, per-platformpaar ontwikkelde koppelingen, wat niet opschaalt naarmate het aantal platformen toeneemt.

Implicaties: Vereist actieve betrokkenheid bij en afstemming met de ontwikkeling van ORCA, en het inbouwen van compatibiliteit met deze interface-laag in nieuwe architectuurbeslissingen.

D6 Neem exit-kosten expliciet mee in de Total Cost of Ownership

Aard: Tijdloos principe **Gewicht:** Aanbevolen principe

Bereken bij elke platform- of leveranciersbeslissing de verwachte kosten van een toekomstige exit als onderdeel van de totale kostenvergelijking.

Beschrijving: Een TCO-berekening die geen rekening houdt met exit-kosten (waaronder migratiekosten, tijdelijke dubbele beheerlasten, en mogelijke functionaliteitsverliezen) onderschat structureel de werkelijke kosten van leverancierssspecifieke oplossingen.

Rationale: De kabinetsreactie op de initiatiefnota Wolken aan de horizon signaleert expliciet dat TCO-berekeningen bij IT-aanbestedingen vaak worden gemaakt zonder exit-kosten mee te wegen, met als gevolg dat leveranciers die op korte termijn goedkoper lijken systematisch worden bevoordeeld.

Implicaties: Vereist een gestandaardiseerde TCO-methodiek waarin exit-kosten als verplicht onderdeel zijn opgenomen, met een expliciete inschatting op basis van eerdere migratie-ervaringen.

D7 Gebruik infrastructure-as-code en GitOps om portabiliteit operationeel afdwingbaar te maken

Aard: Referentiepatroon (tijdelijk van aard) **Gewicht:** Aanbevolen principe

Beschrijf infrastructuur en applicatieconfiguratie declaratief in versiebeheerde bestanden, met een gereedschap dat open, gedocumenteerde configuratieformaten hanteert, en gebruik een GitOps-werkwijze om deze configuratie geautomatiseerd en controleerbaar uit te rollen.

Beschrijving: Infrastructure-as-code maakt een migratiepad reproduceerbaar: dezelfde, reeds geteste configuratie kan in beginsel opnieuw worden toegepast op een ander platform dat de gebruikte standaarden ondersteunt, in plaats van dat een migratie een handmatige, foutgevoelige exercitie is.

Rationale: Zonder deze werkwijze blijft de eis uit D1, dat een migratiepad aantoonbaar getest moet zijn, moeilijk haalbaar: handmatig ingerichte infrastructuur is lastig te reproduceren en de testresultaten verouderen snel na elke handmatige wijziging.

Implicaties: Vereist een keuze voor gereedschap die zelf weer aan de open source- en portabiliteitsprincipes uit deze bijlage wordt getoetst. Het specifieke gereedschap (op het moment van schrijven bijvoorbeeld Terraform of OpenTofu) is zelf een referentiepatroon dat kan wijzigen; het onderliggende, tijdloze principe, declaratieve, versiebeheerde, herbruikbare infrastructuurconfiguratie, blijft ongeacht het gekozen gereedschap gelden. Zie hoofdstuk 5 voor een korte toelichting op hoe een gereedschapskeuze op dit vlak zelf een lock-in-risico kan vormen.

D8 Werk de exit-inspanning vooraf uit in een concreet exitplan

Aard: Tijdloos principe **Gewicht: Kernprincipe**

Stel voor elke workload met een exit-strategie een apart exitplan op waarin de benodigde rollen en capaciteit, de volgorde van stappen en een realistische doorlooptijd zijn vastgelegd, los van de technische migratietest (D1) en de financiële raming (D6).

Beschrijving: Een getest migratiepad (D1) laat zien dat een workload technisch overgezet kán worden; een TCO-raming (D6) laat zien wat dat ongeveer kost. Geen van beide legt vast wie de exit daadwerkelijk uitvoert, in welke volgorde, met welke capaciteit en binnen welke termijn. Het exitplan is dat ontbrekende, organisatorische onderdeel: een concreet uitvoeringsplan, vergelijkbaar met een draaiboek, dat er klaar voor ligt voordat een exit nodig is.

Rationale: Zonder een vooraf uitgewerkt exitplan ontstaat bij een daadwerkelijke exit, bijvoorbeeld door een dreigende overname van de leverancier, kostbare vertraging doordat rolverdeling, planning en volgorde van stappen dan pas voor het eerst worden bedacht, op het moment dat er de minste tijd voor is. Dit sluit aan bij principe H7 (governance-rollen): het exitplan is de plek waar die rollen voor het specifieke scenario van een exit worden geconcretiseerd.

Implicaties: Vereist een gedocumenteerd exitplan per kritieke workload, met daarin minimaal: de benodigde rollen en capaciteit (intern en, waar relevant, bij de leverancier of een consortiumpartner), de stapsgewijze uitvoeringsvolgorde, en een realistische doorlooptijdinschatting. Het exitplan wordt, net als het migratiepad uit D1, periodiek herzien en waar mogelijk mede getoetst tijdens migratieoefeningen.

D9 Documenteer model-hardwareafhankelijkheid als expliciete afweging

Aard: Tijdloos principe **Gewicht: Aanbevolen principe**

Documenteer expliciet wanneer een AI-model of -toepassing is geoptimaliseerd voor specifieke hardware of een specifieke runtime-omgeving, en weeg dit bewust af tegen de resulterende afhankelijkheid.

Beschrijving: Sommige AI-modellen zijn sterk gebonden aan specifieke accelerators, GPU-architecturen of runtime-omgevingen, vergelijkbaar met de platformspecifieke infrastructuur die al eerder in deze bijlage wordt genoemd (zie de introductie van categorie D en principe A2). Dit kan een legitieme keuze zijn wanneer de prestatiewinst substantieel is.

Rationale: Onbewuste hardwareafhankelijkheid bij AI-modellen leidt tot dezelfde soort lock-in als bij cloudplatformen, maar vaak minder zichtbaar, omdat de keuze voor een specifieke runtime-omgeving vroeg in het ontwikkelproces wordt gemaakt en zelden achteraf wordt heroverwogen.

Implicaties: Vereist dat een architectuurbeslissing over modelspecifieke hardware- of runtime-afhankelijkheid expliciet wordt gedocumenteerd en periodiek wordt herzien, op dezelfde manier als andere platformspecifieke keuzes.

DEEL II Weerbaarheid

De principes in dit deel borgen dat een organisatie stand kan houden bij uitval, aanvallen, overname van een leverancier of ongewenste toegang tot gevoelige gegevens.

E. Continuïteit

Principes die de dienstverlening laten doorlopen bij uitval, overname of geopolitieke druk.

E1 Spreid risico over meerdere, federatief samenwerkende platformen

Aard: Tijdloos principe **Gewicht:** Aanbevolen principe

Vermijd concentratie van kritieke workloads binnen één enkel failure domain; benut een federatie van onafhankelijke, samenwerkende voorzieningen.

Beschrijving: Risicospreiding over meerdere, goed geoutilleerde datacenters draagt bij aan weerbaarheid tegen zowel natuurrampen als vijandige aanvallen (fysiek en digitaal), en is een remedie tegen problemen die voortvloeien uit regionale congestie op het elektriciteitsnet.

Rationale: Het federatieve karakter van een samenwerking tussen meerdere aanbieders maakt het mogelijk om bij calamiteiten snel bij te springen of van cloudprovider te wisselen. Weerbaarheid ontstaat door onafhankelijke failure domains te scheiden en systemische single points of failure te vermijden, niet simpelweg door schaal te verkleinen: voor workloads die baat hebben bij grootschalige, sterk geïntegreerde infrastructuur, bijvoorbeeld AI, high-performance computing of data lakes, kan een enkel, groot en goed beveiligd failure domain weerbaarder zijn dan kunstmatige versnippering, mits dat domein zelf onderdeel is van een breder, gespreid geheel.

Implicaties: Vereist architectuurontwerp dat rekening houdt met onafhankelijke failure domains en een multi-site- of multi-provider-opzet vanaf het begin, in plaats van als latere toevoeging. De keuze tussen schaal binnen een failure domain en spreiding over meerdere domeinen is een bewuste afweging per workload, geen universele regel.

E2 Ontwerp voor graceful degradation bij leveranciersuitval

Aard: Tijdloos principe **Gewicht:** Aanbevolen principe

Zorg dat bij uitval van één component of leverancier de dienstverlening in afgeslankte vorm kan doorgaan, in plaats van volledig stil te vallen.

Beschrijving: Graceful degradation betekent dat kritieke functionaliteit expliciet is losgekoppeld van niet-kritieke functionaliteit, zodat uitval van een niet-kritiek onderdeel niet automatisch de kernfunctie van een dienst blokkeert.

Rationale: Een architectuur zonder deze scheiding maakt elke storing, hoe klein ook, potentieel tot een volledige uitval, wat de feitelijke impact van leveranciersafhankelijkheid onnodig vergroot.

Implicaties: Vereist expliciete identificatie van kritieke versus ondersteunende functionaliteit bij elk systeemontwerp, en het testen van degradatiescenario's.

E3 Beoordeel continuïteitsrisico proportioneel aan de kriticiteit van de workload

Aard: Tijdloos principe **Gewicht: Kernprincipe**

> ***Pas een zwaarder continuïteitsregime toe op kritieke, bedrijfskritieke of nationale-veiligheidsgevoelige workloads dan op laag-risico workloads.***

Beschrijving: Niet elke workload rechtvaardigt dezelfde investering in risicospreiding, redundantie en federatief beheer. Een uniforme, maximale toepassing van alle continuïteitsmaatregelen op elke workload is kostbaar en vaak disproportioneel.

Rationale: Dit sluit aan bij het uitgangspunt uit het herziene Rijksbreed cloudbeleid en de BIO2: risicoafweging op basis van de aard van de data en het proces, in plaats van een one-size-fits-all-benadering.

Implicaties: Vereist een gedocumenteerde risicoclassificatie per workload als basis voor het te kiezen continuïteitsregime (zie ook het afwegingskader in hoofdstuk 7).

E4 Verbind continuïteitsplanning aan een geoefend, niet alleen gedocumenteerd, crisisplan

Aard: Tijdloos principe **Gewicht: Aanbevolen principe**

> ***Test continuïteits- en uitwijkplannen periodiek in de praktijk, niet uitsluitend op papier.***

Beschrijving: Een crisisplan dat nooit is beoefend, bevat vrijwel altijd onvoorziene knelpunten die pas tijdens een daadwerkelijke crisis aan het licht komen, op het moment dat het handelen onder tijdsdruk plaatsvindt en fouten het duurst zijn.

Rationale: Verschillende overheidsorganisaties (zoals UWV, in het kader van Business Continuity Management) hebben hun inzet op dit vlak recent geïntensiveerd vanwege de toegenomen aandacht voor digitale weerbaarheid, een ontwikkeling die dit principe onderstreept.

Implicaties: Vereist een jaarlijkse of halfjaarlijkse oefening ("game day" of vergelijkbaar), met evaluatie en bijstelling van het crisisplan op basis van de uitkomsten.

E5 Behoud menselijke expertise als onderdeel van continuïteit

Aard: Tijdloos principe **Gewicht: Aanbevolen principe**

> ***Investeer structureel in kennis en vakmanschap voor het beheer van soevereine cloudomgevingen, als integraal onderdeel van de continuïteitsstrategie.***

Beschrijving: Kennisschaarste is een van de grootste risico's voor de transitie naar een soevereine overheidscloud: zonder voldoende technici die met open standaarden en open source software kunnen werken, blijft elk technisch fundament, hoe goed ontworpen ook, een lege huls.

Rationale: Technische continuïteit zonder personele continuïteit is onvolledig: een architectuur die op papier weerbaar is, faalt alsnog wanneer er onvoldoende mensen zijn die haar kunnen beheren en herstellen bij incidenten.

Implicaties: Vereist samenwerking met onderwijs- en kennisinstellingen, beschikbaarstelling van opleidingsversies van de gebruikte technologiestack, en een HR-beleid dat ruimte biedt aan technische profielen.

E6 Beoordeel bij systemen met een OT-component het regime voor kritieke entiteiten

Aard: Tijdloos principe **Gewicht: Contextafhankelijk principe**

> ***Ga voor workloads die aansturing of monitoring van operationele technologie bevatten expliciet na of de Wet weerbaarheid kritieke entiteiten (Wwke) van toepassing is, en richt de architectuur daarop in.***

Beschrijving: Systemen die vallen onder operationele technologie, zoals aansturing van waterkeringen, energievoorziening, industriële processen of logistiek, hebben een risicoprofiel waarin beschikbaarheid en integriteit minstens zo belangrijk zijn als vertrouwelijkheid. De Wwke (sinds augustus 2026 van kracht, de Nederlandse vertaling van de Europese Critical Entities Resilience-richtlijn) verplicht organisaties die essentiële diensten leveren tot aantoonbare weerbaarheid tegen fysieke en digitale dreigingen.

Rationale: Een cloudprovider die kritieke overheidsapplicaties met een OT-component host, loopt het risico zelf als kritieke entiteit te worden aangewezen, met bijbehorende aanvullende verplichtingen. Dit onderscheidt deze categorie workloads van reguliere bedrijfskritieke systemen, waarvoor de bescherming primair op vertrouwelijkheid van gegevens is gericht.

Implicaties: Vereist een aparte risicoclassificatie voor OT-gerelateerde workloads binnen de indeling uit principe E3, met expliciete toetsing aan het Wwke-regime naast de gebruikelijke BIO2- en Cloud Sovereignty Framework-criteria.

E7 Borg cyber recovery als aparte discipline naast reguliere continuïteitsplanning

Aard: Tijdloos principe **Gewicht:** Aanbevolen principe

Richt onveranderlijke (immutable) back-ups en een geoefend cyber recovery-plan in, los van de reguliere uitwijk- en continuïteitsvoorzieningen uit E1 tot en met E4.

Beschrijving: Een ransomware-aanval of vergelijkbaar incident kan reguliere back-ups en uitwijkvoorzieningen zelf besmetten of versleutelen, waardoor een organisatie die alleen op reguliere continuïteitsmaatregelen leunt, alsnog zonder bruikbaar hersteld punt komt te zitten. Immutable back-ups, die na het wegschrijven niet meer gewijzigd of verwijderd kunnen worden, zijn hiertegen een specifieke waarborg.

Rationale: De NIS2-richtlijn en de Nederlandse Cyberbeveiligingswet vragen expliciet om aantoonbare incident response- en herstelcapaciteit, los van reguliere bedrijfscontinuïteit; cyber recovery is daarmee inmiddels een wettelijk verankerde discipline, niet langer optioneel.

Implicaties: Vereist een apart geoefend herstelscenario voor cyberincidenten (naast het reguliere crisisplan uit E4), inclusief geïsoleerde, immutable back-upvoorzieningen en een gedocumenteerde incident response-procedure.

E8 Borg continuïteit bij deprecatie van AI-modellen

Aard: Tijdloos principe **Gewicht:** Aanbevolen principe

Stel voor elke productie-AI-toepassing vast wat de organisatie doet wanneer het gebruikte model door de aanbieder wordt uitgefaseerd of ingrijpend gewijzigd.

Beschrijving: AI-modellen worden door aanbieders vaker, en met kortere cycli, uitgefaseerd of gewijzigd dan cloudplatformen doorgaans worden aangepast. Een model dat vandaag beschikbaar is, kan binnen enkele maanden zijn vervangen door een nieuwe versie met ander gedrag, of volledig worden stopgezet.

Rationale: Zonder een continuïteitsplan voor modeldeprecatie ontstaat hetzelfde risico als bij leveranciersuitval elders in deze categorie, maar dan op een kortere tijdschaal en vaak zonder dezelfde contractuele waarschuwingstermijnen.

Implicaties: Vereist monitoring van aankondigingen van modelaanbieders, een testregime voor nieuwe modelversies voordat deze in productie worden genomen, en een uitwijkscenario, bij voorkeur in combinatie met de modelgateway uit principe A9.

F. Databescherming, inclusief privacy

Principes die de bescherming van gegevens tegen ongeautoriseerde toegang, verlies of misbruik borgen, met persoonsgegevens als belangrijke, wettelijk verankerde deelverzameling (zie hoofdstuk 3, kapstok Weerbaarheid).

F1 Voer een DPIA uit bij elke verwerking met privacyrisico

Aard: Tijdloos principe **Gewicht: Kernprincipe**

Voordat een workload met persoonsgegevens op een clouddienst wordt ingericht, wordt een data protection impact assessment uitgevoerd en gedocumenteerd.

Beschrijving: Een DPIA brengt vooraf de privacyrisico's van een gegevensverwerking in kaart, zodat passende maatregelen kunnen worden genomen om deze risico's te verkleinen. De verplichting hiertoe volgt uit de AVG en, voor specifieke domeinen, uit de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens. Voor AI-toepassingen geldt een vergelijkbare eis voor de onderliggende trainings-, validatie- en testdata: gegevensgovernance met aandacht voor representativiteit en bias is een verplicht onderdeel van de AI Act voor hoogrisicotoepassingen (zie hoofdstuk 6).

Rationale: Zonder een uitgevoerde DPIA ontbreekt een aantoonbare grondslag voor de manier waarop privacyrisico's zijn afgewogen, wat zowel een compliance-risico als een architectuurrisico is: risico's die niet zijn geïdentificeerd, worden ook niet in het ontwerp geadresseerd.

Implicaties: Vereist dat de DPIA als vast onderdeel van het architectuurproces wordt ingepland, niet als losstaande juridische exercitie na afronding van het ontwerp.

F2 Baseer clouddatabescherming op een erkende PII-standaard

Aard: Tijdloos principe **Gewicht: Aanbevolen principe**

Toets de bescherming van persoonlijk identificeerbare informatie (PII) in clouddiensten aan een erkende standaard zoals ISO/IEC 27018.

Beschrijving: ISO/IEC 27018 biedt richtlijnen voor het beschermen van PII in publieke clouddiensten, specifiek toegespitst op de situatie waarin de clouddienstverlener optreedt als verwerker. De standaard bouwt voort op ISO/IEC 27002 en introduceert beheersmaatregelen die zijn afgestemd op cloudspecifieke risico's.

Rationale: Generieke informatiebeveiligingsnormen zoals ISO/IEC 27001/27002 dekken niet automatisch de specifieke verantwoordelijkheden van een cloudprovider als verwerker van persoonsgegevens; een aparte, cloudspecifieke PII-toets voorkomt een vals gevoel van compliance.

Implicaties: Vereist dat leveranciers expliciet aantonen op welke wijze zij aan ISO/IEC 27018 of een gelijkwaardige standaard voldoen, als aanvulling op algemene beveiligingscertificering.

F3 Behandel privacybeoordeling en soevereiniteitsbeoordeling als aparte, aanvullende stappen

Aard: Tijdloos principe **Gewicht: Aanbevolen principe**

Voer een DPIA en een soevereiniteitsbeoordeling (zie categorie H) altijd afzonderlijk uit, ook wanneer beide voor dezelfde workload gelden.

Beschrijving: Een leverancier die onder Europese jurisdictie valt, voldoet niet automatisch aan de eisen voor verantwoorde verwerking van persoonsgegevens, en omgekeerd biedt een goede DPIA-uitkomst geen garantie tegen blootstelling aan niet-Europese jurisdictie.

Rationale: Het samenvoegen van beide beoordelingen tot één afweging leidt tot het risico dat een sterke uitkomst op het ene vlak een zwakke uitkomst op het andere vlak maskeert, met name bij leveranciers die op één van beide aspecten goed scoren en dit breed communiceren.

Implicaties: Vereist twee gescheiden, expliciet gedocumenteerde uitkomsten in het architectuurdossier: een DPIA-uitkomst en een soevereiniteitsscore, niet samengevoegd tot één oordeel.

F4 Documenteer grondslag en bewaartermijn van persoonsgegevens transparant

Aard: Tijdloos principe **Gewicht:** Aanbevolen principe

Leg voor elke verwerking van persoonsgegevens de wettelijke grondslag en de toepasselijke bewaartermijn expliciet vast, inclusief de wijze waarop verwijdering technisch wordt geborgd.

Beschrijving: Transparantie over grondslag en bewaartermijn is nodig om zowel aan de verantwoordingsplicht uit de AVG te voldoen als om bij een migratie of exit te kunnen bepalen welke gegevens overgezet, gearchiveerd of vernietigd moeten worden.

Rationale: Zonder deze documentatie ontstaat het risico dat persoonsgegevens langer bewaard blijven dan toegestaan, of dat bij een migratie onduidelijk is welke gegevens wel en niet mogen worden overgezet naar de nieuwe omgeving.

Implicaties: Vereist een koppeling tussen het gegevensregister (verwerkingsregister) en de technische inrichting van dataretentie, zodat bewaartermijnen niet alleen op papier maar ook technisch worden gehandhaafd.

G. Security

Principes die de bescherming van netwerken, datacenters, software, databases en clouddiensten tegen digitale dreigingen borgen, als complementaire assurance-laag naast soevereiniteit (zie hoofdstuk 3, kapstok Weerbaarheid, en hoofdstuk 6).

G1 Stel voor elke workload een expliciet security-assurance-niveau vast

Aard: Tijdloos principe **Gewicht: Kernprincipe**

Beoordeel en documenteer voor elke clouddienst een assurance-niveau conform een erkend schema, zoals EUCS Basic, Substantial of High.

Beschrijving: Het EU Cybersecurity Certification Scheme for Cloud Services (EUCS) van ENISA biedt een referentieset van beveiligingsvereisten, inclusief transparantie-eisen zoals de locatie van gegevensverwerking en -opslag, gekoppeld aan drie oplopende assurance-niveaus.

Rationale: Zonder een expliciet vastgesteld niveau blijft onduidelijk of de beveiliging van een dienst is afgestemd op het daadwerkelijke dreigingsprofiel van de workload die erop draait, met als risico een onder- of overinvestering in beveiligingsmaatregelen.

Implicaties: Vereist dat het gekozen assurance-niveau wordt gemotiveerd op basis van de kriticiteit en gevoeligheid van de workload, op dezelfde manier als de risicoclassificatie voor continuïteit in categorie E.

G2 Behandel security-assurance en soevereiniteits-assurance als gescheiden toetsen

Aard: Tijdloos principe **Gewicht: Kernprincipe**

Voer de beoordeling van cybersecurity-assurance (bijvoorbeeld via EUCS) en de beoordeling van soevereiniteit (bijvoorbeeld via het EU Cloud Sovereignty Framework) als twee aparte stappen uit, ook wanneer dezelfde leverancier wordt beoordeeld.

Beschrijving: Beide beoordelingslagen hebben een eigen normenkader en een eigen doel: de een toetst weerbaarheid tegen digitale dreigingen, de ander toetst jurisdictie en zeggenschap. Zie hoofdstuk 6 voor de volledige toelichting op dit onderscheid.

Rationale: Het samenvoegen van beide beoordelingen tot één oordeel verhult dat een leverancier op de ene as sterk en op de andere as zwak kan scoren, wat tot een onterecht gerustgesteld gevoel bij de opdrachtgever kan leiden.

Implicaties: Vereist twee gescheiden, expliciet gedocumenteerde uitkomsten in het architectuurdossier, in lijn met principe H6.

G3 Borg zelfstandig vermogen tot het scannen op kwetsbaarheden

Aard: Tijdloos principe **Gewicht:** Aanbevolen principe

Zorg dat de organisatie, of een aangewezen partij namens de organisatie, zelfstandig in staat is om clouddiensten te scannen op beveiligingsgebreken, in plaats van hiervoor volledig te leunen op de leverancier.

Beschrijving: Deze capaciteit is bij de Nederlandse overheid op dit moment grotendeels beperkt tot het Defensiedomein, terwijl NIS2 en de Cyberbeveiligingswet een bredere, aantoonbare beveiligingscapaciteit vragen van organisaties die essentiële diensten leveren.

Rationale: Zonder eigen scanvermogen is een organisatie volledig afhankelijk van de eigen rapportage van de leverancier over diens beveiligingsniveau, wat het risico op onopgemerkte kwetsbaarheden vergroot.

Implicaties: Vereist investering in eigen of ingehuurde scan- en auditcapaciteit, met contractueel vastgelegde toegang tot de clouddienst om deze scans daadwerkelijk te kunnen uitvoeren. Voor AI-toepassingen die onder een hoogrisicocategorie vallen, geldt aanvullend een wettelijke verplichting tot automatische logging met een bewaartermijn van ten minste zes maanden (zie hoofdstuk 6).

G4 Baseer security-eisen op BIO2, ABRO en het European Cybersecurity Certification Framework

Aard: Tijdloos principe **Gewicht: Kernprincipe**

Toets clouddiensten aan de Baseline Informatiebeveiliging Overheid 2 (BIO2), en waar van toepassing aan de Algemene Beveiligingseisen Rijksoverheidsopdrachten (ABRO) en het bredere European Cybersecurity Certification Framework.

Beschrijving: BIO2 is het tactische normenkader voor informatiebeveiliging bij alle Nederlandse overheidslagen, met specifieke beheersmaatregelen voor leveranciers en cloudgebruik. ABRO stelt aanvullende eisen op contracten die de nationale veiligheid raken.

Rationale: Zonder een eenduidig, verplicht normenkader ontstaat versnippering: elke organisatie hanteert eigen beveiligingseisen, wat vergelijking tussen leveranciers en aanbestedingen bemoeilijkt.

Implicaties: Vereist dat security-eisen in aanbestedingen expliciet naar BIO2 en, waar van toepassing, ABRO verwijzen, in plaats van generieke of leverancierssspecifieke beveiligingsclaims te accepteren.

G5 Beperk de impact van geprivilegieerde toegang

Aard: Tijdloos principe **Gewicht:** Aanbevolen principe

Beperk het aantal medewerkers met geprivilegieerde toegangsrechten tot systemen en data tot het strikt noodzakelijke, en monitor het gebruik van die rechten actief.

Beschrijving: Geprivilegieerde toegang is een van de meest gebruikte aanvalsvectoren bij cloudincidenten: wie toegang heeft tot beheerdersrechten, kan doorgaans ook detectiemaatregelen omzeilen of uitschakelen.

Rationale: Dit principe is complementair aan principe H4 (geprivilegieerde toegang vanuit Europese jurisdictie): H4 regelt wie in aanmerking komt voor geprivilegieerde toegang, dit principe regelt hoe die toegang technisch wordt beperkt en bewaakt.

Implicaties: Vereist toepassing van het least-privilege-principe, verplichte multifactorauthenticatie voor geprivilegieerde accounts, en logging die onafhankelijk van de beheerder zelf kan worden ingezien.

G6 Beheers supply chain security in de softwareketen

Aard: Tijdloos principe **Gewicht:** Aanbevolen principe

Houd een actueel overzicht bij van de software-toeleveringsketen (een software bill of materials, SBOM) voor kritieke platformcomponenten, en scan deze structureel op bekende kwetsbaarheden.

Beschrijving: Zowel open source als commerciële software bestaat doorgaans uit vele onderliggende afhankelijkheden (dependencies), elk met een eigen onderhoudsstatus en kwetsbaarhedenrisico. Een kwetsbaarheid diep in deze keten kan een systeem treffen zonder dat de organisatie dit zelf heeft ontwikkeld of direct beheert.

Rationale: Dit vult principe H5 (transparantie over herkomst van hardware en software) aan met een operationele, doorlopende component: H5 gaat over herkomst en jurisdictie, dit principe gaat over het actief beheersen van kwetsbaarheden in de gehele toeleveringsketen, ongeacht herkomst.

Implicaties: Vereist geautomatiseerde dependency-scanning als vast onderdeel van de softwareontwikkel- en releasecyclus, met een vastgelegd proces voor het opvolgen van gevonden kwetsbaarheden binnen een bepaalde termijn. Software Composition Analysis (SCA) is de gevestigde productcategorie die dit operationaliseert, met platformen die doorlopend scannen op kwetsbaarheden, onderhoudsstatus en licenties (bijvoorbeeld Endor Labs of Sonatype). Het specifieke platform is, net als bij principe D7, een referentiepatroon dat kan wijzigen; de eis dat de toeleveringsketen structureel en geautomatiseerd wordt bewaakt, is het tijdloze onderdeel van dit principe.

G7 Bouw menselijk toezicht in als architectuureis bij AI-toepassingen

Aard: Tijdloos principe **Gewicht:** Contextafhankelijk principe

Bouw menselijk toezicht in de architectuur van AI-toepassingen in als ontwerpvereiste, niet als latere toevoeging.

Beschrijving: Voor AI-systemen, met name hoogrisicotoepassingen, vereist effectief menselijk toezicht een architectuur die interventie en overrule daadwerkelijk mogelijk maakt: zichtbaarheid van de AI-uitkomst, de onderliggende redenering waar mogelijk, en een praktisch bruikbaar mechanisme om in te grijpen voordat een beslissing effect heeft.

Rationale: Menselijk toezicht dat pas achteraf wordt toegevoegd, blijft vaak symbolisch: zonder ingebouwde interventiemogelijkheid en voldoende tijd om te reageren, kan een toezichthouder een AI-beslissing in de praktijk niet daadwerkelijk corrigeren.

Implicaties: Vereist expliciete ontwerpkeuzes voor de interventie-interface, responstijd en escalatiepad, vroeg in het ontwerp van een AI-toepassing, met extra gewicht bij toepassingen die onder een hoogrisicocategorie vallen (zie principe H10).

DEEL III Compliance

De principes in dit deel zorgen dat wendbaarheid en weerbaarheid daadwerkelijk getoetst en geverifieerd kunnen worden.

H. Soevereiniteit, jurisdictie en aantoonbaarheid

Principes die jurisdictie, zeggenschap en aantoonbaarheid van controle over het digitale fundament waarborgen (zie hoofdstuk 6).

H1 Documenteer jurisdictie expliciet en actueel

Aard: Tijdloos principe **Gewicht: Kernprincipe**

Leg voor elke clouddienst vast onder welke jurisdictie(s) de leverancier valt, waar data wordt verwerkt en opgeslagen, en houd dit actueel bij wijzigingen.

Beschrijving: Jurisdictie bepaalt welke buitenlandse wet- en regelgeving (zoals de Amerikaanse CLOUD Act) mogelijk van toepassing is op data, ongeacht waar de fysieke opslag plaatsvindt. Dit moet per dienst, en niet alleen op leveranciersniveau, worden vastgesteld.

Rationale: Jurisdictie-informatie kan wijzigen zonder dat de functionaliteit van een dienst verandert, bijvoorbeeld bij een overname of bij verplaatsing van datacenters. Zonder actieve monitoring blijft een eerder gemaakte soevereiniteitsbeoordeling ten onrechte geldig.

Implicaties: Vereist een vast proces om jurisdictiewijzigingen te signaleren, gekoppeld aan leveranciersmanagement en contractmanagement.

H2 Eis aantoonbaarheid, niet zelfverklaring, van soevereiniteitsclaims

Aard: Tijdloos principe **Gewicht: Kernprincipe**

Beoordeel leveranciersclaims over soevereiniteit altijd op basis van onderliggende scores (zoals SEAL) of onafhankelijke toetsingsinstrumenten, nooit op basis van marketingmateriaal alleen.

Beschrijving: Het EU Cloud Sovereignty Framework is expliciet ontworpen om "sovereignty washing" tegen te gaan: aanbieders die soevereiniteit claimen zonder dat harde controles dit ondersteunen.

Rationale: Zonder deze eis wordt de architectuurbeoordeling afhankelijk van de kwaliteit van de communicatie van een leverancier in plaats van van verifieerbare feiten, wat het risico op een verkeerde inschatting van feitelijke afhankelijkheid vergroot.

Implicaties: Vereist het opvragen en beoordelen van onderliggende SEAL-scores of gelijkwaardige, verifieerbare bewijsstukken bij elke soevereiniteitsclaim.

H3 Borg bescherming tegen ongewenste wijziging van zeggenschap

Aard: Tijdloos principe **Gewicht: Kernprincipe**

Neem contractuele waarborgen op tegen ongewenste overname van een leverancier door een partij van buiten de EU, zoals change-of-control-clausules.

Beschrijving: Een leverancier die op het moment van gunning volledig aan de soevereiniteitscriteria voldoet, kan op een later moment worden overgenomen door een niet-Europese partij. Zonder contractuele voorbereiding hierop verliest de opdrachtgever alle onderhandelingspositie op het moment dat dit gebeurt.

Rationale: Het manifest van de Open Cloud Alliantie noemt dit expliciet als kernvraag: wat gebeurt er bij overname? Contractuele waarborgen (ontbindingsgronden bij wijziging van eigendomsstructuur, consortiumconstructies met exit-clausules, of verankering van "nationaal belang") maken het verschil tussen een theoretisch en een praktisch bruikbaar exitrecht.

Implicaties: Vereist juridische betrokkenheid bij architectuurbeslissingen op het niveau van contractvorming, niet alleen bij de techniek zelf.

H4 Scheid geprivilegieerde toegang naar Europese jurisdictie

Aard: Tijdloos principe **Gewicht: Aanbevolen principe**

Medewerkers met geprivilegieerde ("privileged") toegangsrechten tot systemen en data zijn in dienst van een Europese entiteit, ingezetene van de EU/EER/EFTA, en voeren hun werk fysiek vanuit Europa uit.

Beschrijving: Dit criterium, expliciet benoemd in het EU Cloud Sovereignty Framework, voorkomt dat toegang tot gevoelige systemen via personeel buiten de EU alsnog een niet-Europese jurisdictie in de praktijk introduceert, zelfs wanneer de juridische entiteit en de dataopslag zelf wél Europees zijn.

Rationale: Zonder deze eis kan formele soevereiniteit (juridische vestiging, dataopslag) worden ondermijnd door operationele realiteit (beheer en support vanuit een niet-Europese locatie of door niet-Europees personeel).

Implicaties: Vereist expliciete verificatie bij leveranciers van de locatie en het dienstverband van personeel met geprivilegieerde toegang, niet alleen van de juridische vestigingsplaats van het bedrijf.

H5 Wees transparant over de herkomst van hardware en software

Aard: Tijdloos principe **Gewicht:** Aanbevolen principe

Documenteer de herkomst van kritieke hardware- (chips, GPU's, netwerkcomponenten) en softwarecomponenten, ook waar volledige Europese autonomie (nog) niet haalbaar is.

Beschrijving: Het manifest erkent expliciet dat volledige autonomie niet bestaat: wereldwijde productieketens voor hardware zijn een gegeven. Transparantie over herkomst is daarom een voorwaarde voor een realistische risicobeoordeling, niet een belemmering voor voortgang.

Rationale: Het ontkennen of verzwijgen van resterende niet-Europese afhankelijkheden in de hardwareketen leidt tot een onvolledig en te optimistisch beeld van de daadwerkelijke soevereiniteit van een architectuur.

Implicaties: Vereist dat leveranciersdocumentatie herkomstinformatie van kritieke componenten bevat, zodat een architect een realistisch, gelaagd soevereiniteitsbeeld kan opstellen (welke lagen zijn wél, en welke nog niet volledig Europees).

H6 Behandel security en soevereiniteit als complementair, niet als vervangend

Aard: Tijdloos principe **Gewicht: Kernprincipe**

Een hoge soevereiniteitsscore compenseert geen laag beveiligingsniveau, en omgekeerd; beide worden onafhankelijk van elkaar getoetst.

Beschrijving: Soevereiniteit gaat over controle en jurisdictie; cybersecurity gaat over weerbaarheid tegen aanvallen en incidenten. Een volledig soeverein, onder Nederlandse jurisdictie vallend platform kan nog altijd onvoldoende beveiligd zijn, en vice versa.

Rationale: Zowel het manifest van de Open Cloud Alliantie als de kabinetsreactie op de initiatiefnota Wolken aan de horizon benadrukken expliciet dat de focus op soevereiniteit niet mag leiden tot verminderde aandacht voor security.

Implicaties: Vereist twee gescheiden beoordelingsuitkomsten in elk architectuurdossier: een EUCS-achtige security-assurance-score en een Sovereignty Framework-score, nooit samengevoegd tot één cijfer.

H7 Wijs expliciete governance-rollen toe voor cloud- en dataverantwoordelijkheid

Aard: Tijdloos principe **Gewicht:** Aanbevolen principe

Leg voor elke clouddienst en elke belangrijke dataset vast wie verantwoordelijk is voor de architectuurbeslissing, wie de eigenaar is van de data, en wie het mandaat heeft om bij een incident of migratie te beslissen.

Beschrijving: Compliance zoals in dit hoofdstuk beschreven veronderstelt een organisatie die daadwerkelijk kan handelen op basis van de getoetste normenkaders. Zonder expliciete rolverdeling ontstaat vertraging of besluiteloosheid precies op het moment dat snel handelen nodig is, bijvoorbeeld bij een dreigende overname van een leverancier. Voor beslissingen waarbij architectuurprincipes en bedrijfsbelang kunnen conflicteren, bijvoorbeeld het afwijken van een open standaard vanwege aantoonbare strategische waarde (zie principe B2), ligt het mandaat nadrukkelijk niet bij één rol alleen: business, architectuur en security & continuity dragen die afweging gezamenlijk.

Rationale: Governance ontbreekt vaak niet uit onwil, maar omdat rolverdeling wordt verondersteld in plaats van vastgelegd, met als gevolg dat verantwoordelijkheid pas bij een incident concreet blijkt te ontbreken.

Implicaties: Vereist een actueel gedocumenteerd RACI-schema (of vergelijkbaar) per clouddienst en per kritieke dataset, opgenomen in het architectuurdossier en periodiek herzien. Voor afwegingen tussen strategische waarde en architectuurprincipes vereist dit specifiek een vastgelegd, gezamenlijk besluitvormingsmoment tussen business, architectuur en security & continuity, in plaats van een eenzijdig mandaat bij één van deze partijen.

H8 Borg auditability en continuous compliance, niet alleen een momentopname

Aard: Tijdloos principe **Gewicht: Kernprincipe**

Richt logging, monitoring en periodieke herbeoordeling zodanig in dat compliance op elk moment aantoonbaar is, niet alleen op het moment van de laatste audit of aanbesteding.

Beschrijving: Een architectuurbeoordeling of certificering is een momentopname; de onderliggende infrastructuur, leverancierszeggenschap en dreigingslandschap veranderen continu. Zonder doorlopende monitoring kan een eerder aantoonbaar compliant systeem geruisloos afdrijven van de norm.

Rationale: Dit sluit aan bij principe H1 (jurisdictie actueel houden) en E4 (geoefend crisisplan), maar breidt het uit tot een structureel proces in plaats van incidentele controlemomenten.

Implicaties: Vereist geautomatiseerde compliance-monitoring waar mogelijk, en een vaste cyclus (bijvoorbeeld jaarlijks) voor herbeoordeling van eerder vastgestelde compliance-uitkomsten. De beoordeling van open source-componenten (zie principe C4) illustreert dit goed: voor workloads in een innovatiestream volstaat vaak een eenmalige, lichte toetsing, terwijl kritieke of vitale diensten gebaat zijn bij continue monitoring via een geautomatiseerd platform met vastgelegde drempelwaarden, in lijn met de risicoclassificatie uit hoofdstuk 7.

H9 Pas archivering en records management toe conform de Woo en het bredere informatiebeheer

Aard: Tijdloos principe **Gewicht:** Contextafhankelijk principe

Ontwerp dataopslag en -archivering zodanig dat wordt voldaan aan de Wet open overheid (Woo) en aan de eisen voor duurzame toegankelijkheid van overheidsinformatie.

Beschrijving: Overheidsorganisaties hebben, anders dan private partijen, een wettelijke verplichting tot actieve openbaarmaking en tot zorgvuldig, langdurig beheer van overheidsinformatie als publiek erfgoed. Dit stelt eisen aan formaatkeuzes, retentie en vindbaarheid die verder gaan dan reguliere databescherming (categorie F).

Rationale: Een cloudarchitectuur die wel aan AVG en soevereiniteitscriteria voldoet maar onvoldoende rekening houdt met de Woo-verplichtingen, kan een overheidsorganisatie alsnog in gebreke stellen, ook wanneer alle overige compliance-eisen zijn geborgd.

Implicaties: Vereist afstemming met de verantwoordelijke archief- en informatiebeheerfunctie bij het ontwerpen van dataopslag, met expliciete aandacht voor formaatkeuzes die duurzame toegankelijkheid ondersteunen.

H10 Classificeer AI-toepassingen naar risiconiveau

Aard: Tijdloos principe **Gewicht:** Contextafhankelijk principe

Beoordeel voor elke AI-toepassing expliciet of deze onder een hoogrisicocategorie valt, en richt de governance daarop in.

Beschrijving: Vergelijkbaar met de BIV-classificatie in hoofdstuk 6, vereist een AI-toepassing een eigen risicobeoordeling: valt de toepassing onder een hoogrisicocategorie (bijvoorbeeld werving, kredietbeoordeling, kritieke infrastructuur, rechtshandhaving), met de daarbij horende verplichtingen op het gebied van risicomanagement, gegevensgovernance en documentatie?

Rationale: Zonder deze classificatie loopt een organisatie het risico een AI-toepassing als hoogrisicotoepassing te lanceren zonder de bijbehorende verplichtingen te hebben ingericht, met aantoonbaarheids- en handhavingsrisico's tot gevolg.

Implicaties: Vereist een vast beoordelingsmoment bij elke nieuwe AI-toepassing, vergelijkbaar met de risicoclassificatie in hoofdstuk 7, met documentatie van de uitkomst in het architectuurdossier.

H11 Borg de doorwerking van modeldocumentatie van de leverancier

Aard: Tijdloos principe **Gewicht:** Contextafhankelijk principe

Neem bij gebruik van een extern AI-model de technische documentatie van de modelleverancier over in het eigen architectuurdossier, en houd het eigen gebruik binnen het door de leverancier gedocumenteerde toepassingsgebied.

Beschrijving: Aanbieders van AI-modellen zijn verplicht technische documentatie te leveren over modelarchitectuur, trainingsmethodologie en beoogd gebruik. Een organisatie die op dat model voortbouwt, is zelf verantwoordelijk om binnen dat gedocumenteerde toepassingsgebied te blijven en de documentatie te verwerken in de eigen verantwoording.

Rationale: Vergelijkbaar met de eis om transparant te zijn over de herkomst van hardware en software (zie principe H5), maar dan toegespitst op AI-modellen: zonder deze doorwerking kan een organisatie niet aantonen dat een AI-toepassing binnen het bedoelde en onderbouwde gebruiksdoel van het onderliggende model blijft.

Implicaties: Vereist dat bij elke inzet van een extern AI-model de documentatie van de leverancier wordt opgevraagd, beoordeeld en opgenomen in het eigen architectuurdossier, met een expliciete toets of de eigen toepassing binnen het gedocumenteerde gebruiksdoel past.

Referenties

Onderstaande lijst bevat de externe bronnen die bij het opstellen van deze whitepaper zijn geraadpleegd, geordend naar herkomst: het manifest van de Open Cloud Alliantie, Nederlandse overheidsstukken, Europese beleids- en wetgevingsdocumenten, en overige adviesrapporten en position papers.

Manifest en position papers Open Cloud Alliantie

Open Cloud Alliantie (2026). Een Open Cloud voor Nederland, Manifest, met toelichting. Ondertekend door Centric, Info Support, Intermax, KPN, Nebul, Previder en Uniserver; ondersteund door Stichting Digitale Infrastructuur Nederland (DINL) en TNO. April 2026. www.opencloudalliantie.nl

DINL, Intermax, NBIP, Solvinity e.a. (2025). Strategische digitale autonomie en het Rijksbreed cloudbeleid, position paper. 27 mei 2025.

Nederlandse overheidsstukken

Algemene Rekenkamer (2025). Het Rijk in de cloud: donkere wolken pakken samen. Januari 2025.

Minister van Economische Zaken en Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (2025). Kabinetsreactie op de initiatiefnota van de leden Six Dijkstra en Kathmann over "Wolken aan de horizon". Kamerstuk 36574, nr. 3. 17 januari 2025.

Six Dijkstra, J. en Kathmann, B. (2024). Initiatiefnota "Wolken aan de horizon". Kamerstuk 36574. 18 juni 2024.

Staatssecretaris Digitalisering en Koninkrijksrelaties (2025). Nederlandse Digitaliseringsstrategie (NDS). Gepubliceerd juni 2025.

Ministerraad (2025). Visie "Digitale autonomie en soevereiniteit van de overheid". Bijlage bij Kamerstuk 26643, nr. 1450. 12 december 2025.

Staatssecretaris W.J.M. Aerdts, Economische Zaken en Klimaat (2026). Herziening Rijksbreed Cloudbeleid 2026. Kamerstukdossier 26643, nr. 1541; Kamerbrief 2026Z15738/2026D35294, beleidsdocument 2026D35295. Vastgesteld in de ministerraad, 3 juli 2026.

CIP / Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2026). Baseline Informatiebeveiliging Overheid 2 (BIO2), versie 1.3, definitieve versie. 9 januari 2026, gepubliceerd in de Staatscourant op 5 maart 2026. https://www.bio-overheid.nl/media/dr4inbhc/20260109-baseline-informatiebeveiliging-overheid-2-bio2-v13-def.pdf

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2026). Algemene Beveiligingseisen Rijksoverheidsopdrachten (ABRO 2026).

Tweede Kamer der Staten-Generaal (2025–2026). Cyberbeveiligingswet (Cbw), implementatie van de NIS2-richtlijn. Ingediend 4 juni 2025, aangenomen 15 april 2026.

Nederlandse wetgever. Wet weerbaarheid kritieke entiteiten (Wwke), Nederlandse implementatie van de Europese Critical Entities Resilience-richtlijn (CER). Van kracht sinds augustus 2026.

Nederlandse wetgever. Wet digitale overheid (Wdo), wettelijke basis voor verplichtstelling van open standaarden voor overheidsorganisaties. Van kracht sinds juli 2023, gefaseerde invoering.

Forum Standaardisatie. Lijst met aanbevolen en verplichte open standaarden voor de Nederlandse overheid, inclusief het "pas toe of leg uit"-beleid.

Logius. REST-API Design Rules en API-standaarden voor de Nederlandse overheid.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties / Logius. developer.overheid.nl, Kennisplatform API's.

Europese beleids- en wetgevingsdocumenten

Europese Commissie / ISA² programma, thans Interoperable Europe (2017, doorlopend). European Interoperability Framework (EIF).

Europees Parlement en Raad van de Europese Unie (2024). Verordening (EU) 2024/903, Interoperable Europe Act. Van kracht sinds 12 juli 2024.

Europese Commissie, DG DIGIT (2025). EU Cloud Sovereignty Framework, versie 1.2.1. Oktober 2025. https://commission.europa.eu/document/09579818-64a6-4dd5-9577-446ab6219113_en

Europese Commissie (2026). Voorstel Cloud and AI Development Act (CADA), COM(2026) 502, onderdeel van het Tech Sovereignty Package. 3 juni 2026.

Europese Commissie (2026). EU Open Source Strategy, onderdeel van hetzelfde European Technological Sovereignty Package als CADA. Gepresenteerd 3 juni 2026. Betreft een Communication, geen wetsvoorstel, en is daarmee niet juridisch bindend.

Europees Parlement en Raad van de Europese Unie (2024). Verordening (EU) 2024/1689, AI Act. In werking sinds 1 augustus 2024, met gefaseerde inwerkingtreding tot en met augustus 2028. De deadline voor hoogrisicosystemen (Annex III) is via het "Digital Omnibus"-pakket (goedgekeurd 29 juni 2026) uitgesteld naar 2 december 2027.

Europese Commissie / betrokken lidstaten (2023). Important Project of Common European Interest: Next Generation Cloud Infrastructure and Services (IPCEI-CIS). Goedgekeurd december 2023.

Europees Parlement en Raad van de Europese Unie (2022). Richtlijn (EU) 2022/2555 (NIS2-richtlijn).

Europees Parlement en Raad van de Europese Unie (2023). Verordening (EU) 2023/2854, Data Act. Van toepassing sinds september 2025.

WIK, Decision en Schuman Associates, in opdracht van de Europese Commissie (DG CNECT) (2026). Study on Interoperability of Data Processing Services. Resultaten gepubliceerd 23 februari 2026.

European Union Agency for Cybersecurity (ENISA) (2020, doorontwikkeld). EUCS, Cloud Service candidate cybersecurity certification scheme. https://www.enisa.europa.eu/sites/default/files/publications/EUCS%20–%20Cloud%20Service%20candidate%20cybersecurity%20certification%20scheme.pdf

Wet- en regelgeving privacybescherming en kwaliteitsnormen

Europees Parlement en Raad van de Europese Unie (2016). Verordening (EU) 2016/679, Algemene verordening gegevensbescherming (AVG).

Nederlandse wetgever. Wet politiegegevens (Wpg).

Nederlandse wetgever. Wet justitiële en strafvorderlijke gegevens (Wjsg).

International Organization for Standardization / International Electrotechnical Commission. ISO/IEC 27018, richtlijnen voor de bescherming van persoonlijk identificeerbare informatie (PII) in publieke clouddiensten.

International Organization for Standardization. ISO/IEC 27001:2022 en ISO/IEC 27002:2022, normen voor managementsystemen voor informatiebeveiliging en beheersmaatregelen.

Overige geraadpleegde bronnen

Autoriteit Consument & Markt (ACM). Marktstudie naar clouddiensten.

Linux Foundation. CHAOSS, raamwerk voor community- en gezondheidsmetrics van open source projecten.

Open Source Security Foundation (OpenSSF), Linux Foundation. OpenSSF Scorecard, geautomatiseerde beoordeling van beveiligingspraktijken van open source projecten; aanbevolen door het Amerikaanse CISA.

Nationaal Cyber Security Centrum (NCSC) en ENISA. Advies over risico's in de toeleveringsketen en het beperken van leveranciersafhankelijkheid.

VNG Realisatie. Haven-standaard voor platformonafhankelijke, containerbased hosting van gemeentelijke websites en applicaties, tot standaard verklaard door de VNG op 25 maart 2022; Haven+ is de bijbehorende referentie-implementatie. Beide zijn recent aangewezen als bouwsteen binnen de Generieke Digitale Infrastructuur (GDI).

Cloud Native Computing Foundation / OpenGitOps. GitOps-principes voor declaratieve, versiebeheerde infrastructuur- en applicatieconfiguratie.

Linux Foundation. OpenTofu, open source fork van Terraform, ontstaan in 2023 na de licentiewijziging van HashiCorp naar de Business Source License.

Colofon

Deze whitepaper is opgesteld als adviesstuk voor architecten door de Open Cloud Alliantie (OCA), als praktische verdieping op het manifest Een Open Cloud voor Nederland (april 2026).

Open Cloud Alliantie, ondertekend door

- Centric
- Info Support
- Intermax
- KPN
- Nebul
- Previder
- Uniserver

Ondersteund door

- Stichting Digitale Infrastructuur Nederland (DINL)
- TNO

www.opencloudalliantie.nl

OPEN CLOUD
ALLIANTIE

WWW.OPENCLOUDALLIANTIE.NL