Marktconsultatie
Eisen aan gemeentelijke Cloudvoorzieningen

Inhoudelijke reactie Centric

Datum: 7 september 2026

Inhoudsopgave

Inleiding

Op dit moment merken we op dat er bij uitvragen in marktconsultaties, aanbestedingen en directe vragen verschillende invalshoeken bestaan bij gemeenten over autonomie en soevereiniteit. We juichen het toe dat VNG werkt aan één kader voor clouddiensten die deze samenbrengt. Door een duidelijk kader zorgt dit voor duidelijkheid bij gemeenten en bij leveranciers.

De handreiking brengt verschillende termen bij elkaar, zoals 'autonomie' en 'soevereiniteit', in lijn met het in 2025 gepubliceerde Position Paper Digitale autonomie. In de tussentijd is er echter ook vooruitgang geboekt op Europees niveau met het EU Cloud Sovereignty Framework (PDF) en de bijbehorende implementatiegids en rekenmethode (zie de body van dat bookmark) bij dit framework. Het valt op dat de huidige handreiking afwijkt van het EU-framework. Vanuit het IMG CIO-beraad is in mei 2026 ook een uitvraag gedaan over digitale soevereiniteit. Deze uitvraag hanteert (een specifieke implementatie van) het Cloud Sovereignty Framework. We zouden de beantwoording van deze uitvraag graag samen zien komen met deze eisen aan de cloudvoorziening.

We roepen VNG daarom op om de handreiking onder te brengen bij de 8 thema's van soevereiniteit volgens de implementatie van de Europese Commissie. Dit levert het meest eerlijke speelveld op voor bestaande en nieuwe leveranciers en sluit aan bij een bredere beweging binnen de Europese Unie. Veel van de onderdelen en eisen zijn al compatibel met het Europese Framework. Zeker omdat deze gids moet dienen voor IaaS-, PaaS- en SaaS-diensten is ons advies aan te sluiten bij bestaande frameworks.

De handreiking geeft uitgebreid antwoord hoe een gemeente op basis van risico's in staat is om soevereiniteit, autonomie en betrouwbaarheid te borgen. In deze handreiking wordt echter alleen gekeken naar een framework vanuit risico-beheersing. Verschillende maatregelen die zijn genoemd, gaan ver in de technische en organisatorische eisen die zij stellen aan gemeenten én aan leveranciers. Daarbij vragen wij VNG om het kostenaspect ook in het document zelf te benoemen. Verschillende maatregelen raken niet alleen de investering, maar ook de efficiency van de uitvoering: dubbele omgevingen, gescheiden dataopslag en parallelle stacks vragen structureel meer beheer, meer testcapaciteit en meer coördinatie. Het document besteedt daar op dit moment geen aandacht aan. We vragen VNG om een kostenraming uit te voeren op basis van de risicoclassificaties zodat voor vaststelling duidelijk is welke budgetten gemeenten moeten reserveren wanneer deze additionele eisen worden toegevoegd bij inkoopprocessen. Dit voorkomt dat een gemeente de eisen overneemt zonder de financiële consequenties te hebben belegd.

Wat we onderschrijven

Een deel van de maatregelen sluit aan bij de praktijk die wij nu al hanteren en bij afspraken die al in de GIBIT staan. Om het beeld compleet te houden noemen we die vooraf. We onderschrijven zonder voorbehoud: het gebruik van open standaarden (G06), volledige exporteerbaarheid van data inclusief metadata (G07), contractueel vastgelegde exit- en migratievoorwaarden (G09), een verplicht en toetsbaar migratieplan (G20), het tijdelijk verklaren van niet-Europese oplossingen (G21), periodiek geteste herstel- en uitwijkprocedures (G27), inzicht in de back-upketen (G32), scheiding van back-up- en productieomgeving (G34), Infrastructure as Code en reproduceerbare omgevingen bij PaaS en IaaS (P01 en P03) en onafhankelijk herstel bij PaaS en IaaS (P09).

Onze opmerkingen richten zich daarom niet op de richting van het document. Zij richten zich op de toetsbaarheid, de scope per cloudmodel, de samenhang met bestaand recht en de kosten.

Verhouding tot de GIBIT 2025

De GIBIT 2025 geeft in artikel 2.5 aan dat er een rangorde is in documenten, waarbij de inkoopvoorwaarden (de GIBIT zelf) onderaan staan. Een programma van eisen dat als bijlage bij het bestek of bij de overeenkomst wordt gevoegd, prevaleert daarmee boven de GIBIT. Om de verhouding tussen de GIBIT en deze eisen helder te maken vragen we op verschillende plaatsen expliciet te maken welke maatregelen en eisen al worden ingevuld door de GIBIT. Hiermee is duidelijk wat de GIBIT al regelt, zonder een additionele reeks voorwaarden op te stellen die boven de GIBIT prevaleren en die de voorwaarden onnodig complex en onduidelijk maken.

Concreet vragen we VNG om in het document op te nemen dat een maatregel die een onderwerp raakt dat de GIBIT al regelt, wordt gelezen als een verwijzing naar het betreffende GIBIT-artikel en niet als een afwijking daarvan, tenzij die afwijking uitdrukkelijk en gemotiveerd is opgenomen.

Daarnaast stelt GIBIT 2025 in artikel 1.19 dat de Gemeentelijke ICT-kwaliteitsnormen van tijd tot tijd kunnen worden bijgewerkt. Artikel 8.1 verklaart die normen tot Overeengekomen gebruik en artikel 10.14 sub iv verplicht de leverancier om via Updates en Upgrades ook aan opvolgende versies van die normen te blijven voldoen, voor eigen rekening. Wanneer deze eisen aan gemeentelijke cloudvoorzieningen onderdeel worden van de kwaliteitsnormen, ontstaat een verplichting zonder einde op een document dat eenzijdig kan worden gewijzigd. Dat herziet het speelveld voor aanbieders ná verwerving. We pleiten ervoor om expliciet in het document op te nemen dat deze eisen aanvullend zijn op de GIBIT, geen onderdeel worden van de kwaliteitsnormen, en dat binnen een lopende overeenkomst de versie geldt die bij contractsluiting van kracht was.

Verhouding tot bestaand recht

De handreiking beschrijft zichzelf als handreiking, maar paragraaf 1.1 stelt dat de bepalingen verplicht zijn toe te passen bij inkoop en aanbesteding en bij de exploitatie van eigen cloudomgevingen. Dat verschil in status is niet zonder gevolgen. Voor een leverancier bepaalt het of afwijken bespreekbaar is of niet. We vragen VNG om de status van het document expliciet te kwalificeren, om vast te leggen wie het beheert en wijzigt, met welke consultatie en met welk versiebeheer, en of afwijken mogelijk is met een motivering. Zie voor de uitwerking van dit punt 1.1 - Doel en Reikwijdte.

Een tweede vraag die daar direct uit volgt is het overgangsrecht. Het document bevat geen enkele bepaling over lopende contracten en verlengingen. Voor gemeenten en leveranciers is dat de meest concrete onzekerheid van dit moment. We vragen om een expliciete overgangsbepaling.

Een aanzienlijk deel van de maatregelen regelt onderwerpen die inmiddels in bindend Europees en nationaal recht zijn vastgelegd. Waar dat zo is, verdient een verwijzing de voorkeur boven een eigen formulering. Een eigen formulering die net iets anders luidt dan de wet, levert bij aanbestedingen discussie op zonder dat het beschermingsniveau toeneemt. Het gaat om de volgende kaders:

Kader	Raakt	Toelichting
Verordening (EU) 2023/2854 (Data Act), hoofdstuk VI	R2, R4, G07, G08, G09, G14, G17, S01 t/m S03, S07, S08	Sinds 12 september 2025 volledig van toepassing op IaaS, PaaS én SaaS. Regelt overstapfaciliteiten, functionele gelijkwaardigheid, minimaal 30 dagen migratieondersteuning en het vervallen van overstapkosten per 12 januari 2027. Artikel 32 regelt maatregelen tegen onrechtmatige toegang door overheden van derde landen
AVG artikel 28 en de VNG Standaard Verwerkersovereenkomst	S04, S06	De VWO is via GIBIT artikel 1.49 en 31.1 al van toepassing en regelt transparantie over en wijziging van subverwerkers

Kader	Raakt	Toelichting
BIO2 en de Cyberbeveiligingswet	Hoofdstuk 4, 7, G23, G28, G31	De Cbw treedt op 15 augustus 2026 in werking en verankert de BIO2 als juridisch referentiekader voor de zorgplicht
Aanbestedingswet 2012 en de Gids Proportionaliteit	Hoofdstuk 4, G16, hoofdstuk 11	Knock-out-eisen moeten proportioneel zijn (artikel 1.10 Aw) en technische specificaties moeten gelijkwaardige oplossingen toelaten (artikel 2.75 en 2.76 Aw)
EUCS, het Europese certificeringsschema voor clouddiensten	G11, hoofdstuk 8	Het schema is nog niet vastgesteld. Dat is een argument om nu geen eigen soevereiniteitsniveaus te introduceren

Leeswijzer

Dit document is geordend als gestructureerde feedback op het document "Eisen aan gemeentelijke Cloudvoorzieningen" en volgt de nummering van dat document. Feedback is opgenomen per paragraaf of maatregel met verwijzingen waar nodig. Onder hoofdstuk 4 staat een samenvattend overzicht van onze voorstellen per maatregel. De toelichtingen bij de individuele maatregelen bouwen daarop voort.

Voor de S- en P-codes hanteren wij consequent de nummering van hoofdstuk 6 van de handreiking. Zie 3 - Risico's en maatregelen voor de reden.

Aanbevelingen

1 - Inleiding

1.1 - Doel en Reikwijdte

In 1.1 op pagina 3 staat dat de bepalingen "verplicht toe te passen" zijn bij de inkoop en aanbesteding van clouddiensten en bij de ontwikkeling en exploitatie van eigen cloudomgevingen. Wij vragen om die formulering te heroverwegen, om twee redenen.

Ten eerste past zij niet bij de aard van het document. Het document is gepubliceerd als handreiking, en 1.2 omschrijft het in de eerste alinea als "een kaderstellend beleidsdocument dat richting geeft aan de wijze waarop gemeenten omgaan met cloudvoorzieningen". Richting geven en verplicht toepassen zijn twee verschillende dingen. Nu staan beide kwalificaties op dezelfde pagina.

Ten tweede is er de bevoegdheidsvraag. VNG is een vereniging van gemeenten en geen toezichthouder of regelgever. Een verplichting voor gemeenten volgt uit wet- en regelgeving, of uit een besluit dat gemeenten zelf nemen. VNG kan een kader aanbevelen, als gezamenlijke standaard vaststellen en beheren, maar kan gemeenten niet eenzijdig binden. Gemeenten behouden hun eigen bevoegdheid en hun eigen verantwoordelijkheid, onder meer voor de proportionaliteitstoets per aanbesteding.

Dit is geen formeel punt. Voor een leverancier bepaalt de status of afwijken bespreekbaar is, en voor een gemeente of zij een eis moet overnemen of kan wegen. Wij vragen VNG daarom om één kwalificatie te kiezen en die consequent te gebruiken, en om aan te geven langs welke route het kader eventueel wel bindend wordt: als onderdeel van de Gemeentelijke ICT-kwaliteitsnormen, via een besluit van de leden, of als aanbeveling die per aanbesteding wordt overgenomen. Zie ook Verhouding tot de GIBIT 2025 en Verhouding tot bestaand recht.

1.2 - Positionering binnen het gemeentelijk instrumentarium

In 1.2 op pagina 3 staat: "gemeentelijk cloudbeleid sluit aan bij geldende Europese kaders en richtlijnen". Het is echter onduidelijk in hoeverre het kader overeenkomt met het EU Cloud Sovereignty Framework. We vragen om die relatie expliciet te maken, bij voorkeur met een mapping van de maatregelen op de acht thema's van het framework.

De eerste alinea van 1.2 kwalificeert het document als kaderstellend en richtinggevend. Die kwalificatie verhoudt zich niet tot het verplichtende karakter dat 1.1 op dezelfde pagina beschrijft. Zie 1.1 - Doel en Reikwijdte.

2 - Strategisch kader

2.2 - Publieke waarden: continuïteit, databeschikbaarheid en veiligheid

Het artikel geeft aan dat bedrijfscontinuïteit essentieel is. Gemeenten zijn essentiële entiteiten onder de Cyberbeveiligingswet. Dit is voor diensten een belangrijk uitgangspunt en een verwijzing is hier zeker op haar plaats.

2.3 - Dreigingen en structurele kwetsbaarheden

In deze paragraaf wordt gesproken over aanbieders met een internationale positie. Dit leidt echter niet tot de invloed van buitenlandse wetgeving zolang aanbieders enkel binnen de Europese Unie actief zijn. We bevelen aan om de kwetsbaarheid te herformuleren naar de daadwerkelijke angel: bedrijven die door internationale activiteiten vallen onder wetgeving die eisen stelt aan datatoegang en dienstverlening binnen Europa. Hiermee is duidelijk dat volledig Europese spelers geen onderdeel zijn van deze kwetsbaarheid.

In het algemeen wordt gezegd dat de "cloudmarkt wordt gekenmerkt door een sterke concentratie van aanbieders". Deze manier van formuleren gaat voorbij aan de vele Nederlandse en Europese aanbieders van clouddiensten, zoals verenigd in de Open Cloud Alliantie. Deze formulering laat zien dat er nog veel onbekendheid is met Europese aanbieders en zegt niets over hun mogelijkheid om gemeenten te ondersteunen. We pleiten ervoor dit te herformuleren zodat duidelijk is dat gemeenten de afgelopen jaren veelal hebben gekozen voor niet-Europese clouddiensten en dat er nu een mogelijkheid ontstaat om Europese alternatieven in te zetten.

2.4 - Noodzaak van autonomie

Naast de noodzaak van soevereiniteit in 2.5 benoemt 2.4 de noodzaak van autonomie. De omschrijving daarvan is: "de mate waarin gemeenten zelfstandig keuzes kunnen maken over hun digitale infrastructuur. Dit omvat onder meer de mogelijkheid om leveranciers te selecteren of te vervangen, systemen aan te passen en regie te voeren over de inrichting en werking van de digitale omgeving."

Zo omschreven voegt de paragraaf weinig toe. Gemeenten beschikken op grond van hun bestuurlijke positie al over deze autonomie: zij kiezen zelf hun leveranciers, richten hun eigen processen in en voeren zelf regie. Autonomie is in die betekenis geen te realiseren doel, maar een gegeven.

De praktische vraag is eerder het omgekeerde. Doordat 342 gemeenten die keuzevrijheid ieder afzonderlijk gebruiken, ontstaat versnippering in eisen, architecturen en contractvoorwaarden. Dat maakt collectieve oplossingen duurder en vertraagt juist de beweging die deze handreiking wil maken. Wij zien dat bij vrijwel elke uitvraag terug, en het is ook de reden waarom wij één gezamenlijk kader toejuichen.

Wij bevelen daarom aan om 2.4 te herformuleren. Niet als pleidooi voor meer autonomie, maar als afweging tussen de keuzevrijheid van de individuele gemeente en de uniformiteit die nodig is om als collectief resultaat te boeken. Daarbij hoort ook de vraag welke keuzes gemeenten bewust gezamenlijk maken en welke zij individueel houden. Zonder die afweging blijft onduidelijk welk probleem 2.4 adresseert.

2.5 - Noodzaak van soevereiniteit

Wij bevelen aan om vanaf deze paragraaf en in het hele document consequent te spreken over *digitale soevereiniteit* in plaats van *soevereiniteit*. Soevereiniteit is in staatsrechtelijke zin een eigenschap van de

staat, niet van een gemeente en niet van een cloudvoorziening. In een document dat als bijlage bij bestekken en overeenkomsten wordt gebruikt, kan die ruimere term tot discussie leiden over wat precies bedoeld is. "Digitale soevereiniteit" is de gangbare term in het Position Paper Digitale autonomie, in het EU Cloud Sovereignty Framework en in de uitvraag van het IMG CIO-beraad, en sluit dus ook aan bij de kaders waarnaar wij elders in deze reactie verwijzen.

Differentiatie binnen de Europese Unie

De handreiking stuurt consequent aan op het afnemen van cloudoplossingen binnen de Europese Unie. Als antwoord op de ontwikkelingen buiten Europa is dat een begrijpelijke keuze en wij steunen die richting.

Wij vragen wel aandacht voor de aanname die eronder ligt, namelijk dat "binnen de EU" een homogene en blijvend stabiele categorie is. Ook binnen de Unie verschillen lidstaten in rechtsstatelijke waarborgen, in de wijze waarop nationale veiligheidswetgeving toegang tot gegevens regelt en in geopolitieke positie. Het is niet uitgesloten dat een gemeente op enig moment liever geen verwerking in een specifieke lidstaat wil hebben. Het document biedt daar nu geen instrument voor: na de stap "binnen de EU/EER" is er geen verdere differentiatie mogelijk.

Wij bevelen daarom aan om de lidstaat-dimensie expliciet te maken in plaats van te volstaan met EU/EER. Concreet:

- laat de leverancier per dienst opgeven in welke lidstaten verwerking, opslag, beheer en control-plane zich bevinden, en welk recht daarop van toepassing is;
- maak de locatie van verwerking een gegeven met een meldplicht bij wijziging, zodat een gemeente kan bijsturen als de omstandigheden veranderen;
- geef gemeenten de mogelijkheid om, op objectieve en per opdracht gemotiveerde gronden, de verwerkingslocatie tot een deel van de lidstaten te beperken.

Hiermee ontstaat wat nu ontbreekt: de mogelijkheid om binnen het Europese kader te differentiëren, zonder een nieuw en afwijkend niveau te introduceren. Deze uitwerking sluit ook aan bij het Europese framework, dat locatie en toepasselijk recht al als parameters kent, en bij ons voorstel bij G12 - Transparantie eigendomsstructuur en zeggenschap.

Wij wijzen er daarbij op dat dit iets anders is dan een voorkeur voor Nederlandse leveranciers. Een generieke voorkeur voor aanbieders uit één lidstaat verhoudt zich niet tot het verbod op discriminatie naar nationaliteit binnen de interne markt en tot artikel 1.8 van de Aanbestedingswet 2012. Een per opdracht gemotiveerde beperking van de verwerkingslocatie op grond van een concreet risico is wel mogelijk. Wij adviseren VNG dat onderscheid in de handreiking expliciet te maken, omdat gemeenten er in de praktijk anders zelf een weg in zoeken en dat tot aanvechtbare bestekken leidt.

2.7 - Dimensies van soevereiniteit

De dimensies van soevereiniteit kennen een *operationele dimensie*, een *technische dimensie* en een *data-dimensie*. Dit is anders dan het EU Cloud Sovereignty Framework en anders dan de door het IMG CIO-beraad uitgevraagde inventarisatie. De dimensies zijn begrijpelijk, maar de eenduidigheid vanuit gemeenten ontbreekt en de indeling sluit niet logisch aan bij het Europese kader. Ook worden de scheiding tussen regie en uitvoering en de continuïteit van dienstverlening hier ingebracht. We pleiten voor het aansluiten bij Europese kaders om voor leveranciers een eenduidig speelveld te realiseren.

3 - Risico's en maatregelen

De maatregelen krijgen in dit hoofdstuk voor het eerst een code. Die codes zijn in het document niet stabiel. Voor de G-codes loopt de nummering gelijk. Voor de S- en P-codes verschilt de nummering tussen hoofdstuk 6 enerzijds en de bijlagen 10 en 11 anderzijds. De hoofdstukken 3.1 en 7 volgen de nummering van hoofdstuk 6, de bijlage EMVI volgt die van bijlage 10.

Code	Hoofdstuk 6	Bijlage 10
S03	Datamobiliteit zonder applicatie-afhankelijkheid	Transparantie subverwerkers
S04	Transparantie subverwerkers	Toegangsbeperking leverancier
S05	Toegangsbeperking leverancier	Continuïteit bij beëindiging
S06	Meldplicht wijziging subverwerkers	Toegang tijdens migratie
S07	Continuïteit bij beëindiging	Lifecycle transparantie
S08	Toegang tijdens migratie	Datamobiliteit
S09	Lifecycle en roadmap transparantie	Meldplicht subverwerkers
P03	Reproduceerbare omgevingen	Control-plane binnen EU
P04	Control-plane binnen EU	Logging en monitoring
P05	Onafhankelijk beheer mogelijk	Geo-redundantie
P06	Logging en monitoring	Hersteltests
P07	Geo-redundantie	Onafhankelijk beheer
P08	Periodieke hersteltests	Transparantie infrastructuur
P09	Onafhankelijk herstel mogelijk	Reproduceerbare omgevingen
P10	Transparantie infrastructuur	Onafhankelijk herstel

Wij vragen u de nummering vóór vaststelling gelijk te trekken en daarna vast te zetten, zodat contracten en bestekken er stabiel naar kunnen verwijzen.

Toepassingsgebied per cloudmodel

De maatregelen zijn ingedeeld in algemeen geldend (G), SaaS-specifiek (S) en PaaS/IaaS-specifiek (P). In de gekozen opzet gelden de G-maatregelen per definitie voor alle cloudmodellen, en komen de S- of P-maatregelen daar bovenop.

Die opzet werkt niet voor alle G-maatregelen. Verschillende algemene eisen zijn bij SaaS niet of moeilijk in te vullen, omdat zij een object veronderstellen dat bij SaaS niet aan de afnemer wordt geleverd. G08 vraagt bijvoorbeeld toegang tot "alle technische artefacten, waaronder Infrastructure-as-Code, CI/CD-configuraties, scripts, container images en documentatie". Bij een SaaS-dienst bestaan die artefacten niet als afzonderlijk leverbaar object voor de gemeente. Hetzelfde geldt voor G10 (vendor-agnostische architectuur), G25 (scheiding control-plane en uitvoering) en G33 en G38 (herstel buiten de leverancier). Onze opmerkingen bij die maatregelen werken dat verder uit.

Wij bevelen aan om per maatregel expliciet een toepassingsgebied op te nemen: SaaS, PaaS, IaaS of een combinatie daarvan. Bijlage 10 kent al een kolom Toepassingsgebied, maar die staat voor alle G-maatregelen op 'Algemeen'. Door dat per maatregel te differentiëren wordt de G-set kleiner en scherper, en verdwijnt de noodzaak om per aanbesteding uit te leggen waarom een eis bij SaaS niet van toepassing is. Waar een G-maatregel bij één cloudmodel een andere invulling krijgt, kan dat in de maatregel zelf worden opgenomen, zoals in onze tekstvoorstellen bij G08 - Toegang tot data en technische artefacten, G10 - Vendor-agnostische architectuur en G25 - Scheiding control-plane en uitvoering.

Redactionele opmerkingen bij 3.1

In de afbeelding bij 3.1 op pagina 8 is de bovenste regel leeg. Daardoor ontbreekt in de afbeelding de regel voor R1 (Concentratie), terwijl R1 wel in de tabel op pagina 9 staat. Mogelijk zijn hier ook de kolomkoppen weggevallen; de aanduidingen Risico, Doelen en Maatregelen staan nu alleen als legenda onder de afbeelding.

In de tabel op pagina 9 staat in de kolom Risico bij R1 de omschrijving "Concentratierisico en leveranciersafhankelijkheid" tweemaal, de tweede keer met een afbreekfout.

4 - Handleiding voor PvE

Overzicht van onze voorstellen per maatregel

Onderstaande tabel vat onze voorstellen samen. De toelichtingen in hoofdstuk 5 en 6 werken deze voorstellen uit. Waar wij een tekstvoorstel doen, staat dat bij de betreffende maatregel in hoofdstuk 6.

Wij stellen voor het aantal maatregelen te consolideren door dubbelingen samen te voegen en door te verwijzen naar kaders die hetzelfde al regelen. Van de 59 maatregelen komen er in ons voorstel ongeveer 35 over, met dezelfde dekking van de zeven risico's.

Maatregel	Ons voorstel	Reden
G02 Multi-provider inzet	Herformuleren en scope verduidelijke	Bij SaaS betekent de maatregel dubbele verwerving
G03 Inzicht in ketenafhankelijkheden	Verwijzen naar GIBIT	GIBIT artikel 25 (SBOM)
G04 Spreiding van kritieke workloads	Samenvoegen met G02	Functioneel gelijk
G05 Verkaveling van systemen en leveranciers	Samenvoegen met G02	Functioneel gelijk
G06 Gebruik van open standaarden	Verwijzen naar GIBIT	GIBIT artikel 8
G07 Volledige data-export inclusief metadata	Verwijzen naar GIBIT en aanvullingen	GIBIT artikel 22, Data Act hoofdstuk VI
G08 Toegang tot data en technische artefacten	Verplaatsen naar PaaS/IaaS, tekstvoorstel	Technische artefacten bestaan niet als afzonderlijk object bij SaaS
G09 Contractueel vastgelegde exit- en migratievoorwaarden	Verwijzen naar GIBIT en aanvullingen	GIBIT artikel 29, Data Act artikel 23 tot en met 25
G10 Vendor-agnostische architectuur	Verplaatsen naar PaaS/IaaS, tekstvoorstel	Raakt bij SaaS de interne architectuur van de leverancier
G11 EU/EER-jurisdictie of gelijkwaardig beschermingsniveau	Herformuleren, tekstvoorstel	"Gelijkwaardig" is niet toetsbaar
G12 Transparantie eigendomsstructuur en zeggenschap	Aansluiten bij KVK-registraties, tekstvoorstel	"Volledig inzicht" is ongedefinieerd; KVK-registraties volstaan
G13 Data-eigendom bij gemeente	Herformuleren, tekstvoorstel	Eigendom op data bestaat niet in het Europees en Nederlandse recht
G14 Verplichting tot juridisch betwisten van datavorderingen	Verwijzen naar Data Act en kosten regelen, tekstvoorstel	Data Act artikel 32, GIBIT artikel 19 en 28.6
G15 EU-by-design als uitgangspunt	Definiëren via minimum SEAL-niveau, tekstvoorstel	"Europees" is niet gedefinieerd; reikwijdte in de keten is onbepaald
G16 Beperking inzet niet-EU leveranciers	Verduidelijken en toetsen	"Volwaardig alternatief" is niet objectiveerbaar
G17 Geen contractuele blokkades voor migratie	Samenvoegen met G09	Verwijzen naar GIBIT artikel 27. Met G09 is het één logisch coherente maatregel.
G18 Recht op periodieke heroverweging	Laten vervallen	Reeds mogelijk via looptijd en opzeggingsgronden

Maatregel	Ons voorstel	Reden
G19 Ondersteuning bij toetsing alternatieven	Laten vervallen	Eenzijdig en niet begrensd
G22 Onafhankelijk audit- en toezichtrecht	Verwijzen naar GIBIT en voorwaarden borgen, tekstvoorstel	GIBIT artikel 19, 28 en 38; audits zijn verstorend en brengen kosten mee
G23 Transparantie in logging en processen	Verduidelijken en begrenzen	GIBIT artikel 19, 25.3, 25.4 en 32.8
G24 Geen beperkingen op toezicht	In lijn brengen met GIBIT	GIBIT artikel 28.1, 28.3 en 28.6
G25 Scheiding control-plane en uitvoering	Herformuleren, tekstvoorstel	Onderscheid functioneel en technisch beheer ontbreekt
G26 Contractuele borging continuïteit en incidentrespons	Verwijzen naar GIBIT en aanvullen	GIBIT artikel 10.10 tot en met 10.13, serviceniveaus per BBN ontbreken
G27 Periodieke tests van herstel- en uitwijkscenario's	Samenvoegen met G35 en P08	Deze maatregel is functioneel identiek aan G35 en P08.
G28 Verplichte informatievoorziening bij verstoringen	Verwijzen naar GIBIT en Cbw	GIBIT artikel 32.6 en 32.7, meldplicht Cbw
G29 Geo-redundantie	Verduidelijken en niet verplichten bij BBN1	Strijdig met het profiel van BBN1
G30 Topografische spreiding	Samenvoegen met G29	Verhouding tot G29 is onduidelijk
G31 Crisis- en escalatieprocedures	Verwijzen naar GIBIT	SLA en GIBIT artikel 32.7
G33 Geen afhankelijkheid van één leverancier voor herstel	Herformuleren, tekstvoorstel	Bij SaaS is herstel een leveranciersverantwoordelijkheid
G35 Aantoonbaar geteste herstelprocedures	Samenvoegen met G27	Functioneel (vrijwel) identiek met G27/
G37 Onafhankelijke restore mogelijkheid	Samenvoegen met G33	Functioneel identiek met G33
G38 Aantoonbaar herstel buiten leverancier	Herformuleren, tekstvoorstel	Herstel buiten de omgeving is migratie, geen herstel
S01 Scheiding data en applicatie	Laten vervallen	Gaat op in G07
S02 Volledige data-export inclusief metadata	Laten vervallen	Kopie van G07
S03 Datamobiliteit zonder applicatie-afhankelijkheid	Laten vervallen	Gaat op in G07
S04 Transparantie subverwerkers	Verwijzen naar GIBIT	AVG artikel 28, VNG Standaard Verwerkersovereenkomst
S05 Toegangsbeperking leverancier	Verwijzen naar GIBIT	GIBIT artikel 22.8
S06 Meldplicht wijziging subverwerkers	Verwijzen naar GIBIT	AVG artikel 28, VNG Standaard Verwerkersovereenkomst
S07 Continuïteit bij beëindiging	Verwijzen naar GIBIT	GIBIT artikel 29.8 tot en met 29.11
S08 Toegang tijdens migratie	Verwijzen naar GIBIT	GIBIT artikel 29.11, Data Act artikel 25
S09 Lifecycle en roadmap transparantie	Verwijzen naar GIBIT	GIBIT artikel 16

Maatregel	Ons voorstel	Reden
S10 Continuïteit bij faillissement	Verwijzen naar GIBIT en uitwerken	GIBIT artikel 39, klassieke broncode-escrow is bij SaaS niet toereikend
P01 Infrastructure as Code	Verduidelijken en vertrouwelijkheid borgen	GIBIT artikel 19 en 21.3
P02 Volledige configuratietoegang	Samenvoegen met G08	Zelfde object
P04 Control-plane binnen EU	Samenvoegen met G11	Zelfde norm
P05 Onafhankelijk beheer mogelijk	Samenvoegen met G25	Zelfde norm
P06 Logging en monitoring	Samenvoegen met G23	Zelfde norm
P07 Geo-redundantie	Samenvoegen met G29	Zelfde norm
P08 Periodieke hersteltests	Samenvoegen met G27	Zelfde norm
P10 Transparantie infrastructuur	Verduidelijken, vertrouwelijkheid borgen	Raakt bedrijfsgeheim van de hostingpartij
P11 Parallelle multi-stack inzet	Alleen bij BBN3 en alleen voor workloads zonder downtimetolerantie	Strijdig met het profiel van BBN2

4.1 - Doel en gebruik van deze handleiding

De handleiding belooft in 4.1 dat lichte toepassingen niet onnodig zwaar worden ingericht. Die belofte wordt in de matrix niet waargemaakt. Bij BBN1, het laagste niveau, zijn G26 tot en met G38 verplicht. Dat betekent dat een toepassing met een laag risico verplicht geo-redundant moet zijn (G29), verspreid over gescheiden regio's binnen de EU (G30), met gescheiden opgeslagen datasets (G36) en met aantoonbaar herstel buiten de leverancieromgeving (G38). Tegelijk stelt hoofdstuk 7 voor BBN1 dat een tweede stack niet actief hoeft te draaien en dat rebuild volstaat. Die twee beelden passen niet op elkaar.

We vragen om de verplichte set bij BBN1 terug te brengen tot wat bij het beschreven profiel past: inzicht in back-up en herstel, scheiding van back-up en productie, geteste herstelprocedures en contractuele borging van incidentrespons.

4.2 - Stap 1: bepaal Beveiligingsniveau

De keuze om risicogedreven te werken is waardevol, omdat het de discussie kadert naar de juiste maatregelen. Qua methodiek valt op dat de BBN's uit de BIO 1 worden gebruikt. Zie hiervoor onze suggesties in 7 Bijlage: BBN beveiligingsniveau's.

Er is daarnaast een inhoudelijk bezwaar tegen de systematiek zelf. Het BBN volgt uit de hoogste score op beschikbaarheid, integriteit of vertrouwelijkheid. Een toepassing die alleen op beschikbaarheid hoog scoort, bijvoorbeeld een publiekgerichte voorziening zonder gevoelige gegevens, komt daarmee in BBN3 terecht. In BBN3 is het gebruik van niet-Europese oplossingen niet toegestaan en gelden alle jurisdictiemaatregelen G11 tot en met G16. Jurisdictie is echter een vraagstuk van vertrouwelijkheid en geopolitiek, niet van beschikbaarheid.

Wij bevelen aan om de maatregelen uit R3 los te koppelen van het BBN en uitsluitend te laten aansturen door de V-score en het soevereiniteitsniveau. Daarmee blijft de beschikbaarheidsas doen waar zij voor bedoeld is en komt de jurisdictievraag terecht bij de gegevens waar zij thuishoort.

(interne opmerking): **Zie ook**: Confrontatiematrix BBN × risico's × maatregelen — volledig uitgeschreven

4.3 - Stap 2: bepaal de relevante beheersmaatregelen

Voor hoog risico waarbij continuïteit en soevereiniteit noodzakelijk zijn, is de architectuur bepaald als active-active. Dit is een principe dat sterk kostenverhogend werkt. Zeker omdat P11 zowel bij BBN2 als bij BBN3 een aanvullende verplichting is, zullen de kosten voor gemeenten toenemen. Continuïteit is een risicoafweging met bijbehorende kosten. Om de impact op dienstverlening duidelijk te maken en gemeenten correcte inschattingen te laten maken, bevelen we aan om een kosteninschatting te maken voor de maatregelen, zodat gemeenten voldoende budget kunnen reserveren.

Bij BBN2 gaat het bovendien niet alleen om kosten. De matrix in 4.3 verklaart P11 verplicht bij BBN2, terwijl hoofdstuk 7 voor BBN2 stelt dat de tweede stack technisch is ingericht en periodiek wordt getest, maar niet permanent actief is, en dat een overstap beperkte downtime mag bevatten. P11 vraagt precies het tegenovergestelde, namelijk workloads die gelijktijdig operationeel worden gehouden. Deze twee bepalingen kunnen niet naast elkaar bestaan. Wij vragen P11 te verplaatsen naar BBN3, en daar te beperken tot workloads die geen enkele vorm van downtime kunnen verdragen.

Wat hier verder ontbreekt is de vertaling naar serviceniveaus. De GIBIT kent op dit punt uitgewerkte normen. Wanneer het PvE spreekt over active-active, real-time replicatie en herstel zonder dataverlies, overschrijft het die normen zonder dat te benoemen.

Onderwerp	GIBIT 2025	Eisen aan gemeentelijke cloudvoorzieningen
Beschikbaarheid	Artikel 37.2: 98% per maand op werkdagen tussen 09.00 en 17.00 uur, tenzij anders overeengekomen	BBN3: active-active of hot standby met automatische failover
Dataverlies en hersteltijd	Artikel 32.5: RPO van 28 uur en RTO van 16 werkuren in 85% van de gevallen, tenzij anders overeengekomen	BBN3: real-time replicatie, geen dataverlies
Bereikbaarheid voor onderhoud	Artikel 10.6: werkdagen tussen 09.00 en 17.00 uur	Impliciet doorlopend

Het gat tussen deze twee kolommen is het gat waarin de kosten zitten. Zolang het niet expliciet is, ontstaat per aanbesteding een discussie over welke norm geldt. Wij vragen VNG om per BBN-niveau de bijbehorende beschikbaarheid, RPO en RTO expliciet op te nemen, en om aan te geven hoe die zich verhouden tot de artikelen 32.5, 37.2 en 10.6 van de GIBIT.

Tot slot vragen we aandacht voor de proportionaliteit van knock-outeisen. Maatregelen die een tweede leverancier, een tweede technologiestack of het uitsluiten van niet-Europese partijen verplicht stellen, werken in een aanbesteding als uitsluitingsgrond. Dat vraagt om een toets aan artikel 1.10 van de Aanbestedingswet 2012 en aan de Gids Proportionaliteit, en om een toets of gelijkwaardige oplossingen worden toegelaten.

4.4 - Stap 4: Bepaal het Soevereiniteitsniveau

Voor de goede orde: er is geen stap 3. De handleiding gaat van stap 2 naar stap 4 en sluit af met een paragraaf zonder stapnummer. De zin waarmee 4.4 opent breekt bovendien af bij "In hoofdstuk". Wij nemen aan dat hier een verwijzing naar hoofdstuk 8 was bedoeld.

Belangrijker is dat de twee assen van de handleiding nergens bij elkaar komen. Stap 2 levert een BBN, stap 4 levert een soevereiniteitsniveau, en het document geeft geen regel voor de combinatie. Dat leidt tot uitkomsten die elkaar uitsluiten. Een toepassing die op BBN3 uitkomt maar op S4 wordt geplaatst, moet volgens hoofdstuk 7 alle niet-Europese oplossingen uitsluiten en volgens hoofdstuk 8 commerciële cloud

toestaan. Wij vragen om een expliciete matrix die beide assen verbindt, of om het samenvoegen van beide assen tot één classificatie.

Voor persoonsgegevens en hoge vertrouwelijkheid, en dat zijn vrijwel alle hoofddomeinen bij een gemeente, geldt nu de 'EU-overheidscloud'. Als voorbeeld voor S3 staan echter bedrijfsvoeringsprocessen zoals HR en Financiën. Een financieel systeem kent voor de debiteuren- en crediteurenadministratie echter ook persoonsgegevens en een integratie met de BRP. HR-systemen bevatten per definitie persoonsgegevens van ambtenaren en gevoelige informatie over functioneren en ziekte. De opzet van S2 en S3 spreekt zichzelf daarmee tegen. Het is beter om S2 en S3 samen te voegen tot EU/NL cloud met eisen. Deze opzet sluit ook aan bij het huidige marktlandschap, waarin leveranciers oplossingen vanuit een eigen cloud leveren. Zie ook onze suggesties bij: 8 Bijlage - Soevereiniteitsniveau's GEMMA

Volledigheid van de GEMMA-domeinen

De tabel bij 4.4 wijst per soevereiniteitsniveau een "bijpassend GEMMA-domein" aan. Die toewijzing is niet uitputtend, waardoor voor een aantal gemeentelijke domeinen niet is vast te stellen welk niveau geldt. Belastingen en Leefomgeving worden bijvoorbeeld niet genoemd, terwijl daar zowel persoonsgegevens als financiële en handhavingsgegevens worden verwerkt.

Ook binnen de genoemde domeinen is de afbakening niet scherp. Bij S2 staat "Sociaal domein, zoals jeugdzorg en Wmo". Daaruit is niet af te leiden of S2 voor het volledige sociaal domein geldt, inclusief participatie en inkomen, of alleen voor die onderdelen waar bijzondere persoonsgegevens worden verwerkt. Voor een gemeente die een aanbesteding voorbereidt is dat het verschil tussen twee heel verschillende eisensets. Voor een leverancier is het het verschil tussen wel en niet kunnen inschrijven.

Wij vragen VNG om de toewijzing uitputtend te maken voor alle GEMMA-domeinen, en om per domein aan te geven of het niveau voor het hele domein geldt of alleen voor specifiek benoemde processen of gegevenscategorieën. Zie ook onze opmerkingen bij S2 - Soevereine overheidscloud.

4.5 - Bepaal de EMVI-criteria

Zoals ook aangegeven bij 4.2 - Stap 1: bepaal Beveiligingsniveau vervallen de BBN-niveaus met de BIO2. Een andere systematiek is nodig, en daarmee ook een andere grondslag voor de weging van de EMVI-criteria. Zie verder 11 Bijlage EMVI Gemeentelijke Cloud.

5 - Risico's nader toegelicht

R1 - Concentratie en Leveranciersafhankelijkheid

Marktdefinitie en afhankelijkheid

De markt voor clouddiensten wordt gekenmerkt door een hoge mate van concentratie

Het risico zoals dit benoemd is, klopt waar het gaat om diensten van hyperscalers. Er zijn echter ook voldoende leveranciers van clouddiensten (IaaS en PaaS) van Europese bodem, zoals de deelnemers van de Open Cloud Alliantie. Alleen is de keuze voor deze dienstverleners moeilijker voor gemeenten door het geïntegreerde karakter van de diensten van hyperscalers.

Voor gemeentelijke SaaS ligt het anders en dat verdient een eigen formulering. De markt bestaat uit 342 gemeenten met sociale diensten, samenwerkingen en meer. Zoals blijkt uit de ICT Benchmark voor gemeenten van M&I gaat het grootste deel van het ICT-budget naar medewerkers. De kosten voor software zijn, gecorrigeerd voor inflatie, vrijwel stabiel, ondanks het toenemende aantal SaaS-diensten in gebruik bij gemeenten. Daarnaast is de markt zelf erg klein. En door het beperkte budget en de hoge graad van specialisatie kan de markt niet meer dan twee tot drie leveranciers per domein dragen. Dat is geen marktfalen maar een structureel gevolg van de schaal van de markt. En het geeft gemeenten juist een voordeel. Zoals VNG zelf constateert in haar Position Paper Digitale Autonomie uit oktober 2025 is er juist voor deze specialistische dienstverlening een wederzijdse afhankelijkheid die gemeenten een stevige onderhandelingspositie geeft.

Wat in de beschrijving ontbreekt is dus het onderscheid tussen de lagen. Bij IaaS en PaaS is concentratie reëel en vraagt het om Europees verwervingsbeleid. Bij gemeentelijke SaaS is een beperkt aantal aanbieders het gevolg van schaal, en is de juiste beheersing niet dubbele verwerving maar continuïteit: escrow, gegarandeerde datatoegang en een werkende exit. We pleiten voor een herformulering die dat onderscheid maakt en die de positie van gemeenten tegenover specialistische dienstverleners erkent, zoals VNG dat in het eerdere position paper ook deed.

Continuïteitsmaatregelen

Als beheersingseffect staat escrow opgenomen als maatregel. Escrow is al lange tijd een veelgebruikt instrument. De GIBIT 2025 spreekt in artikel 39 ook over aanvullende mogelijkheden voor een data-escrow. In aanbestedingen komen verschillende typen escrow-vragen voorbij. Wij adviseren om de benodigde escrow-maatregelen verder uit te werken, omdat aan escrow-regelingen hoge kosten verbonden zijn. Door dit uit te werken is het makkelijker voor gemeenten om de juiste escrow-regeling voor de juiste dienst te kiezen.

Wij tekenen daarbij aan dat de klassieke broncode-escrow bij SaaS niet volstaat. Waar wij in deze reactie escrow noemen als beheersing bij SaaS, bedoelen wij een SaaS-passende variant. Zie voor de uitwerking S10 - Continuïteit bij faillissement.

R2 - Technologische lock-in en beperkte verplaatsbaarheid

Het scheiden van data en oplossing en de mogelijkheid om data te hergebruiken is vanzelfsprekend. Door het toepassen van open standaarden, zoals het Gemeentelijk Gegevensmodel, kan data opnieuw worden toegepast in andere gebieden.

Dit risico is inmiddels ook wettelijk geadresseerd. Hoofdstuk VI van de Data Act is sinds 12 september 2025 van toepassing op IaaS, PaaS en SaaS en verplicht aanbieders om contractuele, technische en organisatorische drempels voor een overstap weg te nemen, om functionele gelijkwaardigheid te bieden en om ten minste dertig dagen migratieondersteuning te verlenen. Per 12 januari 2027 vervallen overstapkosten volledig. Wij bevelen aan om R2 en de bijbehorende maatregelen expliciet te koppelen aan dit kader, zodat gemeenten en leveranciers één norm hanteren en niet twee.

Wij vragen daarnaast om de impactbeschrijving te nuanceren. Bij de impact staat dat lock-in leidt tot hoge migratiekosten, beperkte flexibiliteit, afhankelijkheid van de roadmap van de leverancier en belemmering van innovatie. Dat is niet per definitie het geval. Of die gevolgen optreden hangt af van concrete factoren: zijn data en datamodel gedocumenteerd en exporteerbaar, zijn koppelingen gebaseerd op open standaarden, is er een actueel exit-plan, en heeft de gemeente invloed op de roadmap via productmanagement en gebruikersoverleg. Bij een dienst die daaraan voldoet is de feitelijke afhankelijkheid beperkt, ook wanneer er één leverancier is.

Door de impact voorwaardelijk te formuleren wordt het risico beter toetsbaar, en kan een gemeente in een aanbesteding ook belonen dat een inschrijver die voorwaarden invult. Zoals de impact nu is beschreven, is zij een eigenschap van het leveringsmodel in plaats van van de dienst. Datzelfde effect zien we terug in de EMVI-scoring; zie 11 Bijlage EMVI Gemeentelijke Cloud.

Daarnaast stelt de eis ook:

toegang tot alle relevante technische artefacten en configuraties

In het kader van een SaaS-dienst is dit een onduidelijke en brede bewoording. Zeker bij een SaaS-dienst die aan een gemeente wordt geleverd, is onduidelijk wat relevante technische artefacten en configuraties zijn. Het opnemen van deze oplossingsrichting zal leiden tot onduidelijkheid en discussie. We pleiten ervoor om dit te specificeren of met voorbeelden te duiden, zodat bij aanbestedingen geen uitgebreide vragenrondes nodig zijn om deze eis te verduidelijken. Zie voor ons tekstvoorstel G08 - Toegang tot data en technische artefacten.

R3 - Afhankelijkheid van niet-Europese jurisdicties en digitale infrastructuren

Bij de impact van dit risico staat onder meer "verlies van controle over data". Dat is te beperkt geformuleerd. Wanneer een aanbieder onder het recht van een derde land valt, kan niet alleen de toegang tot data worden geraakt, maar ook de continuïteit van de dienstverlening zelf. Denk aan het intrekken of opschorten van licenties, het stoppen van updates en support, het blokkeren van beheertoegang of het beëindigen van de dienst. In die gevallen verliest een gemeente de controle over haar operationele bedrijfsvoering, ook wanneer de gegevens zelf onaangetast binnen de EU staan.

Dit patroon komt op meer plaatsen in de handreiking terug: de formulering zoomt steeds in op data, terwijl de operationele controle even hard wordt geraakt. Wij bevelen aan om bij R3 en bij de bijbehorende maatregelen expliciet twee soorten impact te onderscheiden: verlies van controle over gegevens en verlies van controle over de dienstverlening. Dat maakt ook duidelijker waarom G25 (scheiding control-plane en uitvoering) en P04 (control-plane binnen EU) in dit cluster thuishoren. Die maatregelen adresseren juist de tweede categorie.

Ter voorkoming van misverstand: bij R7 pleiten wij ervoor om de maatregelen wél op datatoegang te richten. Dat is geen tegenstelling. Bij R7 gaat het om herstel na een incident, en dan is data het object. Bij R3 gaat het om zeggenschap, en dan is ook de dienst zelf het object.

R5 - Onvoldoende functiescheiding en afhankelijkheid in governance

Voor betere beheersing op een leverancier staan nu audit- en toezichtrecht en volledige transparantie in logging en operationele processen opgenomen. Wanneer organisaties zich willen verzekeren van de juiste uitvoering van processen, zijn certificeringen en assurance-verklaringen algemeen geaccepteerd. Ook het EU Cloud Sovereignty Framework (PDF) erkent ISO-certificeringen binnen het thema SOV-7 Security & Compliance Sovereignty, net als de bijbehorende sovereignty assessment calculator binnen het thema SOV-6 Technology Sovereignty. Voor verschillende processen zijn ook nu al jaarlijkse audits verplicht, zoals een ISAE 3000 voor diensten die gebruikmaken van DigiD.

In de aanbestedingspraktijk zien we een uiteenlopende lijst van gevraagde certificeringen, zoals ISO 27001, ISO 27017, ISAE 3000 en ISAE 3402 type II. Auditrecht is al geborgd in artikel 28 van de GIBIT 2025 en leveranciers hebben al een zorgplicht voor cyberbeveiliging, mede onder de Cyberbeveiligingswet. Logging is onderdeel van verschillende maatregelen in de BIO 2.

De GIBIT stelt daarbij een complete reeks voorwaarden aan de controle, die in deze maatregelen niet terugkomt:

- artikel 28.1: de controle wordt uitgevoerd door een onafhankelijke, ter zake deskundige en aan geheimhouding gebonden derde, en niet door een directe concurrent;
- artikel 28.2: de gemeente maakt eerst de aanleiding kenbaar en vraagt bij generieke Dienstverlening op Afstand eerst de derdenverklaring van artikel 38 op;
- artikel 28.3: de controle vindt alleen plaats bij gerede twijfel of een ander gerechtvaardigd belang;
- artikel 28.6: de kosten komen in beginsel voor rekening van de gemeente;
- artikel 38: de leverancier beschikt bij generieke Dienstverlening op Afstand over een jaarlijks hernieuwde derdenverklaring of geldige certificering, op eigen kosten, met een verbeterplanplicht bij kritische bevindingen.

Artikel 38 is daarmee precies het instrument dat de handreiking zoekt. Breng de bewoordingen en verdere maatregelen bij G22 - Onafhankelijk audit- en toezichtrecht, G23 - Transparantie in logging en processen en G24 - Geen beperkingen op toezicht in lijn met de artikelen 28 en 38 van de GIBIT.

Om leveranciers en gemeenten te helpen de juiste inschatting te maken over de betrouwbaarheid van dienstverleners pleiten we ervoor om per type dienst op te nemen welke certificeringen vereist zijn. Hiermee is de zekerheid voor gemeenten direct geborgd en zijn specifieke audits per gemeente zo min mogelijk nodig.

R7 - Onvoldoende borging van databeschikbaarheid en herstel

De borging van dataherstel is ambigu. Bij R2, R4 en R6 zijn al regels opgenomen rondom de toegang tot data, open standaarden, eigenaarschap en spreiding. Bij dataherstel van een SaaS-dienst is de data deels verworven met het gebruikte systeem. Back-up en herstel van data binnen de dienst zijn dan ook de verantwoordelijkheid van de leverancier.

Het eisen van *data shattering* en herstel buiten de leverancieromgeving is logisch wanneer het gaat over algemene informatie zoals documenten en bestanden van netwerkschijven. Voor SaaS-diensten gaat het voorbij aan de technische en functionele verantwoordelijkheid van de SaaS-leverancier. Het herstel van data buiten de omgeving van een SaaS-dienst is geen herstel maar een migratie van systemen. Focus daarom op de toegang en de beschikbaarheid van data, zoals de escrow-regeling die ook in S10 is opgenomen.

We bevelen aan in R7 te specificeren voor welke typen diensten en data dit geldt, om verwarring in aanbestedingen te voorkomen over wat er van een SaaS-leverancier kan worden verwacht.

Zie ook onze beantwoording bij G33 - Geen afhankelijkheid van één leverancier voor herstel, G36 - Data shattering en G38 - Aantoonbaar herstel buiten leverancier.

6 Bijlage: Beheersingsmaatregelen nader toegelicht

De S- en P-codes in dit hoofdstuk verschillen van die in bijlage 10. Wij hanteren de nummering van dit hoofdstuk. Zie 3 - Risico's en maatregelen.

Vooraf een algemene opmerking over dit hoofdstuk. De toelichtingen per maatregel bestaan doorgaans uit twee korte alinea's: een omschrijving en een onderbouwing. Voor een deel van de maatregelen is dat voldoende. Voor een ander deel is het te kort om er praktisch invulling aan te kunnen geven. Dat geldt in het bijzonder voor de SaaS-specifieke maatregelen S01 tot en met S10, waar de toelichting vaak uit één regel bestaat die het doel herhaalt zonder te beschrijven wat er van een gemeente of van een leverancier concreet wordt verwacht. S03 ("Data is zelfstandig bruikbaar zonder afhankelijkheid van de oorspronkelijke SaaS-applicatie") en S05 ("Toegang van leveranciers tot data wordt beperkt en gecontroleerd") zijn daarvan voorbeelden.

Wil de handreiking dienen als handvat voor gemeenten en als basis voor eisen in aanbestedingen, dan is per maatregel meer nodig: wat is de norm, hoe wordt daaraan invulling gegeven, welk bewijsmiddel geldt als voldoende, en wie is waarvoor verantwoordelijk. Wij vragen VNG om de maatregelen langs die vier punten uit te werken. Zonder die uitwerking ontstaat per aanbesteding een eigen interpretatie, en dat is precies wat een gezamenlijk kader moet voorkomen. Onze opmerkingen per maatregel hieronder zijn op verschillende plaatsen een concreet voorstel voor die uitwerking.

6.1 - Cluster 1 - Afhankelijkheid en marktstructuur

G02 - Multi-provider inzet

De maatregel noemt spreiding over meerdere technologiestacks, met CPU-architectuur en Kubernetes-distributie als voorbeeld. Het inzetten van Kubernetes binnen IaaS en PaaS is inderdaad een belangrijke manier om oplossingen agnostisch op een onderlaag te draaien. Het gelijktijdig inzetten van meerdere cloudproviders is echter complex vanwege netwerken, synchronisatie van data, load balancing en andere technische factoren. Wie Kubernetes goed beheerst, hoeft bijna nooit active-active te draaien, omdat een nieuwe omgeving snel kan worden gerealiseerd. Om complexiteit en kosten te besparen raden wij aan om dit bij BBN2 niet verplicht te stellen en bij BBN3 alleen verplicht te stellen voor die kritieke workloads die geen enkele vorm van downtime kunnen verdragen. Leg tegelijkertijd de relatie met de GIBIT eisen aan beschikbaarheid.

In 3.1 is deze maatregel opgenomen als algemene maatregel. Bij een traditionele SaaS-dienst is de leverancier verantwoordelijk voor de totale dienst. De vertaling van deze maatregel is dan onduidelijk. Zoals de maatregel nu is opgenomen, betekent het dat elke gemeente vrijwel alle SaaS-diensten die zij nodig heeft voor haar uitvoering tweemaal moet verwerven. Een voorbeeld maakt dat concreet. Het sociaal domein valt in het huidige model onder S2 (zie 4.4 - Stap 4: Bepaal het Soevereiniteitsniveau) met waarschijnlijk BBN2. Dat betekent dat elke gemeente twee oplossingen voor het sociaal domein moet afnemen. Verduidelijk deze maatregel en pas de scope aan naar die diensten die zich lenen voor het verplaatsen over meerdere providers, zoals bij diensten waarvoor een gemeente IaaS of PaaS afneemt. Zie ook Toepassingsgebied per cloudmodel.

G03 - Inzicht in ketenafhankelijkheden

De GIBIT 2025 stelt in artikel 25 eisen aan de Software Bill of Materials, die grotendeels invulling geeft aan het inzicht in ketenafhankelijkheden. Artikel 25.1 vraagt daarbij expliciet om inzicht in de toeleveringsketen, de ontvangers van data en de fysieke locaties van dataverwerking. Laat de maatregel verwijzen naar de GIBIT, zodat de samenhang duidelijk is.

G04 - Spreiding van kritieke workloads

Deze beheersingsmaatregel lijkt sterk op G02 - Multi-provider inzet. Het advies is om deze samen te voegen tot één beheersmaatregel, met inachtneming van ons advies bij G02.

G05 - Verkaveling van systemen en leveranciers

Deze beheersingsmaatregel lijkt sterk op G02 - Multi-provider inzet en G04 - Spreiding van kritieke workloads. Het advies is om deze samen te voegen tot één beheersmaatregel, met inachtneming van ons advies bij G02.

Cluster 2 - Portabiliteit en lock-in

G06 - Gebruik van open standaarden

De GIBIT 2025 stelt in artikel 8 al eisen aan interoperabiliteit, normen en standaarden. Laat de maatregel verwijzen naar de GIBIT, zodat de samenhang duidelijk is.

G07 - Volledige data-export inclusief metadata

De GIBIT 2025 stelt in artikel 22 al eisen aan de toegang tot data. Artikel 22.3 schrijft daarbij een algemeen leesbaar elektronisch bestandsformaat voor, met documentatie van de onderliggende datamodellen. Hoofdstuk VI van de Data Act (EUR-Lex) stelt dezelfde norm wettelijk verplicht. Laat de maatregel naar beide verwijzen, zodat de samenhang duidelijk is.

Artikel 22.4 van de GIBIT biedt daarnaast bescherming voor het datamodel als bedrijfsgeheim, door een geheimhoudingsovereenkomst mogelijk te maken voor iedereen die inzage krijgt. Die bescherming ontbreekt in deze maatregel. Maak expliciet dat informatie vertrouwelijk kan zijn, zoals ook in de GIBIT is opgenomen.

G08 - Toegang tot data en technische artefacten

Deze maatregel staat in 3.1 gekoppeld als 'Algemeen' in plaats van bij PaaS en IaaS. Bij een SaaS-dienst bestaan technische artefacten niet als afzonderlijk leverbaar object voor de afnemer. Zij zijn de bouwstenen van de dienst zelf, en de continuïteit daarvan wordt geborgd via databeschikbaarheid en escrow. Verplaats deze technische maatregel naar de plek waar zij thuishoort, namelijk bij PaaS en IaaS. P02 kan daarin worden opgenomen. Deze maatregel is het duidelijkste voorbeeld van het scopevraagstuk dat wij bij Toepassingsgebied per cloudmodel beschrijven.

Ons tekstvoorstel:

G08 (PaaS/IaaS) Opdrachtgever behoudt gedurende de looptijd van de overeenkomst toegang tot de technische artefacten van de door haar afgenomen platform- en infrastructuurdiensten, waaronder

Infrastructure as Code, CI/CD-configuraties, scripts, container images en de bijbehorende documentatie, alsmede tot de volledige configuratie daarvan. Deze artefacten worden aangemerkt als vertrouwelijke informatie in de zin van artikel 19 GIBIT 2025 en worden verstrekt onder een gebruiksrecht voor de eigen omgeving van Opdrachtgever.

Voor SaaS-diensten geldt in plaats hiervan dat de leverancier toegang geeft tot de data, de bijbehorende datamodeldocumentatie en de koppeldocumentatie, conform artikel 22 GIBIT 2025.

G09 - Contractueel vastgelegde exit- en migratievoorwaarden

De GIBIT 2025 stelt in artikel 29 al eisen aan een exit en overstap, inclusief het exit-plan, de jaarlijkse actualisatie daarvan en de mogelijkheid tot beperkte voortzetting en verlengd gebruik. De artikelen 23 tot en met 25 van de Data Act (EUR-Lex) verplichten daarnaast tot het wegnemen van contractuele drempels voor een overstap. Laat de maatregel naar beide verwijzen, zodat de samenhang duidelijk is.

G10 - Vendor-agnostische architectuur

Deze maatregel staat in 3.1 gekoppeld als 'Algemeen' in plaats van bij PaaS en IaaS. De technische architectuur van een SaaS-dienst is de verantwoordelijkheid van de SaaS-leverancier. Een eis dat die architectuur geen leveranciersspecifieke componenten mag bevatten, is bij SaaS niet uitvoerbaar en ook niet nodig: wat de gemeente nodig heeft is verplaatsbaarheid van data en werkende koppelingen, niet inzage in en zeggenschap over de bouw van het product.

Ons tekstvoorstel:

G10 (PaaS/IaaS) De door Opdrachtgever op het platform geplaatste workloads en configuraties worden zodanig ontworpen dat zij zonder significante herontwikkeling op een ander platform kunnen worden gehervestigd.

Voor SaaS-diensten geldt dat de dienst voldoet aan de overeengekomen open standaarden en interoperabiliteitseisen als bedoeld in artikel 8 GIBIT 2025, en dat data en metadata volledig exporteerbaar zijn conform G07. Er worden geen eisen gesteld aan de interne architectuur van de leverancier.

Cluster 3 - Juridische soevereiniteit

G11 - EU/EER-jurisdictie of gelijkwaardig beschermingsniveau

Deze maatregel is de kern van het hele R3-cluster. De formulering bevat echter een uitweg die de norm ondermijnt. "Een gelijkwaardig beschermingsniveau" is niet gedefinieerd, niet toetsbaar en niet weerlegbaar. Wie bepaalt of het beschermingsniveau gelijkwaardig is, en waaraan wordt dat gemeten? Zolang die vraag open staat, kan iedere inschrijver zich erop beroepen en kan geen enkele gemeente het beoordelen. Bij aanbestedingen leidt dat tot lange vragenrondes en tot beslissingen die achteraf moeilijk te verdedigen zijn.

Ons tekstvoorstel:

G11 Alle data, dienstverlening, beheeractiviteiten en control-plane componenten vallen onder het recht van een lidstaat van de Europese Unie of de Europese Economische Ruimte.

Een beroep op een gelijkwaardig beschermingsniveau is uitsluitend mogelijk indien dit wordt aangetoond aan de hand van een adequaatheidsbesluit van de Europese Commissie of van een door de Europese Commissie erkend certificeringsschema, en indien Opdrachtgever dit beroep schriftelijk aanvaardt.

P04 kan hierin worden opgenomen. Zolang het EUCS-schema niet is vastgesteld, is dit ook de meest toekomstvaste formulering: zij groeit mee zonder dat de handreiking hoeft te worden herzien.

Zie voor de vraag of "EU/EER" als één ongedeelde categorie moet worden behandeld ook Differentiatie binnen de Europese Unie.

G12 - Transparantie eigendomsstructuur en zeggenschap

Wij onderschrijven het doel van deze maatregel. De maatregel vraagt om "volledig inzicht" in eigendomsstructuren, zonder te bepalen wat dat omvat en hoe diep dat in de keten reikt. Daarmee ontstaat onduidelijkheid, of erger: een eigen administratieve last rond iets dat al geregistreerd ligt. Wij bevelen aan om aan te sluiten bij de bestaande registraties bij de KVK. Het UBO-register geeft invulling aan deze transparantie-eis en Nederlandse ondernemingen zijn verplicht die registratie bij te houden. Omdat het UBO-register niet publiek toegankelijk is, kan een gemeente die bron niet zelf raadplegen; zij kan wel vragen om de stukken die de onderneming daar zelf kan opvragen.

Ons voorstel sluit aan bij de staande praktijk in aanbestedingen: een uittreksel uit het handelsregister, aangevuld met een verklaring over de groepsstructuur en de zeggenschapsverhoudingen. Voor specifieke diensten kan aanvullend een door de onderneming zelf opgevraagd uittreksel uit het UBO-register worden gevraagd. Leg vast op welk moment die stukken worden overlegd: bij inschrijving en opnieuw bij een wijziging in de zeggenschapsverhoudingen, zonder periodieke herlevering.

G13 - Data-eigendom bij gemeente

In maatregel G13 wordt opgenomen dat het eigenaarschap van data contractueel bij de gemeente komt te liggen. In het Nederlandse recht bestaat eigendom op data echter niet als juridisch concept. Eigendom in de zin van artikel 5:1 van het Burgerlijk Wetboek heeft betrekking op zaken, en artikel 3:2 BW definieert een zaak als een voor menselijke beheersing vatbaar stoffelijk object. Dat is bevestigd in de uitspraak van de rechtbank Amsterdam van 21 april 2023, ECLI:NL:RBAMS:2023:2540, waarin de eiser wel eigenaar was van de fysieke documenten maar niet van de digitale gegevens. Het hof heeft dit vonnis in juni 2025 vernietigd, maar op een ander punt, namelijk de uitleg van de overeenkomst. De eigendomsvraag heeft het hof uitdrukkelijk onbeslist gelaten. De redenering dat op data geen eigendom kan rusten staat daarmee onaangetast. Op Europees niveau komt de EC-rapport eigenaarschap van data (PDF) tot dezelfde conclusie.

Een contractuele bepaling die eigendom vestigt op iets waarop geen eigendom kan rusten, geeft schijnzekerheid. Wat de gemeente nodig heeft is niet eigendom maar zeggenschap, en dat is wel goed te regelen. De GIBIT doet dat ook al.

Ons tekstvoorstel:

G13 In de overeenkomst wordt vastgelegd dat alle rechten op de data die van Opdrachtgever afkomstig zijn, ten behoeve van Opdrachtgever zijn verzameld of door Leverancier worden verzameld bij het gebruik van de ICT Prestatie, bij Opdrachtgever (blijven) rusten, ongeacht waar deze data zijn opgeslagen en ongeacht of de data na initiële ontvangst zijn bewerkt, conform artikel 21.2 GIBIT 2025.

Daarbij wordt vastgelegd dat Leverancier deze data uitsluitend gebruikt voor de uitvoering van de overeenkomst en de nakoming van op hem rustende wettelijke verplichtingen (artikel 22.8 sub i), Opdrachtgever kosteloos in staat stelt de data in te zien en op te slaan en op eerste verzoek een kopie verstrekt (artikel 22.2), de data verstrekt in een algemeen leesbaar elektronisch bestandsformaat met documentatie van de onderliggende datamodellen (artikel 22.3), en de data op eerste verzoek vernietigt onder afgifte van een verklaring van vernietiging (artikel 22.8 sub ii GIBIT 2025).

G14 - Verplichting tot juridisch betwisten van datavorderingen

Wij onderschrijven de gedachte achter deze maatregel. Zij is echter al wettelijk geregeld. Artikel 32 van de Data Act verplicht aanbieders van dataverwerkingsdiensten tot technische, organisatorische en juridische maatregelen om overheidstoegang en internationale doorgifte tegen te gaan die in strijd zijn met het recht van de Unie of van een lidstaat. Een eigen formulering naast die verplichting levert twee normen op waar één norm volstaat.

Twee punten vragen daarnaast om begrenzing. Ten eerste de kosten: een verplichting tot procederen zonder plafond is voor geen enkele leverancier te calculeren, en dus ook niet te beprijzen. Ten tweede de verhouding tot de geheimhoudingsplicht: artikel 19.1 sub i en ii van de GIBIT verplicht juist tot bekendmaking wanneer een wettelijk voorschrift of een bevoegde toezichthouder daartoe verplicht. De maatregel moet duidelijk maken dat het uitsluitend gaat om vorderingen die geen grondslag hebben in het recht van de Unie of van een lidstaat.

De begrenzing moet ook het meest concrete scenario afdekken. Een vordering van de Officier van Justitie in een Nederlandse strafzaak, inclusief een sommatie tot overlegging, heeft een grondslag in het recht van een lidstaat. Zo'n vordering hoeft niet te worden betwist en mag ook niet worden geblokkeerd. De betwistingsplicht geldt uitsluitend voor vorderingen zonder grondslag in het recht van de Unie of van een lidstaat, zoals vorderingen op grond van extraterritoriale wetgeving van derde landen.

Daarnaast vragen wij om de kosten te regelen en niet alleen te begrenzen. Wanneer een leverancier op verzoek juridische stappen onderneemt tegen een vordering zonder geldige rechtsgrondslag, handelt hij in het belang van de gemeente en van de gemeenten die dezelfde dienst afnemen. Het is redelijk dat de kosten daarvan, binnen het overeengekomen maximum, voor rekening van de gemeente komen, vergelijkbaar met de kostenverdeling van artikel 28.6 GIBIT bij controles.

Wij vragen om G14 te herformuleren als een verwijzing naar artikel 32 van de Data Act, aangevuld met een informatieplicht richting de gemeente en met een redelijke begrenzing van de te maken kosten.

Ons tekstvoorstel:

G14 Leverancier neemt conform artikel 32 van Verordening (EU) 2023/2854 alle redelijke technische, organisatorische en juridische maatregelen om toegang tot data door overheden van derde landen tegen te gaan, voor zover die toegang geen grondslag heeft in het recht van de Unie of van een lidstaat.

Vorderingen en bevelen met een geldige rechtsgrondslag in het recht van de Unie of van een lidstaat, waaronder vorderingen van het Openbaar Ministerie en bevoegde toezichthouders, worden nageleefd. Leverancier stelt Opdrachtgever van elke vordering onverwijld in kennis, voor zover de vordering of de wet dat toelaat.

Juridische maatregelen tegen een vordering zonder geldige rechtsgrondslag worden genomen na overleg met Opdrachtgever, binnen een bij overeenkomst vastgesteld maximum. De redelijke kosten daarvan komen binnen dat maximum voor rekening van Opdrachtgever.

G15 - EU-by-design als uitgangspunt en G16 - Beperking inzet niet-EU leveranciers

Wat beide maatregelen missen, is een definitie van "Europees". Zonder die definitie kan geen enkele leverancier vooraf weten of hij aan de eis voldoet, en kan geen enkele gemeente controleren of dat zo is. Een definitie via eigendom lost dat niet op. Is een leverancier Europees bij een meerderheidsbelang van Europese aandeelhouders? Bij vijftig procent? Bij een Europees hoofdkantoor met een Amerikaans minderheidsbelang en vetorechten? Elk afkappunt is te verdedigen en daarmee willekeurig.

Wij stellen daarom voor om "Europees" niet zelf te definiëren, maar af te leiden uit een minimumniveau in het EU Cloud Sovereignty Framework, conform ons hoofdpleidooi in deze reactie. Dat framework beoordeelt een dienst op acht thema's, met per thema een niveau van SEAL-0 tot en met SEAL-4. Het framework is ontworpen voor inkoop: de aanbestedende dienst stelt het minimaal vereiste SEAL-niveau vast en vergelijkt de inschrijvingen die dat niveau halen vervolgens op de sovereignty score. De Europese Commissie hanteerde in de eerste aanbesteding waarin zij het framework toepaste SEAL-2 als minimum. Dat was in april 2026, bij de gunning van een soevereine-cloudaanbesteding van maximaal 180 miljoen euro over zes jaar aan vier aanbieders. Het framework is daarmee geen theoretisch model maar een bewezen inkoopinstrument.

SEAL-2 is ook het logische minimum voor de definitie van "Europees". Op dat niveau is het recht van de Unie van toepassing en afdwingbaar, met zichtbare en beheerste afhankelijkheden. Een niveau lager, bij SEAL-1, geldt EU-recht slechts formeel en zonder praktische afdwingbaarheid. Een dienst die aan SEAL-2 voldoet, is dus een Europese dienst in juridisch relevante zin. Daarboven is ruimte voor ambitie: SEAL-3 voor de hogere soevereiniteitsniveaus, SEAL-4 zodra de markt daar realistisch aan kan voldoen. De Commissie concludeert in de evaluatie van die eerste aanbesteding overigens zelf dat SEAL-4, gelet op afhankelijkheden in chips en hardware, op dit moment niet haalbaar is. Dat ondersteunt ons voorstel bij S1 - Hoog geclassificeerd om met een groeipad te werken.

Deze definitie lost de vraag uit de consultatie op zonder afkappunten. Het overall niveau is het laagst scorende van de acht thema's, dus een dienst kan zich niet presenteren als Europese dienst door sterke thema's te tonen en zwakke te verzwijgen. Een leverancier met voor de helft Europese en voor de helft Amerikaanse aandeelhouders valt niet buiten de definitie via een percentage, maar scoort per thema. Zeggenschapsverhoudingen zijn daarbij invoer voor de beoordeling, niet de beoordeling zelf. De gemeente ziet de score en kan die per aanbesteding meewegen, in samenhang met de openlegging van de eigendomsstructuur bij G12 - Transparantie eigendomsstructuur en zeggenschap.

Voor de uitvoering hoeft VNG het wiel niet uit te vinden. Het IMG CIO-beraad heeft in mei 2026 een uitvraag gedaan die het framework voor de Nederlandse praktijk implementeert, ook voor SaaS. Wij hebben die uitvraag voor ons volledige portfolio aan SaaS-diensten voor de decentrale overheid beantwoord en de uitkomst met het CIO-beraad gedeeld. Onze ervaring is dat de methode ook voor specialistische SaaS-diensten een betrouwbaar beeld geeft, mits per thema één beargumenteerd niveau wordt vastgesteld in plaats van losse deelvragen afzonderlijk te scoren. Wij vragen VNG om bij deze uitvraag aan te sluiten, conform ons voorstel in de inleiding, en om de uitkomsten samen te brengen met deze handreiking.

Met deze koppeling wordt het instrumentarium ook eenvoudiger, aansluitend bij ons pleidooi bij 8 Bijlage - Soevereiniteitsniveau's GEMMA. De eigen soevereiniteitsniveaus hoeven geen eigen definities meer te bevatten, maar stellen alleen in welk minimum SEAL-niveau per niveau of domein geldt. Eén meetlat voor gemeenten en leveranciers, gelijk aan de instrumenten die het IMG CIO-beraad en DICTU al hanteren.

Als uitgangspunt onderschrijven wij G15. De uitwerking roept wel vragen op over de reikwijdte in de keten. Ook een volledig Nederlandse SaaS-leverancier gebruikt onderdelen die niet uit de EU komen: opensourcebibliotheken, hardware, firmware en microcode. Zoals wij bij S1 - Hoog geclassificeerd toelichten, is volledige onafhankelijkheid op dit moment niet haalbaar. Wij vragen daarom om expliciet te maken tot welke laag in de keten G15 reikt, en om aan te sluiten bij de systematiek van SOV-5 Supply Chain Sovereignty uit het Europese framework.

Bij G16 gaat het om de toets zelf. "Uitsluitend indien geen volwaardig Europees alternatief beschikbaar is" vraagt van een gemeente een marktoordeel dat zij niet objectief kan onderbouwen en dat een afgewezen inschrijver eenvoudig kan aanvechten. Wie stelt vast dat een alternatief volwaardig is, en op welk moment? Wij vragen om een objectiveerbaar criterium, bijvoorbeeld een gedocumenteerd marktonderzoek of een score op het Europese framework, en om de maatregel te laten toetsen aan het gelijkheidsbeginsel van artikel 1.8 van de Aanbestedingswet 2012 en aan de internationale verplichtingen die op aanbestedende

diensten rusten. Dat is geen bezwaar tegen het doel van de maatregel. Het is een voorwaarde om haar in een bestek te kunnen gebruiken zonder juridisch risico voor de gemeente.

Aanvullend vragen wij om deze toets niet bij iedere gemeente afzonderlijk te leggen. Achter de eenvoudige formulering zit een omvangrijke afweging. Of een Europees alternatief "volwaardig" is, is in de praktijk vrijwel altijd discutabel, en dat geldt in het bijzonder voor breed gebruikte kantoor-, samenwerkings- en analyseplatformen. Wanneer 342 gemeenten daar ieder afzonderlijk een oordeel over vormen, ontstaan verschillende uitkomsten voor hetzelfde product, met verschillende motiveringen en dus verschillende juridische risico's.

Wij bevelen daarom aan dat VNG hiervoor een centrale, periodiek geactualiseerde inventarisatie opstelt: per toepassingsgebied of productcategorie een overzicht van beschikbare Europese alternatieven, met een beoordeling op functionaliteit, schaal en volwassenheid, en met de peildatum erbij. Gemeenten kunnen die inventarisatie dan als leidraad gebruiken en er in hun motivering naar verwijzen. Dat verlaagt de uitvoeringslast, maakt de uitkomsten uniform en geeft leveranciers zicht op de norm waaraan zij worden gemeten. Het geeft VNG bovendien een instrument om de ontwikkeling van het Europese aanbod over de jaren te volgen. De Europese Commissie signaleert in de evaluatie van de eerste aanbesteding onder het framework bovendien dat het beoordelen van de zelfdeclaraties van inschrijvers veel werk is voor aanbestedende diensten, en pleit voor standaardisering van vragen en bewijsstukken. Dat is een extra argument om deze beoordeling, net als de inventarisatie, centraal bij VNG te beleggen.

Ons tekstvoorstel:

Definitie van Europees Een dienst geldt als Europees in de zin van deze handreiking wanneer de dienst, beoordeeld conform het EU Cloud Sovereignty Framework, het niveau SEAL-2 behaalt. Het overall niveau is daarbij het laagst scorende van de acht thema's. Voor de hogere soevereiniteitsniveaus geldt ten minste SEAL-3. Diensten die aan deze definitie voldoen, gelden als Europees alternatief in de zin van G16; de toets of dat alternatief volwaardig is, wordt gemaakt op functionaliteit, schaal en volwassenheid.

G17 - Geen contractuele blokkades voor migratie

De GIBIT 2025 stelt in artikel 27 al voorwaarden aan de beëindiging van overeenkomsten. Laat de maatregel verwijzen naar de GIBIT, zodat de samenhang duidelijk is. Daarnaast is er overlap met G09 - Contractueel vastgelegde exit- en migratievoorwaarden. Wij pleiten ervoor deze maatregelen samen te voegen.

G18 - Recht op periodieke heroverweging

De betekenis en reikwijdte van deze maatregel zijn onduidelijk. Het is al mogelijk om contracten af te sluiten met een vaste einddatum en met eenzijdige verlenging. Ook is het mogelijk om specifieke opzeggingsgronden in een overeenkomst vast te leggen. Omdat de bedoeling en de scope onduidelijk zijn, pleiten we ervoor deze maatregel te laten vervallen.

G19 - Ondersteuning bij toetsing alternatieven

Het is vanzelfsprekend dat organisaties de mogelijkheid hebben alternatieven te onderzoeken voor bestaande diensten. Het is echter onduidelijk wat wordt bedoeld met "Leveranciers ondersteunen gemeenten bij het evalueren en testen van alternatieve oplossingen". Wat er van een leverancier kan worden verwacht is niet bepaald, en de verplichting ligt volledig aan één kant. Daarnaast hebben organisaties voldoende instrumenten, zoals marktconsultaties en aanbestedingen, om een afgewogen vergelijking te maken. Wij pleiten ervoor deze maatregel te laten vervallen.

Cluster 5 - Governance en functiescheiding

G22 - Onafhankelijk audit- en toezichtrecht

Zie ook onze opmerking bij R5 - Onvoldoende functiescheiding en afhankelijkheid in governance. Dit is al geborgd in de GIBIT 2025 in artikel 28 en is beter op te lossen door duidelijke eisen rondom certificeringen en derdenverklaringen, zoals de GIBIT die in artikel 38 al voorschrijft. Audits in een operationele omgeving zijn verstorend en brengen kosten met zich mee, voor de leverancier én voor de gemeente. Zonder voorwaarden wordt het auditrecht een open eind. Wij vragen om de maatregel te laten verwijzen naar de artikelen 28 en 38 GIBIT, met inbegrip van de voorwaarden die de GIBIT aan de controle stelt, en om die aan te vullen met de voorwaarden die de praktijk vraagt.

Ons tekstvoorstel:

G22 Opdrachtgever kan de naleving van de overeengekomen verplichtingen laten controleren, conform artikel 28 GIBIT 2025, onder de volgende voorwaarden:

> de controle wordt aangekondigd met een redelijke termijn, tenzij de aanleiding zodanig is dat aankondiging het doel doorkruist;
> de controle wordt uitgevoerd door een onafhankelijke, ter zake deskundige derde die geen directe concurrent is, gebonden aan geheimhouding conform artikel 19 GIBIT, vastgelegd in een door Leverancier opgestelde geheimhoudingsovereenkomst;
> de kosten van de controle, inclusief die van een door Opdrachtgever ingeschakelde externe auditor, komen voor rekening van Opdrachtgever;
> de uitkomsten zijn vertrouwelijk en worden niet gedeeld buiten de organisatie van Opdrachtgever, behoudens verstrekking aan het CSIRT of aan een bevoegde toezichthouder;
> de controle vindt alleen plaats bij gerede twijfel of een ander gerechtvaardigd belang, conform artikel 28.3 GIBIT.

Artikel 38 GIBIT blijft daarbij het uitgangspunt: de jaarlijks vernieuwde derdenverklaring of geldige certificering, op kosten van Leverancier, maakt individuele audits per gemeente zo veel mogelijk overbodig.

G23 - Transparantie in logging en processen

Volledige inzage in logging, prestaties en operationele processen is voor toezicht en incidentanalyse begrijpelijk. Er zit echter een grens aan die de maatregel nu niet trekt. Logging en operationele processen bevatten informatie over de getroffen beveiligingsmaatregelen, en de GIBIT merkt die informatie in artikel 32.8 uitdrukkelijk aan als vertrouwelijk. Hetzelfde geldt voor onderdelen van de SBOM waarvan het prijsgeven reverse engineering mogelijk maakt, zie artikel 25.3 en 25.4.

Wij vragen om in de maatregel op te nemen dat inzage plaatsvindt onder de geheimhoudingsbepaling van artikel 19 GIBIT, en dat onderdelen waarvan verstrekking een aantoonbaar veiligheidsrisico oplevert kunnen worden gedeeld met het CSIRT in plaats van met iedere afzonderlijke gemeente. De GIBIT kent die constructie al voor de SBOM in artikel 25.5. P06 kan in deze maatregel worden opgenomen.

G24 - Geen beperkingen op toezicht

Deze maatregel is zo breed geformuleerd dat onduidelijk is wat een beperking op toezicht of controle inhoudt. Gekoppeld aan een auditrecht, zie G22 - Onafhankelijk audit- en toezichtrecht, is de betekenis niet vast te stellen. Letterlijk gelezen schrapt de maatregel bovendien de waarborgen die de GIBIT juist bewust heeft opgenomen: geen audit door een directe concurrent, een aanleiding vooraf, gerede twijfel als drempel en een kostenverdeling. Breng deze maatregel in lijn met artikel 28 van de GIBIT.

G25 - Scheiding control-plane en uitvoering

Wij onderschrijven het doel van deze maatregel, maar de formulering maakt geen onderscheid tussen functioneel en technisch beheer. Dat onderscheid is bepalend. Functioneel beheer, waaronder het beheer van gebruikers, autorisaties, inrichting en parametrisering, kan een gemeente of een door haar aangewezen derde bij onze diensten zelfstandig uitvoeren. Daar is deze maatregel goed uitvoerbaar.

Technisch beheer en het beheer van de control-plane liggen anders. Bij een multi-tenant SaaS-dienst raakt beheertoegang van een afnemer per definitie ook de omgeving van andere afnemers. Een eis dat een derde die taken moet kunnen uitvoeren, staat daarmee op gespannen voet met de functiescheiding die ISO 27001 en de BIO2 juist vragen.

Ons tekstvoorstel:

G25 Opdrachtgever kan het functioneel beheer van de ICT Prestatie zelfstandig of door een door haar aangewezen derde laten uitvoeren, waaronder in ieder geval het beheer van gebruikers, autorisaties, inrichting en parametrisering.

Voor het technisch beheer en het beheer van de control-plane geldt deze maatregel uitsluitend bij PaaS- en IaaS-diensten. Bij SaaS blijft het technisch beheer bij de leverancier, waarbij de continuïteit wordt geborgd via de maatregelen voor exit, datatoegang en escrow.

P05 kan hierin worden opgenomen. Deze maatregel is daarnaast een van de weinige die de operationele kant van R3 adresseert; zie R3 - Afhankelijkheid van niet-Europese jurisdicties en digitale infrastructuren.

Cluster 6 - Continuïteit

G26 - Contractuele borging continuïteit en incidentrespons

De GIBIT regelt dit onderwerp al uitgebreid. Artikel 10.10 verplicht tot het sluiten van een SLA met reactietijd en functieherstelttijd als resultaatsverbintenissen, artikel 10.11 geeft de gemeente rechten bij herhaald niet halen van Service Levels, artikel 10.12 maakt een malusregeling mogelijk en artikel 10.13 laat het recht op schadevergoeding onverlet. Laat de maatregel daarnaar verwijzen.

Wat de maatregel wél zou moeten toevoegen, ontbreekt: de vertaling van BBN-niveaus naar concrete serviceniveaus. Zonder die vertaling blijft onduidelijk of de GIBIT-defaults gelden of de architectuurbeelden uit hoofdstuk 7. Zie de tabel bij 4.3 - Stap 2: bepaal de relevante beheersmaatregelen.

G28 - Verplichte informatievoorziening bij verstoringen

Ook dit onderwerp is al geregeld, en straks ook wettelijk. Artikel 32.6 van de GIBIT verplicht tot rapportage over informatiebeveiligingsincidenten en artikel 32.7 schrijft voor dat de leverancier bij een significant incident in de zin van de Cyberbeveiligingswet contact opneemt met het CSIRT, waarna partijen samen verantwoordelijkheden verdelen. De Cbw zelf kent sinds 15 augustus 2026 een meldplicht in drie stappen: een vroegtijdige waarschuwing binnen 24 uur, een uitgebreidere melding binnen 72 uur en een eindrapport binnen een maand.

Wij vragen om G28 te laten aansluiten op die keten en op die termijnen, zodat leveranciers niet per gemeente een afwijkend meldregime krijgen op hetzelfde incident.

G29 - Geo-redundantie

Geo-redundantie is een goede maatregel voor toepassingen waar uitval van een locatie tot onaanvaardbare gevolgen leidt. Zij is echter verplicht gesteld vanaf BBN1. Dat past niet bij het profiel dat hoofdstuk 7 voor BBN1 schetst, waarin een tweede stack niet actief hoeft te draaien en rebuild volstaat. Het past ook niet bij de belofte in 4.1 dat lichte toepassingen niet onnodig zwaar worden ingericht.

Wij vragen om G29 verplicht te stellen vanaf BBN2 en bij BBN1 als wenselijk op te nemen. G30 en P07 kunnen in deze maatregel worden opgenomen.

G30 - Topografische spreiding

De reikwijdte en impact van deze maatregel zijn onduidelijk. Veel leveranciers gebruiken al geografische spreiding over datacenters. Wat "gescheiden regio's binnen de EU" precies behelst is niet bepaald. Maak duidelijk wat geldt als een gescheiden regio, bijvoorbeeld fysiek gescheiden datacenters in Nederland.

Ook is het onderscheid tussen G29 en G30 onduidelijk. Beide maatregelen beogen dat uitval van één locatie niet leidt tot uitval van de dienst. Als G30 daaraan een eigen norm toevoegt, bijvoorbeeld een minimale afstand, een grens tussen lidstaten of gescheiden stroom- en netwerkvoorziening, dan zou die norm expliciet moeten worden gemaakt. Doet G30 dat niet, dan voegt de maatregel geen toetsbaar element toe aan G29 en kan zij daarin opgaan.

G31 - Crisis- en escalatieprocedures

Duidelijke en geteste procedures voor incidentrespons en escalatie zijn vanzelfsprekend. Zij horen echter thuis in de SLA en in de afspraken met het CSIRT op grond van artikel 32.7 GIBIT, niet als afzonderlijk aan te leveren document per aanbesteding. Laat de maatregel daarnaar verwijzen.

Cluster 7 - Dataherstel en databeschikbaarheid

G33 - Geen afhankelijkheid van één leverancier voor herstel

Zie ook onze aanbevelingen bij R7 - Onvoldoende borging van databeschikbaarheid en herstel. Voor reguliere SaaS-diensten die gemeenten gebruiken, is herstel van data onderdeel van de dienst en de verantwoordelijkheid van de SaaS-leverancier. Bij uitval van een leverancier, bijvoorbeeld door faillissement, zijn er escrow-regelingen om data beschikbaar te houden, zie S10 - Continuïteit bij faillissement.

De maatregel wint aan kracht wanneer zij de vraag verlegt. Niet: wie kan de dienst herstellen. Maar: beschikt de gemeente altijd over haar data in een vorm die herstelbaar is. Dat is bij een SaaS-dienst wél afdwingbaar en het levert dezelfde bescherming op. Deze toegang, inclusief inzicht in het datamodel is echter al geregeld in G07 - Volledige data-export inclusief metadata.

Voor IaaS/PaaS-diensten geldt deze afhankelijkheid wel. Ons tekstvoorstel:

G33 De leverancier geeft Opdrachtgever gedurende de looptijd van de overeenkomst continue toegang tot data, zoals geëist in G07 - Volledige data-export inclusief metadata. Het herstel van de dienst zelf blijft bij SaaS de verantwoordelijkheid van de leverancier.

Voor PaaS- en IaaS-diensten geldt aanvullend maatregel P09.

G37 kan hierin worden opgenomen.

G35 - Aantoonbaar geteste herstelprocedures

Deze maatregel is vrijwel identiek aan G27, Periodieke tests van herstel- en uitwijkscenario's. Voeg deze samen tot één coherente maatregel. P08 kan daarin worden opgenomen.

G36 - Data shattering

Deze maatregel vraagt om drie verduidelijkingen.

De eerste is terminologisch. "Data shattering" is geen gangbare term in de markt. De begrippenlijst geeft een definitie, maar in bestekken en offertetrajecten zal de term worden gelezen als sharding of als datasegregatie, en dat zijn verschillende dingen. Wij vragen om aan te sluiten bij terminologie die aanbieders herkennen.

De tweede is technisch. Het logisch of fysiek gescheiden opslaan van datasets over meerdere omgevingen werkt goed voor ongestructureerde data, zoals documentopslag en bestanden. Voor een relationeel SaaS-datamodel ligt dat anders. Het splitsen van samenhangende datasets raakt de referentiële integriteit, de transactionele consistentie en de consistentie van back-ups. De maatregel dient dan de vertrouwelijkheid, maar werkt tegen de integriteit uit dezelfde BIV-classificatie en tegen de eisen die artikel 32 AVG aan integriteit stelt.

De derde is proportionaliteit. G36 is verplicht vanaf BBN1. Voor toepassingen met een laag risico is dat een zware architectuureis met een navenante kostenpost.

Wij bevelen aan om G36 in scope te beperken tot ongestructureerde data en documentopslag, en voor diensten met een relationeel datamodel een gelijkwaardig alternatief toe te staan, bijvoorbeeld een referentieel integere kopie en gesegmenteerde back-ups. Daarnaast vragen we de verhouding tot G34 en G05 te verduidelijken, omdat beide maatregelen deels hetzelfde beogen.

G37 - Onafhankelijke restore mogelijkheid

Deze maatregel is functioneel identiek aan G33 - Geen afhankelijkheid van één leverancier voor herstel. Voeg deze maatregelen samen.

G38 - Aantoonbaar herstel buiten leverancier

Zoals toegelicht bij R7 - Onvoldoende borging van databeschikbaarheid en herstel en G33 - Geen afhankelijkheid van één leverancier voor herstel is herstel bij een SaaS-dienst de verantwoordelijkheid van de leverancier. Herstel buiten de leverancieromgeving is geen herstel maar een migratie. Het is dan ook niet redelijk om van een leverancier te verlangen dat hij het herstel van zijn eigen dienst door derden laat uitvoeren.

Wat wel redelijk en toetsbaar is, is dat de gemeente kan vaststellen dat de data die zij ontvangt buiten de leverancieromgeving bruikbaar is. Dat is namelijk precies het risico dat G38 wil afdekken.

Ons tekstvoorstel:

G38 De leverancier toont periodiek aan dat de op grond van G33 verstrekte dataset buiten zijn eigen omgeving leesbaar en interpreteerbaar is, door middel van een leesbaarheidstest op een door Opdrachtgever aangewezen omgeving.

Een verplichting tot het herstellen van de dienst zelf buiten de omgeving van de leverancier vervalt. Voor PaaS- en IaaS-diensten geldt maatregel P09.

SaaS-specifiek

S01 - Scheiding data en applicatie

De bedoeling en reikwijdte van S01 zijn onduidelijk. De GIBIT 2025 stelt in artikel 22 al eisen aan de toegang tot data en de betekenis van 'zelfstandig beschikbaar' is ambigu. Toegang tot data is al geregeld in G07 - Volledige data-export inclusief metadata. Interoperabiliteit is geborgd in G06 - Gebruik van open standaarden en exit en migratie zijn geborgd in G09 - Contractueel vastgelegde exit- en migratievoorwaarden en artikel 29 van de GIBIT 2025. Wij pleiten ervoor deze maatregel op te nemen in G07.

S02 - Volledige data-export inclusief metadata

Deze maatregel is een kopie van G07 - Volledige data-export inclusief metadata en kan vervallen.

S03 - Datamobiliteit zonder applicatie-afhankelijkheid

De bedoeling en reikwijdte van S03 zijn onduidelijk en de maatregel is functioneel identiek aan S01 - Scheiding data en applicatie. Wij pleiten ervoor deze maatregel op te nemen in G07, zoals we ook voor S01 aanbevelen.

S04 - Transparantie subverwerkers

Transparantie over subverwerkers is al volledig geregeld. Artikel 28 lid 2 en lid 4 AVG stelt de eisen, en de VNG Standaard Verwerkersovereenkomst werkt die uit. Die verwerkersovereenkomst is via artikel 1.49 en 31.1 van de GIBIT 2025 al van toepassing op iedere overeenkomst waarbij persoonsgegevens worden verwerkt. Laat de maatregel daarnaar verwijzen in plaats van een eigen regime te introduceren.

S05 - Toegangsbeperking leverancier

De toegangsbeperking tot data is in de normale operatie al beperkt en geborgd, bijvoorbeeld via de ISO 27001-certificering van de leverancier. Daarnaast stelt de GIBIT 2025 in artikel 22.8 al eisen aan de toegang tot data door de leverancier. Verwijs hierbij naar artikel 22.8 GIBIT om deze maatregel te duiden.

S06 - Meldplicht wijziging subverwerkers

Zie S04 - Transparantie subverwerkers. Ook het vooraf melden van wijzigingen in subverwerkers volgt al uit artikel 28 lid 2 AVG en uit de VNG Standaard Verwerkersovereenkomst. Laat de maatregel daarnaar verwijzen.

S07 - Continuïteit bij beëindiging

Dit onderwerp is uitgewerkt in de GIBIT 2025 en preciezer dan in deze maatregel. Artikel 29.8 en 29.9 regelen de beperkte voortzetting van de dienst na beëindiging, inclusief duur, kosten en voorwaarden. Artikel 29.10 regelt overdracht en artikel 29.11 verlengd gebruik wanneer de exit niet tijdig is afgerond. Laat de maatregel naar deze artikelen verwijzen.

S08 - Toegang tijdens migratie

De toegang tijdens migratie is uitwerkt in artikel 29.11 van de GIBIT 2025 en in artikel 25 van de Data Act (EUR-Lex), dat aanbieders verplicht de functionaliteit gedurende het overstapproces in stand te houden. Laat de maatregel daarnaar verwijzen.

Zie ook onze opmerkingen bij R1 - Concentratie en Leveranciersafhankelijkheid.

S09 - Lifecycle en roadmap transparantie

De GIBIT 2025 stelt in artikel 16 al eisen aan productmanagement, waaronder het periodiek en tijdig informeren over planning en beoogde functionaliteiten. Laat de maatregel verwijzen naar de GIBIT, zodat de samenhang duidelijk is.

S10 - Continuïteit bij faillissement

De GIBIT 2025 biedt in artikel 39 al mogelijkheden voor continuïteit, waaronder data-escrow, hoofdelijke verbondenheid van een derde en een tripartiete overeenkomst. Laat de maatregel daarnaar verwijzen en werk uit welke variant bij welk type dienst passend is. Zie ook onze opmerkingen bij R1 - Concentratie en Leveranciersafhankelijkheid.

PaaS/IaaS-specifiek

P01 - Infrastructure as Code en P03 - Reproduceerbare omgevingen

Wij onderschrijven beide maatregelen. Voor platform- en infrastructuurdiensten is vastlegging in code de meest betrouwbare manier om portabiliteit en herbouwbaarheid te borgen, en de artefacten beschrijven de omgeving van de gemeente zelf.

Er is één punt dat aandacht vraagt, en dat is de vraag die bij deze maatregelen vaak opkomt: gaat het hier nog om bedrijfsgeheim? Voor de configuratie van de omgeving van de gemeente is het antwoord nee. Voor de generieke platformbouwstenen waarmee een leverancier die omgeving opbouwt, ligt het genuanceerder. Die bouwstenen worden hergebruikt over meerdere klanten en zijn onderdeel van het intellectueel eigendom van de leverancier. Wij vragen daarom om in de maatregel op te nemen dat de artefacten worden verstrekt onder een gebruiksrecht voor de eigen omgeving van de gemeente in de zin van artikel 21.3 GIBIT, en dat zij vertrouwelijk zijn in de zin van artikel 19 GIBIT. Daarmee kan de gemeente doen wat zij nodig heeft, namelijk zelfstandig beheren, migreren en herbouwen, zonder dat exploitatierechten overgaan.

Wij geven in overweging om Haven-conformiteit te laten gelden als bewijs voor deze maatregelen. Haven en HavenPlus staan wel in de begrippenlijst, maar worden door geen enkele maatregel aangeroepen. Zie 9 Bijlage: Begrippenlijst.

P02 - Volledige configuratietoegang

Deze maatregel heeft overlap met G08 - Toegang tot data en technische artefacten. Het is logisch om deze eis te behouden en met G08 te consolideren, waarbij G08 wordt verplaatst naar dit hoofdstuk.

P04 - Control-plane binnen EU

Deze maatregel heeft overlap met G11 - EU/EER-jurisdictie of gelijkwaardig beschermingsniveau. Voeg deze maatregel samen met G11.

P05 - Onafhankelijk beheer mogelijk

Deze maatregel overlapt met G25 - Scheiding control-plane en uitvoering. Voeg deze maatregel samen met G25.

P06 - Logging en monitoring

Deze maatregel overlapt met G23 - Transparantie in logging en processen. Voeg deze maatregel samen met G23.

P07 - Geo-redundantie

Deze maatregel overlapt met G29 - Geo-redundantie. Voeg deze maatregel samen met G29.

P08 - Periodieke hersteltests

Deze maatregel overlapt met G27, Periodieke tests van herstel- en uitwijkscenario's. Voeg deze maatregel samen met G27.

P09 - Onafhankelijk herstel mogelijk

Wij onderschrijven deze maatregel voor PaaS- en IaaS-diensten. Zie onze opmerkingen bij R7 - Onvoldoende borging van databeschikbaarheid en herstel en G33 - Geen afhankelijkheid van één leverancier voor herstel.

P10 - Transparantie infrastructuur

Inzicht in de onderliggende infrastructuur is nodig om afhankelijkheden zichtbaar te maken, en in zoverre onderschrijven wij de maatregel. Zij reikt echter verder dan de omgeving van de gemeente. De architectuur en de leveranciersketen van de onderliggende hostingpartij raken het bedrijfsgeheim van die partij, en gedetailleerde infrastructuurinformatie is bovendien zelf een beveiligingsrisico. De GIBIT 2025 erkent dat in artikel 25.3, waar een uitzondering geldt voor onderdelen waarvan verstrekking reverse engineering mogelijk maakt, en in artikel 32.8 voor informatie over beveiligingsmaatregelen.

Wij bevelen aan om P10 te laten invullen via de SBOM van artikel 25 GIBIT en de derdenverklaring van artikel 38 GIBIT, met de mogelijkheid om gevoelige onderdelen aan het CSIRT te verstrekken in plaats van aan iedere gemeente afzonderlijk, conform artikel 25.5 GIBIT.

P11 - Parallelle multi-stack inzet

Zie onze opmerkingen bij 4.3 - Stap 2: bepaal de relevante beheersmaatregelen en G02 - Multi-provider inzet. De maatregel is bij BBN2 onverenigbaar met het profiel dat hoofdstuk 7 voor BBN2 beschrijft. Wij vragen om P11 uitsluitend bij BBN3 te verplichten, en daar te beperken tot workloads die geen enkele vorm van downtime kunnen verdragen.

7 Bijlage: BBN beveiligingsniveau's

Het is opvallend dat de risicoclassificatie uitgaat van de basisbeveiligingsniveaus (BBN) uit de BIO 1. In plaats daarvan gaat de BIO2 uit van risicosturing binnen een managementsysteem op basis van NEN-EN-ISO/IEC 27001. Met de Cyberbeveiligingswet die sinds 15 augustus 2026 geldt, is de BIO2 het juridische referentiekader voor de zorgplicht van overheidsorganisaties.

Een handreiking die nu wordt vastgesteld op basis van de BBN's is daarmee bij publicatie al gebaseerd op een systematiek die is vervallen. Dat raakt niet alleen hoofdstuk 7, maar ook de matrix in 4.3 en de weging van de EMVI-criteria in 4.5, die beide op het BBN steunen.

Voor een bruikbaar cloudbeleid vragen we om een herziening van de risicoclassificatie zodat die aansluit bij de BIO2. Zie ook:

- BIO 2, paragraaf 6.2 voor de risicomanagementmethodiek, pagina 7

- Beschrijving belangrijke wijzigingen BIO2 op DigitaleOverheid.nl

Zie daarnaast onze opmerking bij 4.2 - Stap 1: bepaal Beveiligingsniveau over het aansturen van jurisdictie-eisen via de beschikbaarheidsscore.

8 Bijlage - Soevereiniteitsniveau's GEMMA

In het algemeen is onduidelijk hoe de soevereiniteitsniveaus zijn ontstaan en opgezet. De niveaus verschillen van de SEAL-niveaus van het EU Cloud Sovereignty Framework (PDF) en van het DICTU toetsingsinstrument, en wijken af van de uitvraag van het IMG CIO-beraad. Ons advies is om aan te sluiten bij het Europese kader en die implementatie handzaam te maken voor gemeenten en leveranciers.

Verder bevat het niveau S2 de verplichting om een soevereine overheidscloud te gebruiken. Op dit moment is er geen overheidscloud beschikbaar. Er is recent een verkenning gepubliceerd over een overheidscloud waarbij er geen budget of tijdslijn beschikbaar is. Ook is het onduidelijk in hoeverre en op welke termijn gemeenten en decentrale overheden bij deze cloud kunnen aansluiten. Het is beter om S2 en S3 samen te voegen tot EU/NL cloud met eisen. Deze opzet sluit ook aan bij het huidige marktlandschap, waarin leveranciers oplossingen vanuit een eigen cloud leveren.

De defiinitie van S4 "Marktcloud (hyperscaler)" is onduidelijk. Ook hyperscalers bieden clouddiensten binnen de Europese Unie. Bij Microsoft Azure is het bijvoorbeeld mogelijk om aan te geven welke datacenters gebruikt mogen worden. Hiermee kan ook door een hyperscaler worden voldaan aan de eisen die gelden bij S3. Omdat het hier over soevereiniteitsniveau's gaat, wil de GEMMA hier waarschijnlijk voorkomen dat extraterretoriale juridische regimes zich toegang tot de data verschaffen. Dit blijkt echter niet uit de definitie van het cloudniveau. Daarbij is het onduidelijk in hoeverre technische maatregelen zoals het sleutelbeheer bij de gemeente leggen een afdoende beperking zijn dat dit risico. Door deze onduidelijkheid is het nu niet duidelijk wat het verschil is tussen een EU/NL cloud en een Marktcloud is onduidelijk. We vragen u dit te specificeren en aan te geven welke technische maatregelen voldoende zijn om de waarborgen binnen de cloud van een hyperscaler in te zetten voor welk vertrouwelijkheidsniveau van data.

S1 - Hoog geclassificeerd

Als eis is gesteld dat er geen afhankelijkheid mag zijn van externe control planes en dat hardware, software en beheer binnen de EU of onder nationale controle moeten liggen.

Volledige onafhankelijkheid is echter niet mogelijk, omdat er zeker op het gebied van hardware en microcode altijd afhankelijkheden zijn van niet-Europese partijen. De EU zet met de European Chips Act (EC-beleidspagina) stappen om ook op hardwareniveau onafhankelijker te worden. Zolang die stappen niet zijn afgerond, leidt een eis om nu op S1 te werken vooral tot onbegrip over wat GEMMA van de markt vraagt.

Het is beter om te werken met een groeipad, zodat duidelijk is wat op dit moment haalbaar is en wat niet.

S2 - Soevereine overheidscloud

Op dit moment is er geen soevereine overheidscloud waar gemeenten op kunnen aansluiten. Gegeven de eisen die zijn gesteld, is het bovendien niet nodig om niveau S2 te onderscheiden. De eisen voor verwerking binnen de EU en de EER, juridische afscherming tegen extraterritoriale claims en transparantie in de keten verschillen inhoudelijk nauwelijks van wat bij S3 wordt gevraagd.

Voor het sleutelbeheer onder gemeentelijke controle zijn verschillende toepassingen denkbaar. De uitvoering is echter complex en sluit niet aan bij de manier waarop de markt nu is ingericht. Ook dit brengt aanvullende kosten met zich mee.

Zoals het nu staat is het niveau langs twee verschillende assen te bepalen, met verschillende uitkomsten. Wij vragen om één as te kiezen: indeling op domein óf indeling op gegevensclassificatie, in beide gevallen uitputtend uitgewerkt. Zie ook Volledigheid van de GEMMA-domeinen.

Aanvullend vragen wij om de omschrijving van het toepassingsgebied te preciseren. Bij S2 staan drie categorieën naast elkaar: sociaal domein, burgerzaken en "persoonsgegevens (hoog vertrouwelijk)". Die categorieën zijn van verschillende orde. De eerste twee zijn domeinen, de derde is een gegevenscategorie. Daardoor blijven twee vragen open. Geldt S2 voor het volledige sociaal domein, inclusief participatie en inkomen, of alleen voor de onderdelen met bijzondere persoonsgegevens? En geldt S2 voor elke oplossing waarin persoonsgegevens worden vastgelegd? Want dat zijn en blijven voorlopig vrijwel alle gemeentelijke toepassingen. Of geldt S2 alleen wanneer die persoonsgegevens als hoog vertrouwelijk zijn geclassificeerd?

Zie voor meer achtergrond over S2 ook onze suggesteis bij: 4.4 - Stap 4: Bepaal het Soevereiniteitsniveau

S3 - EU/NL cloud met eisen

Bij dit niveau staat "contractuele bescherming (GIBIT)" als eis opgenomen. Dat is de enige plaats in het hele document waar de GIBIT wordt genoemd. Daarmee blijft de verhouding tussen beide documenten ongeregeld, terwijl de GIBIT op vrijwel elk niveau relevant is.

S4 - Marktcloud

De naam van S4 is onduidelijk, omdat er een verschil is tussen een veilige en soevereine cloud van bijvoorbeeld deelnemers aan de Open Cloud Alliantie en clouddiensten die mogelijk onder een andere jurisdictie vallen. Beide leveren een commerciële cloud voor IaaS-, PaaS- en SaaS-diensten. De terminologie is daarmee incorrect.

Bij de toepassingen staat 'standaard SaaS' opgenomen. Het is echter niet duidelijk wanneer S4 geldt en wanneer S3. Het lijkt erop dat alleen publieke informatie, zoals gemeentelijke websites, op deze cloud kan staan. Wat 'standaard SaaS' onderscheidt van de S3-onderdelen bedrijfsvoering, generieke gemeentelijke processen en samenwerkingstools, is niet helder.

9 Bijlage: Begrippenlijst

De begrippenlijst definieert soevereiniteit als de mate waarin de kans is verlaagd dat statelijke actoren met een offensief cyberprogramma de bedrijfsvoering plat kunnen leggen of zich ongeautoriseerd toegang verschaffen tot data. Dat is aanzienlijk smaller dan de vier dimensies uit paragraaf 2.7 en dan het Europese framework. Omdat de begrippenlijst in aanbestedingen als uitleg wordt gebruikt, vragen we om beide definities gelijk te trekken. Wij vragen daarbij ook om in de definitie het begrip *digitale soevereiniteit* te hanteren; zie 2.5 - Noodzaak van soevereiniteit.

Daarnaast bevat de lijst begrippen die nergens anders in het document terugkomen. Bij "Bi-Modal" wordt verwezen naar "Kavel 1B/2B", de "Mondiale Stack" en de "Europese Stack". Die termen komen in de rest van het document niet voor en suggereren overname uit een specifieke aanbesteding. Wij vragen om deze passages te verwijderen of om de begrippen alsnog in het document uit te werken, zodat het kader generiek toepasbaar blijft.

Tot slot: Haven en HavenPlus zijn uitgebreid gedefinieerd, maar geen enkele maatregel verwijst ernaar. Zie ons voorstel bij P01 - Infrastructure as Code en P03 - Reproduceerbare omgevingen om Haven-conformiteit als bewijsmiddel te laten gelden.

10 Bijlage PvE Gemeentelijke Cloud

De S- en P-codes in deze bijlage verschillen van die in hoofdstuk 6. Zie 3 - Risico's en maatregelen.

Status van maatregelen: eis of wens

De bijlage kent een kolom Eis/Wens. Die status komt niet overeen met de matrix in paragraaf 4.3. Volgens 4.3 zijn bij BBN2 de maatregelen G01 tot en met G10 en G17 tot en met G38 vereist, en bij SaaS aanvullend S01 tot en met S03 en S07 tot en met S10. In de bijlage staan verschillende van die maatregelen als wens.

Maatregel	Bijlage 10	Matrix 4.3 bij BBN2
G18 Recht op periodieke heroverweging	Wens	Vereist
G19 Ondersteuning bij toetsing alternatieven	Wens	Vereist
S07 Lifecycle transparantie (nummering bijlage 10)	Wens	Vereist
P08 Transparantie infrastructuur (nummering bijlage 10)	Wens	Vereist

Voor een aanbesteding is dit verschil bepalend. Een wens telt mee in de gunning, een eis is een uitsluitingsgrond. Wij vragen u de status per maatregel eenduidig vast te leggen, en daarbij aan te geven welke bron leidend is: de matrix in 4.3 of de kolom in deze bijlage. Zie ook 11 Bijlage EMVI Gemeentelijke Cloud.

Wij vragen daarnaast om de kolom Toepassingsgebied per maatregel te differentiëren in plaats van alle G-maatregelen op 'Algemeen' te zetten. Zie Toepassingsgebied per cloudmodel.

Aan te leveren documenten

De eisen vanuit het PvE vereisen de aanlevering van de volgende documenten bij een aanbesteding:

- Subverwerkersoverzicht
- Architectuurdocument van de oplossing voor het invullen van verschillende maatregelen
- Testrapporten verplaatsbaarheid, migratie en databeschikbaarheid, waarbij de scope en inrichting onduidelijk zijn
- Overzicht van de eigendomsstructuur
- Verklaring over niet-Europese jurisdicties
- Motivatie voor geen of beperkte afhankelijkheid van niet-Europese jurisdicties en digitale infrastructuren
- Rapportage voor toetsing van Europese alternatieven
- Migratieplan voor niet-structurele Europese afhankelijkheid
- Auditrapport functiescheiding en governance-afhankelijkheid
- Monitoringrapport logging en processen
- Plan voor incidentmanagement
- Continuïteitsplan voor beëindiging
- Exit-plan voor migratie
- Repository voor toegang tot Infrastructure as Code
- Monitoringrapport prestaties en security
- Broncode voor reproductie van omgevingen
- Tests voor onafhankelijk herstel

Verschillende van deze documenten, zoals het continuïteitsplan en het exit-plan, zijn standaard onderdeel bij aanbestedingen. Door dit expliciet te koppelen aan de GIBIT wordt duidelijk welke maatregelen samenvallen met verplichtingen die al bestaan.

Voor verschillende rapportages is onduidelijk of aanlevering eenmalig is bij inschrijving, zoals bij een monitoringrapport, of dat deze periodiek moet worden herhaald. Daarnaast is onduidelijk aan welke eisen een auditrapportage over functiescheiding moet voldoen, omdat geen koppeling is gelegd met bestaande certificeringen zoals ISO 27001 of met de derdenverklaring van artikel 38 GIBIT.

Al met al werken de uitgebreide architectuurdocumenten en rapportages sterk verzwarend voor een inschrijving. Bovendien vereisen deze documenten dat delen van het intellectueel eigendom van oplossingen worden vrijgegeven. Naast onze inhoudelijke reactie op individuele maatregelen pleiten we ervoor om voor veel van deze documenten één manier van aanleveren en verwerken in te regelen. De GIBIT kent daar in artikel 25.5 al een vorm voor, waarbij partijen kunnen overeenkomen dat de leverancier de SBOM niet aan de gemeente maar aan het CSIRT toestuurt. Door dit generiek te regelen, kan dit net als bij de SBOM eenmalig worden ingeregeld voor alle gemeenten. Dat voorkomt veel individueel werk voor leveranciers en gemeenten en houdt gevoelige documentatie bij één partij.

Wij bevelen daarnaast aan om per maatregel expliciet te maken welke bestaande artefacten als voldoende bewijs gelden. Wij denken daarbij aan ISO 27001 met de bijbehorende Verklaring van Toepasselijkheid, ISO 27017, ISAE 3402 type II, ISAE 3000 voor DigiD, de derdenverklaring van artikel 38 GIBIT en de BIO2-verantwoording. Het uitgangspunt zou moeten zijn dat een leverancier zich één keer verantwoordt en dat alle gemeenten die verantwoording kunnen gebruiken.

11 Bijlage EMVI Gemeentelijke Cloud

Deze bijlage bepaalt hoe inschrijvingen worden gescoord en is daarmee commercieel de meest bepalende van het document. Zij roept vier vragen op.

Ten eerste de scoring van EMVI1. Een score van 5 vereist een volledig multi-vendor ontwerp met aantoonbare spreiding over leveranciers en technologiestacks. Een score van 1 geldt bij "single vendor of sterke concentratie". Elke SaaS-dienst scoort daarmee per definitie een 1, ongeacht de kwaliteit van de dienst, de escrow-regeling, de dataportabiliteit of de exit-voorzieningen. Dat is geen beoordeling van de inschrijving maar van het leveringsmodel. Wij bevelen aan om voor SaaS een vervangend criterium te hanteren dat scoort op continuïteit, dataportabiliteit en aantoonbare exit, in lijn met ons voorstel bij R1 - Concentratie en Leveranciersafhankelijkheid en met onze opmerking over de voorwaardelijke impact bij R2 - Technologische lock-in en beperkte verplaatsbaarheid.

Ten tweede de schaal. De tabel kent alleen de waarden 1, 3 en 5, zonder tussenwaarden en zonder voorschrift voor onderlinge weging. Voor een gunningsbeslissing is dat grofmazig en daarmee kwetsbaar. Wij vragen om een fijnmaziger schaal met beschreven tussenniveaus.

Ten derde de verwijzingen. De EMVI-tabel verwijst naar P-codes in de nummering van bijlage 10, terwijl de toelichting in hoofdstuk 6 een andere nummering hanteert. Zie 3 - Risico's en maatregelen. Zolang dat niet is opgelost, is niet vast te stellen waarop precies wordt gegund.

Ten vierde de grondslag. Paragraaf 4.5 koppelt de weging van de EMVI-criteria aan het BBN. Die grondslag vervalt met de BIO2. Zie 7 Bijlage: BBN beveiligingsniveau's.