



# Eisen aan gemeentelijke Cloudvoorzieningen

Kaderstelling, handreiking, basis-bestek

Handreiking

# Inhoud

|           |                                                                   |           |
|-----------|-------------------------------------------------------------------|-----------|
| <b>1</b>  | <b>Inleiding</b>                                                  | <b>3</b>  |
| 1.1       | Doel en Reikwijdte                                                | 3         |
| 1.2       | Positionering binnen het gemeentelijk instrumentarium             | 3         |
| 1.3       | Documentopbouw / leeswijzer                                       | 4         |
| <b>2</b>  | <b>Strategisch Kader</b>                                          | <b>5</b>  |
| 2.1       | Gemeentelijke dienstverlening als uitgangspunt                    | 5         |
| 2.2       | Publieke waarden: continuïteit, databeschikbaarheid en veiligheid | 5         |
| 2.3       | Dreigingen en structurele kwetsbaarheden                          | 5         |
| 2.4       | Noodzaak van autonomie                                            | 6         |
| 2.5       | Noodzaak van soevereiniteit                                       | 6         |
| 2.6       | Autonomie en soevereiniteit als middel                            | 6         |
| 2.7       | Dimensies van soevereiniteit                                      | 6         |
| 2.8       | Vertaling naar beheersing                                         | 7         |
| <b>3</b>  | <b>Risico's en maatregelen</b>                                    | <b>8</b>  |
| 3.1       | Overzicht van risico's en maatregelen                             | 8         |
| <b>4</b>  | <b>Handleiding voor PvE</b>                                       | <b>12</b> |
| 4.1       | Doel en gebruik van deze handleiding                              | 12        |
| 4.2       | Stap 1: bepaal Beveiligingsniveau                                 | 12        |
| 4.3       | Stap 2: bepaal de relevante beheersmaatregelen                    | 12        |
| 4.4       | Stap 4: Bepaal het Soevereiniteitsniveau                          | 13        |
| 4.5       | Bepaal de EMVI-criteria                                           | 14        |
| <b>5</b>  | <b>Bijlage: Risico's nader toegelicht</b>                         | <b>15</b> |
| <b>6</b>  | <b>Bijlage: Beheersingsmaatregelen nader toegelicht</b>           | <b>20</b> |
| 6.1       | Cluster 1 – Afhankelijkheid en marktstructuur                     | 20        |
| 6.2       | Cluster 2 – Portabiliteit en lock-in                              | 22        |
| 6.3       | Cluster 3 – Juridische soevereiniteit                             | 23        |
| 6.4       | Cluster 4 – Toekomstvastheid en migratie                          | 25        |
| 6.5       | Cluster 5 – Governance en functiescheiding                        | 26        |
| 6.6       | Cluster 6 – Continuïteit                                          | 27        |
| 6.7       | Cluster 7 – Dataherstel en databeschikbaarheid                    | 29        |
| 6.8       | SaaS-specifiek                                                    | 30        |
| 6.9       | PaaS/IaaS-specifiek                                               | 33        |
| <b>7</b>  | <b>Bijlage: BBN beveiligingsniveau's</b>                          | <b>36</b> |
| <b>8</b>  | <b>Bijlage: Soevereiniteitsniveaus GEMMA</b>                      | <b>40</b> |
| <b>9</b>  | <b>Bijlage: Begrippenlijst</b>                                    | <b>42</b> |
| <b>10</b> | <b>Bijlage PvE Gemeentelijke Cloud</b>                            | <b>46</b> |
| <b>11</b> | <b>Bijlage EMVI Gemeentelijke Cloud</b>                           | <b>49</b> |

# 1

## Inleiding

### 1.1 Doel en Reikwijdte

Dit document beschrijft het Gemeentelijk Cloudbeleid en vormt het kader waarbinnen gemeenten clouddiensten verwerven, ontwikkelen en beheren. Het document bevat de generieke uitgangspunten, eisen en richtlijnen die van toepassing zijn op alle vormen van cloudgebruik binnen gemeenten.

Deze kaders gelden voor:

- Software-as-a-Service (SaaS), zowel standaard marktproducten als gemeentelijke oplossingen
- Platform- en infrastructuurdiensten (PaaS en IaaS)
- Cloudoplossingen die in eigen datacenters (on-premise) worden gerealiseerd

De in dit document opgenomen bepalingen vormen gezamenlijk de **generieke Programma van Eisen (PvE)** voor gemeentelijke cloudvoorzieningen. Deze PvE-bepalingen omvatten:

- inhoudelijke eisen en randvoorwaarden
- wensen ten aanzien van kwaliteit en toekomstbestendigheid
- contractuele borging richting leveranciers

Deze bepalingen zijn verplicht toe te passen bij:

- de inkoop en aanbesteding van clouddiensten
- de ontwikkeling en exploitatie van eigen cloudomgevingen

Hiermee wordt geborgd dat alle gemeentelijke cloudoplossingen voldoen aan een uniform en consistent normenkader.

### 1.2 Positionering binnen het gemeentelijk instrumentarium

Dit document is een kaderstellend beleidsdocument dat richting geeft aan de wijze waarop gemeenten omgaan met cloudvoorzieningen. Het beschrijft de uitgangspunten, risico's en maatregelen die bepalend zijn voor het verantwoord inzetten van cloudtechnologie binnen de gemeentelijke context.

Het Gemeentelijk Cloudbeleid staat niet op zichzelf, maar maakt onderdeel uit van een bredere interbestuurlijke ontwikkeling. Om te voorkomen dat elke gemeente afzonderlijk invulling geeft aan het gebruik van cloudvoorzieningen, is dit document opgesteld vanuit een collectieve benadering. Gemeenten werken hierin samen met andere overheden binnen het gezamenlijke programma van de Nederlandse Digitaliseringsstrategie (NDS).

Binnen dit kader wordt toegewerkt naar een samenhangende digitale overheid, waarin overheden onderling en met private partijen samenwerken in ketens. Door gemeenschappelijke uitgangspunten en eisen te hanteren, wordt geborgd dat deze ketens bestaan uit consistente en robuuste schakels. Dit voorkomt versnippering en draagt bij aan de betrouwbaarheid, veiligheid en interoperabiliteit van de digitale overheid als geheel. Daarnaast wordt nadrukkelijk rekening gehouden met de bredere Europese context. Het gemeentelijk cloudbeleid sluit aan bij geldende Europese kaders en richtlijnen en draagt bij aan de ontwikkeling van een versterkte Europese digitale infrastructuur. Hiermee wordt niet alleen nationale, maar ook Europese samenhang en weerbaarheid bevorderd.

Tegelijkertijd staan gemeenten voor concrete uitvoeringsopgaven. In de praktijk is er een voortdurende noodzaak om digitale infrastructuur te verwerven en te vernieuwen. Lopende contracten lopen af, systemen worden gemoderniseerd en nieuwe applicatieve concepten, zoals Common Ground, worden in productie gebracht. Dit vraagt om duidelijke en direct toepasbare kaders voor cloudgebruik.

Het in dit document beschreven gemeentelijk cloudbeleid vormt daarmee de gemeentelijke bijdrage aan een interbestuurlijk kader voor cloudbeleid. Het biedt gemeenten houvast bij het maken van keuzes, terwijl tegelijkertijd wordt aangesloten bij bredere nationale en Europese ontwikkelingen.

De verdere operationalisering vindt plaats via:

- een separaat document met PvE- en EMVI-bepalingen, waarin de eisen concreet zijn uitgewerkt en genummerd: PvE en EMVI gemeentelijke cloud.
- de “Handreiking voor cloudbestellingen”, die gemeenten ondersteunt bij het toepassen van de eisen in concrete aanbestedingen en implementaties

Deze combinatie van beleid, normen en praktische hulpmiddelen zorgt voor een samenhangend en toepasbaar geheel.

### **1.3 Documentopbouw / leeswijzer**

Dit document is opgebouwd van strategie naar praktische toepassing. Hoofdstuk 1 introduceert het doel, de reikwijdte en de positionering van het gemeentelijk cloudbeleid. In hoofdstuk 2 wordt het strategisch kader geschetst, waarin publieke waarden, dreigingen en de noodzaak van autonomie en soevereiniteit centraal staan. Deze uitgangspunten worden in hoofdstuk 3 vertaald naar concrete risico's en bijbehorende beheersmaatregelen.

Hoofdstuk 4 biedt vervolgens een praktische handleiding om deze maatregelen risicogestuurd toe te passen bij cloudvraagstukken en aanbestedingen, via een stapsgewijze aanpak (BBN, maatregelen, soevereiniteit en EMVI). De bijlagen (hoofdstuk 5 t/m 10) bevatten nadere toelichtingen op risico's, maatregelen, beveiligings- en soevereiniteitsniveaus, evenals definities en bronverwijzingen.

Het document kan zowel integraal worden gelezen als gericht worden geraadpleegd per onderdeel, afhankelijk van de rol en informatiebehoefte van de lezer.

# 2

## Strategisch Kader

### 2.1 Gemeentelijke dienstverlening als uitgangspunt

Gemeenten voeren essentiële publieke taken uit op het gebied van dienstverlening aan burgers en ondernemers. Deze taken omvatten onder meer burgerzaken, het sociaal domein, openbare orde en veiligheid en vergunningverlening.

De uitvoering van deze taken is in toenemende mate afhankelijk van digitale systemen en gegevensverwerking. De digitale infrastructuur waarop deze processen draaien is daarmee niet langer ondersteunend, maar vormt een integraal onderdeel van de gemeentelijke dienstverlening.

Dit betekent dat verstoringen in digitale systemen direct kunnen leiden tot verstoringen in publieke dienstverlening en daarmee tot maatschappelijke impact. Digitale infrastructuur moet daarom worden beschouwd als kritische publieke infrastructuur.

### 2.2 Publieke waarden: continuïteit, databeschikbaarheid en veiligheid

De digitale ondersteuning van gemeentelijke taken moet voldoen aan een aantal fundamentele publieke waarden.

In de eerste plaats is bedrijfscontinuïteit essentieel. Gemeentelijke processen moeten onder alle omstandigheden kunnen doorgaan. Verstoring van digitale systemen mag niet leiden tot langdurige onderbreking van dienstverlening.

Daarnaast is databeschikbaarheid cruciaal. Gegevens moeten beschikbaar, volledig en correct zijn op de momenten dat zij nodig zijn. Tevens moet worden geborgd dat gegevens herstelbaar zijn bij incidenten of calamiteiten.

De derde pijler betreft informatiebeveiliging, die wordt vormgegeven langs de aspecten beschikbaarheid, integriteit en vertrouwelijkheid (BIV).

Deze drie elementen vormen gezamenlijk de basis voor het handelen van gemeenten in het digitale domein.

### 2.3 Dreigingen en structurele kwetsbaarheden

In het huidige digitale en geopolitieke landschap worden deze publieke waarden onder druk gezet door een aantal structurele ontwikkelingen.

De cloudmarkt wordt gekenmerkt door een sterke concentratie van aanbieders, waardoor afhankelijkheden ontstaan van een beperkt aantal grote partijen. Daarnaast hebben veel aanbieders een internationale positie, waardoor buitenlandse wetgeving invloed kan hebben op toegang tot data en systemen. Tegelijkertijd nemen cyberdreigingen en geopolitieke spanningen toe, wat de kwetsbaarheid van digitale infrastructuren vergroot. Deze ontwikkelingen leiden tot risico's voor de continuïteit, veiligheid en controle over gemeentelijke digitale voorzieningen.

## 2.4 Noodzaak van autonomie

Om deze risico's het hoofd te bieden, is het noodzakelijk dat gemeenten beschikken over voldoende autonomie.

Autonomie betreft 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.

Een hoge mate van autonomie vergroot de flexibiliteit van gemeenten en verkleint de afhankelijkheid van individuele partijen. Dit draagt direct bij aan de weerbaarheid van de digitale infrastructuur.

## 2.5 Noodzaak van soevereiniteit

Naast autonomie is ook soevereiniteit een cruciale randvoorwaarde.

Soevereiniteit heeft betrekking op de mate waarin gemeenten beschermd zijn tegen ongewenste externe invloeden op hun digitale infrastructuur. In het bijzonder gaat het om het beperken van de kans dat externe, waaronder statelijke, actoren de bedrijfsvoering verstoren of ongeautoriseerde toegang verkrijgen tot gegevens.

De borging van soevereiniteit draagt daarmee direct bij aan de bescherming van publieke waarden en de continuïteit van dienstverlening.

## 2.6 Autonomie en soevereiniteit als middel

Gemeenten streven ernaar maximale controle te behouden over data, systemen en processen, afhankelijkheden van individuele leveranciers te minimaliseren en kritieke dienstverlening onder alle omstandigheden te kunnen continueren.

Autonomie en soevereiniteit zijn in dit kader geen doel op zich, maar vormen noodzakelijke randvoorwaarden om deze doelstellingen te realiseren. Zij versterken de garanties op continuïteit en databeschikbaarheid en verminderen de kwetsbaarheid voor externe invloeden.

Gemeenten streven naar digitale autonomie en soevereiniteit, waarbij zij:

- maximale controle houden over data, systemen en processen
- afhankelijkheden van individuele leveranciers minimaliseren
- kritieke dienstverlening onder alle omstandigheden kunnen continueren

## 2.7 Dimensies van soevereiniteit

Soevereiniteit manifesteert zich langs verschillende dimensies, die elk een specifiek aspect van controle en weerbaarheid adresseren.

De juridische dimensie heeft betrekking op de toepasselijke wet- en regelgeving en de mate waarin deze onder Europese jurisdictie valt. Dit omvat onder meer bescherming tegen de invloed van niet-Europese wetgeving en transparantie in eigendoms- en governance-structuren. Dit sluit aan bij het risico van afhankelijkheid van niet-Europese jurisdicties.

De operationele dimensie betreft de inrichting en beheersing van processen, inclusief de scheiding tussen regie en uitvoering en de mogelijkheid om dienstverlening voort te zetten bij verstoringen. Dit is nauw verbonden met risico's rondom continuïteit en governance.

De technische dimensie ziet op de architectuur en inrichting van systemen, waaronder het voorkomen van afhankelijkheden van specifieke technologieën of leveranciers (lock-in) en het gebruik van open standaarden ter bevordering van portabiliteit.

De data-dimensie betreft de controle over data zelf, inclusief eigendom, toegang, opslag en herstelbaarheid. Dit omvat onder meer het borgen van onafhankelijke back-upvoorzieningen en het voorkomen van afhankelijkheid van één partij voor dataherstel.

## **2.8 Vertaling naar beheersing**

De combinatie van publieke waarden, risico's en de noodzaak tot autonomie en soevereiniteit vormt de basis voor het gemeentelijk cloudbeleid.

Hieruit volgen concrete beheersmaatregelen die zijn gericht op:

- het beperken van afhankelijkheden
- het vergroten van controle en transparantie
- het borgen van continuïteit en herstelbaarheid

Deze maatregelen worden in de volgende hoofdstukken verder uitgewerkt en vormen uiteindelijk de basis voor de generieke PvE-bepalingen die gemeenten hanteren bij cloudoplossingen.

# 3

## Risico's en maatregelen

Dit hoofdstuk beschrijft de risico's die zijn gemoeid met cloud en de risico-mitigerende maatregelen, in termen van eisen, wensen en contractuele borging. Deze maatregelen zijn ingedeeld naar algemeen geldende (aangeduid als G), SaaS-specifiek (aangeduid als S) en PaaS/IaaS-specifiek (aangeduid als P).

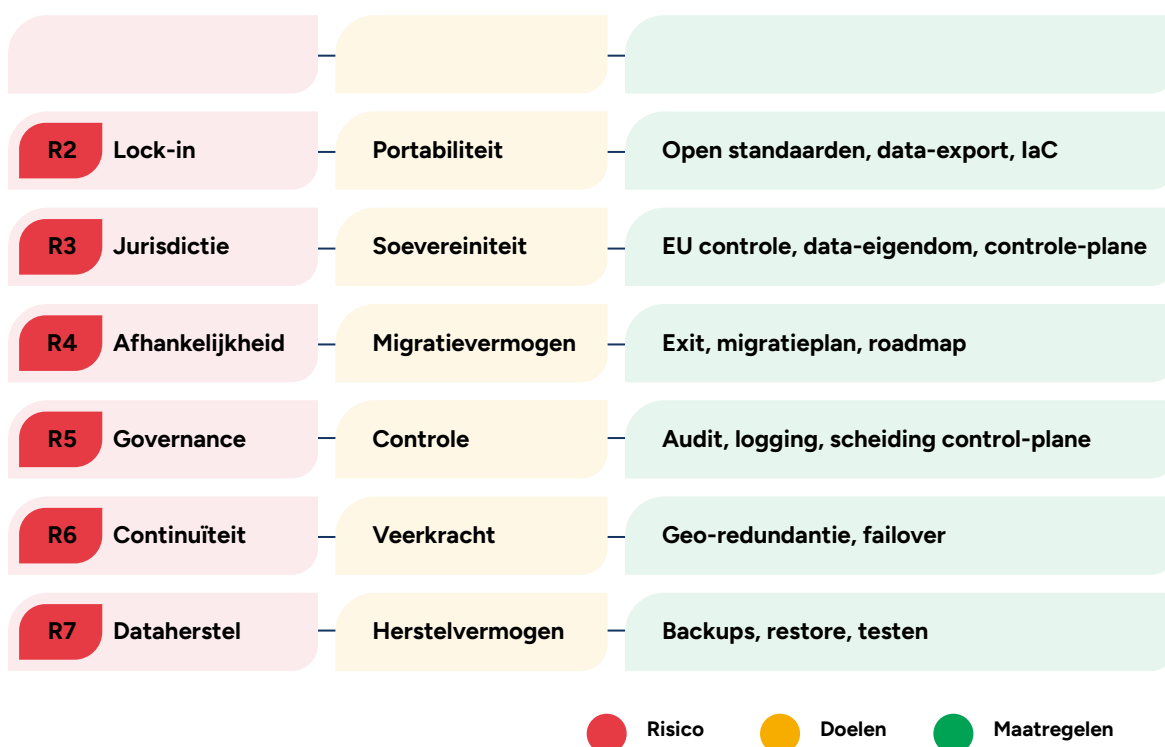
In paragraaf 1 is het overzicht opgenomen van de risico, de bijbehorende duiding en de maatregelen die bijdragen aan de beheersing daarvan, uitgesplitst naar generieke, SaaS- en PaaS/IaaS-specifieke eisen.

De in dit hoofdstuk uitgewerkte risico's, maatregelen leiden tot een samenhangende set uitgangspunten voor gemeentelijke cloudvoorzieningen:

- Gemeenten streven naar maximale controle over data, systemen en processen en beperken afhankelijkheden van individuele leveranciers waar mogelijk.
- Gemeentelijke dienstverlening wordt zodanig ingericht dat continuïteit onder alle omstandigheden kan worden gewaarborgd.
- Digitale infrastructuur wordt ingericht volgens een multi-provider benadering, waarbij spreiding van leveranciers en technologieën wordt toegepast om risico's te beheersen.
- De Europese digitale infrastructuur vormt het uitgangspunt voor cloudtoepassingen, waarbij oplossingen binnen de Europese rechtsorde worden geprefereerd.
- In situaties waarin gebruik wordt gemaakt van mondiale aanbieders, wordt gestuurd op het beperken van afhankelijkheden en het realiseren van een aantoonbaar migratiepad naar Europese alternatieven.

### 3.1 Overzicht van risico's en maatregelen

In onderstaande afbeelding zijn de risico's, de doelstellingen en de maatregelen samengevat.





In onderstaande tabel zijn de risico, de bijbehorende duiding en de maatregelen die bijdragen aan de beheersing daarvan, uitgesplitst naar generieke, SaaS- en PaaS/IaaS-specifieke eisen.

In toelichting op de risico's is te vinden in hoofdstuk 5 en op de risico-beheersende maatregelen in hoofdstuk 6.

In het document PvE en EMVI Gemeentelijke Cloud zijn de maatregelen verder uitwerkt tot eisen, wensen en contractuele borging.

| ID | Risico                                                                                                                                     | Risico-adressering                                                                                                                                           | Risico-beheersingsmaatregel                                                                                                                                                                                                                                                |
|----|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| R1 | <b><u>Concentratie</u></b><br><br>Concentratierisico en leveranciers-afhankelijkheid<br>Concentratierisico en leveranciers-afhankelijkheid | Afhankelijkheid van één leverancier of ecosysteem en concentratie van kritieke functionaliteit bij een beperkt aantal aanbieders                             | <b><u>Algemeen:</u></b><br>G01 – Beperking leveranciersafhankelijkheid<br>G02 – Multi-provider inzet<br>G03 – Inzicht in ketenafhankelijkheden<br>G04 – Spreiding van kritieke workloads<br>G05 – Verkaveling van systemen en leveranciers                                 |
|    |                                                                                                                                            |                                                                                                                                                              | <b><u>SaaS:</u></b><br>S07 – Continuïteit bij beëindiging<br>S08 – Toegang tijdens migratie<br>S09 – Lifecycle en roadmap transparantie (zie ook R4)<br>S10 – Continuïteit bij faillissement                                                                               |
|    |                                                                                                                                            |                                                                                                                                                              | <b><u>PaaS/IaaS:</u></b><br>P10 – Transparantie infrastructuur<br>P11 – Parallele multi-stack inzet (continuïteit en uitwijkbaarheid)                                                                                                                                      |
| R2 | <b><u>Lock-in</u></b><br><br>Technologische lock-in en beperkte verplaatsbaarheid                                                          | Beperkte verplaatsbaarheid van systemen, data en configuraties, leidend tot hoge migratiekosten en afhankelijkheid van leveranciers-specifieke technologieën | <b><u>Algemeen:</u></b><br>G06 – Gebruik van open standaarden<br>G07 – Volledige data-export inclusief metadata<br>G08 – Toegang tot data en technische artefacten<br>G09 – Contractueel vastgelegde exit- en migratievoorwaarden<br>G10 – Vendor-agnostische architectuur |
|    |                                                                                                                                            |                                                                                                                                                              | <b><u>SaaS:</u></b><br>S01 – Scheiding data en applicatie<br>S02 – Volledige data-export inclusief metadata<br>S03 – Datamobiliteit zonder applicatie-afhankelijkheid                                                                                                      |
|    |                                                                                                                                            |                                                                                                                                                              | <b><u>PaaS/IaaS:</u></b><br>P01 – Infrastructure as Code<br>P02 – Volledige configuratietoegang<br>P03 – Reproduceerbare omgevingen                                                                                                                                        |

| ID | Risico                                                                                                                    | Risico-adres-<br>ring                                                                                                                                                                                                                 | Risico-beheersingsmaatregel                                                                                                                                                                                                                                                                                                                 |
|----|---------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| R3 | <b><u>Jurisdictie</u></b><br><br>Afhankelijkheid van niet-EU jurisdicties en digitale infrastructuren                     | Afhankelijkheid van niet EU jurisdicties en digitale infrastructuren, met risico op externe toegang, juridische beïnvloeding en geopolitieke afhankelijkheid                                                                          | <b><u>Algemeen:</u></b><br>G11 – EU/EER-jurisdictie of gelijkwaardig beschermingsniveau<br>G12 – Transparantie eigendomsstructuur en zeggenschap<br>G13 – Data-eigendom bij gemeente<br>G14 – Verplichting tot juridisch betwisten van datavorderingen<br>G15 – EU-by-design als uitgangspunt<br>G16 – Beperking inzet niet-EU leveranciers |
|    |                                                                                                                           |                                                                                                                                                                                                                                       | <b><u>SaaS:</u></b><br>S04 – Transparantie subverwerkers<br>S05 – Toegangsbeperking leverancier<br>S06 – Meldplicht wijziging subverwerkers                                                                                                                                                                                                 |
|    |                                                                                                                           |                                                                                                                                                                                                                                       | <b><u>PaaS/laaS:</u></b><br>P04 – Control-plane binnen EU                                                                                                                                                                                                                                                                                   |
| R4 | <b><u>Afhankelijkheid</u></b><br><br>Structurele afhankelijkheid door beperkte beschikbaarheid van Europese alternatieven | Structurele afhankelijkheid van niet EU oplossingen door beperkte beschikbaarheid van volwaardige Europese alternatieven en een gebrek aan effectieve migratiemogelijkheden                                                           | <b><u>Algemeen:</u></b><br>G17 – Geen contractuele blokkades voor migratie<br>G18 – Recht op periodieke heroverweging<br>G19 – Ondersteuning bij toetsing alternatieven<br>G20 – Verplicht en toetsbaar migratieplan<br>G21 – Tijdelijkheid niet-EU oplossingen                                                                             |
|    |                                                                                                                           |                                                                                                                                                                                                                                       | <b><u>SaaS:</u></b><br>S09 – Lifecycle en roadmap transparantie (zie ook R1)                                                                                                                                                                                                                                                                |
|    |                                                                                                                           |                                                                                                                                                                                                                                       | <b><u>PaaS/laaS:</u></b><br>Geen aanvullende specifieke PaaS/laaS eisen                                                                                                                                                                                                                                                                     |
| R5 | <b><u>Governance</u></b><br><br>Onvoldoende functiescheiding en afhankelijkheid in governance                             | Onvoldoende functiescheiding tussen sturing, uitvoering en toezicht, en afhankelijkheid van leveranciers voor beheer van systemen en control-plane, waardoor transparantie, controle en onafhankelijke besluitvorming worden beperkt. | <b><u>Algemeen:</u></b><br>G22 – Onafhankelijk audit- en toezichtrecht<br>G23 – Transparantie in logging en processen<br>G24 – Geen beperkingen op toezicht<br>G25 – Scheiding control-plane en uitvoering                                                                                                                                  |
|    |                                                                                                                           |                                                                                                                                                                                                                                       | <b><u>SaaS:</u></b><br>Geen aanvullende specifieke SaaS eisen                                                                                                                                                                                                                                                                               |
|    |                                                                                                                           |                                                                                                                                                                                                                                       | <b><u>PaaS/laaS:</u></b><br>P05 – Onafhankelijk beheer mogelijk<br>P06 – Logging en monitoring                                                                                                                                                                                                                                              |

| ID | Risico                                                                                   | Risico-adres-<br>ring                                                                                                                      | Risico-beheersingsmaatregel                                                                                                                                                                                                                                                                                                                                       |
|----|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| R6 | <b><u>Continuïteit</u></b><br><br>Onvoldoende operationele continuïteit bij verstoringen | Risico op uitval van dienstverlening bij verstoringen door onvoldoende spreiding, uitwijkcapaciteit en herstelvoorzieningen                | <b><u>Algemeen:</u></b><br>G26 – Contractuele borging continuïteit en incidentrespons<br>G27 – Periodieke tests van herstel- en uitwijkscenario's<br>G28 – Verplichte informatievoorziening bij verstoringen<br>G29 – Geo-redundantie<br>G30 – Topografische spreiding<br>G31 – Crisis- en escalatieprocedures                                                    |
|    |                                                                                          |                                                                                                                                            | <b><u>SaaS:</u></b><br>S07 – Continuïteit bij beëindiging<br>S08 – Toegang tijdens migratie                                                                                                                                                                                                                                                                       |
|    |                                                                                          |                                                                                                                                            | <b><u>PaaS/IaaS:</u></b><br>P09 – Onafhankelijk herstel mogelijk                                                                                                                                                                                                                                                                                                  |
| R7 | <b><u>Dataherstel</u></b><br><br>Onvoldoende borging van data-beschikbaarheid en herstel | Onvoldoende borging van data-beschikbaarheid en herstel, leidend tot risico op dataverlies en grootschalige impact bij datacompromittering | <b><u>Algemeen:</u></b><br>G32 – Inzicht in back-up- en herstelprocessen<br>G33 – Geen afhankelijkheid van één leverancier voor herstel<br>G34 – Scheiding van back-up- en productieomgeving<br>G35 – Aantoonbaar geteste herstelprocedures<br>G36 – Data shattering<br>G37 – Onafhankelijke restore mogelijkheid<br>G38 – Aantoonbaar herstel buiten leverancier |
|    |                                                                                          |                                                                                                                                            | <b><u>SaaS:</u></b><br>Geen aanvullende specifieke SaaS eisen                                                                                                                                                                                                                                                                                                     |
|    |                                                                                          |                                                                                                                                            | <b><u>PaaS/IaaS:</u></b><br>P09 – Onafhankelijk herstel mogelijk                                                                                                                                                                                                                                                                                                  |

# 4

## Handleiding voor PvE

### 4.1 Doel en gebruik van deze handleiding

Deze handleiding ondersteunt gemeenten bij het toepassen van het Programma van Eisen (PvE) op concrete cloudvraagstukken en aanbestedingen.

Het PvE bevat een omvangrijke set maatregelen. Niet elke maatregel is echter in gelijke mate relevant voor elke toepassing. Daarom is een risicogestuurde toepassing noodzakelijk.

De kern van deze handleiding is:

Bepaal eerst de classificatie van de workload of toepassing, en pas vervolgens de passende maatregelen toe.

Hiermee wordt voorkomen dat:

- lichte toepassingen onnodig zwaar worden ingericht
- kritische systemen onvoldoende beschermd zijn

### 4.2 Stap 1: bepaal Beveiligingsniveau

De toepassing van het Cloud-PvE begint bij het bepalen van de classificatie van het digitaal te ondersteunen bedrijfsproces en de dataverzameling. Hierbij wordt de BIV-classificeringsmethode gehanteerd:

- Beschikbaarheid (B) → hoe kritisch is het proces voor dienstverlening en hoe kritisch is de applicatie/voorziening die het proces ondersteund
- Integriteit (I) → hoe belangrijk is correctheid van de gegevens die in de applicatie/voorziening worden opgeslagen en beheerd
- Vertrouwelijkheid (V) → hoe gevoelig zijn de gegevens die in de applicatie/voorziening worden opgeslagen en beheerd

Hieruit volgen beveiligingsscores. De hoogste score bepaalt het minimale beveiligingsniveau, uitgedrukt in 'basisbeveiligingsniveau' (BBN)

### 4.3 Stap 2: bepaal de relevante beheersmaatregelen

Bepaal aan de hand van onderstaande overzichten welke beheersmaatregelen gelden voor bij het betreffende beveiligingsniveau. In het spreadsheet 'PvE en EMVI gemeentelijke cloud' zijn vervolgens de eisen te vinden die dan kunnen worden meegenomen in het PvE. Onderstaand is per BBN is aangegeven welke maatregelen daarbij minimaal zijn vereist en welke maatregelen gewenst zijn. Samenvattend liggen daarbij de volgende accenten:

| ID   | Risico-niveau | Kenmerk              | Doel                                          | Architectuur      |
|------|---------------|----------------------|-----------------------------------------------|-------------------|
| BBN1 | Laag risico   | Rebuild mogelijk     | continuïteit en herstelbaarheid (basisniveau) | cold/warm standby |
| BBN2 | Middel risico | Snelle activatie     | continuïteit en herstelbaarheid (geborgd)     | warm standby      |
| BBN3 | Hoog risico   | Direct overschakelen | continuïteit en soevereiniteit                | active-active     |

Het onderstaand overzicht geeft aan welke cloud gerelateerde risico's en bijbehorende beheersmaatregelen van toepassing zijn op welk BBN niveau. Hierbij is onderscheid gemaakt tussen vereiste maatregelen, die als knock-out moeten worden meegenomen in een aanbesteding, en wenselijke maatregelen. In hoofdstuk 7 zijn de BBN-niveaus nader toegelicht.

Tevens is hierbij onderscheid gemaakt tussen SaaS en PaaS/IaaS.

| BBN t/m niveau | Primaire risico's         | Neven t/m geschikte risico's | Vereiste maatregelen bij SaaS, PaaS/IaaS | Aanvullend vereist bij SaaS | Aanvullend vereist bij PaaS/IaaS | Gewenste maatregelen bij SaaS, PaaS/IaaS | Aanvullend gewenst bij SaaS | Aanvullend gewenst bij PaaS/IaaS |
|----------------|---------------------------|------------------------------|------------------------------------------|-----------------------------|----------------------------------|------------------------------------------|-----------------------------|----------------------------------|
| <b>BBN1</b>    | R6, R7                    | R1, R2, R4, R5               | G26 t/m G31, G32 t/m G38                 | Geen                        | Geen                             | G01 t/m G10, G17 t/m G25                 | S01 t/m S03, S07 t/m S10    | P07 t/m P09, P11                 |
| <b>BBN2</b>    | R1, R2, R4, R5, R6, R7    | R3                           | G01 t/m G10, G17 t/m G38                 | S01 t/m S03, S7 t/m S10,    | P01 t/m P03, P07 t/m P09, P11    | G11 t/m G16,                             | S04 t/m S06,                | P04 t/m P06                      |
| <b>BBN3</b>    | R1 t/m R7 (alle risico's) | Geen                         | G01 t/m G38                              | S01 t/m S10,                | P01 t/m P11                      | Geen                                     | Geen                        | Geen                             |

#### 4.4 Stap 4: Bepaal het Soevereiniteitsniveau

Om proportionele eisen te stellen aan cloudvoorzieningen, wordt gebruik gemaakt van een indeling in soevereiniteitsniveaus conform de GEMMA. In hoofdstuk

Bepaal aan de hand van deze soevereiniteitsniveaus welke aanscherpingen nog noodzakelijk zijn op de in stap 2 bepaalde beheersingsmaatregelen.

De soevereiniteitsniveaus bepalen:

- welke cloudvorm is toegestaan
- welke aanvullende eisen gelden
- welk risiconiveau acceptabel is

| Niveau | Naam                 | Beschrijving                                                | Bijpassend GEM-MA-domein              | Toegestane cloud                         |
|--------|----------------------|-------------------------------------------------------------|---------------------------------------|------------------------------------------|
| S1     | Hoog geclassificeerd | Kritieke overheidstaken, staatsveiligheid, crisisbeheersing | Openbare orde, zoals crisismanagement | Volledig soeverein, strikt gecontroleerd |

| Niveau | Naam                      | Beschrijving                                                           | Bijpassend GEM-MA-domein                 | Toegestane cloud               |
|--------|---------------------------|------------------------------------------------------------------------|------------------------------------------|--------------------------------|
| S2     | Soevereine overheidscloud | Gegevens met hoge vertrouwelijkheid (persoonsgegevens, sociale domein) | Sociaal domein, zoals jeugdzorg en Wmo   | EU-overheidscloud              |
| S3     | EU/NL cloud met eisen     | Bedrijfsvoering, generieke processen                                   | Bedrijfsvoering, zoals HR en financiën   | EU-cloud met aanvullende eisen |
| S4     | Marktcoud (hyperscaler)   | Algemene applicaties, lage gevoeligheid                                | Generieke tools, zoals publieke websites | Commerciële cloud toegestaan   |

#### 4.5 Bepaal de EMVI-criteria

Bepaal de EMVI-criteria aan de hand van het spreadsheet 'PvE en EMVI gemeentelijke cloud'.

Hanteer een weging langs volgende tabel.

| BBN  | Belangrijkste EMVI                       |
|------|------------------------------------------|
| BBN1 | Portabiliteit (R2)                       |
| BBN2 | Continuïteit + Governance (R5/R6)        |
| BBN3 | Continuïteit + Soevereiniteit (R3/R6/R7) |

# 5

## Bijlage:

### Risico's nader toegelicht

#### R1 – Concentratierisico en leveranciersafhankelijkheid

##### **Uitleg risico**

De markt voor clouddiensten wordt gekenmerkt door een hoge mate van concentratie, waarbij een beperkt aantal aanbieders een dominante positie inneemt. Hierdoor ontstaat het risico dat gemeenten afhankelijk worden van één leverancier of één technologisch ecosysteem.

Deze afhankelijkheid kan zich manifesteren op verschillende niveaus:

- technisch (bijvoorbeeld door gebruik van leveranciersspecifieke oplossingen)
- contractueel (zoals exclusiviteitsclausules)
- Organisatorisch (door beperkte alternatieven in de keten)

In sommige cloudmodellen, met name commerciële SaaS-oplossingen, is afhankelijkheid van één leverancier inherent aan het leveringsmodel. In deze gevallen kan het risico niet volledig worden voorkomen, maar dient dit actief te worden beheerst.

##### **Impact van het risico**

Dit risico kan zich manifesteren door technische storingen, economische discontinuïteit of geopolitieke ontwikkelingen, waarbij meerdere gemeentelijke processen gelijktijdig worden geraakt. Dit kan leiden tot grootschalige verstoringen van dienstverlening en een verminderde bestuurlijke handelingsvrijheid.

Dit risico kan leiden tot:

- grootschalige verstoringen in de gemeentelijke dienstverlening bij uitval van een leverancier
- verminderde onderhandelingspositie
- beperkte flexibiliteit bij wijzigingen of uitbreidingen
- keteneffecten (cascade failures) bij verstoringen

Dit beperkt de operationele soevereiniteit en vormt een direct risico voor de continuïteit van gemeentelijke dienstverlening.

##### **Richting voor beheersing**

Gemeenten beperken afhankelijkheden waar mogelijk en nemen gerichte maatregelen wanneer afhankelijkheid niet kan worden voorkomen.

Dit omvat de volgende maatregelen:

- spreiding van leveranciers en systemen
- verkaveling van functionaliteiten en workloads over meerdere omgevingen
- volledig inzicht in ketenafhankelijkheden
- aanvullende waarborgen bij SaaS-oplossingen, inclusief exit-voorzieningen, data-portabiliteit en continuïteitsmaatregelen zoals escrow

### **Effect van de beheersing**

Deze maatregelen verminderen de kans dat verstoringen bij één leverancier leiden tot volledige uitval, versterken de onderhandelingspositie van gemeenten en vergroten de weerbaarheid van digitale infrastructuren.

## **R2 – Technologische lock-in en beperkte verplaatsbaarheid**

### **Uitleg risico**

Technologische lock-in ontstaat wanneer systemen, data en processen afhankelijk worden van specifieke leveranciers of technologieën, bijvoorbeeld door gebruik van propriëtaire standaarden of gesloten ecosystemen.

Hierdoor wordt het moeilijk of kostbaar om:

- systemen te migreren
- data te hergebruiken
- over te stappen naar alternatieve oplossingen

### **Impact van het risico**

Lock-in leidt tot:

- hoge migratiekosten
- beperkte flexibiliteit
- afhankelijkheid van de roadmap van de leverancier
- belemmering van innovatie

Dit beperkt de technische soevereiniteit en ondermijnt de mogelijkheid tot strategische sturing.

### **Richting voor beheersing**

Gemeenten treffen maatregelen die portabiliteit en reproduceerbaarheid waarborgen.

Dit omvat de volgende maatregelen:

- toepassing van open en gedocumenteerde standaarden
- volledige exporteerbaarheid van data, inclusief metadata
- toegang tot alle relevante technische artefacten en configuraties
- contractueel geborgde exit- en migratievoorzieningen
- toepassing van Infrastructure as Code voor reproduceerbaarheid van omgevingen
- scheiding van data en applicatie, met name bij SaaS-oplossingen

### **Effect van de beheersing**

Deze maatregelen waarborgen dat systemen en data verplaatsbaar blijven, verlagen migratiedrempels en versterken de flexibiliteit en strategische wendbaarheid van gemeenten.

## **R3 – Afhankelijkheid van niet Europese jurisdicties en digitale infrastructuur**

### **Uitleg risico**

Clouddiensten worden vaak geleverd door aanbieders die onderworpen zijn aan niet Europese wet- en regelgeving. Hierdoor kan toegang tot data of systemen worden gevorderd door externe partijen, waaronder statelijke actoren.



Daarnaast ontstaat een bredere afhankelijkheid van niet Europese digitale infrastructuur, wat de autonomie en handelingsvrijheid van gemeenten kan beperken.

#### **Impact van het risico**

Dit risico kan leiden tot:

- verlies van controle over data
- juridische onzekerheid
- aantasting van vertrouwelijkheid
- geopolitieke afhankelijkheid

Dit raakt zowel de juridische als strategische soevereiniteit van gemeenten.

#### **Richting voor beheersing**

Gemeenten treffen maatregelen gericht op het waarborgen van controle over data en infrastructuur.

Dit omvat de volgende maatregelen:

- borging van EU/EER-jurisdictie
- transparantie in eigendom en governance-structuren
- contractuele borging van data-eigendom
- verplichting tot juridisch betwisten van datavorderingen
- toepassing van het principe "EU-by-design"
- beperking van inzet van niet Europese leveranciers

#### **Effect van de beheersing**

Deze maatregelen verminderen juridische en geopolitieke risico's en vergroten de zekerheid dat data en systemen onder Europese controle blijven.

## **R4 – Structurele afhankelijkheid door beperkte beschikbaarheid van Europese alternatieven**

#### **Uitleg risico**

De beschikbaarheid van volwaardige Europese cloudoplossingen is beperkt. Hierdoor ontstaat structurele afhankelijkheid van niet Europese aanbieders, ook wanneer dit beleidsmatig onwenselijk is.

#### **Impact van het risico**

Dit leidt tot:

- langdurige afhankelijkheid van mondiale aanbieders
- beperkte beleidsvrijheid
- vertraging in de transitie naar Europese oplossingen

#### **Richting voor beheersing**

Gemeenten sturen actief op het verkleinen van deze afhankelijkheid.

Dit omvat de volgende maatregelen:

- het opstellen en hanteren van concrete migratiepaden naar Europese oplossingen
- het expliciet tijdelijk maken van niet Europese oplossingen
- het contractueel en technisch borgen van flexibiliteit en overstapmogelijkheden
- het actief monitoren van de markt op beschikbare Europese alternatieven

### **Effect van de beheersing**

Deze maatregelen zorgen ervoor dat afhankelijkheid niet alleen wordt beheerst, maar ook structureel wordt verminderd en dat gemeenten kunnen toewerken naar een meer soevereine digitale infrastructuur.

## **R5 – Onvoldoende functiescheiding en afhankelijkheid in governance**

### **Uitleg risico**

Wanneer leveranciers verantwoordelijk zijn voor zowel levering, beheer als controle van systemen, ontstaat onvoldoende functiescheiding tussen sturing, uitvoering en toezicht. Dit geldt in versterkte mate wanneer leveranciers de control-plane beheren.

### **Impact van het risico**

Dit kan leiden tot:

- beperkte transparantie
- verminderde controle
- belangenverstrengeling
- afhankelijkheid bij operationeel beheer

Dit raakt direct de bestuurlijke controle en operationele soevereiniteit.

### **Richting voor beheersing**

Gemeenten borgen functiescheiding en onafhankelijke controle.

Dit omvat de volgende maatregelen:

- scheiding van sturing, uitvoering en toezicht (functiescheiding)
- onafhankelijk audit- en toezichtrecht
- volledige transparantie in logging en operationele processen
- mogelijkheid tot onafhankelijk beheer, inclusief scheiding van de control-plane

### **Effect van de beheersing**

Deze maatregelen versterken de bestuurlijke controle, vergroten transparantie en maken het mogelijk om onafhankelijk toezicht en sturing uit te oefenen.

## **R6 – Onvoldoende operationele continuïteit bij verstoringen**

### **Uitleg risico**

Digitale infrastructuren kunnen worden verstoord door technische storingen, cyberincidenten of geopolitieke ontwikkelingen. Zonder adequate maatregelen kan dit leiden tot uitval van dienstverlening.

### **Impact van het risico**

Dit kan leiden tot:

- stilstand van dienstverlening
- maatschappelijke ontwrichting
- verlies van vertrouwen

### **Richting voor beheersing**

Gemeenten treffen maatregelen gericht op het waarborgen van continuïteit.

Dit omvat de volgende maatregelen:

- geo-redundantie en topografische spreiding van systemen
- inrichting van uitwijkscenario's en failovermechanismen
- periodieke tests van herstelprocedures
- inzet van parallelle multi-stack architecturen voor kritieke systemen
- inrichting van duidelijke crisis- en escalatieprocedures

### **Effect van de beheersing**

Deze maatregelen vergroten de weerbaarheid tegen verstoringen en zorgen ervoor dat dienstverlening kan worden voortgezet, ook bij uitval van systemen of leveranciers.

## **R7 – Onvoldoende borging van databeschikbaarheid en herstel**

### **Uitleg risico**

Wanneer dataherstel afhankelijk is van één leverancier of onvoldoende is ingericht, bestaat het risico dat data niet tijdig of volledig kan worden hersteld. Daarnaast kan onvoldoende scheiding van data leiden tot grootschalige impact bij incidenten.

### **Impact van het risico**

Dit kan leiden tot:

- dataverlies
- langdurige verstoringen
- integriteitsproblemen
- grootschalige impact bij datacompromittering

### **Richting voor beheersing**

Gemeenten borgen dat data beschikbaar en herstelbaar blijft.

Dit omvat de volgende maatregelen:

- toepassing van multi-backupstrategieën
- scheiding van back-up- en productieomgevingen
- scheiding van datasets (data shattering)
- inrichting van onafhankelijke herstelmogelijkheden
- periodieke tests van herstelprocedures
- aantoonbaar herstel van data buiten de oorspronkelijke leverancieromgeving

# 6

## Bijlage:

# Beheersingsmaatregelen

## nader toegelicht

In dit hoofdstuk worden de beheersmaatregelen nader toegelicht. De toelichting beschrijft de praktische invulling van de maatregel, terwijl de onderbouwing inzicht geeft in de bijdrage aan het beheersen van de geïdentificeerde risico's.

### 6.1 Cluster 1 – Afhankelijkheid en marktstructuur

#### G01 – Beperking leveranciersafhankelijkheid

##### Toelichting

Gemeenten voorkomen afhankelijkheid van één leverancier waar mogelijk door het inzetten van multi-vendor strategieën. Dit betekent dat meerdere cloudleveranciers gelijktijdig worden gecontracteerd en ingezet. Hierdoor ontstaat de mogelijkheid om bij uitval, prestatieproblemen of contractuele beperkingen direct over te schakelen naar een alternatieve leverancier zonder herontwerp van de dienstverlening.

Hierbij geldt dat leveranciers:

- onafhankelijk opereren (geen gedeelde moederorganisatie)
- geen kritieke componenten delen, zoals control-plane of identityvoorzieningen

Indien afhankelijkheid inherent is aan de gekozen oplossing, met name bij SaaS, worden aanvullende maatregelen getroffen die deze afhankelijkheid mitigeren.

##### Onderbouwing

Leveranciersafhankelijkheid beperkt de handelingsvrijheid en vergroot risico's bij faillissement, prijsstijgingen of geopolitieke ontwikkelingen. Door leveranciers onafhankelijk naast elkaar in te zetten, wordt het risico van single points of failure verminderd. Bij SaaS-oplossingen is afhankelijkheid vaak onvermijdelijk, waardoor mitigatie via exit-, data- en continuïteitsmaatregelen noodzakelijk is.

## **G02 – Multi-provider inzet**

### **Toelichting**

Cloudoplossingen worden zodanig ontworpen dat kritieke workloads en gegevens worden verdeeld over minimaal twee cloudproviders en, waar relevant, meerdere technologiestacks (bijvoorbeeld CPU-architectuur of Kubernetes-distributie).

### **Onderbouwing**

Multi-provider gebruik reduceert concentratierisico en voorkomt dat uitval van één leverancier of compromittering van één technologiestack leidt tot volledige uitval van dienstverlening.

## **G03 – Inzicht in ketenafhankelijkheden**

### **Toelichting**

Leveranciers verschaffen volledig inzicht in onderliggende infrastructuur, subleveranciers en afhankelijkheden in de keten. Dit omvat expliciet inzicht in mogelijke concentraties van kritieke componenten, zoals hardware, firmware, software of geografische locaties.

### **Onderbouwing**

Zonder keteninzicht blijven verborgen concentratierisico's bestaan, bijvoorbeeld wanneer meerdere leveranciers feitelijk dezelfde infrastructuur gebruiken. Transparantie maakt het mogelijk deze afhankelijkheden actief te mitigeren.

## **G04 – Spreiding van kritieke workloads**

### **Toelichting**

Kritieke systemen en workloads worden verdeeld over meerdere omgevingen en leveranciers, zonder contractuele beperkingen op gecombineerde inzet.

### **Onderbouwing**

Spreiding voorkomt dat één incident – technisch, organisatorisch of contractueel – alle dienstverlening simultaan raakt en draagt daarmee direct bij aan de continuïteit.

## **G05 – Verkaveling van systemen en leveranciers**

### **Toelichting**

Kritieke functionaliteit en data worden opgesplitst over minimaal twee logisch en organisatorisch gescheiden omgevingen of leveranciers.

### **Onderbouwing**

Verkaveling voorkomt cascade failures, waarbij een verstoring zich door de gehele keten verspreidt, en verhoogt de weerbaarheid tegen storingen en cyberaanvallen.

## **6.2 Cluster 2 – Portabiliteit en lock-in**

## **G06 – Gebruik van open standaarden**

### **Toelichting**

Digitale voorzieningen worden ingericht op basis van open en breed gedragen standaarden voor data, interfaces en integraties.

### **Onderbouwing**

Open standaarden maken interoperabiliteit en migratie mogelijk en beperken afhankelijkheid van leveranciersspecifieke technologieën.

## **G07 – Volledige data-export inclusief metadata**

### **Toelichting**

Alle data, inclusief metadata, datamodellen en configuraties, is volledig exporteerbaar in open en gedocumenteerde formaten.

### **Onderbouwing**

Zonder volledige exporteerbaarheid blijft migratie afhankelijk van leveranciers en is feitelijke overdraagbaarheid niet mogelijk.

## **G08 – Toegang tot data en technische artefacten**

### **Toelichting**

Gemeenten behouden toegang tot alle technische artefacten, waaronder Infrastructure-as-Code, CI/CD-configuraties, scripts, container images en documentatie.

**Onderbouwing**

Toegang tot deze artefacten is noodzakelijk om systemen zelfstandig te beheren, te migreren of opnieuw op te bouwen, ook door derden.

**G09 – Contractueel vastgelegde exit- en migratievoorwaarden****Toelichting**

Exit- en migratievoorwaarden worden vooraf contractueel vastgelegd, inclusief ondersteuning van de leverancier.

**Onderbouwing**

Dit voorkomt blokkades bij beëindiging van contracten en waarborgt dat migratie uitvoerbaar blijft.

**G10 – Vendor-agnostische architectuur****Toelichting**

Systemen worden zodanig ontworpen dat zij niet afhankelijk zijn van leveranciersspecifieke componenten.

**Onderbouwing**

Een vendor-agnostische architectuur maakt hervestiging in een andere omgeving mogelijk zonder significante herontwikkeling.

**6.3 Cluster 3 – Juridische soevereiniteit****G11 – EU/EER-jurisdictie of gelijkwaardig beschermingsniveau****Toelichting**

Alle data, dienstverlening, beheeractiviteiten en control-plane componenten vallen onder Europese wetgeving of een gelijkwaardig beschermingsniveau.

**Onderbouwing**

Dit voorkomt ongewenste toegang tot data via niet Europese wetgeving en borgt naleving van Europese normen.

## **G12 – Transparantie eigendomsstructuur en zeggenschap**

### **Toelichting**

Leveranciers verschaffen volledig inzicht in eigendomsstructuren, zeggenschap en relevante juridische entiteiten.

### **Onderbouwing**

Dit maakt inzichtelijk welke juridische regimes van toepassing zijn en voorkomt verborgen afhankelijkheid van niet Europese partijen.

## **G13 – Data-eigendom bij gemeente**

### **Toelichting**

Contractueel wordt vastgelegd dat alle data eigendom blijft van de gemeente, inclusief gebruiksrechten en toegang.

### **Onderbouwing**

Dit waarborgt dat gemeenten volledige zeggenschap behouden over hun data, ongeacht de leverancier.

## **G14 – Verplichting tot juridisch betwisten van datavorderingen**

### **Toelichting**

Leveranciers zijn verplicht externe datavorderingen actief juridisch te betwisten en gemeenten hierover te informeren.

### **Onderbouwing**

Dit verkleint de kans dat data zonder medeweten of controle van de gemeente wordt opgevraagd of verstrekt.

## **G15 – EU-by-design als uitgangspunt**

### **Toelichting**

Europese oplossingen vormen het uitgangspunt bij de inrichting van cloudvoorzieningen en architecturen.

### **Onderbouwing**

Dit versterkt strategische autonomie en vermindert structurele afhankelijkheid van niet Europese infrastructuur.



#### **G16 – Beperking inzet niet Europese leveranciers**

**Toelichting**

Niet Europese leveranciers worden uitsluitend ingezet indien geen volwaardig Europees alternatief beschikbaar is.

**Onderbouwing**

Hiermee wordt structurele afhankelijkheid beperkt en wordt de ontwikkeling van Europese alternatieven gestimuleerd.

### **6.4 Cluster 4 – Toekomstvastheid en migratie**

#### **G17 – Geen contractuele blokkades voor migratie**

**Toelichting**

Contracten bevatten geen bepalingen die migratie, overstap of beëindiging belemmeren.

**Onderbouwing**

Dit voorkomt langdurige afhankelijkheid en waarborgt flexibiliteit in de toekomst.

#### **G18 – Recht op periodieke heroverweging**

**Toelichting**

Gemeenten behouden het recht om dienstverlening periodiek te evalueren en te heroverwegen.

**Onderbouwing**

Dit ondersteunt strategische sturing en voorkomt langdurige contractuele lock-in.

#### **G19 – Ondersteuning bij toetsing alternatieven**

**Toelichting**

Leveranciers ondersteunen gemeenten bij het evalueren en testen van alternatieve oplossingen.

**Onderbouwing**

Dit maakt een realistische vergelijking mogelijk en voorkomt afhankelijkheid door informatiegebrek.

## **G20 – Verplicht en toetsbaar migratieplan**

### **Toelichting**

Voor oplossingen met afhankelijkheidsrisico's is een concreet en toetsbaar migratieplan beschikbaar.

### **Onderbouwing**

Dit maakt toekomstige overstap uitvoerbaar en voorkomt dat afhankelijkheid structureel wordt.

## **G21 – Tijdelijkheid niet Europese oplossingen**

### **Toelichting**

Gebruik van niet Europese oplossingen wordt expliciet als tijdelijk aangemerkt.

### **Onderbouwing**

Dit dwingt tot actieve afbouw van afhankelijkheid en voorkomt permanente lock-in.

## **6.5 Cluster 5 – Governance en functiescheiding**

## **G22 – Onafhankelijk audit- en toezichtrecht**

### **Toelichting**

Gemeenten verkrijgen het recht om audits uit te laten voeren door onafhankelijke partijen.

### **Onderbouwing**

Dit waarborgt objectieve toetsing van dienstverlening en beveiliging.

## **G23 – Transparantie in logging en processen**

### **Toelichting**

Leveranciers bieden volledige inzage in logging, prestaties en operationele processen.

### **Onderbouwing**

Transparantie is noodzakelijk voor toezicht, controle en incidentanalyse.

## **G24 – Geen beperkingen op toezicht**

### **Toelichting**

Contracten bevatten geen beperkingen die toezicht of controle door gemeenten belemmeren.

### **Onderbouwing**

Dit voorkomt afhankelijkheid en waarborgt bestuurlijke controle.

## **G25 – Scheiding control-plane en uitvoering**

### **Toelichting**

Beheer van cloudvoorzieningen wordt zodanig ingericht dat gemeenten of onafhankelijke derden essentiële beheertaken kunnen uitvoeren zonder exclusieve afhankelijkheid van de leverancier.

### **Onderbouwing**

Dit voorkomt volledige afhankelijkheid van leveranciers voor operationeel beheer en maakt onafhankelijk toezicht en sturing mogelijk.

## **6.6 Cluster 6 – Continuïteit**

## **G26 – Contractuele borging continuïteit en incidentrespons**

### **Toelichting**

Continuïteit en incidentrespons worden expliciet contractueel vastgelegd.

### **Onderbouwing**

Dit waarborgt dat leveranciers verantwoordelijk zijn voor het leveren van afgesproken beschikbaarheids- en herstelniveaus.

## **G27 – Periodieke tests van herstel- en uitwijkscenario's**

### **Toelichting**

Herstel- en uitwijkprocedures worden periodiek getest.

### **Onderbouwing**

Dit valideert de werking van continuïteitsmaatregelen en voorkomt schijnzekerheid.

## **G28 – Verplichte informatievoorziening bij verstoringen**

### **Toelichting**

Leveranciers zijn verplicht gemeenten tijdig en volledig te informeren bij verstoringen.

### **Onderbouwing**

Dit maakt snelle en effectieve besluitvorming mogelijk tijdens incidenten.

## **G29 – Geo-redundantie**

### **Toelichting**

Systemen worden verdeeld over meerdere geografische locaties en datacenters.

### **Onderbouwing**

Dit beschermt tegen uitval van één locatie of regio.

## **G30 – Topografische spreiding**

### **Toelichting**

Systemen worden verspreid over geografisch gescheiden regio's binnen de EU.

### **Onderbouwing**

Dit verkleint de impact van grootschalige verstoringen zoals geopolitieke gebeurtenissen of infrastructuurstoringen.

## **G31 – Crisis- en escalatieprocedures**

### **Toelichting**

Er zijn duidelijke en geteste procedures voor incidentrespons en escalatie.

### **Onderbouwing**

Dit zorgt voor snelle en gecontroleerde reactie bij verstoringen en beperkt de impact van incidenten.

## 6.7 Cluster 7 – Dataherstel en databeschikbaarheid

### G32 – Inzicht in back-up- en herstelprocessen

**Toelichting**

Gemeenten krijgen volledig inzicht in back-up- en herstelprocessen.

**Onderbouwing**

Dit maakt controle en toetsing van herstelmogelijkheden mogelijk.

### G33 – Geen afhankelijkheid van één leverancier voor herstel

**Toelichting**

Herstel van data is niet afhankelijk van één leverancier of platform.

**Onderbouwing**

Dit voorkomt dat herstel onmogelijk wordt bij uitval van een leverancier.

### G34 – Scheiding van back-up- en productieomgeving

**Toelichting**

Back-upomgevingen zijn logisch en organisatorisch gescheiden van productieomgevingen.

**Onderbouwing**

Dit voorkomt dat incidenten in productie ook back-ups raken.

### G35 – Aantoonbaar geteste herstelprocedures

**Toelichting**

Herstel- en uitwijkprocedures worden periodiek getest en gevalideerd.

**Onderbouwing**

Niet-geteste back-ups geven schijnzekerheid en vergroten het risico op falend herstel.

### **G36 – Data shattering**

**Toelichting**

Data wordt logisch en/of fysiek gescheiden opgeslagen over meerdere omgevingen.

**Onderbouwing**

Dit beperkt de impact van datalekken, cyberaanvallen en systeemfalen.

### **G37 – Onafhankelijke restore mogelijkheid**

**Toelichting**

Data kan worden hersteld zonder afhankelijkheid van de oorspronkelijke leverancier.

**Onderbouwing**

Dit voorkomt afhankelijkheid bij incidenten en vergroot de herstelbaarheid.

### **G38 – Aantoonbaar herstel buiten leverancier**

**Toelichting**

Herstel wordt aantoonbaar getest buiten de primaire leverancieromgeving.

**Onderbouwing**

Dit toont aan dat onafhankelijk herstel daadwerkelijk uitvoerbaar is.

## **6.8 SaaS-specifiek**

### **S01 – Scheiding data en applicatie**

**Toelichting**

Data is logisch gescheiden van applicatielogica en zelfstandig beschikbaar.

**Onderbouwing**

Dit voorkomt lock-in en maakt hergebruik en migratie mogelijk.

## **S02 – Volledige data-export inclusief metadata**

### **Toelichting**

SaaS-oplossingen faciliteren volledige export van data, inclusief metadata, in open formaten.

### **Onderbouwing**

Dit maakt migratie en hergebruik buiten de applicatie mogelijk.

## **S03 – Datamobiliteit zonder applicatie-afhankelijkheid**

### **Toelichting**

Data is zelfstandig bruikbaar zonder afhankelijkheid van de oorspronkelijke SaaS-applicatie.

### **Onderbouwing**

Dit voorkomt lock-in op applicatieniveau.

## **S04 – Transparantie subverwerkers**

### **Toelichting**

Leveranciers geven volledig inzicht in subverwerkers.

### **Onderbouwing**

Dit maakt ketenrisico's inzichtelijk.

## **S05 – Toegangsbeperking leverancier**

### **Toelichting**

Toegang van leveranciers tot data wordt beperkt en gecontroleerd.

### **Onderbouwing**

Dit verkleint risico op ongeautoriseerde toegang.

## **S06 – Meldplicht wijziging subverwerkers**

### **Toelichting**

Wijzigingen in subverwerkers worden vooraf gemeld.

### **Onderbouwing**

Dit voorkomt onverwachte risico's.

## **S07 – Continuïteit bij beëindiging**

### **Toelichting**

Leveranciers ondersteunen continuïteit bij beëindiging.

### **Onderbouwing**

Dit maakt gecontroleerde overgang mogelijk.

## **S08 – Toegang tijdens migratie**

### **Toelichting**

Gemeenten behouden toegang tot systemen tijdens migratie.

### **Onderbouwing**

Dit voorkomt dat migratie wordt belemmerd.

## **S09 – Lifecycle en roadmap transparantie**

### **Toelichting**

Leveranciers geven inzicht in lifecycle en productontwikkeling.

### **Onderbouwing**

Dit ondersteunt strategische planning en migratie.



## **S10 – Continuïteit bij faillissement**

### **Toelichting**

Continuïteitsvoorzieningen zoals escrow-regelingen worden ingericht voor SaaS-oplossingen.

### **Onderbouwing**

Dit waarborgt voortzetting van dienstverlening bij uitval van de leverancier.

## **6.9 PaaS/IaaS-specifiek**

### **P01 – Infrastructure as Code**

#### **Toelichting**

Infrastructuur wordt volledig vastgelegd in code en is reproduceerbaar en overdraagbaar.

#### **Onderbouwing**

Dit is een essentiële randvoorwaarde voor portabiliteit en herbouwbaarheid van systemen.

### **P02 – Volledige configuratietoegang**

#### **Toelichting**

Gemeenten hebben toegang tot alle configuraties van infrastructuur en platform.

#### **Onderbouwing**

Dit maakt onafhankelijk beheer en migratie mogelijk.

### **P03 – Reproduceerbare omgevingen**

#### **Toelichting**

Omgevingen zijn volledig reproduceerbaar.

#### **Onderbouwing**

Dit ondersteunt portabiliteit en herstel.

#### **P04 – Control-plane binnen EU**

**Toelichting**

Control-plane componenten bevinden zich binnen de EU.

**Onderbouwing**

Dit voorkomt externe juridische beïnvloeding.

#### **P05 – Onafhankelijk beheer mogelijk**

**Toelichting**

Beheer kan door derden of de gemeente zelf worden uitgevoerd.

**Onderbouwing**

Dit voorkomt afhankelijkheid van leveranciers.

#### **P06 – Logging en monitoring**

**Toelichting**

Volledige logging en monitoring zijn beschikbaar voor gemeenten.

**Onderbouwing**

Dit maakt toezicht en analyse mogelijk.

#### **P07 – Geo-redundantie**

**Toelichting**

Infrastructuur is over meerdere locaties verdeeld.

**Onderbouwing**

Dit borgt continuïteit.

## **P08 – Periodieke hersteltests**

### **Toelichting**

Herstelprocedures worden regelmatig getest.

### **Onderbouwing**

Dit voorkomt falend herstel.

## **P09 – Onafhankelijk herstel mogelijk**

### **Toelichting**

Herstel kan onafhankelijk van leverancier plaatsvinden.

### **Onderbouwing**

Dit vergroot weerbaarheid.

## **P10 – Transparantie infrastructuur**

### **Toelichting**

Gemeenten krijgen inzicht in de onderliggende infrastructuur.

### **Onderbouwing**

Dit maakt afhankelijkheden zichtbaar en beheersbaar.

## **P11 – Parallele multi-stack inzet (continuïteit en uitwijkbaarheid)**

### **Toelichting**

Workloads worden gelijktijdig operationeel gehouden op meerdere technologiestacks, afgestemd op het vereiste beveiligingsniveau.

### **Onderbouwing**

Dit voorkomt downtime doordat direct kan worden overgeschakeld bij uitval van één stack zonder herconfiguratie of herbouw.

# 7

## Bijlage: BBN beveiligingsniveau's

In dit hoofdstuk worden BBN-niveau's nader toegelicht. De toelichting beschrijft de risico's waarop focus ligt in het betreffende beveiligingsniveau, de kenmerken van de beveiligingsoplossing en de vereiste, respectievelijk gewenste cloud-beheersmaatregelen die van toepassing zijn op het betreffende beveiligingsniveau.

### BBN1 – Laag (beperkt kritisch)

Voor BBN1-workloads wordt geborgd dat overstapmogelijkheden bestaan, zonder dat directe redundantie noodzakelijk is.

| Focus                                                                                                                                                                                                                                                                                                                                                                                                                                 | Kenmerken                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>De focus ligt op:</p> <ul style="list-style-type: none"><li>• operationele continuïteit (R6)</li><li>• herstelbaarheid van data (R7)</li></ul> <p>Daarnaast wordt basis portabiliteit geborgd zodat:</p> <ul style="list-style-type: none"><li>• toekomstige migratie mogelijk blijft (R2, R4 – nevengeschiedt)</li><li>• geen onomkeerbare afhankelijkheid ontstaat (R5)</li></ul> <p>Jurisdictie (R3) speelt beperkt een rol</p> | <p>Een tweede stack hoeft niet actief te draaien, maar dient wel beschikbaar en startbaar te zijn.</p> <p>Gebruik van niet-EU oplossingen is acceptabel, mits:</p> <ul style="list-style-type: none"><li>• geen gevoelige data wordt verwerkt</li><li>• geen kritisch proces wordt ondersteund</li></ul> |

#### Verplichte beheersmaatregelen (conform matrix – R6, R7)

- contractuele borging continuïteit en incidentrespons (G26–G31)
- back-up en herstel ingericht en aantoonbaar getest (G32–G38)

#### Gewenst beheersmaatregelen (ondersteunend voor R1, R2, R4, R5)

- data exporteerbaar (G07)
- basis exit-strategie aanwezig (G09)
- Infrastructure as Code voorbereid (P01)
- eenvoudige migratiemogelijkheid naar alternatieve omgeving
- alternatieve omgeving voorbereid (cold/warm standby)

#### 4.3.2. BBN2 – Middel (bedrijfskritisch)

Voor BBN2-workloads wordt een tweede technologiystack ingericht die is getest en binnen vooraf bepaalde tijd activeerbaar is.

| Focus                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Kenmerken                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>De focus ligt op:</p> <ul style="list-style-type: none"><li>• continuïteit van dienstverlening (R6)</li><li>• herstelbaarheid van data en systemen (R7)</li><li>• vermijden van concentratie (R1) en lock-in (R2)</li><li>• beheersing van afhankelijkheden van non-EU (R4) en in governance (R5)</li></ul> <p>Daarnaast wordt basis portabiliteit geborgd zodat:</p> <ul style="list-style-type: none"><li>• overstap mogelijk is zonder herontwerp</li><li>• afhankelijkheid van één leverancier wordt beperkt</li><li>• governance en controle behouden blijven</li></ul> <p>Nevengeschiedt wordt rekening gehouden met:</p> <ul style="list-style-type: none"><li>• jurisdictierisico's (R3), door beheersing en mitigatie</li></ul> | <p>Tweede stack is technisch ingericht, wordt periodiek getest, maar is niet permanent actief.</p> <p>Overstap naar andere stack vereist geen herontwerp en kan beperkte downtime bevatten.</p> <p>Gebruik van non-EU oplossingen is alleen toegestaan indien beheerst en gemitigeerd en met aantoonbaar migratiepad richting EU.</p> |

#### Verplicht beheersmaatregelen (volledige dekking primaire risico's)

##### **Architectuur en afhankelijkheden (R1, R2, R4)**

- multi-stack voorbereid en inzetbaar (P11)
- reproduceerbare omgevingen (P01–P03)
- gebruik van open standaarden (G06)
- volledige data-export en toegang (G07, G08)
- contractueel geborgde exit en migratie (G09, G17–G21)
- spreiding van workloads en leveranciers (G01–G05)

##### **Governance (R5)**

- transparantie in logging en processen (G23)
- geen beperkingen op toezicht (G24)
- scheiding control-plane en uitvoering (G25)

##### **Continuïteit (R6)**

- warm standby omgeving
- geo-redundantie (G29, P07)
- periodieke failover-tests (G27, P08)
- contractuele incidentrespons (G26, G31)
- continuïteit bij beëindiging (S07, S08, S10)

##### **Dataherstel (R7)**

- aantoonbaar geteste herstelprocedures (G35)

- scheiding back-up en productie (G34)
- geen afhankelijkheid van één partij voor herstel (G33)
- inzicht in back-upketen (G32)
- onafhankelijk herstel mogelijk (P09)

#### ***SaaS/PaaS invulling***

- datamobilititeit en scheiding data/applicatie (S01–S03)
- configuratie- en infrastructuurcontrole (P01–P03)

#### ***Gewenste beheersmaatregelen (jurisdictie – R3)***

- EU/EER positionering of gelijkwaardig (G11)
- transparantie eigendom en subverwerkers (G12, S04–S06)
- data-eigendom expliciet vastgelegd (G13)
- mitigatie buitenlandse toegang (G14–G16)
- control-plane in EU (P04)
- onafhankelijk beheer en logging-uitbreiding (P05, P06)

### **4.3.3. BBN3 – Hoog (maatschappelijk kritisch)**

Voor BBN3-workloads worden meerdere technologiestacks gelijktijdig actief gehouden, zodat:

- directe omschakeling mogelijk is
- geen dataverlies optreedt
- geen herconfiguratie nodig is

| Focus                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Kenmerken                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>De focus ligt op:</p> <ul style="list-style-type: none"> <li>• ononderbroken continuïteit (R6)</li> <li>• volledige herstelzekerheid zonder dataverlies (R7)</li> <li>• strategische autonomie en onafhankelijkheid (R1, R2, R4, R5)</li> <li>• juridische en geopolitieke beheersing (R3)</li> </ul> <p>Daarbij wordt geborgd dat:</p> <ul style="list-style-type: none"> <li>• geen single point of failure bestaat</li> <li>• geen afhankelijkheid van één leverancier of ecosysteem ontstaat</li> <li>• volledige controle over data, processen en infrastructuur behouden blijft</li> </ul> | <ul style="list-style-type: none"> <li>• active-active of hot standby</li> <li>• real-time synchronisatie</li> <li>• automatische failover</li> <li>• geen herconfiguratie bij uitval</li> </ul> <p>Geen afhankelijkheid van:</p> <ul style="list-style-type: none"> <li>• dezelfde leverancier (R1)</li> <li>• dezelfde control-plane (R5)</li> <li>• niet-EU jurisdicties (R3)</li> </ul> <p>Gebruik van non-EU oplossingen is niet toegestaan.</p> |

#### **Verplichte beheersmaatregelen:**

##### ***Architectuur en afhankelijkheden (R1, R2, R4)***

- parallel draaiende multi-cloud / multi-vendor omgevingen (G02, G04, G05, P11)
- vendor-agnostische architectuur en open standaarden (G06, G10)
- volledige data- en configuratieportabiliteit (G07, G08, P02, P03)
- contractueel afdwingbare exit- en migratievoorwaarden (G09, G17–G21)

#### ***Juridictie en soevereiniteit (R3)***

- verwerking binnen EU/EER of gelijkwaardig beschermingsniveau (G11, P04)
- volledige transparantie over eigendom en subverwerkers (G12, S04–S06)
- data-eigendom expliciet bij de organisatie (G13)
- maatregelen tegen ongewenste buitenlandse toegang (G14, G15, G16)

#### ***Governance en controle (R5)***

- scheiding tussen control-plane en uitvoering (G25)
- onafhankelijk beheer en toezicht mogelijk (G22, P05)
- volledige transparantie in logging en processen (G23, P06)
- geen beperkingen op audit en toezicht (G24)

#### ***Continuïteit (R6)***

- active-active of hot standby architectuur
- geo-redundantie en topografische spreiding (G29, G30, P07)
- automatische failover zonder handmatige interventie
- periodieke en aantoonbare failover-tests (G27, P08)
- contractueel geborgde incidentrespons en escalatie (G26, G31)
- continuïteit bij beëindiging en migratie (S07, S08, S10)

#### ***Dataherstel en robuustheid (R7)***

- real-time replicatie en data shattering (G36)
- volledige scheiding van back-up en productie (G34)
- onafhankelijke restore-mogelijkheid buiten leverancier (G37, G38, P09)
- aantoonbaar geteste herstelprocedures (G35)
- geen afhankelijkheid van één partij voor herstel (G33)
- volledig inzicht in back-upketen (G32)

#### ***SaaS-specifiek (indien van toepassing)***

- scheiding tussen data en applicatie (S01)
- volledige datamobiliteit zonder afhankelijkheid (S02, S03)
- transparantie in lifecycle en roadmap (S09)

# 8

## Bijlage:

### Soevereiniteitsniveaus

### GEMMA

In dit hoofdstuk worden de soevereiniteitsniveaus uit de GEMMA nader toegelicht. De toelichting beschrijft per niveau het toepassingsgebied in termen van GEMMA-domeinen, de soevereiniteitseisen en de relatie naar de cloud-beheersmaatregelen.

#### S1 – Hoog geclassificeerd

**Toepassing:**

- Openbare orde en veiligheid
- crisismanagement
- kritieke infrastructuurbesturing

**Eisen:**

- volledige operationele controle bij overheid
- geen afhankelijkheid van externe control planes
- hardware, software en beheer binnen EU / nationale controle
- maximale isolatie van externe invloeden

**Relatie met risico's:**

- R3 (jurisdictie): volledig geëlimineerd
- R6 (continuïteit): maximale waarborgen
- R7 (dataherstel): volledig autonoom herstel

#### S2 – Soevereine overheidscloud

**Toepassing:**

- sociaal domein
- burgerzaken
- persoonsgegevens (hoog vertrouwelijk)

**Eisen:**

- verwerking volledig binnen EU/EER
- juridische afscherming tegen extraterritoriale claims
- encryptiesleutels onder gemeentelijke controle



- transparantie in supply chain

**Relatie met risico's:**

- R3: sterk beperkt
- R2: migratie moet mogelijk blijven
- R5: strikte governance

### S3 – EU/NL cloud met eisen

**Toepassing:**

- bedrijfsvoering (ERP, HR)
- generieke gemeentelijke processen
- samenwerkingstools

**Eisen:**

- datalokatie binnen EU
- contractuele bescherming (GIBIT)
- exit-strategie verplicht
- open standaarden aanbevolen

**Relatie met risico's:**

- R1: spreiding verplicht
- R2: beperken lock-in
- R4: migratiepad EU

### S4 – Marktccloud (hyperscaler)

**Toepassing:**

- niet-kritieke applicaties
- publieke informatie
- standaard SaaS

**Eisen:**

- minimale compliance (AVG, BIO)
- transparantie leverancier
- exit-mogelijkheid (basis)

**Relatie met risico's:**

- R1: toegestaan maar monitoren
- R3: expliciet risico accepteren
- R4: tijdelijk gebruik

# 9

## Bijlage:

### Begrippenlijst

| Term                                                  | Betekenis                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Afhankelijkheid (leveranciers-afhankelijkheid)</b> | De mate waarin een organisatie afhankelijk is van één leverancier, technologie of ecosysteem voor het functioneren van systemen of dienstverlening. Deze afhankelijkheid kan technisch, contractueel of organisatorisch van aard zijn.                                                                                                                                                                                                                                                                                                                       |
| <b>Autonomie (digitale autonomie)</b>                 | Mate van bestuurlijke en operationele handelingsvrijheid zodat gemeenten hun digitale infrastructuur zelfstandig beheren en keuzes kunnen maken.                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>BBN</b>                                            | De Basisbeveiligingsniveaus (BBN) bepalen de vereiste set aan beveiligingsmaatregelen. De hoogste score op een van de BIV-aspecten bepaalt welk BBN-niveau (BBN1, BBN2 of BBN3) van toepassing is op de IT-oplossing die het proces ondersteunt.                                                                                                                                                                                                                                                                                                             |
| <b>Bi-Modal</b>                                       | IT-strategie die uitgaat van twee type IT-systemen:<br>Mode 1 (Regulier): Focus op stabiliteit, continuïteit en maximale soevereiniteit voor kritieke kernprocessen (sociaal domein, burgerzaken, OOV).<br>Mode 2 (Experimenteel): Focus op snelheid en innovatie voor kortcyclische projecten, waarbij tijdelijk gebruik van de Mondiale Stack (Kavel 1B/2B) vaker voorkomt, mits de portabiliteit naar de Europese Stack geborgd blijft.                                                                                                                   |
| <b>BIV-classificatie</b>                              | Methode op de datagevoeligheid én de bedrijfskritiekheid van een bedrijfsproces of IT-oplossing vast te stellen. <ul style="list-style-type: none"> <li>• Beschikbaarheid (B): De mate waarin de dienst of IT-oplossing beschikbaar moet zijn voor gebruikers op de momenten dat zij die nodig hebben.</li> <li>• Integriteit (I): De mate waarin de informatie juist, volledig en actueel moet zijn (ook wel betrouwbaarheid genoemd).</li> <li>• Vertrouwelijkheid (V): De mate waarin informatie beschermd moet worden tegen onbevoegde inzage</li> </ul> |
| <b>Cloudprovider</b>                                  | Een aanbieder van cloudinfrastructuur of -diensten (zoals IaaS, PaaS of SaaS) waarop applicaties en data worden gehost.                                                                                                                                                                                                                                                                                                                                                                                                                                      |

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Control-plane</b>   | <p>De control-plane omvat de beheerlaag van een IT-omgeving waarin configuratie, orchestration, provisioning en aansturing van systemen plaatsvindt.</p> <p>Dit betreft onder andere:</p> <ul style="list-style-type: none"> <li>• beheerinterfaces</li> <li>• API's</li> <li>• orchestration tooling (bijv. Kubernetes control-plane)</li> <li>• identity- en accessmanagement op beheerniveau</li> </ul> <p>De control-plane is essentieel voor het functioneren en beheer van systemen en vormt daarmee een kritisch onderdeel van afhankelijkheids- en governancevraagstukken. Wanneer de control-plane volledig door een leverancier wordt beheerd, ontstaat directe afhankelijkheid voor operationeel beheer.</p>                                                                        |
| <b>Data shattering</b> | <p>Het zodanig opsplitsen van data in meerdere logisch of fysiek gescheiden datasets, zodat compromittering of verlies van één dataset niet leidt tot volledige uitval of dataverlies.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Exit-strategie</b>  | <p>De vooraf vastgelegde aanpak om een leverancier of oplossing gecontroleerd te verlaten, inclusief migratie van data, systemen en processen naar een alternatieve omgeving.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Georedundantie</b>  | <p>Het opslaan en verwerken van data en systemen over meerdere geografische locaties, zodat uitval van één locatie geen impact heeft op de beschikbaarheid.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Haven</b>           | <p>Haven is een door de Vereniging van Nederlandse Gemeenten (VNG) ontwikkelde referentie-architectuur en implementatiestandaard voor cloud-native platformhosting, gebaseerd op Kubernetes.</p> <p>Het doel van Haven is om applicaties op een gestandaardiseerde, overdraagbare en platformonafhankelijke manier te kunnen deployen en beheren, zodat:</p> <ul style="list-style-type: none"> <li>• applicaties tussen cloudomgevingen kunnen worden verplaatst</li> <li>• samenwerking tussen gemeenten wordt bevorderd</li> <li>• afhankelijkheid van specifieke cloudproviders wordt verminderd</li> </ul> <p>Haven beschrijft hoe een platform is ingericht, en is daarmee een architectuurkader, geen techniek.</p> <p>Concreet stelt Haven eisen aan de inrichting van Kubernetes.</p> |

|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>HavenPlus</b>                              | <p>HavenPlus is een uitbreiding op Haven en omvat een set van gestandaardiseerde aanvullende platformdiensten die nodig zijn voor productieklare omgevingen.</p> <p>Deze diensten omvatten onder andere:</p> <ul style="list-style-type: none"> <li>• monitoring en logging</li> <li>• identity &amp; access management</li> <li>• certificaatbeheer</li> <li>• database- en platformdiensten</li> </ul> <p>Deze diensten kunnen ook worden afgenomen bij de cloudaanbieders. Echter, door hiervoor zelf componenten te hosten blijft het geheel onafhankelijk van een specifieke provider (cloud agnostisch) en soeverein.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>IaaS<br/>(Infrastructure as a Service)</b> | <p>Cloudmodel waarbij infrastructuur zoals compute, opslag en netwerken als dienst wordt aangeboden, waarbij de gebruiker controle heeft over de configuratie.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Infrastructure as Code (IaC)</b>           | <p>Methode voor het inrichten en beheren van IT-infrastructuur door middel van machineleesbare configuratiebestanden en scripts, waarmee infrastructuur geautomatiseerd, consistent en reproduceerbaar wordt opgebouwd.</p> <p>In plaats van handmatige configuratie worden alle componenten — zoals netwerk, compute, opslag en platformdiensten — vastgelegd in versiebeheerbare code.</p> <p>Hiermee kunnen omgevingen:</p> <ul style="list-style-type: none"> <li>• volledig opnieuw worden opgebouwd</li> <li>• consistent worden beheerd</li> <li>• worden uitgerold op verschillende cloudplatforms</li> </ul> <p>IaC is een generieke techniek en staat los van specifieke platforms of architecturen.</p> <p>Onderscheid met Haven en HavenPlus</p> <ul style="list-style-type: none"> <li>• IaC = hoe je bouwt (techniek)</li> <li>• Haven = hoe het platform is ontworpen (architectuur)</li> <li>• HavenPlus = welke platformdiensten beschikbaar zijn (invulling)</li> </ul> <p>IaC kan worden gebruikt om Haven- en HavenPlus-omgevingen uit te rollen, maar is daar conceptueel los van.</p> |
| <b>Lock-in</b>                                | <p>De situatie waarin een organisatie niet of alleen tegen hoge kosten kan overstappen naar een andere leverancier of technologie, door afhankelijkheid van propriëtaire standaarden, dataformaten of integraties. De overstap is gemoeid met een complexe juridische en/of technische migratie met lange doorloop en hoge risico's op continuïteitsverstoringen in de uitvoeringsorganisatie van gemeenten.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

|                                     |                                                                                                                                                                                                                                |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Multi-provider strategie</b>     | Het gelijktijdig inzetten van meerdere cloudproviders om risico's van afhankelijkheid en uitval te beperken.                                                                                                                   |
| <b>Multi-stack strategie</b>        | Architectuurprincipe waarbij workloads gelijktijdig operationeel zijn op meerdere technologisch verschillende stacks, zodat bij uitval of compromittering direct kan worden overgeschakeld zonder herconfiguratie of migratie. |
| <b>PaaS (Platform as a Service)</b> | Cloudmodel waarbij een platform wordt aangeboden voor het ontwikkelen en draaien van applicaties, zonder dat de onderliggende infrastructuur door de gebruiker wordt beheerd.                                                  |
| <b>Portabiliteit</b>                | De mate waarin systemen, data en applicaties eenvoudig kunnen worden verplaatst tussen verschillende omgevingen of leveranciers.                                                                                               |
| <b>Reproduceerbaarheid</b>          | Het vermogen om een IT-omgeving volledig opnieuw op te bouwen op basis van configuraties en code, zonder handmatige handelingen.                                                                                               |
| <b>SaaS (Software as a Service)</b> | Cloudmodel waarbij applicaties volledig als dienst worden aangeboden en beheerd door de leverancier, inclusief infrastructuur, platform en software.                                                                           |
| <b>Soevereiniteit</b>               | Mate waarin de kans is verlaagd dat statelijke actoren met offensief cyberprogramma onze bedrijfsvoering plat kunnen leggen of zich ongeautoriseerd toegang verschaffen tot onze data.                                         |
| <b>Technologiestack</b>             | De combinatie van technologieën waarop een systeem draait, zoals: <ul style="list-style-type: none"> <li>• cloudprovider</li> <li>• besturingssysteem</li> <li>• runtime</li> <li>• containerplatform</li> </ul>               |
| <b>Verkaveling</b>                  | Het verdelen van systemen, data en functionaliteiten over meerdere logisch en organisatorisch gescheiden omgevingen of leveranciers om afhankelijkheden en risico's te beperken.                                               |

# 10

## Bijlage PvE Gemeentelijke Cloud

| ID  | Eis/<br>Wens | Toepassings-<br>gebied | Risico | Risico-adressering                                                         | PvE-bepaling                                             | Toelichting                                                                                                                                      | Borging                        | Bewijs               | Aan te leveren bij<br>aanbesteding |
|-----|--------------|------------------------|--------|----------------------------------------------------------------------------|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|----------------------|------------------------------------|
| G01 | Eis          | Algemeen               | R1     | Afhankelijkheid van één leverancier of ecosysteem                          | Beperking leveranciersafhankelijkheid                    | Contractuele bepalingen staan de inzet van andere leveranciers toe en voorkomen afhankelijkheid van één partij.                                  | Contractueel                   | Contract             | Conceptcontract                    |
| G02 | Eis          | Algemeen               | R1     | Afhankelijkheid van één leverancier of ecosysteem                          | Multi-provider inzet                                     | De gemeente kan meerdere leveranciers gelijktijdig inzetten en combineren binnen één oplossing of architectuur.                                  | Contractueel / Architectonisch | Architectuurdocument | Architectuurbeschrijving           |
| G03 | Eis          | Algemeen               | R1     | Afhankelijkheid van één leverancier of ecosysteem                          | Inzicht in ketenafhankelijkheden                         | Leverancier verschaft volledig inzicht in onderliggende infrastructuur, subverwerkers en afhankelijkheden.                                       | Contractueel                   | Ketenoverzicht       | Subverwerkersoverzicht             |
| G04 | Eis          | Algemeen               | R1     | Afhankelijkheid van één leverancier of ecosysteem                          | Spreiding van kritieke workloads                         | Kritieke workloads kunnen technisch worden verdeeld over meerdere omgevingen.                                                                    | Architectonisch                | Architectuurdocument | Architectuurprincipes              |
| G05 | Eis          | Algemeen               | R1     | Afhankelijkheid van één leverancier of ecosysteem                          | Verkaveling van systemen en leveranciers                 | Functionele componenten en data worden verdeeld over meerdere logisch gescheiden omgevingen om afhankelijkheid en cascade failures te voorkomen. | Architectonisch                | Architectuurdocument | Ontwerpbeschrijving                |
| G06 | Eis          | Algemeen               | R2     | Beperkte verplaatsbaarheid van systemen, data en configuraties             | Gebruik van open standaarden                             | Systemen maken gebruik van open standaarden zodat migratie en interoperabiliteit mogelijk blijven.                                               | Technisch                      | Architectuurdocument | Technische beschrijving            |
| G07 | Eis          | Algemeen               | R2     | Beperkte verplaatsbaarheid van systemen, data en configuraties             | Volledige data-export inclusief metadata                 | Data inclusief structuur en metadata is volledig exporteerbaar in open formaat zodat migratie mogelijk blijft.                                   | Technisch                      | Testrapport          | Exportbeschrijving                 |
| G08 | Eis          | Algemeen               | R2     | Beperkte verplaatsbaarheid van systemen, data en configuraties             | Toegang tot data en technische artefacten                | Leverancier garandeert toegang tot configuraties, scripts en technische documentatie zodat systemen opnieuw ingericht kunnen worden.             | Contractueel                   | Contract             | Verklaring toegang                 |
| G09 | Eis          | Algemeen               | R2     | Beperkte verplaatsbaarheid van systemen, data en configuraties             | Contractueel vastgelegde exit- en migratievoorwaarden    | Exit en migratie zijn vooraf contractueel geregeld inclusief ondersteuning door leverancier.                                                     | Contractueel                   | Contract             | Exitplan                           |
| G10 | Eis          | Algemeen               | R2     | Beperkte verplaatsbaarheid van systemen, data en configuraties             | Vendor-agnostische architectuur                          | Oplossing is ontworpen zonder afhankelijkheid van specifieke leverancierscomponenten.                                                            | Architectonisch                | Architectuurdocument | Architectuurtoelichting            |
| G11 | Eis          | Algemeen               | R3     | Afhankelijkheid van niet-Europese jurisdicties en digitale infrastructuren | EU/EER-jurisdictie of gelijkwaardig beschermingsniveau   | Data en dienstverlening vallen onder Europese wetgeving of gelijkwaardige bescherming.                                                           | Contractueel                   | Contract             | Juridische structuur               |
| G12 | Eis          | Algemeen               | R3     | Afhankelijkheid van niet-Europese jurisdicties en digitale infrastructuren | Transparantie eigendomsstructuur en zeggenschap          | Leverancier geeft inzicht in eigendom en governance zodat juridische afhankelijkheden inzichtelijk zijn.                                         | Contractueel                   | Overzicht            | Eigendomsstructuur                 |
| G13 | Eis          | Algemeen               | R3     | Afhankelijkheid van niet-Europese jurisdicties en digitale infrastructuren | Data-eigendom bij gemeente                               | Alle data blijft volledig eigendom van de gemeente.                                                                                              | Contractueel                   | Contract             | Verklaring                         |
| G14 | Eis          | Algemeen               | R3     | Afhankelijkheid van niet-Europese jurisdicties en digitale infrastructuren | Verplichting tot juridisch betwisten van datavorderingen | Leverancier betwist externe toegangsvorderingen en informeert de gemeente.                                                                       | Contractueel                   | Verklaring           | Leveranciersverklaring             |
| G15 | Eis          | Algemeen               | R3     | Afhankelijkheid van niet-Europese jurisdicties en digitale infrastructuren | EU-by-design                                             | Europese oplossingen vormen het uitgangspunt bij architectuurkeuzes.                                                                             | Architectonisch                | Architectuurdocument | Architectuurkeuze                  |

| ID  | Eis/<br>Wens | Toepassings-<br>gebied | Risico | Risico-adressering                                                         | PvE-bepaling                                          | Toelichting                                                                                         | Borging                       | Bewijs               | Aan te leveren bij<br>aanbesteding |
|-----|--------------|------------------------|--------|----------------------------------------------------------------------------|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------|-------------------------------|----------------------|------------------------------------|
| G16 | Eis          | Algemeen               | R3     | Afhankelijkheid van niet-Europese jurisdicties en digitale infrastructuren | Beperking inzet niet-EU leveranciers                  | Niet-EU leveranciers alleen indien geen alternatief beschikbaar is.                                 | Contractueel                  | Motivatie            | Onderbouwing                       |
| G17 | Eis          | Algemeen               | R4     | Structurele afhankelijkheid door beperkte Europese alternatieven           | Geen contractuele blokkades voor migratie             | Contracten bevatten geen beperkingen op overstap naar alternatieve leveranciers.                    | Contractueel                  | Contract             | Contract                           |
| G18 | Wens         | Algemeen               | R4     | Structurele afhankelijkheid door beperkte Europese alternatieven           | Recht op periodieke heroverweging                     | Gemeente kan contract periodiek evalueren en aanpassen.                                             | Contractueel                  | Contract             | Herijkingsmechanisme               |
| G19 | Wens         | Algemeen               | R4     | Structurele afhankelijkheid door beperkte Europese alternatieven           | Ondersteuning bij toetsing alternatieven              | Leverancier levert informatie voor vergelijking van alternatieven.                                  | Procesmatig                   | Rapport              | Beschrijving aanpak                |
| G20 | Eis          | Algemeen               | R4     | Structurele afhankelijkheid door beperkte Europese alternatieven           | Verplicht migratieplan                                | Er is een toetsbaar en uitvoerbaar migratieplan beschikbaar.                                        | Procesmatig                   | Plan                 | Migratieplan                       |
| G21 | Eis          | Algemeen               | R4     | Structurele afhankelijkheid door beperkte Europese alternatieven           | Tijdelijkheid niet-EU oplossingen                     | Gebruik van niet-EU oplossingen is expliciet tijdelijk en wordt periodiek heroverwogen.             | Contractueel                  | Contract             | Motivatie                          |
| G22 | Eis          | Algemeen               | R5     | Onvoldoende functiescheiding en governance-afhankelijkheid                 | Onafhankelijk audit- en toezichtrecht                 | Gemeente kan audits laten uitvoeren door onafhankelijke partijen op dienstverlening en beveiliging. | Contractueel                  | Auditrapport         | Auditafspraken                     |
| G23 | Eis          | Algemeen               | R5     | Onvoldoende functiescheiding en governance-afhankelijkheid                 | Transparantie in logging en processen                 | Logging en processen zijn volledig inzichtelijk voor toezicht en controle.                          | Technisch                     | Monitoringrapport    | Loggingbeschrijving                |
| G24 | Eis          | Algemeen               | R5     | Onvoldoende functiescheiding en governance-afhankelijkheid                 | Geen beperkingen op toezicht                          | Leverancier legt geen beperkingen op voor toezicht door derden.                                     | Contractueel                  | Contract             | Verklaring                         |
| G25 | Eis          | Algemeen               | R5     | Onvoldoende functiescheiding en governance-afhankelijkheid                 | Scheiding control-plane en uitvoering                 | Beheer kan onafhankelijk van leverancier plaatsvinden.                                              | Architectonisch               | Architectuurdocument | Beheermodel                        |
| G26 | Eis          | Algemeen               | R6     | Onvoldoende operationele continuïteit bij verstoringen                     | Contractuele borging continuïteit en incidentrespons  | Continuïteit en incidentafhandeling zijn contractueel vastgelegd inclusief responstijden.           | Contractueel /<br>Procesmatig | SLA                  | Continuïteitsplan                  |
| G27 | Eis          | Algemeen               | R6     | Onvoldoende operationele continuïteit bij verstoringen                     | Periodieke tests van herstel- en uitwijkscenario's    | Herstel- en uitwijkprocedures worden periodiek getest en gevalideerd.                               | Procesmatig                   | Testrapport          | Verklaring                         |
| G28 | Eis          | Algemeen               | R6     | Onvoldoende operationele continuïteit bij verstoringen                     | Verplichte informatievoorziening bij verstoringen     | Gemeente wordt tijdig geïnformeerd bij incidenten en verstoringen.                                  | Procesmatig                   | Rapport              | Procesbeschrijving                 |
| G29 | Eis          | Algemeen               | R6     | Onvoldoende operationele continuïteit bij verstoringen                     | Geo-redundantie                                       | Systemen zijn verdeeld over meerdere geografische locaties.                                         | Architectonisch               | Architectuurdocument | DR-ontwerp                         |
| G30 | Eis          | Algemeen               | R6     | Onvoldoende operationele continuïteit bij verstoringen                     | Topografische spreiding                               | Spreiding over geografisch gescheiden regio's.                                                      | Architectonisch               | Architectuurdocument | Ontwerp                            |
| G31 | Eis          | Algemeen               | R6     | Onvoldoende operationele continuïteit bij verstoringen                     | Crisis- en escalatieprocedures                        | Incidentmanagement en escalatieprocessen zijn ingericht.                                            | Procesmatig                   | Plan                 | Procedures                         |
| G32 | Eis          | Algemeen               | R7     | Onvoldoende borging van databeschikbaarheid en herstel                     | Inzicht in back-up- en herstelprocessen               | Gemeente heeft inzicht in hoe data wordt beschermd en hersteld.                                     | Procesmatig                   | Documentatie         | Back-upbeschrijving                |
| G33 | Eis          | Algemeen               | R7     | Onvoldoende borging van databeschikbaarheid en herstel                     | Geen afhankelijkheid van één leverancier voor herstel | Back-up en herstel zijn onafhankelijk uitvoerbaar van één leverancier.                              | Architectonisch               | Architectuur         | Beschrijving                       |
| G34 | Eis          | Algemeen               | R7     | Onvoldoende borging van databeschikbaarheid en herstel                     | Scheiding van back-up- en productieomgeving           | Back-upomgeving is gescheiden van productieomgeving.                                                | Architectonisch               | Architectuurdocument | Ontwerpbeschrijving                |
| G35 | Eis          | Algemeen               | R7     | Onvoldoende borging van databeschikbaarheid en herstel                     | Aantoonbaar geteste herstelprocedures                 | Herstelprocedures zijn getest en aantoonbaar effectief.                                             | Procesmatig                   | Testrapport          | Verklaring                         |

| ID  | Eis/<br>Wens | Toepassings-<br>gebied | Risico | Risico-adressering                                        | PvE-bepaling                           | Toelichting                                                                                                      | Borging         | Bewijs               | Aan te leveren bij<br>aanbesteding |
|-----|--------------|------------------------|--------|-----------------------------------------------------------|----------------------------------------|------------------------------------------------------------------------------------------------------------------|-----------------|----------------------|------------------------------------|
| G36 | Eis          | Algemeen               | R7     | Onvoldoende borging van<br>databeschikbaarheid en herstel | Data shattering                        | Data wordt zodanig gescheiden opgeslagen dat<br>compromittering van één dataset niet leidt tot<br>totaalverlies. | Architectonisch | Ontwerp              | Beschrijving                       |
| G37 | Eis          | Algemeen               | R7     | Onvoldoende borging van<br>databeschikbaarheid en herstel | Onafhankelijke restore mogelijkheid    | Data kan hersteld worden zonder afhankelijkheid<br>van de leverancier.                                           | Architectonisch | Test                 | Beschrijving                       |
| G38 | Eis          | Algemeen               | R7     | Onvoldoende borging van<br>databeschikbaarheid en herstel | Aantoonbaar herstel buiten leverancier | Herstel wordt getest buiten de primaire<br>leverancieromgeving.                                                  | Procesmatig     | Testrapport          | Rapport                            |
| S01 | Eis          | SaaS                   | R2     | Beperkte verplaatsbaarheid                                | Scheiding data en applicatie           | Data is logisch gescheiden van applicatielogica<br>zodat hergebruik mogelijk blijft.                             | Architectonisch | Architectuurdocument | Datamodel                          |
| S02 | Eis          | SaaS                   | R2     | Beperkte verplaatsbaarheid                                | Volledige data-export                  | Data blijft functioneel bruikbaar na export.                                                                     | Technisch       | Testrapport          | Exportbeschrijving                 |
| S03 | Eis          | SaaS                   | R3     | Afhankelijkheid niet-EU                                   | Transparantie subverwerkers            | Volledig inzicht in subverwerkers en locaties.                                                                   | Contractueel    | Register             | Subverwerkerslijst                 |
| S04 | Eis          | SaaS                   | R3     | Afhankelijkheid niet-EU                                   | Toegangsbeperking leverancier          | Toegang tot data is beperkt, gecontroleerd en<br>gelogd.                                                         | Technisch       | Auditrapport         | Securitybeschrijving               |
| S05 | Eis          | SaaS                   | R6     | Continuïteitsrisico                                       | Continuïteit bij beëindiging           | Dienst blijft beschikbaar tijdens exitfase.                                                                      | Contractueel    | Plan                 | Exitplan                           |
| S06 | Eis          | SaaS                   | R6     | Continuïteitsrisico                                       | Toegang tijdens migratie               | Gemeente behoudt toegang tot data tijdens<br>migratie.                                                           | Contractueel    | Plan                 | Transitieplan                      |
| S07 | Wens         | SaaS                   | R4     | Structurele afhankelijkheid                               | Lifecycle transparantie                | Leverancier geeft inzicht in roadmap en lifecycle.                                                               | Procesmatig     | Roadmap              | Roadmap                            |
| S08 | Eis          | SaaS                   | R2     | Beperkte verplaatsbaarheid                                | Datamobiliteit                         | Data kan onafhankelijk van applicatie worden<br>hergebruikt.                                                     | Technisch       | Test                 | Beschrijving                       |
| S09 | Eis          | SaaS                   | R3     | Afhankelijkheid niet-EU                                   | Meldplicht subverwerkers               | Wijzigingen in subverwerkers worden actief gemeld.                                                               | Contractueel    | Rapport              | Meldprocedure                      |
| S10 | Eis          | SaaS                   | R1     | Afhankelijkheid leverancier                               | Continuïteit bij faillissement         | Escrow of vergelijkbare regeling voor continuïteit.                                                              | Contractueel    | Contract             | Escrowregeling                     |
|     |              |                        |        |                                                           |                                        |                                                                                                                  |                 |                      |                                    |
| P01 | Eis          | PaaS/laaS              | R2     | Beperkte verplaatsbaarheid                                | Infrastructure as Code                 | Omgevingen zijn volledig reproduceerbaar via code.                                                               | Technisch       | Repository           | IaC voorbeeld                      |
| P02 | Eis          | PaaS/laaS              | R2     | Beperkte verplaatsbaarheid                                | Configuratie-toegang                   | Gemeente heeft toegang tot alle configuraties.                                                                   | Technisch       | Architectuurdocument | Toegangsmodel                      |
| P03 | Eis          | PaaS/laaS              | R3     | Afhankelijkheid niet-EU                                   | Control-plane binnen EU                | Control-plane valt onder EU-jurisdictie.                                                                         | Architectonisch | Architectuurdocument | Architectuur                       |
| P04 | Eis          | PaaS/laaS              | R5     | Governance-afhankelijkheid                                | Logging en monitoring                  | Volledige inzichtelijkheid in prestaties en security.                                                            | Technisch       | Monitoringrapport    | Toolingbeschrijving                |
| P05 | Eis          | PaaS/laaS              | R6     | Continuïteitsrisico                                       | Geo-redundantie                        | Systemen verdeeld over locaties.                                                                                 | Architectonisch | Architectuurdocument | DR-ontwerp                         |
| P06 | Eis          | PaaS/laaS              | R6     | Continuïteitsrisico                                       | Hersteltests                           | Herstel wordt periodiek getest.                                                                                  | Procesmatig     | Testrapport          | Verklaring                         |
| P07 | Eis          | PaaS/laaS              | R5     | Governance-afhankelijkheid                                | Onafhankelijk beheer                   | Beheer kan door derden worden uitgevoerd.                                                                        | Contractueel    | Governance           | Beheermodel                        |
| P08 | Wens         | PaaS/laaS              | R1     | Concentratierisico                                        | Transparantie infrastructuur           | Inzicht in onderliggende infrastructuur en<br>afhankelijkheden.                                                  | Contractueel    | Documentatie         | Infrastructuuroverzicht            |
| P09 | Eis          | PaaS/laaS              | R2     | Beperkte verplaatsbaarheid                                | Reproduceerbare omgevingen             | Omgevingen kunnen opnieuw worden opgebouwd.                                                                      | Technisch       | Code                 | Beschrijving                       |
| P10 | Eis          | PaaS/laaS              | R6     | Continuïteitsrisico                                       | Onafhankelijk herstel                  | Herstel kan zonder leverancier plaatsvinden.                                                                     | Architectonisch | Test                 | Beschrijving                       |
| P11 | Eis          | PaaS/laaS              | R6     | Continuïteitsrisico                                       | Parallele multi-stack inzet            | Workloads draaien gelijktijdig op meerdere<br>technologiestacks zodat directe failover mogelijk is.              | Architectonisch | Architectuurdocument | Architectuurbeschrijving           |



# 11

## Bijlage

### EMVI Gemeentelijke Cloud

| EMVI                                      | Risico | PvE                                 | Waar beoordelen we op                 | Score | Omschrijving                                                                                                                        |
|-------------------------------------------|--------|-------------------------------------|---------------------------------------|-------|-------------------------------------------------------------------------------------------------------------------------------------|
| EMVI1 – Marktspreiding & afhankelijkheden | R1     | G01–G05, S10, P08, P11              | Mate van multi-vendor inzet           | 5     | Volledig multi-vendor ontwerp met aantoonbare spreiding van leveranciers en technologiestacks, zonder gedeelde kritieke componenten |
|                                           |        |                                     |                                       | 3     | Beperkte multi-vendor inzet, gedeeltelijke spreiding                                                                                |
|                                           |        |                                     |                                       | 1     | Single vendor of sterke concentratie                                                                                                |
| EMVI1 – Marktspreiding & afhankelijkheden | R1     | G01–G05, S10, P08, P11              | Inzicht in ketenafhankelijkheden      | 5     | Volledig inzicht in subverwerkers, infrastructuur en concentratierisico's                                                           |
|                                           |        |                                     |                                       | 3     | Gedeeltelijk inzicht                                                                                                                |
|                                           |        |                                     |                                       | 1     | Geen of beperkt inzicht                                                                                                             |
| EMVI1 – Marktspreiding & afhankelijkheden | R1     | G01–G05, S10, P08, P11              | Spreiding van workloads en systemen   | 5     | Workloads aantoonbaar verdeeld over meerdere leveranciers/omgevingen met failover                                                   |
|                                           |        |                                     |                                       | 3     | Beperkte spreiding                                                                                                                  |
|                                           |        |                                     |                                       | 1     | Geen spreiding                                                                                                                      |
| EMVI2 – Portabiliteit & lock-in           | R2     | G06–G10, S01–S03, S08, P01–P03, P09 | Gebruik van open standaarden          | 5     | Volledig gebaseerd op open standaarden, geen proprietary afhankelijkheden                                                           |
|                                           |        |                                     |                                       | 3     | Deels open, deels proprietary                                                                                                       |
|                                           |        |                                     |                                       | 1     | Sterk proprietary                                                                                                                   |
| EMVI2 – Portabiliteit & lock-in           | R2     | idem                                | Datamobilititeit en exporteerbaarheid | 5     | Volledige export inclusief metadata, direct bruikbaar elders                                                                        |
|                                           |        |                                     |                                       | 3     | Deels exporteerbaar                                                                                                                 |
|                                           |        |                                     |                                       | 1     | Beperkte export                                                                                                                     |
| EMVI2 – Portabiliteit & lock-in           | R2     | idem                                | Reproduceerbaarheid en IaC            | 5     | Volledig reproduceerbaar via IaC, aantoonbaar getest                                                                                |
|                                           |        |                                     |                                       | 3     | Gedeeltelijk reproduceerbaar                                                                                                        |
|                                           |        |                                     |                                       | 1     | Niet reproduceerbaar                                                                                                                |
| EMVI3 – Juridische soevereiniteit         | R3     | G11–G16, S04–S06, S09, P04          | EU-jurisdictie en control-plane       | 5     | Volledig EU-gebaseerd inclusief control-plane en governance                                                                         |
|                                           |        |                                     |                                       | 3     | Gedeeltelijk EU                                                                                                                     |
|                                           |        |                                     |                                       | 1     | Niet-EU afhankelijk                                                                                                                 |
| EMVI3 – Juridische soevereiniteit         | R3     | idem                                | Datacontrole en eigenaarschap         | 5     | Volledige zeggenschap en contractuele borging                                                                                       |
|                                           |        |                                     |                                       | 3     | Gedeeltelijk geborgd                                                                                                                |
|                                           |        |                                     |                                       | 1     | Onvoldoende geborgd                                                                                                                 |

| EMVI                                     | Risico | PvE                       | Waar beoordelen we op                    | Score | Omschrijving                                             |
|------------------------------------------|--------|---------------------------|------------------------------------------|-------|----------------------------------------------------------|
| EMVI3 – Juridische soevereiniteit        | R3     | idem                      | Transparantie in keten en subverwerkers  | 5     | Volledige transparantie inclusief wijzigingsmechanismen  |
|                                          |        |                           |                                          | 3     | Beperkte transparantie                                   |
|                                          |        |                           |                                          | 1     | Geen transparantie                                       |
| EMVI4 – Toekomstvastheid & flexibiliteit | R4     | G17–G21, S07, S09         | Migratiemogelijkheden                    | 5     | Volledig uitgewerkt migratiepad, aantoonbaar uitvoerbaar |
|                                          |        |                           |                                          | 3     | Beperkt migratiepad                                      |
|                                          |        |                           |                                          | 1     | Geen migratiemogelijkheid                                |
| EMVI4 – Toekomstvastheid & flexibiliteit | R4     | idem                      | Contractuele flexibiliteit               | 5     | Geen blokkades, volledige exit-ondersteuning             |
|                                          |        |                           |                                          | 3     | Beperkte flexibiliteit                                   |
|                                          |        |                           |                                          | 1     | Sterke lock-in                                           |
| EMVI4 – Toekomstvastheid & flexibiliteit | R4     | idem                      | Roadmap en lifecycle transparantie       | 5     | Volledige roadmap en proactieve updatevisie              |
|                                          |        |                           |                                          | 3     | Beperkt inzicht                                          |
|                                          |        |                           |                                          | 1     | Geen inzicht                                             |
| EMVI5 – Governance & transparantie       | R5     | G22–G25, P05–P07          | Auditmogelijkheden                       | 5     | Volledig onafhankelijk auditrecht en uitvoering mogelijk |
|                                          |        |                           |                                          | 3     | Beperkt auditrecht                                       |
|                                          |        |                           |                                          | 1     | Geen onafhankelijk auditrecht                            |
| EMVI5 – Governance & transparantie       | R5     | idem                      | Logging en transparantie                 | 5     | Volledige real-time inzage en controle                   |
|                                          |        |                           |                                          | 3     | Beperkt inzicht                                          |
|                                          |        |                           |                                          | 1     | Geen inzicht                                             |
| EMVI5 – Governance & transparantie       | R5     | idem                      | Onafhankelijk beheer en functiescheiding | 5     | Volledig gescheiden control-plane en beheer              |
|                                          |        |                           |                                          | 3     | Gedeeltelijke scheiding                                  |
|                                          |        |                           |                                          | 1     | Vendor lock-in beheer                                    |
| EMVI6 – Continuïteit & herstel           | R6–R7  | G26–G38, S05–S06, P07–P11 | Continuïteitsarchitectuur                | 5     | Volledige geo-redundantie, multi-stack en failover       |
|                                          |        |                           |                                          | 3     | Basis redundantie                                        |
|                                          |        |                           |                                          | 1     | Onvoldoende                                              |
| EMVI6 – Continuïteit & herstel           | R6–R7  | idem                      | Herstelcapaciteit                        | 5     | Volledig onafhankelijk herstel, aantoonbaar getest       |
|                                          |        |                           |                                          | 3     | Beperkt herstel                                          |
|                                          |        |                           |                                          | 1     | Herstel afhankelijk van leverancier                      |
| EMVI6 – Continuïteit & herstel           | R6–R7  | idem                      | Testbaarheid en validatie                | 5     | Periodiek getest, inclusief failover en restore          |
|                                          |        |                           |                                          | 3     | Beperkt getest                                           |
|                                          |        |                           |                                          | 1     | Niet getest                                              |