Digitalisering in de gemeentelijke uitvoeringspraktijk

3 september 2026

Regiobijeenkomst Utrecht
Sessie Digitale autonomie

Dirk van Brederode - VNG
Arjan van Kempen – SSC Ons

Inhoud

1. Landelijk en Europees veld & wapenfeiten
2. Autonomie, soevereiniteit & BCM
3. Vier handvatten voor uw eigen organisatie
4. Wat u niet alleen kunt
5. Drie dingen om deze maand te doen
6. Eén vraag om mee terug te nemen

Algemene aanpak Digitale autonomie

- Belangrijke politiek-bestuurlijke doelstellingen stellen (bijvoorbeeld: ‘x-aantal kritieke processen / data autonoom in x-jaartal’)

- Gericht op coördinatie / regie, digitale autonomie realiseren in andere opgaven (zoals data, cloud, AI)

- Per techstacklaag wapenfeiten realiseren

Beoogde wapenfeiten

- **AI**
  - Ontwikkeling GPT-NL
  - Inkoopvoorwaarden bij AI die digitale autonomie borgen
- **Data**
  - Federatief Datastelsel, met standaarden die interoperabiliteit en dataportabiliteit bevorden
- **Software**
  - Programma van eisen gericht op SAAS-leveranciers om hun software op Europese infrastructuur te hosten
- **Cloud (platform en infrastructuur)**
  - Soevereine overheidscloud, overheidbreed in te zetten
  - Cloudmarktplaats, waar aanbod alleen bestaat waarin kwaliteitsvereisten aan de voorkant zijn meegenomen

Nederlandse Digitaliseringsstrategie (NDS)

- Routekaart digitale autonomie
  - Overheidsbrede strategie voor 10 jaar, met doelstellingen en mijlpalen in de tijd

- Beleidskaders
  - Referentiekader: vertaalt EU SEAL-niveaus naar technische vereisten
  - Classificatiesystematiek: normeert door minimale SEAL-niveaus te koppelen aan specifieke processen / systemen / data

- Handelingsperspectief: Digitale Autonomie Competentiecentrum (DACC)
  - Volwassenheidsmodel digitale autonomie:
  - IT-verkavelingsstrategie:

Sovereignty Effectiveness Assurance Levels (SEAL)

Sovereignty Effectiveness Assurance Levels	Sovereignty Effectiveness Assurance Levels Descriptions
SEAL-0	*No Sovereignty*: Service, technology or operations under **exclusive control of non-EU third parties**, governed entirely in **non-EU jurisdictions**.
SEAL-1	*Jurisdictional Sovereignty*: **EU law formally applies** with **limited practical enforceability**; service, technology or operations under exclusive control of non-EU third parties.
SEAL-2	*Data Sovereignty*: **EU law applicable and enforceable**, with **material non-EU dependencies remaining**; service, technology or operations under indirect control of non-EU third parties.
SEAL-3	*Digital Resilience*: **EU law applicable and enforceable**, EU actors exercising **meaningful but not full influence**; service, technology or operations under marginal control of non-EU third parties.
SEAL-4	*Full Digital Sovereignty*: Technology and operations under **complete EU control**, subject only to **EU law**, with **no critical non-EU dependencies**.

Europa

- Tech Sovereignty Package (3 juni 2026 gepubliceerd)
  - Cloud and AI Development Act
  - Europese open-source strategie
- Herziening Aanbestedingsrichtlijn (Q3/4 2026)

Europa: Cloud and AI Development Act

- Wettelijk bepaald dat clouddiensten die gebruikt worden door overheden aan minimale betrouwbaarheidsniveaus moeten voldoen
- Certificatieschema voor cloudaanbieders op de EU-markt (anders geen toetreding)
- Verplichte soevereiniteitsrisicobeoordeling voor overheden
- VNG is gestart met een uitvoeringstoets op dit wetsvoorstel en voert gesprekken in Europa hierover

Digitale autonomie

Handelingsvrijheid:

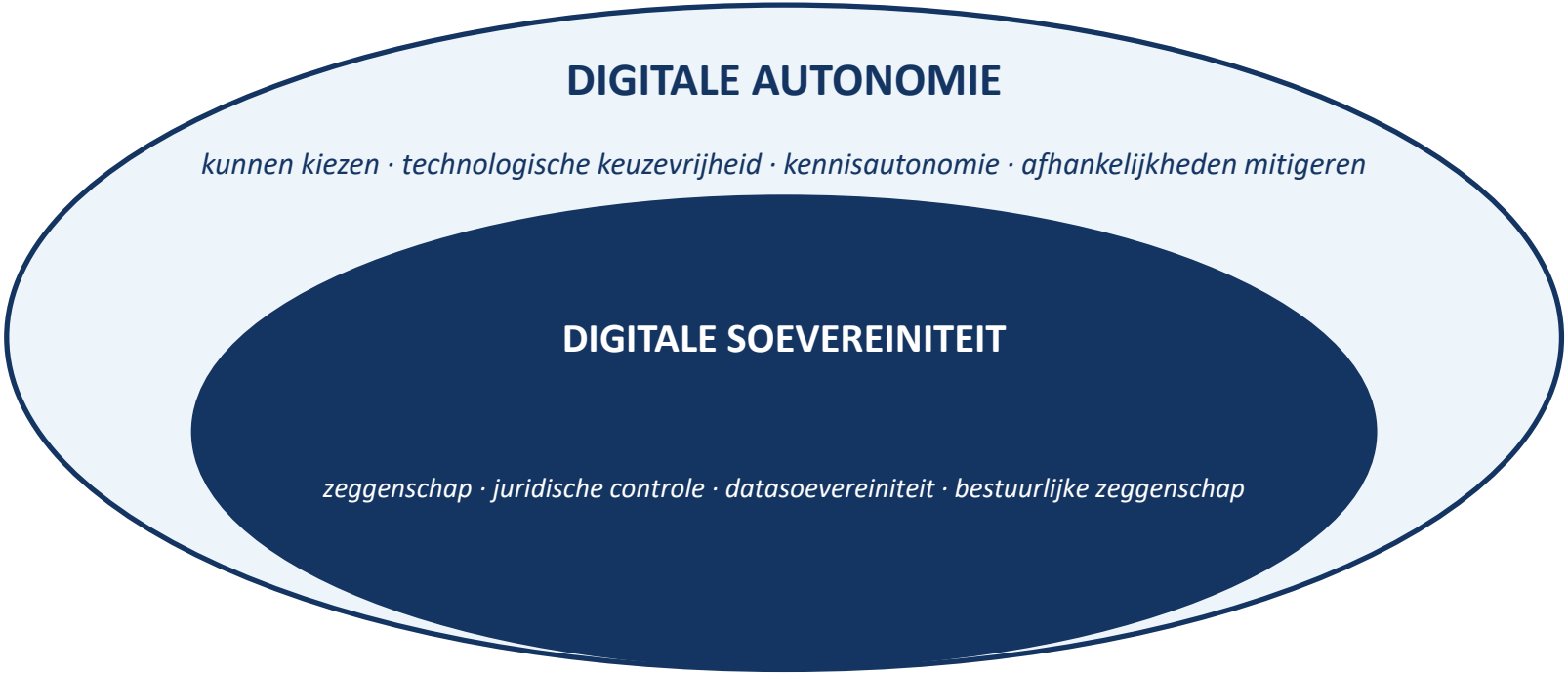
- Technologische keuzevrijheid
- Kennisautonomie
- Bewust mitigeren van strategische afhankelijkheden.

Digitale soevereiniteit

Zeggenschap:

- Juridische controle
- Datasoevereiniteit
- Bestuurlijke zeggenschap.

Overlap en verschil



BCM perspectief

Wat klassieke BCM (ISO 22301) al doet

- **Business Impact Analyse** — impact van uitval per systeem, afhankelijkheden, hoe lang zonder
- **Recovery Time Objectives** en **Recovery Point Objectives**
- **Risicoanalyse** — brand, stroomuitval, pandemie, leveranciersfaillissement, cyberaanval
- **Gedocumenteerd plan** — BCP, DRP — met eigenaarschap
- **Beproefde tests**, periodiek uitgevoerd, met geverifieerde uitkomst
- **Governance** — een aanwijsbare eigenaar, een cyclus, een rapportagelijn

Wat digitale autonomie eraan toevoegt

- **Jurisdictie-risico**
  Buitenlandse overheid kan via wetgeving (CLOUD Act, sancties, exportrestricties) toegang of dienst blokkeren — los van de wil van de leverancier.

- **Concentratie-risico**
  Wanneer een groot deel van de overheid op één leverancier hangt, is uitval geen incident maar een systeemschok.

- **Geopolitiek risico**
  Beide bewegen niet random, maar met geopolitieke verschuivingen — buiten uw invloedssfeer. Klassieke BCM rekent met stabiele dreigingen; deze beweegt.

Handvat 1: Classificeer voordat u meet

Niet alles hoeft even autonoom te zijn.

Frameworks:

- Cloud Sovereignty Framework - Europese Commissie (DG DIGIT)
- Soevereiniteit clouddiensten: Toetsingsinstrument – DICTU
- Soevereiniteitsscan: Borgen van publieke waarden, Gemeente Venlo / Gartner
- Digital Autonomy Assessment Framework (DAAF) - Universiteit Utrecht
- Volwassenheidsniveau - DACC

Handvat 2: Stel twee vragen, niet één

Vraag A

Waar moet ik eerst handelen?

Prioriteert uw portfolio op urgentie.

Vraag B

Hoe autonoom ben ik bij deze leverancier?

Beoordeelt een leverancier op het niveau dat hij haalt.

Handvat 3: Streefniveau als bestuurlijk besluit

NIET

“We gaan voor zo hoog mogelijk.”

WEL

“Voor deze applicatie willen we op deze thema's binnen achttien maanden niveau N halen — afgewogen tegen kosten, gebruiksgemak en kwaliteit van dienstverlening, op deze gronden.”

Handvat 4: Begin met de exit-vraag

Voor uw top-5 kritieke applicaties:

Hebben wij ooit een exit getest?

Het antwoord is bijna altijd nee — er staat een clausule in het contract die nooit is uitgevoerd. Op de dag dat een leverancier wegvalt door sanctie, overname of exportrestrictie blijkt die clausule waardevol papier en operationeel niets.

Samengevat:

DIGITALE AUTONOMIE — kunnen kiezen

DIGITALE SOEVEREINITEIT — te zeggen hebben (juridisch, data, bestuurlijk)

Klassieke BCM-discipline	Vertaling naar autonomie-werk
BIA — classificatie van toepassingen	Classificatie (Vitaal / Kritisch / Gevoelig / Licht, of SEAL niveau's)
RTO/RPO + risicoaanvaarding	Gemotiveerd streefniveau, met datum
Beproefde DR-test	Exit-test inclusief data; degraded-mode-plan
Periodieke BCM-review	Herijking op vaste cadans + triggergebeurtenissen

1. Classificeer voordat u meet.

2. Stel twee vragen, niet één.

3. Streefniveau als bestuurlijk besluit — gedateerd.

4. Begin met de exit-vraag, niet de leveranciersvraag.

Wat u niet alleen kunt

- **Beproefde exit voor de zwaarste hyperscaler-afhankelijkheden**
  Geteste data-exit + degraded-mode-continuïteitsplan; gezamenlijk vaststellen — geen gemeente voor gemeente.

- **Marktvorming en gebundelde vraag**
  Eén gemeente verandert geen concentratie. Een blok gemeenten via de VNG kan dat wel.

- **Geopolitieke horizon-scanning**
  Eén keer collectief, niet 342 keer — wat het DACC en de NDS-aanjaagstructuren beogen te leveren.

Drie dingen om deze maand te doen:

1. Maak een lijst van uw top-10 applicaties en classificeer ze (BIA-stijl+: gebruik een framework).
2. Stel voor de eerste vijf de exit-vraag en noteer eerlijk het antwoord.
3. Identificeer wie bij u de regie-rol heeft en check of die tijd heeft.

"Wie is bij ons aanwijsbaar verantwoordelijk voor de regie op clouddiensten en de afhankelijkheden die we daarmee aangaan — en heeft die persoon ook tijd?”

Dank voor uw tijd en aandacht!

Contact:

Tim Kies

Arjan van Kempen