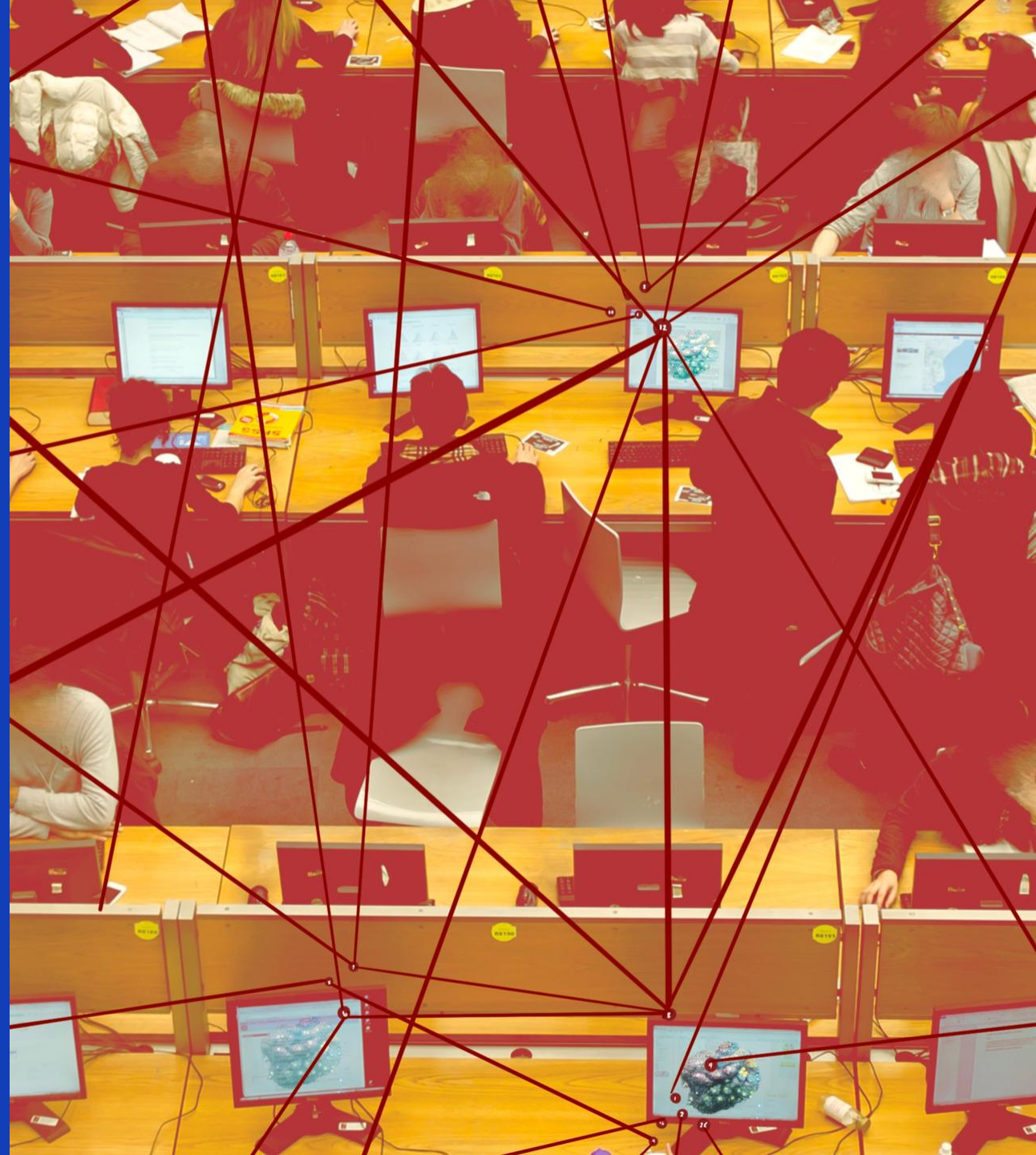


Informatie- management producten voor AI opschaling bij gemeenten

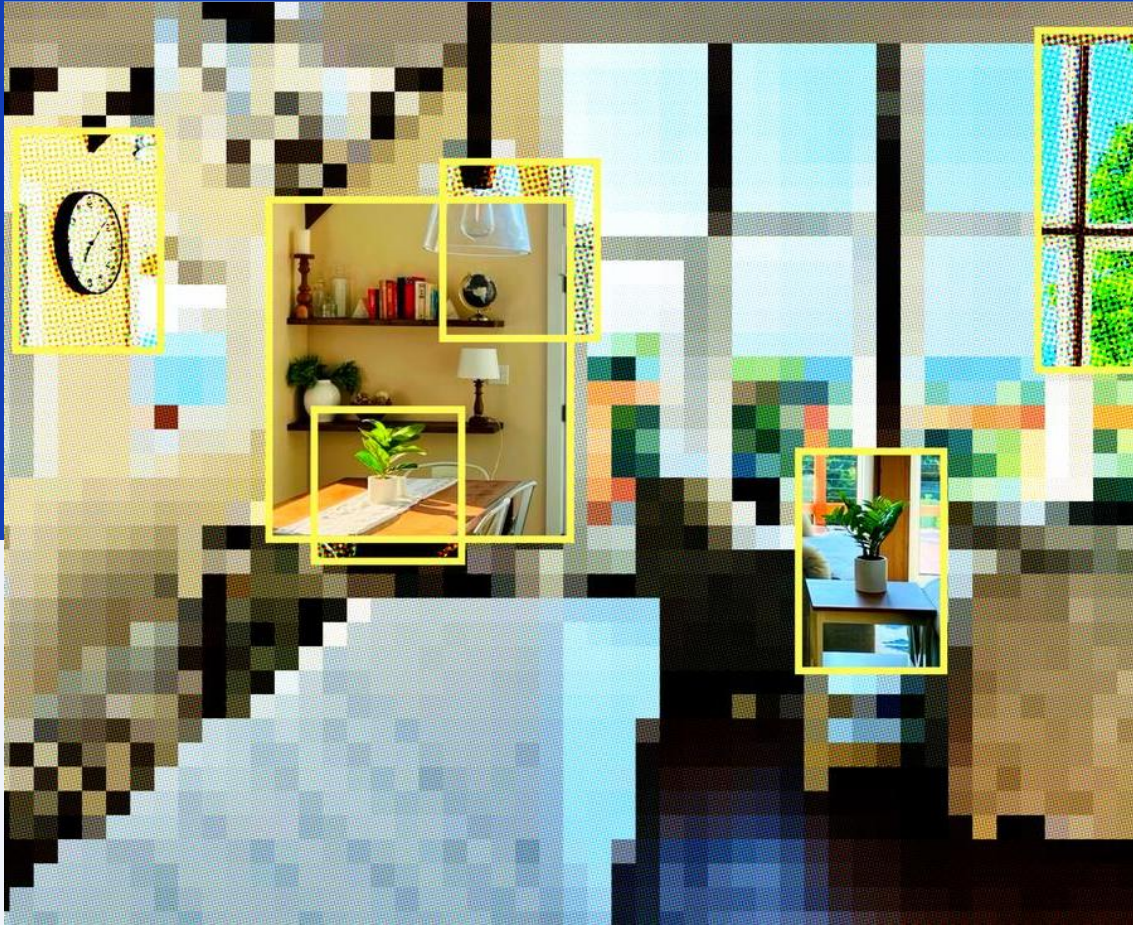
Tessa Bruijne, Noah Smeets & Annelieke van den Berg

In opdracht van de Vereniging van Nederlandse Gemeenten (VNG)

Hanna Barakat & Cambridge Diversity Fund /
<https://betterimagesofai.org> /
<https://creativecommons.org/licenses/by/4.0/>



Inhoudsopgave



Elise Racine / <https://betterimagesofai.org> / <https://creativecommons.org/licenses/by/4.0/>

1. [Introductie](#)
2. [AI procesplaat](#)
3. [Inkoopproces voor AI bij gemeenten](#)
4. [AI referentiearchitectuur](#)
5. [Bronnen](#)

Introductie

De Nederlandse overheid experimenteert met de inzet van artificiële intelligentie (AI) bij het uitvoeren van hun diensten en het behalen van hun doelen. Ook gemeenten zijn bezig of willen gaan beginnen met het experimenteren en inzetten van AI. De praktijkervaring leert echter dat dezelfde ontwikkelingen op meerdere plekken plaatsvinden, of dat gemeenten met minder kennis en capaciteit niet weten waar ze het best kunnen starten.

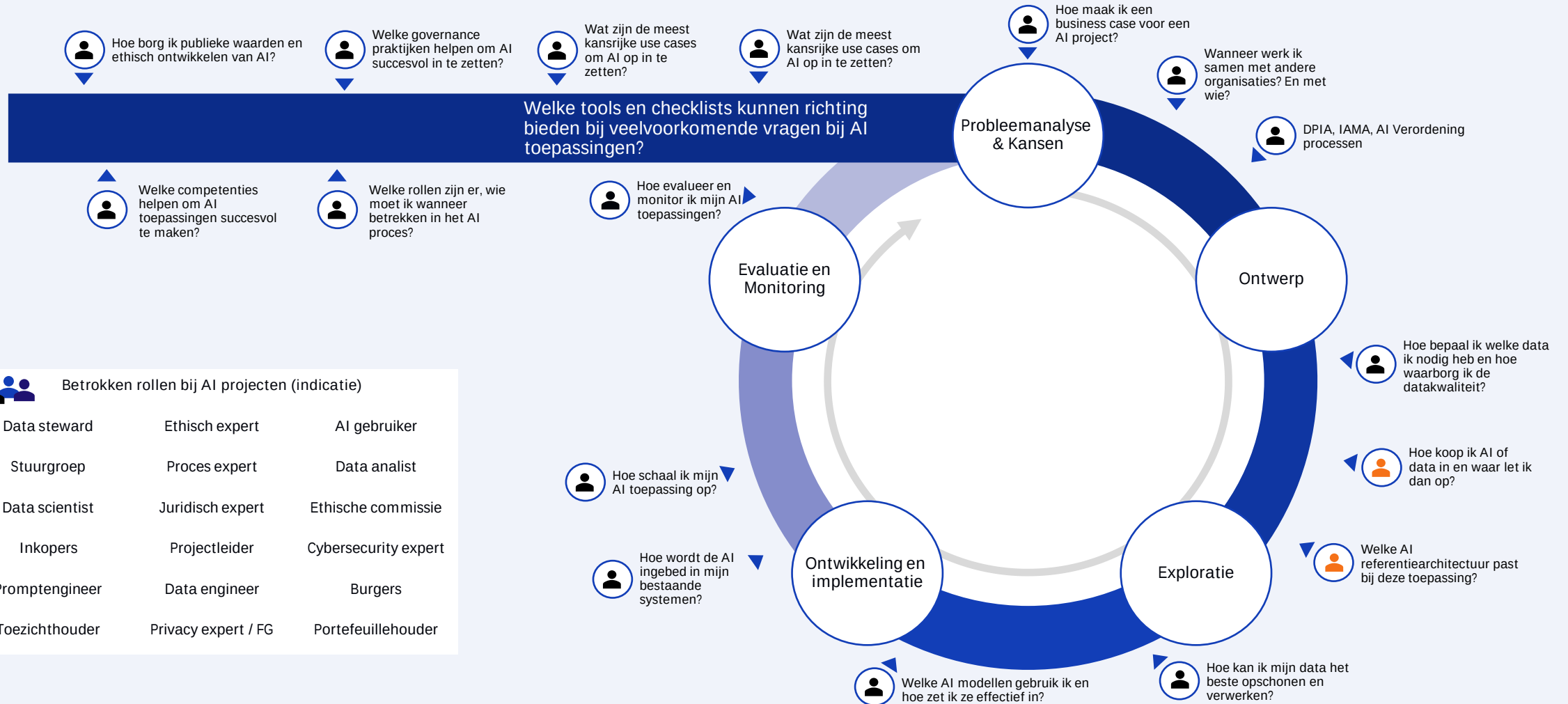
De Vereniging van Nederlandse Gemeenten (VNG) heeft TNO de opdracht gegeven om bij voorlopende gemeenten te inventariseren welke informatiemanagementproducten (IM-producten) beschikbaar zijn en verspreid kunnen worden om alle gemeenten binnen Nederland verder te helpen met AI innovatie.

Op basis van interviews met sleutelfiguren op AI bij vier gemeenten of gemeentelijke samenwerkingsverbanden, zijn twee onderwerpen verder ontwikkeld als IM-product: het AI inkoopproces en Referentiearchitectuur.

- **AI Inkoopproces:** De introductie van AI vergt meer aandacht in het inkoopproces dan reguliere IT, door de veranderlijkheid van de technologie, maar ook de wet- en regelgeving en maatschappelijke vraagstukken.
- **Referentiearchitectuur:** Om AI goed in te bedden in de organisatie, is het belangrijk om goed overzicht te hebben op de technische bouwblokken en patronen voor AI toepassingen.

Hierna volgt eerst de AI procesplaat: een globaal overzicht van vragen die opkomen wanneer een gemeente wil starten met een AI innovatietraject. De vragen zijn verdeeld over verschillende fases: vragen die opkomen vóórdat er gestart wordt met AI en vragen die opkomen tijdens de AI levenscyclus. Op dezelfde plaat staat ook een overzicht van de (mogelijk) betrokken rollen bij AI projecten, om aan te geven welke expertise nodig kan zijn bij AI innovatietrajecten.

AI procesplaat: veel voorkomende vragen



Betrokken rollen bij AI projecten (indicatie)

Data steward	Ethisch expert	AI gebruiker
Stuurgroep	Proces expert	Data analist
Data scientist	Juridisch expert	Ethische commissie
Inkopers	Projectleider	Cybersecurity expert
Promptengineer	Data engineer	Burgers
Toeziachter	Privacy expert / FG	Portefeuillehouder

AI inkoopproces bij gemeenten

AI wordt steeds vaker en op verschillende manieren toegepast binnen de overheid, waaronder gemeenten. Het doel van AI inzet is onder andere om processen efficiënter in te richten en effectiever uit te voeren. De innovatie van AI kan gezien worden als een opvolging van eerdere digitalisering, maar brengt ook unieke uitdagingen met zich mee. Enkele van deze uitdagingen zijn relevant voor het inkoopproces.

Het inkopen van AI vraagt om meer aandacht dan traditionele IT inkoop. De technologie is veranderlijker door de input data en gebruik, heeft sterkere ethische impact en verlegt (mogelijk) verantwoordelijkheden. Waar aanbieders momenteel nog wettelijk verplicht zijn om risico's af te dekken voor de IT systemen die zij aanbieden, blijken er op dit gebied al complicaties te zijn wanneer het AI toepassingen betreft. Gemeenten zijn verantwoordelijk voor de technologie die zij gebruiken en de impact die daaruit volgt. Het is daarom belangrijk om goed zicht te hebben op inhoudelijke onderwerpen en daar de juiste informatie over in te winnen, zodat er goede afspraken gemaakt kunnen worden met aanbieders en andere stakeholders.

Dit document is relevant voor inkopers, innovatieteams, ethisch en privacy experts, beleidsmakers, en andere stakeholders van AI projecten bij gemeenten.

Om inkoopprocessen zo goed mogelijk uit te voeren, gelden de volgende best practices:

- **Doelstelling:** Een concrete doelstelling opstellen is de beste start, niet alleen voor AI projecten maar ook voor inkoopprocessen. Hiermee wordt de behoefte van de gemeente en opdracht voor aanbieders duidelijker. Een doelstelling moet ook aandacht hebben voor de maatschappelijke meerwaarde en publieke waarden die beschermd moeten worden.
- **Multidisciplinair team:** Samenwerking met verschillende experts zorgt dat alle relevante onderwerpen zo goed mogelijk meegenomen worden. Denk aan: innovatieteam, bedrijfsarchitect, juridische afdeling, IT en security, ethisch expert, FG of privacy expert.
- **Tijdige betrokkenheid:** Door het inkoopteam al vroeg betrekken bij innovatieprojecten kunnen kansen optimaal benut en barrières tijdig opgelost worden. Dit vraagt ook om een proactieve houding van en initiatief nemen door het inkoopteam.
- **Open houding:** Innovatie mogelijk maken moet op een gebalanceerde manier gebeuren, waarbij niet alleen de risico's en complexiteit aandacht krijgt, maar ook de mogelijkheden en kansen voor de gemeente.

AI projecten en het inkoopproces: leeswijzer

Om extra houvast te geven in het inkoopproces, staat op de volgende slide/pagina een procesweergave van (het begin) van AI projecten en hoe deze projecten interacteren met het standaard inkoopproces (gebaseerd op Van Weele).

Het proces begint links boven. De blauwe blokken geven aan wat voor een proces moet worden uitgevoerd. De roze ruiten geven aan dat er een belangrijke beslissing gemaakt moet worden. Na elke beslissing volgen meerdere opties die volgen uit de gemaakte keuze. Belangrijk: beide processen zijn lineair weergegeven, maar hebben baat bij revisies en iteraties door de veranderlijkheid van AI en relevante wet- en regelgeving. In de praktijk kan het zijn dat de verschillende stappen mogelijk door elkaar heen lopen of in een andere volgorde doorlopen worden.

De inkoopfases Bestellen, Bewaken en Nazorg zijn niet expliciet gekoppeld, maar natuurlijk ook erg belangrijk in de praktijk. De nodige aandachtspunten voor inkoop voor deze fases voor AI zijn echter eerder in het proces uitgediept en (waar relevant) vastgelegd in contracten of afspraken met aanbieders.

De volgende pagina's geven verdieping voor de fases Specificering en Selectie van het inkoopproces. Deze verdiepingen geven het inkoopteam houvast om de juiste vragen te stellen, zonder dat zij AI expert hoeven te worden. Zo kunnen de relevante onderwerpen voor het inkopen van data, model en/of toepassing of dienst goed worden meegenomen.

Verdere informatie over relevante onderwerpen kan worden ingewonnen via de bronnen aan het eind van dit document.

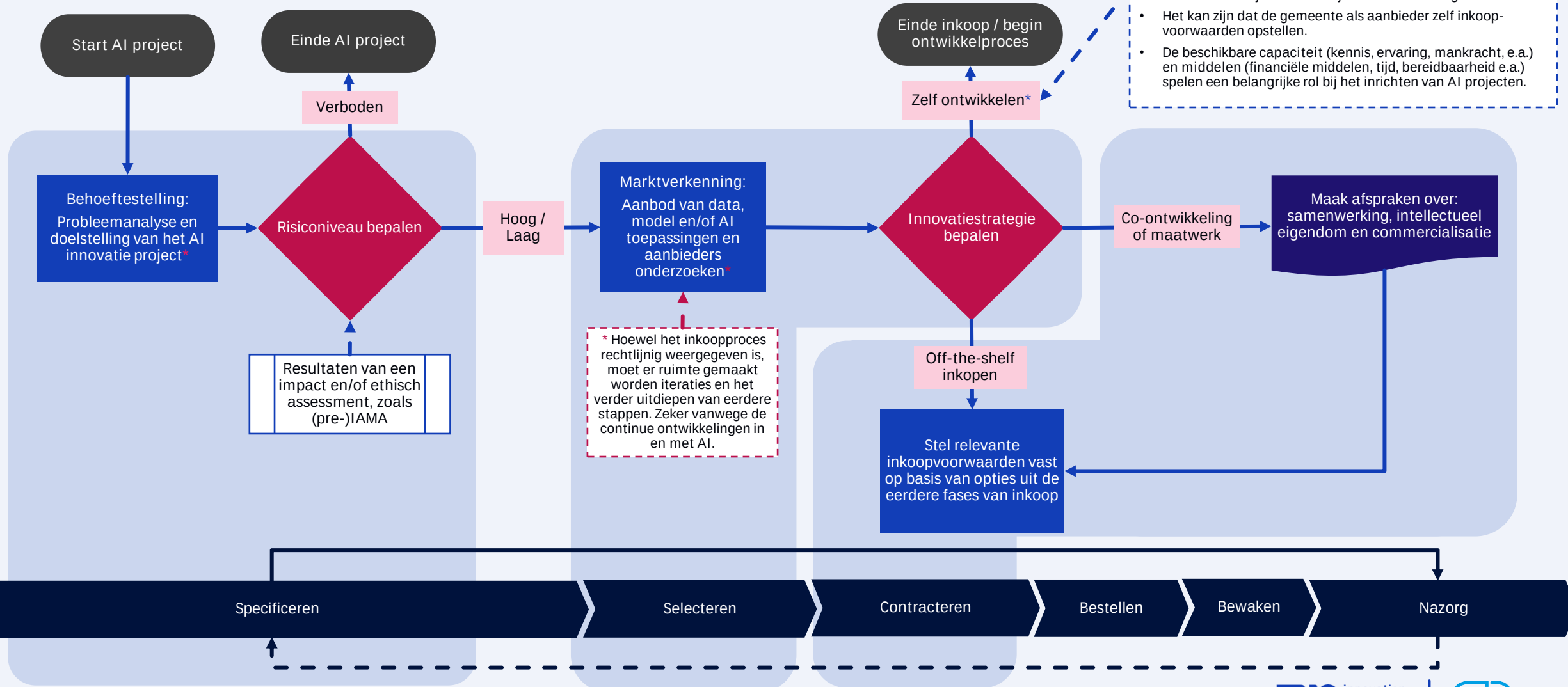
Onderwerpen voor AI inkoopprocessen:

Data: Een succesvol AI projecten begint bij data. Data vormt een belangrijke voorwaarde voor de ontwikkeling en prestatie van AI toepassingen. Om aan voldoende en de juiste data te komen, moet gemeentes dit vaak inkopen. Hierbij is het belangrijk dat er aandacht is voor verschillende onderwerpen, bijvoorbeeld: de manier waarop data is verzameld, of de gemeente deze data in huis mag hebben, en wat de rechten tot de data zijn gedurende de hele AI levenscyclus.

Model: AI modellen zijn naast data een belangrijk onderwerp voor inkoop. Modellen kunnen als een opzichzelfstaand product ingekocht worden, waarna een gemeente deze verder uitwerkt voor hun toepassingsgebied. Hoewel de overheidsrichtlijnen uitgaan van 'open source, tenzij' kan het zijn dat er geen goede open source modellen beschikbaar zijn of dat de gemeente niet de juiste capaciteit of middelen beschikbaar heeft om deze modellen te gebruiken. Dan is inkoop een goede oplossing.

Applicatie of dienst: Gemeentes kunnen ook volledige applicaties of diensten inkopen waarin AI is toegepast. Dit brengt extra onderwerpen met zich mee waar voorwaarden over gesteld kunnen worden, waaronder afspraken over monitoring en evaluatie van AI toepassingen en inbegrepen service.

AI projecten en het inkoopproces



Verdieping van de Specificeringsfase

Het AI inkoopproces verloopt efficiënter en effectiever wanneer verschillende disciplines samenwerken, zoals technische, juridisch en ethische experts. Het is echter nuttig voor inkopers om zelf inzichtelijk te hebben welke vragen of onderwerpen spelen bij AI-toepassingen, aangezien de praktijk laat zien dat daar andere uitdagingen spelen dan bij reguliere informatietechnologieën.

In de Specificeringsfase van het inkoopproces moet er aandacht worden besteed aan een breed scala aan onderwerpen als het gaat om AI. De relevante onderwerpen zijn in onderstaande visualisatie uitgesplitst over de AI levenscyclus. Het overzicht geeft niet een volledige uitputting van onderwerpen of nodige diepgang.

AI levenscyclus en onderwerpen voor inkoop van data en model

	Probleemanalyse	Ontwerp	Verkenning en preparatie	Ontwikkelen	Verificatie en validatie	Implementatie	Gebruik	Monitoring en beheer	Uitfasering
Data	Welke en hoeveel data is er intern al beschikbaar en ontsluitbaar? Is de beschikbare data gepast voor de geplande toepassing? Hoe (privacy) gevoelig is de data? Wie heeft controle over en toegang tot de data?	Wat is het aanbod en geschiktheid van externe databronnen? Verzamelingsprocedure van data en data minimalisatie Wie heeft eigenaarschap? • Toegang en rechten • Intellectueel eigendom • Commercialisatie	Mogelijkheden en risico's voor data-verzameling en combineren van datasets? Data kwaliteit: • Actualiteit • Geschiktheid • Accuraatheid, volledigheid, representativiteit	Hoe wordt data verzameld en verwerkt? Hoe wordt data gebruikt voor training en toetsing van een model?	Welke controles en tests op data kwaliteit zijn mogelijk, nodig of al uitgevoerd? Welke controles en tests op consistentie van de in- en output zijn mogelijk, nodig of al uitgevoerd?	Hoe wordt nieuw-gegenereerde data gevoed in: • Het model? • Bestaand (data) ecosysteem? Data management processen • Correctie van data • Toegang • Ontsluitbaarheid	Wie heeft de rechten en toegang tot gegenereerde data bij gebruik? Hoe is de veiligheid van de toepassing, systeem en gebruikers gewaarborgd? Hoe is privacy van datasubjects en gebruikers gewaarborgd?	Auditing en evaluatie: hoe wordt data gecontroleerd na implementatie? • Data kwaliteit • Data management • Toegang tot en eigenaarschap over de data	Welke afspraken zijn er over bewaren, archiveren, verder gebruik of vernietiging van data met/via: • Aanbieder • Gebruikers • Data subjects • Wet- en regelgeving?
Model	Is de geplande AI oplossing wenselijk? Risiconiveau van de AI toepassing? Welke publieke waarden gelden? Welke oplossingen en modellen bestaan al? • Risico op vendor lock-in? • Digitale autonomie bij niet-NL oplossingen Kosten	Is het model of toepassing schaalbaar? Fit for purpose Hoe is menselijk overzicht ingebed? Wat is de duurzaamheid? • Energieverbruik/ milieu impact • Toekomstbestendigheid van de toepassing	Selectie van het model: • Geschikt voor het toepassingsgebied? • Geeft het model de gewenste output? Samenhang met beschikbare data voor ontwikkeling en gebruik Aansluiting bij een datamodel (e.g., GGM)	Welke open source oplossingen kunnen gebruikt worden? ("Open source, tenzij") Welke verantwoorde ontwerp en ontwikkel principes worden/zijn toegepast? Voorbereiden op en faciliteren van aansluiting bij bestaande architectuur en infrastructuur	Evaluatie van model en performance • Prestatie statistieken (metrics) • Prestatie baseline Opties voor model beheersing: • Finetuning • Training • Inferentie • Retrieval Augmented Generation (RAG)	Aansluiting bij en integratie met: • Bestaande systemen (architectuur en infrastructuur) • Huidige technische processen • Werkprocessen Wat is de mogelijke impact op medewerkers en burgers?	Hoe wordt omgegaan met wijzigingen in het model? • Finetunen • Leren door gebruik • Versiebeheer en updates door aanbieder Hoe worden gebruikers en hun feedback meegenomen? Hoe worden publieke waarden gewaarborgd?	Onderhoud en performance • Kwaliteit uitkomsten • Volume van aanvragen • Bronverbruik (bijv. energie) • Kosten Auditing en evaluatie • Verantwoordelijkheid aanbieder • Toegang tot het model door externe auditors/evaluators	Mogelijkheid voor hergebruik van het model door aanbieder en/of gebruiker (gemeente) Vervangbaarheid van het model Afhankelijkheid van derden

Verdieping van de Selectiefase

Bij AI projecten kunnen verschillende innovatiestrategieën toegepast worden: zelf ontwikkelen, co-ontwikkelen of volledig inkopen. In de Selectiefase van het inkoopproces is het belangrijk dat het duidelijk wordt welke vorm van innoveren wordt gekozen. Belangrijke punten die het verloop van het AI project bepalen zijn hier niet alleen wat de markt te bieden heeft, maar ook wat de gemeente zelf aan middelen, capaciteit en kennis beschikbaar heeft.

Er zijn ook hybride vormen van innovatie mogelijk, waarbij een of meerdere onderdelen worden ingekocht, waar het innovatieteam of de data scientists van de gemeente vervolgens zelf mee aan de slag gaan. Er wordt onderscheid gemaakt op drie componenten die kunnen worden ingekocht, welke elk hun eigen aandachtspunten hebben: Data, Model en Applicatie of Dienst.

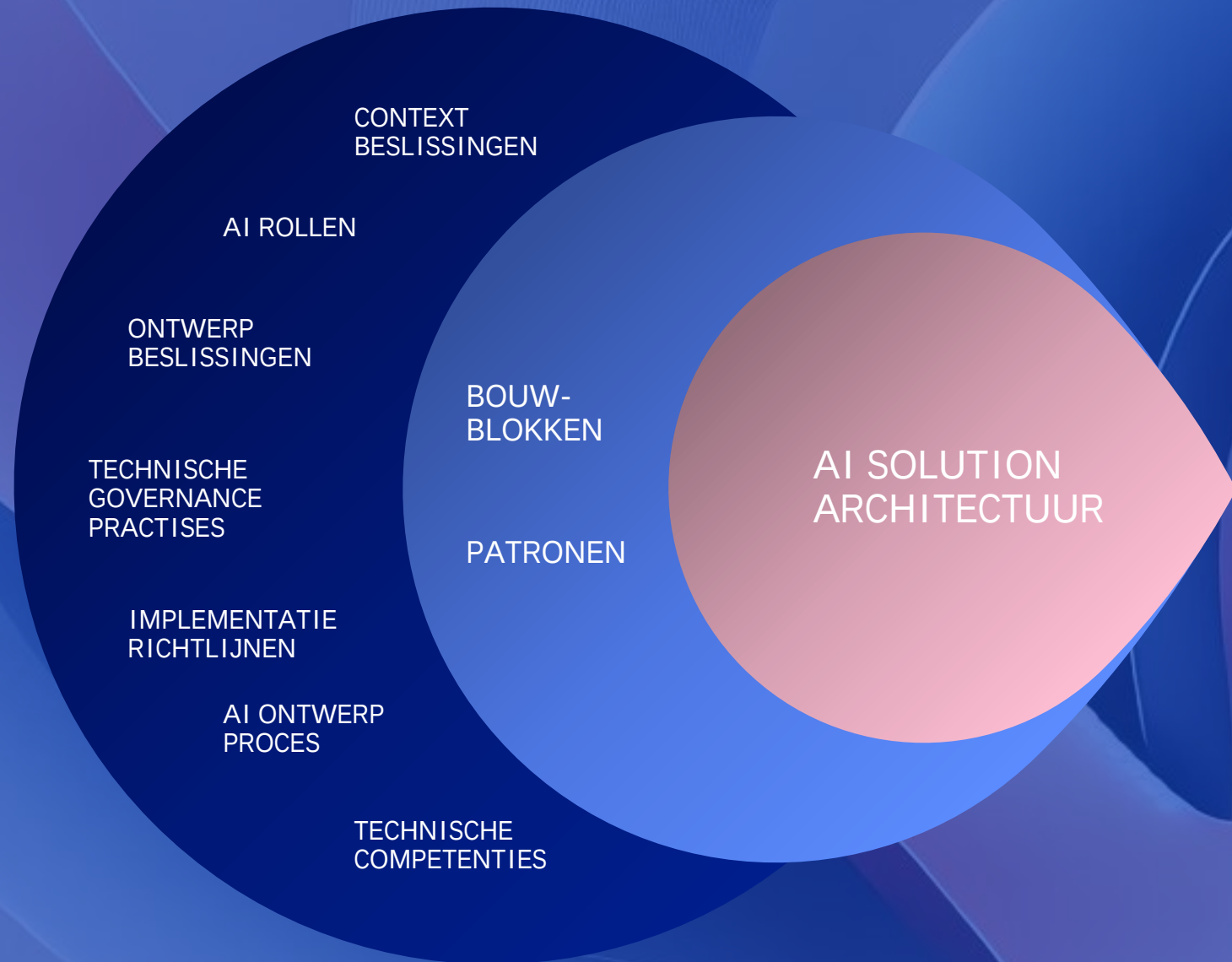
Data Bijv. geo data, sensordata, luchtfoto's	Model Bijv. taalmodel, beslismodel	Applicatie of dienst Bijv. Microsoft 365 Copilot
• Voldoet de dataset aan verantwoorde verzameling en verwerkingspraktijken? Of is daar voldoende inzicht in? • Wat is de kwaliteit van de data? • Is de data geschikt voor het doel van de toepassing? • Is de data accuraat, volledig en representatief? • Indien van toepassing: Sluit de data aan bij de bestaande data van de gemeente? • Eigenaarschap: wat zijn de rechten en toegang tot de data na aanschaf voor zowel aanbieder als afnemer? • Welke privacy overwegingen zijn relevant, zoals gevoeligheid of data minimalisatie? • Hoe wordt de data beschikbaar of benaderbaar gemaakt en opgeslagen? Denk bijvoorbeeld aan security of server locatie. • Regels rondom onderhoud en controle op de data: hoe wordt de kwaliteit gewaarborgd?	• Is het model geschikt en gepast voor het beoogde doel? • Hoe is het model ontwikkeld en getraind? • Wat is de kwaliteit van het model en diens uitkomsten? • Performance • Veiligheid en robuustheid • Accuraatheid • Rechtsgelijkheid, bias, discriminatie • Transparantie • Is er ruimte voor menselijk overzicht en hoe kan er controle uitgeoefend worden? • Eigenaarschap: hoe zijn rechten en toegang tot het model ingebed? • Hoe is controle op het zelf-leerproces door/tijdens gebruik ingericht? • Welke computing bronnen (cloud dienst, energiegebruik, etc.) moeten worden ingezet?	• Controleer op: • Vendor lock-in en digitale autonomie: kan er gemakkelijk worden overstapt naar een andere aanbieder? • Is de toepassing compliant met GIBIT en andere relevante frameworks, of zijn er uitdagingen? • Vervangbaarheid als de toepassing niet meer werkt of uitgefaseerd wordt door de aanbieder? • Welke Service Level Agreements kunnen worden afgestemd met aanbieders? • Uptime en storingen • Monitoring en evaluatie (zoals logging, prompt analyse, gebruikersfeedback) • Hosting • Auditing en inzichtelijkheid voor derden • Einde contract en doorgebruik/heraanbieding • Controle van afspraken met huidige aanbieders: • Implementatie van AI in bestaande producten • Update van modellen in bestaande AI producten

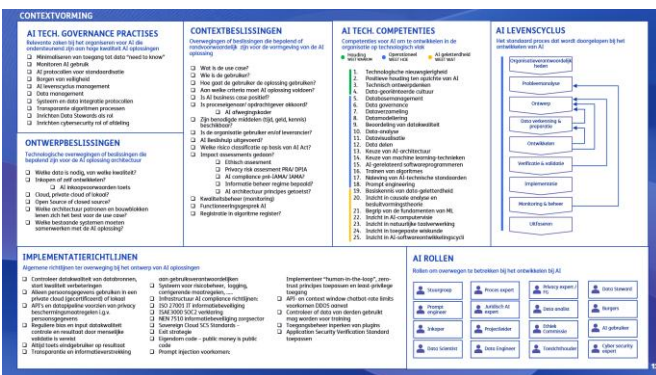
Aanzet tot een AI referentie-architectuur

Een AI referentiearchitectuur is een generiek raamwerk dat hergebruikt kan worden bij het ontwerpen van AI toepassingen. Een referentie-architectuur kan worden gebruikt als startpunt om een AI solution architectuur te ontwerpen.

Dit document bevat een eerste aanzet voor een AI referentie-architectuur voor gemeenten in Nederland.

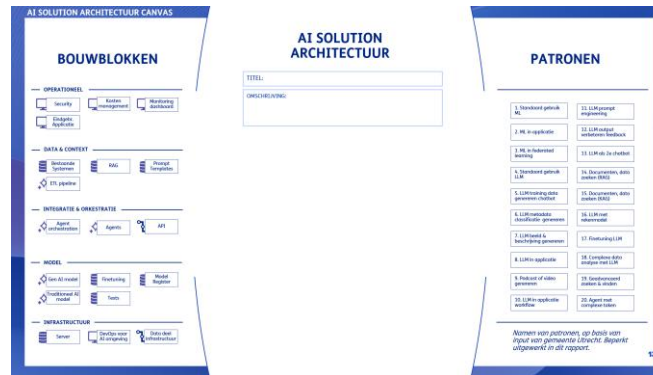
Het succesvol toepassen van AI vergt interdisciplinaire kennis, bijvoorbeeld over ethische, juridische, innovatie en technische aspecten. Dit document beschrijft technische bouwblokken en patronen voor AI toepassingen. Aanvullend worden aspecten van andere disciplines die mede bepalend zijn voor het ontwerp van de AI toepassing beschreven. Deze beschrijving is indicatief en niet exhaustief.





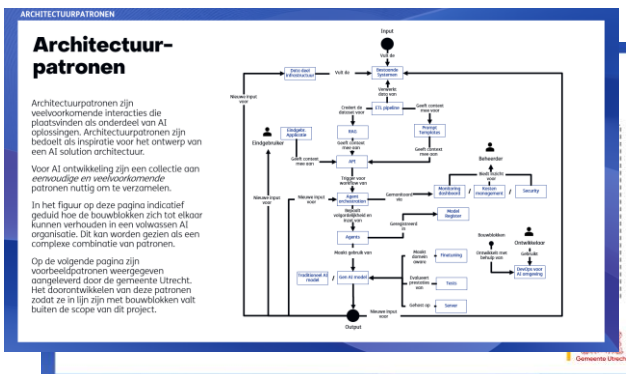
1. Contextvorming

Dient als compleetheidscheck voordat
ontwikkeling van een AI toepassing start



2. AI solution architectuur canvas

Canvas om bouwblokken en patronen te combineren in een hoogover technische schets van de AI toepassing



4. Architectuurpatronen

Veelvoorkomende configuraties van
bouwblokken met een specifieke functie
(*beperkte uitwerking*)



5. Richtingen voor doorontwikkeling

Suggesties om de AI
referentiearchitectuur eenvoudig
toepasbaar en bruikbaar te maken



3. Bouwblokken

Toelichting van - en verdiepende informatie over - elk bouwblok



6. Bronnen

AI TECH. GOVERNANCE PRACTISES

Relevante zaken bij het organiseren voor AI die ondersteunend zijn aan hoge kwaliteit AI oplossingen

- ❑ Minimaliseren van toegang tot data “need to know”
- ❑ Monitoren AI gebruik
- ❑ AI protocollen voor standaardisatie
- ❑ Borgen van veiligheid
- ❑ AI levenscyclus management
- ❑ Data management
- ❑ Systeem en data integratie protocollen
- ❑ Transparante algoritmen processen
- ❑ Inrichten Data Stewards als rol
- ❑ Inrichten cybersecurity rol of afdeling

ONTWERPBESLISSINGEN

Technologische overwegingen of beslissingen die bepalend zijn voor de AI oplossing architectuur

- ❑ Welke data is nodig, van welke kwaliteit?
- ❑ Inkopen of zelf ontwikkelen?
 - ❑ AI inkoopvoorwaarden toets
- ❑ Cloud, private cloud of lokaal?
- ❑ Open Source of closed source?
- ❑ Welke architectuur patronen en bouwblokken lenen zich het best voor de use case?
- ❑ Welke bestaande systemen moeten samenwerken met de AI oplossing?

CONTEXTBESLISSINGEN

Overwegingen of beslissingen die bepalend of randvoorwaardelijk zijn voor de vormgeving van de AI oplossing

- ❑ Wat is de use case?
- ❑ Wie is de gebruiker?
- ❑ Hoe gaat de gebruiker de oplossing gebruiken?
- ❑ Aan welke criteria moet AI oplossing voldoen?
- ❑ Is AI business case positief?
- ❑ Is proceseigenaar/ opdrachtgever akkoord?
 - ❑ AI afwegingskader
- ❑ Zijn benodigde middelen (tijd, geld, kennis) beschikbaar?
- ❑ Is de organisatie gebruiker en/of leverancier?
- ❑ AI Beslissing uitgevoerd?
- ❑ Welke risico classificatie op basis van AI Act?
- ❑ Impact assessments gedaan?
 - ❑ Ethisch assesment
 - ❑ Privacy risk assesment PRA/ DPIA
 - ❑ AI compliance pré-IAMA/ IAMA?
 - ❑ Informatie beheer regime bepaald?
 - ❑ AI architectuur principes getoetst?
- ❑ Kwaliteitsbeheer (monitoring)
- ❑ Functioneeringsgesprek AI
- ❑ Registratie in algoritme register?

AI TECH. COMPETENTIES

Competenties voor AI om te ontwikkelen in de organisatie op technologisch vlak

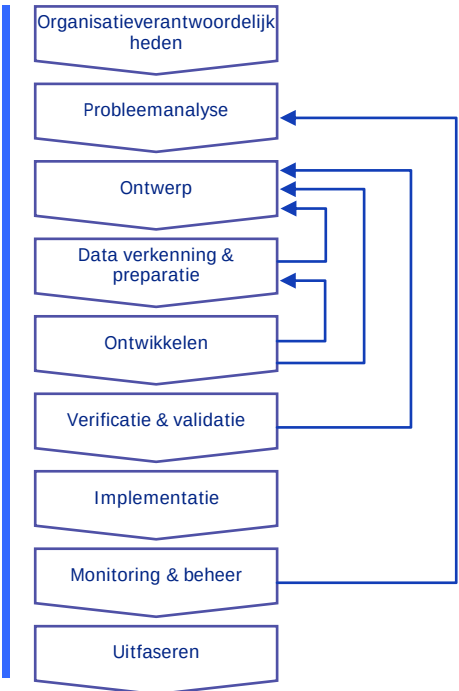
- Houding
WEET WAAROM

Operationeel
WEET HOE

AI geletterdheid
WEET WAT
1. Technologische nieuwsgierigheid
 2. Positieve houding ten opzichte van AI
 3. Technisch ontwerpdenken
 4. Data-georiënteerde cultuur
 5. Databasemanagement
 6. Data governance
 7. Dataverzameling
 8. Datamodellering
 9. Beoordeling van datakwaliteit
 10. Data-analyse
 11. Datavisualisatie
 12. Data delen
 13. Keuze van AI-architectuur
 14. Keuze van machine learning-technieken
 15. AI-gerelateerd softwareprogrammeren
 16. Trainen van algoritmes
 17. Naleving van AI-technische standaarden
 18. Prompt engineering
 19. Basiskennis van data-geletterdheid
 20. Inzicht in causale analyse en besluitvormingstheorie
 21. Begrip van de fundamenteën van ML
 22. Inzicht in AI-computervisie
 23. Inzicht in natuurlijke taalverwerking
 24. Inzicht in toegepaste wiskunde
 25. Inzicht in AI-softwareontwikkelingscycli

AI LEVENSCYCLUS

Het standaard proces dat wordt doorgelopen bij het ontwikkelen van AI



IMPLEMENTATIERICHTLIJNEN

Algemene richtlijnen ter overweging bij het ontwerp van AI oplossingen

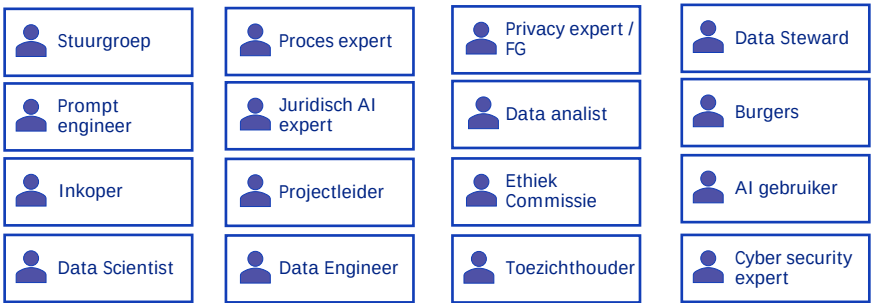
- ❑ Controleer datakwaliteit van databronnen, start kwaliteit verbeteringen
- ❑ Alleen persoonsgegevens gebruiken in een private cloud (gecertificeerd) of lokaal
- ❑ API's en datapipeline voorzien van privacy beschermingsmaatregelen i.g.v. persoonsgegevens
- ❑ Reguliere bias en input datakwaliteit controle en resultaat door menselijke validatie is vereist
- ❑ Altijd toets eindgebruiker op resultaat
- ❑ Transparantie en informatieverstrekking
- aan gebruiksverantwoordelijken
 - ❑ Systeem voor risicobeheer, logging, corrigerende maatregelen,
 - ❑ Infrastructuur AI compliance richtlijnen:
 - ❑ ISO 27001 IT informatiebeveiliging
 - ❑ ISAE3000 SOC2 verklaring
 - ❑ NEN 7510 informatiebeveiliging zorgsector
 - ❑ Sovereign Cloud SCS Standards –
 - ❑ Exit strategie
 - ❑ Eigendom code – public money is public code
 - ❑ Prompt injection voorkomen:

Implementeer “human-in-the-loop”, zero-trust principes toepassen en least-privilege toegang

- ❑ API- en context window chatbot-rate limits voorkomen DDOS aanval
- ❑ Controleer of data van derden gebruikt mag worden voor training
- ❑ Toegangsbeheer inperken van plugins
- ❑ Application Security Verification Standard toepassen

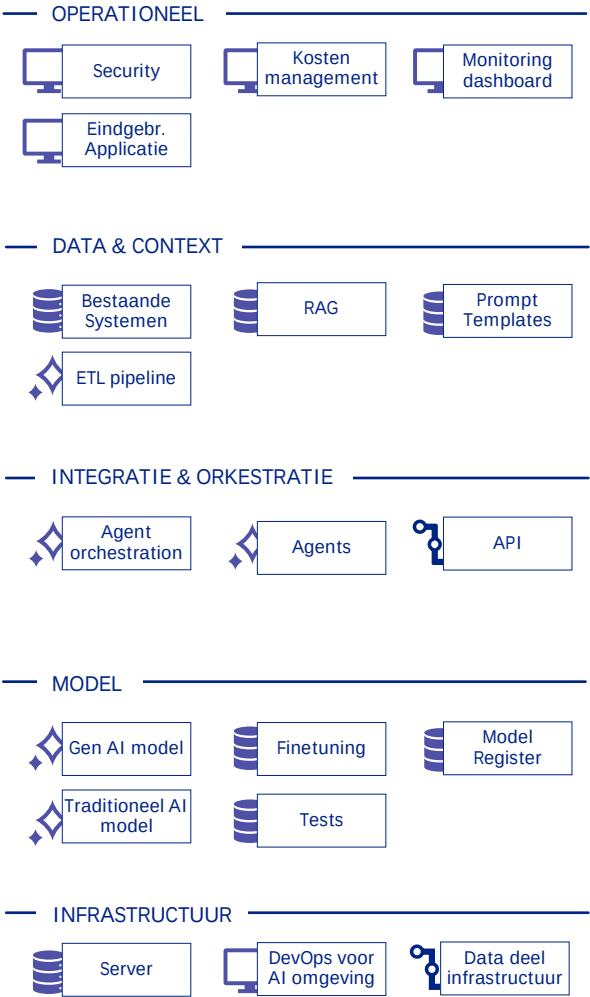
AI ROLLEN

Rollen om overwegen te betrekken bij het ontwikkelen bij AI



BOUWBLOKKEN

Een bouwblok is een modulair component met een specifieke functie binnen het AI ontwikkel proces



AI SOLUTION ARCHITECTUUR

TITEL:

OMSCHRIJVING:

PATRONEN

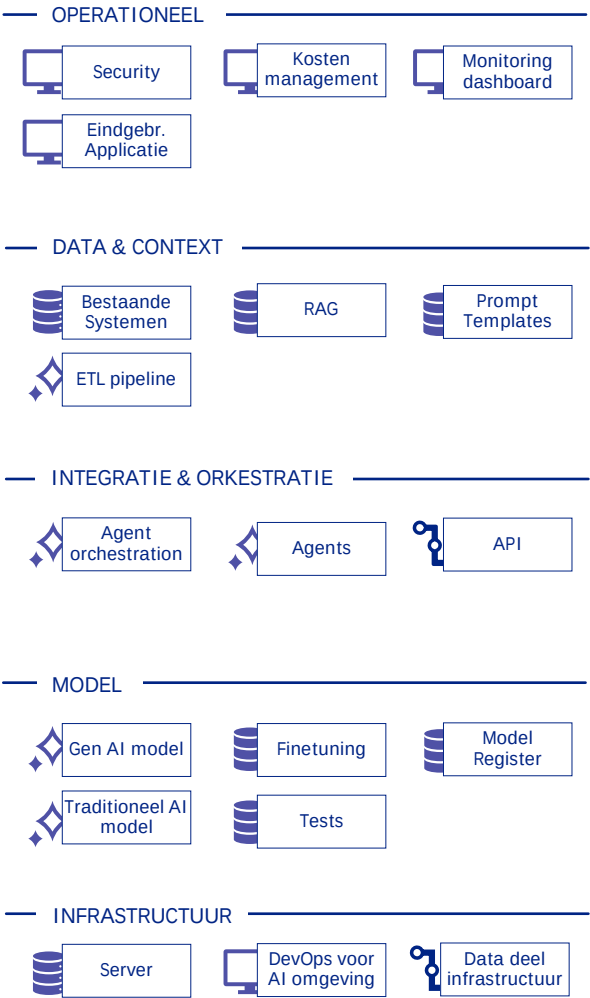
Patronen zijn veelvoorkomende interacties van bouwblokken in AI toepassingen

1. Standaard gebruik ML	11. LLM prompt engineering
2. ML in applicatie	12. LLM output verbeteren feedback
3. ML in federated learning	13. LLM als 2e chatbot
4. Standaard gebruik LLM	14. Documenten, data zoeken (RAG)
5. LLM training data genereren chatbot	15. Documenten, data zoeken (KAG)
6. LLM metadata classificatie genereren	16. LLM met rekenmodel
7. LLM beeld & beschrijving genereren	17. Finetuning LLM
8. LLM in applicatie	18. Complexe data analyse met LLM
9. Podcast of video genereren	19. Geavanceerd zoeken & vinden
10. LLM in applicatie workflow	20. Agent met complexe taken

Hierboven staan namen van patronen op basis van input van gemeente Utrecht. Patronen zijn beperkt uitgewerkt in dit rapport.

BOUWBLOKKEN

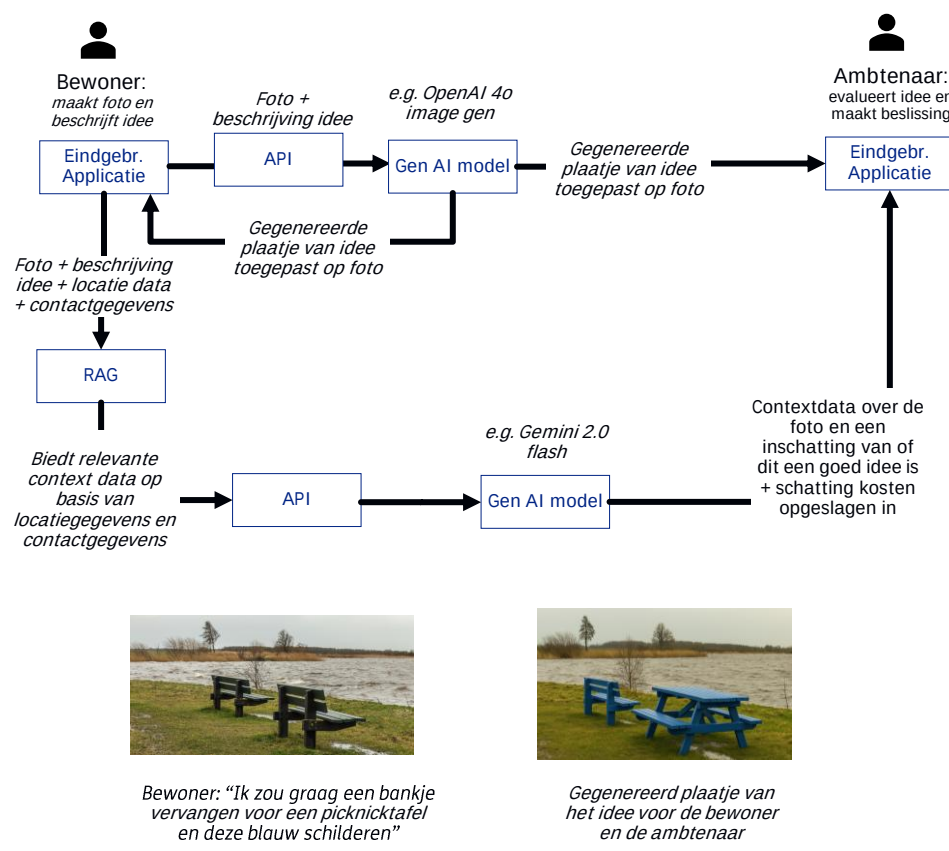
Een bouwblok is een modulair component met een specifieke functie binnen het AI ontwikkel proces



AI SOLUTION ARCHITECTUUR

Buurtbloei - Fictief voorbeeld

Veel gemeenten hebben kleine budgetten (zoals wijkbudgetten) waarmee inwoners hyperlokale verbeteringen kunnen voorstellen, zoals een klein stukje met wilde bloemen, een buurtprikbord, een extra bankje, of het beschilderen van een elektriciteitskastje. De "Buurtbloei" tool zou op basis van een beschrijving en foto van de bewoner al een voorstelling kunnen maken voor hoe het eindresultaat eruit ziet en maakt een eerste inschatting van of het idee past bij de buurt en gemeente ter overweging voor de betreffende ambtenaar.



PATRONEN

Patronen zijn veelvoorkomende interacties van bouwblokken in AI toepassingen

- | | |
|---|------------------------------------|
| 1. Standaard gebruik ML | 11. LLM prompt engineering |
| 2. ML in applicatie | 12. LLM output verbeteren feedback |
| 3. ML in federated learning | 13. LLM als 2e chatbot |
| 4. Standaard gebruik LLM | 14. Documenten, data zoeken (RAG) |
| 5. LLM training data genereren chatbot | 15. Documenten, data zoeken (KAG) |
| 6. LLM metadata classificatie genereren | 16. LLM met rekenmodel |
| 7. LLM beeld & beschrijving genereren | 17. Finetuning LLM |
| 8. LLM in applicatie | 18. Complexe data analyse met LLM |
| 9. Podcast of video genereren | 19. Geadvanceerd zoeken & vinden |
| 10. LLM in applicatie workflow | 20. Agent met complexe taken |

Hierboven staan namen van patronen op basis van input van gemeente Utrecht. Patronen zijn beperkt uitgewerkt in dit rapport.

Bouwblokken

Een bouwblok is een modulair component met een specifieke functie binnen het AI ontwikkel proces. De bouwblokken zijn opgedeeld in een “basis”, “gevorderd”, en “expert” niveau. Naarmate de IT maturiteit van de organisatie hoger is kunnen complexere vormen van bouwblokken worden verkent. Dit is een indicatieve opdeling; wat past bij de organisatie en use case kan van deze opdeling afwijken.

Het “basis” niveau vraagt weinig voorkennis om mee te kunnen experimenteren. Het aanbevolen startpunt voor organisaties om te beginnen met de data voor een use case. Is de beschikbare data in de bestaande systemen van voldoende kwaliteit? En, is de data die relevant is voor de use case voldoende beschikbaar? De data is vaak het startpunt voor hoge kwaliteit AI toepassingen. Daarnaast kunnen beginners gebruik maken van bestaande, goed presterende AI modellen en deze beschikbaar stellen

aan de gebruikers.

Het “gevorderde” niveau breidt uit op ‘off-the-shelf’ AI oplossingen en maakt AI meer specifiek voor de organisatiecontext. Dit door data toe te voegen en AI voor specifieke doeleinden in te zetten. Dit vereist meer zicht op de in- en output van de AI modellen.

Het “expert” niveau zet AI in om verregaande integratie en automatiseren te realiseren. Dit gaat over het beschikbaar maken tools en memory voor AI agents, het orchestreren van agents en het opschalen van AI toepassingen. Security van AI oplossingen is randvoorwaardelijk, maar wordt nog belangrijker naarmate AI meer autonoom opereert.



*= connecties
tussen systemen*



*=software ten
behoefte van AI
& AI modellen*



*= systeem /
data / dataset*



*= applicatie(s)
met front-end*



Bestaande systemen

Bestaande Systemen – data voor AI

De huidige IT-infrastructuur en dataopslag in de organisatie.

Basis

Stel datasets beschikbaar voor AI ontwikkeling. De totale set aan data in de organisatie vormt een waardevolle kennisbasis van de organisatie voor AI toepassingen. Zorgt voor connectie met legacy systemen en bestaande databronnen. Data management in de bestaande systemen is cruciaal voor succesvolle AI. Het preprocessen van data voor AI is vaak nodig om voldoende hoge kwaliteit datasets te creëren (e.g. zie CRISP-DM proces).

Gevorderd

Verbind de output van AI modellen aan

bestaande systemen en applicaties. AI functionaliteiten kunnen worden toegevoegd aan bestaande systemen, bijvoorbeeld om data kwaliteit te bevorderen.

Expert

Alle systemen in de organisatie zijn geïntegreerd met de AI van de organisatie.

Best Practises:

- Maak gebruik van gestandaardiseerde data modellen waar mogelijk. Bijvoorbeeld het Gemeentelijk Gegevens Model (GGM)
- Monitor en verbeter de data kwaliteit
- Creëer overzicht in welke data beschikbaar is, en welke nog (meer) moet worden verzameld om waardevolle use cases in de toekomst uit te kunnen voeren.

GenAI model

GenAI model –voorgetrainde AI

Het kernmodel dat tekst, code, beelden, of andere content genereert. Basis van de generatieve capaciteiten en beredeneervermogen.

Basis

Maak gebruik van voorgetrainde modellen, bijvoorbeeld LLMs, om administratieve en tekstgerelateerde taken te ondersteunen. Via een developer API kan worden geïnteracteed.

Gevorderd

Gebruik GenAI modellen zoals VLMs, of LLMs in combinatie met traditionele AI (e.g. OCR, ASR) om met andere vormen van data dan tekst te kunnen werken.

Expert

Zelf ontwikkelen van GenAI modellen, bijvoorbeeld voortbouwend op open source pre-trained modellen. Voor de meeste bedrijven is dit op dit moment geen realistische optie door de benodigde investeringen.

Best practises:

- AI modellen ontwikkelen snel. Niet elk GenAI model is even goed in elke taak. Bij het kiezen van een GenAI model, evalueer de performance op dat moment. (e.g. [Lmarena](#))
- Experimenteer eerst met het model in de context van de use case. In hoeverre helpt het model met de use case zonder enige aanpassingen of context?
- In Nederland wordt GPT-NL ontwikkelt in lijn met Europese waarden rondom data verzameling en training. De kwaliteit van het model zal niet even hoog zijn als de modellen van grote bedrijven, maar voor specifieke use cases kan dit een wenselijke optie zijn.

Traditioneel AI model

Traditioneel AI model

Modellen die voorspellingen maken op basis van rule-based, machine learning, of deep learning technieken.

Basis

Implementatie van standaard machine learning algoritmen zoals regressie, classificatie of clustering voor specifieke taken.

Gevorderd

Combinatie van verschillende traditionele AI-technieken in ensembles, met feature engineering en model optimalisatie.

Expert

Hybride systemen die traditionele AI combineren met GenAI, met automatische model selectie en adaptieve

leerstrategieën.

Best Practises:

- Evalueer of een traditioneel model beter geschikt is voor je use case dan GenAI
- Begin met eenvoudige modellen en schaal alleen op als prestaties niet voldoen
- Documenteer datapreprocessen en feature engineering stappen
- Implementeer version control voor datasets, code en modellen
- Zorg voor explainability van model beslissingen
- Train de modellen regelmatig op nieuwe data om concept drift tegen te gaan



API for AI and Agents

AI API – het beschikbaar stellen van AI
Interfaces voor communicatie tussen applicaties, AI-modellen en Agents. Standaardiseert de toegang tot AI-functionaliteit.

Basis

Maak gebruik van reeds beschikbare APIs.

Gevorderd

Ontwikkel eigen APIs voor AI toepassingen. Denk hierbij ook aan toegangscontrole. Sluit aan bij gestandaardiseerde protocollen (e.g. MCP voor Agent tools en het Agent2Agent protocol om agents publiek te maken).

Expert

-

Best practises:

- Ga voorzichtig om met de secret keys
- Maak gebruik van gestandaardiseerde interfaces waar mogelijk. Dat maakt data delen eenvoudiger
- Gebruik open standaarden om de APIs te specificeren (e.g. OpenAPI)
- Denk goed na over hoe de eindgebruiker kan interacteren met de API



Prompt Templates

Prompt Templates

Set van gestandaardiseerde invoerstructuren voor consistente GenAI-interacties die het optimaliseren van invoer voor gewenste uitvoer mogelijk maken.

Basis

Voor terugkerende vragen een goed gestructureerde opzet van de vraag, met bijbehorende eisen die worden gesteld aan de output.

Gevorderd

Ontwikkeling van dynamische prompt templates die zich aanpassen aan gebruikerscontext en beschikbare data. Hierbij worden parameters in de prompt automatisch gevuld op basis van de gebruikersinteractie.

Expert

Geautomatiseerde ontwikkeling en optimalisatie van prompts via A/B-testen en feedback loops. Het systeem leert welke prompts het beste werken voor specifieke gebruikersgroepen en use cases.

Best Practises:

- Experimenteer met verschillende prompts en evalueer de output systematisch
- Maak de context die mensen in hun hoofd hebben expliciet
- Wees specifiek over de eisen waaraan de output moet voldoen
- Beperk de prompt tot alleen de meest relevante informatie
- Gebruik een consistente stijl en tone-of-voice voor prompts
- Documenteer succesvolle prompt patronen en deel deze binnen je organisatie



Kosten management

Kosten management

Systeem voor het monitoren, voorspellen en optimaliseren van kosten die gerelateerd zijn aan AI-oplossingen.

Basis

Monitoring van basiskosten zoals API-gebruik en serverkosten, met maandelijkse rapportages.

Gevorderd

Gedetailleerde analyse en voorspellingen van kostencomponenten per AI-toepassing en gebruiker.

Expert

-

Best Practises:

- Maak gebruik van dashboards voor de

kosten van AI toepassingen, combineer deze in een overzicht als er veel verschillende kostenposten zijn.

- Begrijp goed waardoor kosten worden gemaakt: type model, input tokens, output tokens, reasoning tokens, subscriptions, hardware kosten, etc.
- Implementeer kostenlimieten en waarschuwingen bij onverwachte pieken
- Optimaliseer prompt lengte en modelkeuze op basis van kosten/kwaliteit verhouding
- Gebruik caching strategieën om herhaalde identieke vragen niet opnieuw te hoeven verwerken
- Overweeg finetuning voor veelgebruikte toepassingen om tokens te besparen



RAG

Retrieval Augmented Generation (RAG)

Verbeterd AI-generatie door relevante informatie uit externe bronnen op te halen en te combineren met generatieve capaciteiten.

Basis

-

Gevorderd

Implementatie waarbij documenten worden opgeslagen in een (vector, graaf) database en op basis van semantic search worden opgehaald om context te bieden aan een GenAI model.

Expert

Adaptieve RAG systemen die leren van gebruikersinteracties welke bronnen en informatie relevant zijn en automatisch

worden ge-update met nieuwe relevante informatie.

Best Practises:

- Gebruik de RAG eerst als interne search naar documenten, voordat je de RAG aan het AI model koppelt. Zo weet je of de RAG goed functioneert.
- Monitor en evalueer de kwaliteit van de retrieval componenten apart van de generatie
- Experimenteer met verschillende chunking strategieën voor optimale informatie retrieval
- Implementeer metadata filtering om de relevantie van zoekresultaten te verbeteren
- Gebruik reranking om de meest relevante documenten bovenaan te krijgen
- Houd bronverwijzingen bij om traceerbaarheid te garanderen
- Houd rekening met de contextwindow van het GenAI model dat wordt gebruikt. De RAG behoort kleiner te zijn dan de contextwindow van het model



Finetuning

Finetuning

Aanpassing van het basismodel voor specifieke toepassingen door het trainen van pre-trained modellen op domein-specifieke data.

Basis

-

Gevorderd

Finetunen van bestaande modellen met domain-specifieke data, met focus op specifieke doeleinden

Expert

Continue leren en iteratief finetuning met human feedback loops (RLHF)

Best Practises:

- Evalueer eerst of RAG, prompt

engineering of andere technieken voldoende zijn voordat je finetuning overweegt

- Zorg voor hoge kwaliteit, representatieve trainingdata die de beoogde use case goed afdekt
- Gebruik parameter-efficiënte methoden zoals LoRA of QLoRA voor kosteneffectief finetunen
- Implementeer evaluatiemethoden voor het vergelijken van prestatieverbeteringen
- Documenteer het finetuning proces en bewaar checkpoints voor reproduceerbare resultaten
- Voorkom overfitting door goede validatie datasets en early stopping



Eindgebruiker Applicatie

Eindgebruiker Applicatie

Interface waarmee eindgebruikers met de AI interacteren en die toegang biedt tot AI-functionaliteiten.

Basis

Eenvoudige chat-interface of formulier waarmee gebruikers kunnen communiceren met de AI-functionaliteit.

Gevorderd

Ingebouwd in bestaande applicaties om te integreren met bestaande werkprocessen. Multimodale interfaces met ondersteuning voor tekst, spraak, beeld en documenten.

Expert

Context-bewuste interfaces die zich aanpassen aan gebruikersgedrag en

intenties, met proactieve suggesties en integratie tussen verschillende systemen.

Best Practises:

- Ontwerp de interface vanuit gebruikersperspectief, niet primair vanuit technische mogelijkheden
- Maak verwachtingen over capaciteiten en beperkingen van de AI duidelijk
- Ben transparant over wanneer AI wordt gebruikt naar de gebruiker
- Implementeer feedback mechanismen zodat gebruikers output kunnen beoordelen
- Bouw mechanismen voor het verklaren van AI-beslissingen (explainable AI)
- Test de interface met diverse gebruikersgroepen voordat je breed uitrolt
- Bied verschillende interactiemethoden aan die passen bij verschillende gebruikersbehoeften



Tests

Tests

Validatiemechanismen om de AI-oplossing te controleren en evalueren.

Basis

Handmatige evaluatie van AI-output op basis van vooraf gedefinieerde testcases en acceptatiecriteria.

Gevorderd

Geautomatiseerde test frameworks met benchmarkdatasets en metrieken voor evaluatie van model prestaties, zoals accuraatheid, mate van hallucinaties en consistentie.

Expert

-

Best Practises:

- Definieer duidelijke evaluatiemetrieken die aansluiten bij de use case
- Creëer een representatieve testset die edge cases en veelvoorkomende scenario's bevat
- Implementeer zowel automatische als menselijke evaluatie
- Test niet alleen op functionaliteit maar ook op veiligheid, bias en hallucinaties
- Implementeer continuous testing bij updates van modellen of datasets



Server

Server

Infrastructuur die de AI-modellen en gerelateerde diensten host. Deze servers kunnen lokaal worden gehost, in een private cloud, of in de publieke cloud.

Basis

Gebruik van cloud-gebaseerde infrastructure as a service (IaaS) of platform as a service (PaaS) oplossingen voor het hosten van AI-toepassingen.

Gevorderd

Overweeg gebruik van private cloud oplossingen en lokale hosting van AI modellen op kleine schaal voor specifieke toepassingen.

Expert

Lokaal schaalbare en veerkrachtige serverarchitectuur.

Best Practises:

- Overweeg in hoeverre de organisatie werkt met gevoelige data. Hoe gevoeliger de data, hoe meer waarde het heeft om gecertificeerde private cloud of lokale servers te overwegen voor specifieke use cases.
- Kies de juiste hardware voor je specifieke AI-workload (CPU, GPU, TPU) (e.g. Hoe veel gebruikers zijn er in parallel, en hoe veel token per seconde moeten kunnen worden gegenereerd per gebruiker?)
- Implementeer effectieve caching strategieën om herhaalde berekeningen te voorkomen
- Zorg voor schaalbaarheid om pieken in het gebruik op te vangen
- Monitor resource gebruik en optimaliseer waar mogelijk
- Implementeer robuuste backup en disaster recovery strategieën



Monitoring Dashboard

Monitoring Dashboard

Visualisatie en controle van pipelines, AI prestaties en -gebruik van AI-oplossingen.

Basis

Reguliere Monitoring van technische metrics zoals server uptime, responstijden en aantal verzoeken, inclusief evaluaties van AI model prestaties voor eindgebruikers.

Gevorderd

Continue monitoring van model-specifieke metrics zoals token gebruik, model performance, en gebruikersinteractie-patronen met alerts bij afwijkingen of onwenselijk gedrag van de AI.

Expert

Geavanceerde analytics met predictieve

monitoring, anomaliedetectie, en geautomatiseerde diagnostiek voor proactief beheer van de AI-infrastructuur.

Best Practises:

- Definieer key performance indicators (KPIs) die relevant zijn voor zowel technische als business doelen. Sommige KPIs gelden voor elke use case, maar er zijn aanpassingen nodig die specifiek zijn voor de use cases.
- Implementeer real-time monitoring voor snelle detectie van problemen via een live dashboard
- Creëer alerts voor kritieke metriek-drempelwaarden of specifiek woord/zinsgebruik in prompts en AI output, privacy van gebruikers in acht nemend.
- Visualiseer trends over tijd om patronen te identificeren
- Maak dashboards toegankelijk voor verschillende stakeholders met relevante views
- Verzamel en analyseer gebruikersfeedback naast technische metrics



Agents

Agents

Autonome componenten die taken kunnen uitvoeren met of namens de AI. Gebruikt (Gen)AI model als kern voor intelligentie.

Basis

Maak gebruik van APIs van agents gebouwd door anderen

Gevorderd

Creëer gerichte single-task agents die specifieke functies uitvoeren zoals information retrieval of data transformatie.

Met toegang tot verschillende tools, databases en APIs om taken uit te voeren. Maak gebruik van een low-code platform (e.g. N8N)

Expert

Zelf-lerende agents die op basis van geheugen steeds beter worden in het uitvoeren van taken. Integratie met agent orkestratie.

Best Practises:

- Definieer duidelijke scope en verantwoordelijkheden voor elke agent
- Implementeer robuuste feedback mechanismen voor agent acties
- Bouw veiligheidsmaatregelen in om ongewenst gedrag te voorkomen
- Zorg voor transparantie in agent besluitvorming en houd, zeker voor taken met impact op mensen een human-in-the-loop
- Implementeer logging van alle agent acties voor audit en debuggen
- Test agents uitgebreid in gecontroleerde omgevingen voor productie
- Maak gebruik van gestandaardiseerde protocollen voor Agent tools (MCP van Anthropic) en Agent to Agent communicatie (A2A van google)



Agent orkestratie

Agent orkestratie

Coördineert de werkstroom tussen verschillende agents en beheert de volgorde en afhankelijkheden tussen AI-componenten. Kun je zien als een assistent die voor een eindgebruiker andere agents aanstuurt.

Basis

-

Gevorderd

Taakverdeling tussen agents op basis van een verzoek van een gebruiker. Weet welke agents voor welke functionaliteiten worden aangeroepen en wanneer welke feedback terug te geven aan de gebruiker

Expert

Zelforganiserende agent ecosystemen met emergente samenwerkingspatronen

en adaptieve optimalisatie van werkprocessen.

Best Practises:

- Begin met duidelijk gedefinieerde, eenvoudige workflows voordat je opschaaft
- Test werkstromen uitvoerig, zeker als ze impact hebben op mensen
- Implementeer effectieve communicatieprotocollen tussen agents en baseer je op bestaande standaarden (e.g. MCP, A2A)
- Bouw fail-safe mechanismen in wanneer een agent faalt en communicatieprotollen in geval van falen
- Creëer evaluatiemechanismen voor de kwaliteit van agent output
- Ontwerp herbruikbare orchestration patterns voor verschillende use cases



DevOps voor AI omgeving

DevOps voor AI omgeving

Tooling voor ontwikkeling, deployment en onderhoud van AI-modellen gedurende hun volledige levenscyclus.

Basis

Basistools voor versiebeheer van code en modellen, met handmatige deployment processen.

Gevorderd

Geautomatiseerde CI/CD pipelines specifiek voor AI-modellen, met geautomatiseerde testing en deployment mechanismen.

Expert

Volledig geïntegreerde MLOps omgeving met feature stores, model registers, experiment tracking en geautomatiseerde

model governance.

Best Practises:

- Implementeer model versioning en experiment tracking vanaf het begin van implementeren van AI
- Automatiseer het testen van modellen als onderdeel van de CI/CD pipeline
- Creëer reproduceerbare development environments
- Houd een centrale registry bij van getrainde modellen en hun metadata
- Implementeer rollback strategieën voor nieuwe modellen

Security

Security

Beveiligingsmaatregelen om AI-systemen te beschermen tegen misbruik en aanvallen. Een centrale vraag is: wie mag welke data wanneer inzien? Gebruikmaken van AI buiten de gemeente. Onderzoeken

Basis

Standaard beveiligingsmaatregelen zoals authenticatie, autorisatie en input validatie voor AI-systemen.

Gevorderd

Implementatie van prompt injection detectie, data privacy maatregelen en monitoring van verdacht gebruik.

Expert

Geautomatiseerd handhaven van de regels over die welke data wanneer mag inzien.

Geavanceerde AI-specifieke beveiligingsmaatregelen, zoals adversarial testing, model forensics en continuous security validation van zowel model als infrastructuur.

Best Practises:

- Implementeer robuuste authenticatie en autorisatie voor alle AI-interfaces
- Scan inputs op prompt injection en malintenties
- Beperk token quota's en API rate limits om misbruik te voorkomen
- Versleutel gevoelige data, zowel in transit als at rest
- Evalueer preprocessing van data op het succesvol filteren van – en omgaan met - Personally Identifiable Information (PII)
- Voer regelmatig penetratietesten uit op de AI toepassingen en infrastructuur van de organisatie



Model Register

Model Register

Centraal registratiesysteem voor het beheren, volgen en documenteren van AI-modellen, Agents en hun versies gebruikt in de organisatie.

Basis

-

Gevorderd

Eenvoudige documentatie van modelversies, agents, prompts, RAG, parameter en training datasets in een gestructureerde repository.

Expert

Geautomatiseerd model registratiesysteem met metadata, performance metrics, lineage tracking en model/agent approval workflows.

Best Practises:

- Documenteer elk model of agent met minimaal: versie, trainingsdatum, dataset informatie, performance metrics en intended use
- Implementeer een formeel goedkeuringsproces voor productiemodellen
- Leg modelafhankelijkheden vast om impact van wijzigingen te kunnen bepalen
- Zorg voor traceerbaarheid tussen model versies en productieresultaten
- Maak rollback naar eerdere versies eenvoudig mogelijk
- Integreer het model register met de CI/CD pipeline en monitoring systemen



ETL Pipeline

ETL pipeline

Systeem voor het Extracten, Transformeren en Laden van data uit diverse bronnen naar AI-geschikte formaten en opslagsystemen.

Basis

Handmatige of geplande batch processen voor het verzamelen en prepareren van data uit primaire bronnen, inclusief data cleaning, normalisatie en feature engineering voor het voorbereiden van data voor specifieke AI-modellen of agents.

Gevorderd

Geautomatiseerde ((near) real-time) pijplijnen, met error handling en monitoring en een set functies om datatransformaties uit te voeren.

Expert

-

Best Practises:

- Maak een bibliotheek van functies die veel worden gebruikt in het verwerken van de data van jouw organisatie
- Documenteer transformaties en hun rationale duidelijk
- Implementeer validatiestappen om data kwaliteit na transformatie te garanderen
- Bouw preprocessing pijplijnen modulair voor hergebruik en onderhoud
- Zorg dat preprocessing functies zowel in development als productie identiek werken
- Monitor data drift om te detecteren wanneer preprocessing aanpassingen nodig zijn
- Bouw data kwaliteitscontroles in op kritieke punten in de pipeline
- Creëer metadata over data lineage voor audit en compliance doeleinden



Data deel infrastructuur

Data deel infrastructuur – het delen van data voor AI

Afspraken en technische componenten die het delen van data tussen organisaties faciliteren.

Basis

Ad hoc dataset delen

Gevorderd

Afspraken met partners over data delen inclusief over data modellen

Expert

Netwerk van partners waarmee eenvoudig en continue data kan worden gedeeld voor AI doeleinden.

Best practises:

- Maak gebruik van gestandaardiseerde

interfaces waar mogelijk. Dat maakt data delen eenvoudiger. Bijvoorbeeld het Gemeentelijk Gegevens Model (GGM).

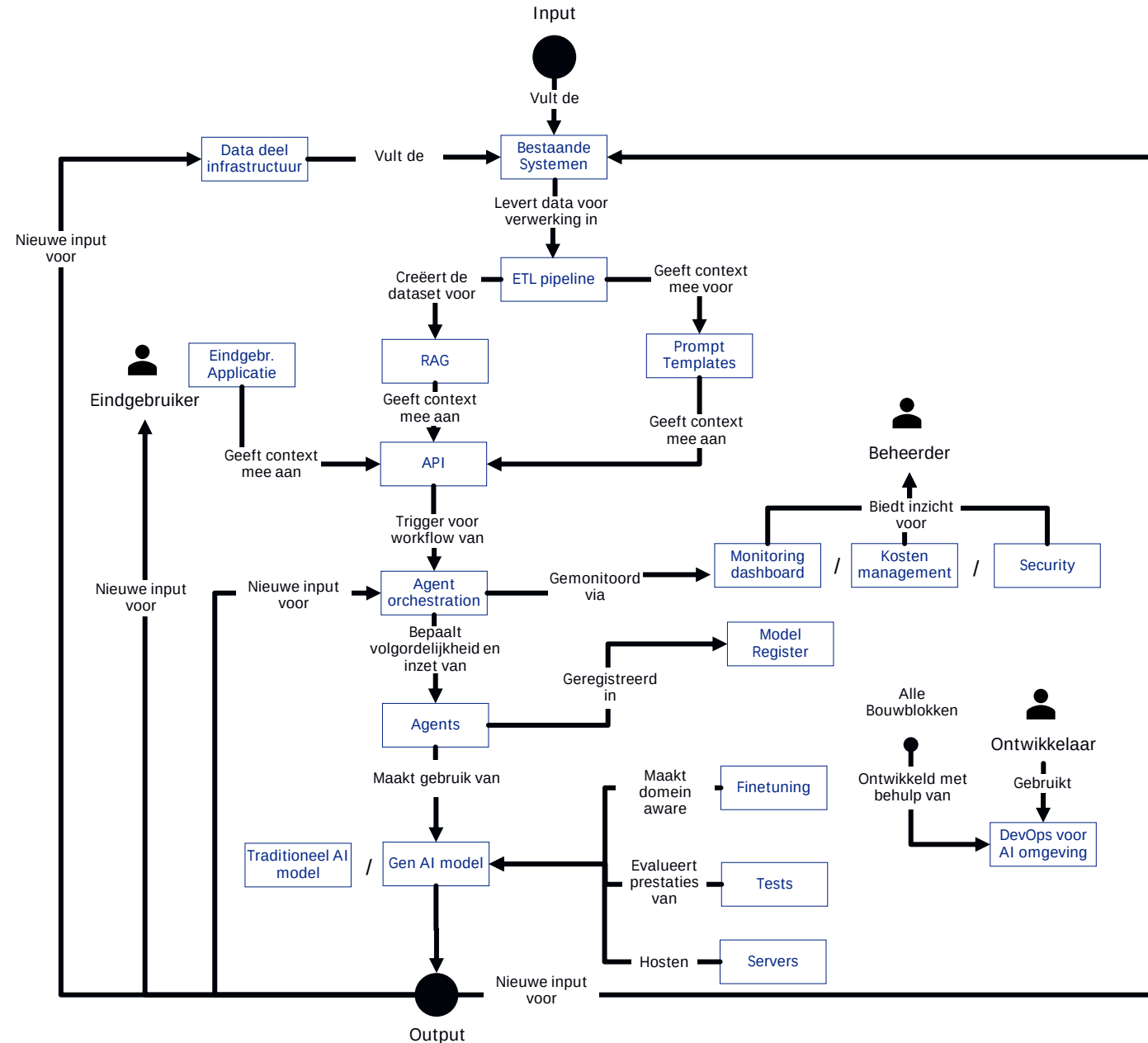
- Overweeg het gebruik van Data Spaces als afsprakenstelsels voor data delen voor AI (lees meer over data spaces in het Data Space Support Centre (DSSC))

Architectuurpatronen

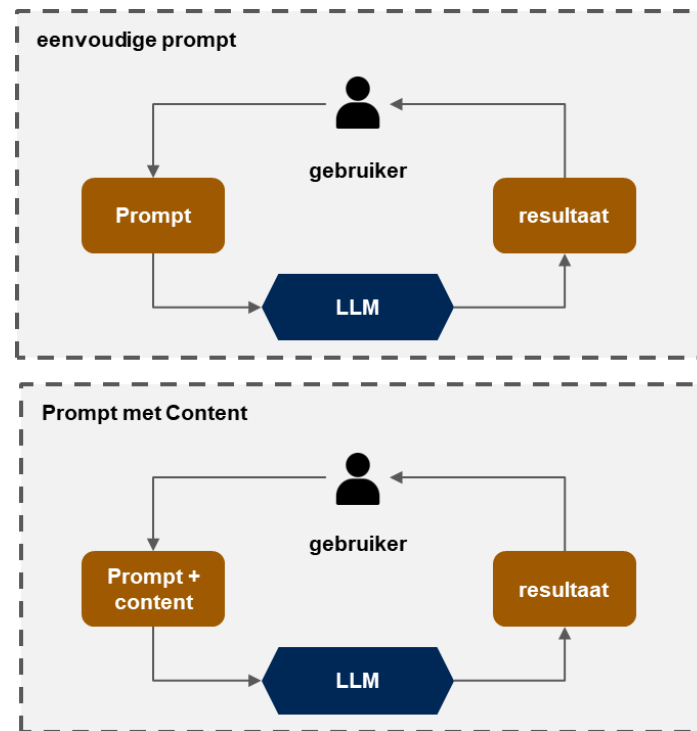
Architectuurpatronen zijn veelvoorkomende interacties die plaatsvinden als onderdeel van AI toepassingen. Architectuurpatronen zijn bedoelt als inspiratie voor het ontwerp van een AI solution architectuur.

Voor AI ontwikkeling is het nuttig om een collectie aan *eenvoudige en veelvoorkomende* patronen te verzamelen.

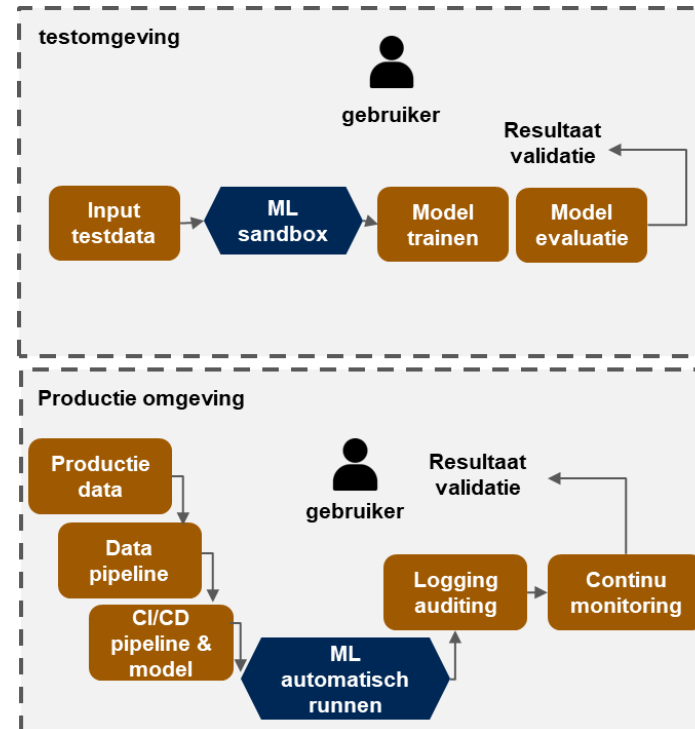
In het figuur op deze pagina indicatief geduid hoe de bouwblokken zich tot elkaar kunnen verhouden in een volwassen AI organisatie. Dit kan worden gezien als een complexe combinatie van patronen.



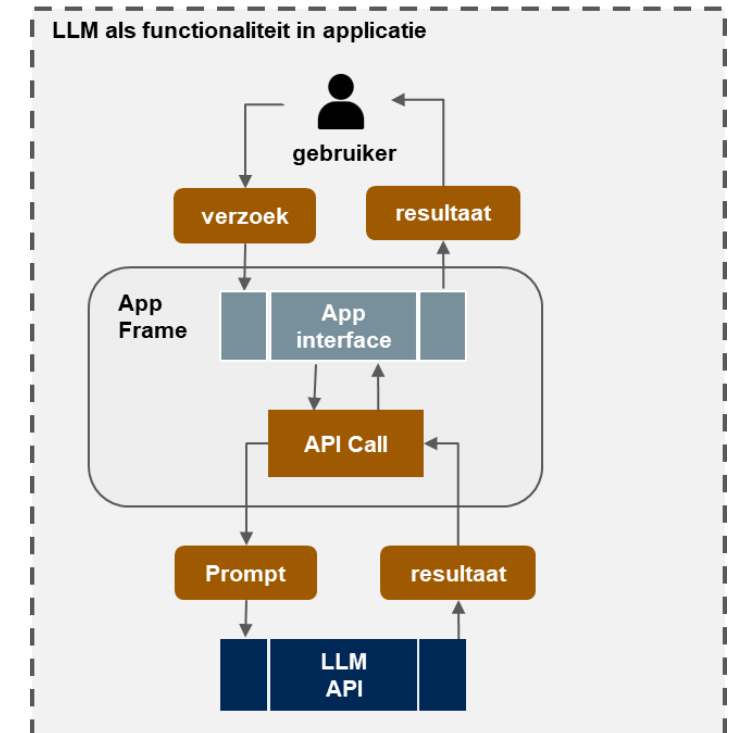
1. Eenvoudige prompt



2. Omgevingen



3. LLM als functionaliteit in applicatie



Voorbeelden van patronen geïdentificeerd door gemeente Utrecht (nog niet in lijn met de bouwblokken). Het doorontwikkelen van Architectuurpatronen valt buiten de scope van dit project.

Bron

Richtingen voor doorontwikkeling

1. Verfijning van de AI Referentiearchitectuur

De huidige referentiearchitectuur biedt een brede basis van AI kennis, maar is complex en met een beperkt aantal partijen ontwikkeld. Deze kan verder worden versterkt door:

Validatie met bestaande AI oplossingen: Bestaande AI-oplossingen van gemeenten kunnen worden ingetekend op de referentiearchitectuur. Hiermee kan de volledigheid en praktische toepasbaarheid worden getoetst.

Iteratieve verbetering door nieuwe praktijktoepassingen : De architectuur gebruiken en iteratief doorontwikkelen bij de start van nieuwe AI-projecten binnen gemeenten. Dit helpt bij het aanscherpen van de bouwblokken en herbruikbare (architectuur)patronen te specificeren.

Verzamel eenvoudige startpunten: de complexiteit de referentiearchitectuur kan

een drempel vormen. Startpunten om met AI aan de slag te gaan kunnen worden gemaakt. Bijvoorbeeld door voorbeelden van ingevulde solution architectures van eenvoudige, impactvolle use cases beschikbaar te stellen.

Inzet als Communicatiemiddel ('Praatplaat'): De architectuur positioneren als een startpunt voor een gemeenschappelijke taal en visueel hulpmiddel om de communicatie en afstemming tussen verschillende disciplines (zoals architecten, data scientists, beleidsmakers, informatiemanagers) binnen en tussen gemeenten te verbeteren.

2. Verzamelen, ontwikkelen en beschikbaar stellen van implementatierichtlijnen en software componenten

Om de stap van architectuur naar implementatie te verkleinen, stellen we voor om het volgende te verkennen:

Het uitwerken van de implementatierichtlijnen bij elk bouwblok. De implementatierichtlijnen kunnen richting geven bij praktische uitdagingen tijdens het ontwikkelen van AI

toepassingen. Denk hierbij aan aansluiting op standaarden zoals het Gemeentelijk GegevensModel (GGM), Common Ground principes (bijv. MCP, API-strategie/A2A), beveiligingsnormen (OWASP), cloudstrategieën (publiek/privaat/lokaal) en data-deelinfastructuren (zoals data spaces).

Beschikbaar stellen van een veilige sandboxomgeving en productieomgeving voor gemeenten: Overweeg om open source AI-modellen gecentraliseerd (lokaal / private cloud) aan te bieden. Dit stelt gemeenten in staat om op een veilige, gecontroleerde manier te experimenteren met AI-technologie, zonder direct grote investeringen te hoeven doen in eigen infrastructuur.

Softwarecomponenten beschikbaar te stellen: Zoeken naar voorbeelden van software (e.g. bestaand bij gemeenten of open source) die passen bij de verschillende bouwblokken van de referentiearchitectuur. Hierbij focussen op generieke taken die als eenvoudig implementeerbare (collectieve) oplossingen aangeboden kunnen worden aan gemeenten. Bepalen wat zich leent voor collectivisering. E.g. software om prompts automatisch te anonimiseren.

Bronnen en verdere informatie

- 2024/1689 geharmoniseerde regels betreffende artificiële intelligentie <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32024R1689#d1e2816-1-1>
- Binnenlandse Zaken en Koninkrijksrelaties (2025). Algoritmekader 2.0. [Het algoritmeregister van de Nederlandse overheid](#)
- Gemeente Amsterdam (z.d.). Modelbepalingen voor gemeenten voor verantwoord gebruik van algoritmische toepassingen. [Modelbepalingen voor gemeenten voor verantwoord gebruik van Algoritmische toepassingen - openresearch.amsterdam](#)
- Gemeente Utrecht (z.d.). Aanvulling op inkoopvoorwaarden AI. [niet publiek beschikbaar]
- Gemeente Utrecht (z.d.). AI referentiearchitectuur. [niet publiek beschikbaar]
- Europese Commissie (2024). EU model contractual AI clauses (updated version). [Updated EU AI model contractual clauses | Public Buyers Community](#)
- European Commission: Joint Research Centre, MEDAGLIA, R., MIKALEF, P. and TANGI, L., (2024) Competences and governance practices for artificial intelligence in the public sector (JRC138702). Geraadpleegd via <https://data.europa.eu/doi/10.2760/7895569>
- Europees Parlement (2024). Artificial Intelligence Act. Geraadpleegd via https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf
- Hoekstra, M., Dom, L. & van Veenstra, A. F. (2024). Quickscan AI in de Publieke Dienstverlening III. Geraadpleegd via <https://www.tno.nl/nl/newsroom/2024/06/kunstmatige-intelligentie-inzet-overheid/>
- Interne communicatie met TNO experts
- Interviews en vervolgesprekken met deelnemende gemeenten/gemeentelijke samenwerkingsverbanden
- ISO/IEC (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements <https://www.iso.org/standard/27001>
- Ministerie van Infrastructuur en Waterstaat (2024). AI Impact Assessment. <https://www.rijksoverheid.nl/documenten/rapporten/2022/11/30/ai-impact-assessment-ministerie-van-infrastructuur-en-waterstaat>

Bronnen en verdere informatie (vervolg)

- OWASP (2025). OWASP Application Security Verification Standard (ASVS). <https://owasp.org/www-project-application-security-verification-standard/>
- PIANOo Het kopen of laten ontwikkelen van algoritmes en AI: het inkopersperspectief. [Leidraad Community of Practice Digitale Innovaties](#)
- Rathenau Instituut (2023). Generatieve AI. [Generatieve AI | Rathenau Instituut](#)
- Redactie (2025, 2 januari). Het inkoopproces volgens van Weele. *Maanagement Platform*. [Het inkoopproces volgens van Weele – Management Platform](#)
- Responsible Sensing Lab (2024). Beta procurement tool for cities to safeguard autonomy. [Beta procurement tool for cities to safeguard autonomy |...](#)
- Rijksoverheid (2021). Impact Assessment Mensenrechten en Algoritmes. <https://www.rijksoverheid.nl/documenten/rapporten/2021/02/25/impact-assessment-mensenrechten-en-algoritmes>
- Sovereign Cloud Stack (2025). Sovereign Cloud Standards. <https://docs.scs.community/standards/scs-0001-v1-sovereign-cloud-standards/>
- TNO (2024). Whitepaper Verantwoorde AI door het faciliteren van bewuste keuzes. [Verantwoorde AI door het faciliteren van bewuste keuzes : Geleerde lessen in de publieke sector](#)
- Van Weele, J. H. (2018). *Purchasing and supply chain management*. Cengage Learning EMEA
- Vereniging van Nederlandse Gemeenten (2023). Gemeentelijke Inkoop bij IT Toolbox (GIBIT). [GIBIT | VNG](#)

TNO



Contact

Tessa.bruijne@tno.nl
noah.smeets@tno.nl

Disclaimer

Alle rechten voorbehouden

Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook zonder voorafgaande schriftelijke toestemming van TNO. Derden kunnen aan dit onderzoeksrapport geen rechten ontleen. Dit rapport is ontwikkeld met ondersteuning van Generatieve AI modellen. Mocht u vragen hebben over dit document of menen dat deze onjuistheden bevat, dan zijn wij daarvoor graag beschikbaar.

Hanna Barakat & Cambridge Diversity Fund /
<https://betterimagesofai.org/> /
<https://creativecommons.org/licenses/by/4.0/>

