MEMORIE VAN ANTWOORD

Memorie van Antwoord m.b.t. gestelde vóórvragen ex. artikel 10 van de "Verordening op de raadscommissies en beeldvormende-, informatieve- en opiniërende bijeenkomsten Beekdaelen 2023" van de raadsfractie **GL/PvdA** ten aanzien van het agendapunt **C1 Datagedreven werken in Beekdaelen** ter behandeling in de raadscommissie **SLO/B&M/FLO** van **2.12.2025.**

Vraag 1: Datagedreven werken wordt in de toekomst steeds belangrijker. De fracties van GroenLinks en de Partij van de Arbeid staan in principe achter het nu ingediend voorstel. Wij zouden alleen graag willen weten waarop de genoemde bedragen voor 2025 en verder gebaseerd zijn.

Antwoord:
In het Raadsvoorstel zijn de verwachte uitgaven van 2026 t/m 2029 opgenomen:

	2026	2027	2028	2029
Restant krediet	4.798			
Eenmalige kosten	53.100	53.100	41.100	41.100
Structurele kosten	110.138	137.577	163.277	189.470
Bij te ramen eenmalige kosten (tekort)	48.302	53.100	41.100	41.100
Bij te ramen structurele kosten (tekort)	110.138	137.577	163.277	189.470

De eenmalige kosten hebben betrekking op implementatiekosten, ondersteuning van leveranciers, trainingen en workshops voor het dataportaal, de fasegewijze invoering van AI en GIS-technologie.
De structurele kosten hebben betrekking op: licentiekosten, beheer, onderhoud en hosting van het dataplatform bij Solido, gebruiks-, beheer en onderhoudskosten van andere dataportalen (Vrijetijdseconomie, Parkstadmonitor), tooling die nodig is om dashboards te bouwen en te gebruiken, AI- en GIS-tooling (GIS staat voor geografisch informatiesysteem).

Vraag 2: Tussen de regels door lezen we dat de mens altijd centraal moet staan. Wij zouden echter graag expliciet vermeld willen zien dat menselijk contact voor de digitaal wat minder redzame burgers altijd mogelijk zal zijn (via balie of telefonisch). De overheid mag zich o.i. nooit kunnen verschuilen achter chatbots of door ChatGPT en anderen digitaal gegenereerde antwoorden.

Antwoord:
Wij kunnen ons volledig vinden in dit standpunt. Dit past volledig bij de uitgangspunten van de dienstverleningsvisie gemeente Beekdaelen 2024-20230 die het College eind 2023 heeft vastgesteld. De titel van deze visie is "*Passende dienstverlening voor elke Beekdaelenaar: klantgericht, dichtbij, duidelijk en transparant"* . Uitgangspunten zijn inclusiviteit, digitaal waar mogelijk en persoonlijk waar nodig. In deze dienstverleningsvisie is expliciet vermeld dat de gemeente zowel digitale alsook fysieke contactkanalen ondersteunt. Op 1 juli 2025 heeft het College het beleidskader voor AI vastgesteld. Een belangrijke maatregel die wij in ons beleid hebben vastgelegd is dat AI weliswaar mag ondersteunen maar dat er altijd een menselijke eindcontrole wordt uitgevoerd (`*human in the loop*`). Wij laten het nemen van beslissingen niet aan AI over. AI ondersteunt maar vervangt niet alle menselijke kwaliteiten waaronder expertise, creativiteit, empathie en ethisch oordeel. De mens heeft de regie.

Vraag 3: In het verlengde hiervan: datagedreven werken levert veel output op, waarmee de gemeente haar voordeel kan doen. Wie houdt toezicht op de kwaliteit van de digitaal gegenereerde informatie?

Antwoord:
De vakafdeling zelf is verantwoordelijk om vanuit haar eigen expertise de kwaliteit van de digitaal gegenereerde informatie inclusief de hierbij vermelde bronnen te controleren op juistheid. Dit hebben wij vastgelegd in het beleidskader voor AI dat het College op 1 juli 2025 heeft vastgesteld.
Daarnaast moeten gemeenten voor het gebruik van AI voldoen aan de wettelijke verplichtingen zoals vastgelegd in de AI-verordening en het AI-beleidskader van de gemeente Beekdaelen. Verder doorloopt de gemeente jaarlijks controles en audits waaronder de ENSIA-audit. Hierover legt de gemeente jaarlijks verantwoording af aan de uw Gemeenteraad (horizontaal toezicht). De volgende instanties houden toezicht op veiligheid, privacy, transparantie, betrouwbaarheid en naleving van AI-wetgeving:

- De Autoriteit Persoonsgegevens (AP) ziet toe op naleving van de privacywetgeving, op grondrechten en transparantie van AI-toepassingen, inclusief gemeentelijke systemen zoals beslisalgoritmes en chatbots;
- De Rijksinspectie Digitale Infrastructuur (RDI) krijgt een belangrijke rol in het toezicht op digitale infrastructuur en AI, vooral bij kritieke systemen en op de samenwerking met andere toezichthouders;
- De RDI wordt ook de formele toezichthouder op naleving van de Cyberbeveiligingswet (NIS2) en controleert of gemeenten voldoen aan de zorgplicht, meldplicht en beveiligingsnormen (BIO 2.0).

Momenteel werkt het kabinet aan een uitvoeringswet om het nationaal toezichtstelsel verder vorm te geven.

Vraag 4: De meerwaarde van het koppelen van databases is evident. Wij zouden echter graag een toelichting willen hebben over hoe de gemeente de privacy van haar burgers beschermt (AVG).

Antwoord:
De gemeente moet bij datagedreven werken zeer zorgvuldig omgaan met beveiliging van gegevens en de privacy van inwoners. Dit is wettelijk verplicht (AVG) én essentieel voor het vertrouwen. De belangrijkste maatregelen zijn:

- We verwerken uitsluitend persoonsgegevens als hiervoor een wettelijke basis is (grondslag) en een duidelijk omschreven doel (doelbinding).
- Wij verzamelen uitsluitend de gegevens die noodzakelijk zijn voor het omschreven doel (dataminimalisatie).
- Bij het ontwikkelen van rapportages en dashboards passen wij de regel: "Privacy by design en privacy by default" toe, m.a.w. zijn de rapportages en dashboards per definitie zo ontworpen en in te richten dat de privacy maximaal geborgd is.
- We werken zoveel mogelijk met geaggregeerde gegevens (bijv. postcodes i.p.v. adressen). Dit verkleint privacy risico's.
- Verder treffen we de nodige beveiligings- en autorisatiemaatregelen, zoals versleuteling, logging, veilige opslag en toegangsbeheer. Voor het toegangsbeheer geldt ook weer: doelbinding en dataminimalisatie. De Chief Information Security Officer (CISO) checkt de beveiligings- en autorisatiemaatregelen.
- Voorafgaand aan het ontwikkelen van rapportages en dashboards toetsen wij met de Functionaris Gegevensbescherming (FG) of de Privacy Officer (PO) op bovenstaande maatregelen. Mocht het nodig zijn om persoonsgegevens van inwoners te verwerken, dan voeren we vooraf een DPIA (Data Protection Impact Assessment) uit onder begeleiding van de FG/PO.
- Voor ingebruikname testen wij onze dashboards en rapportages zorgvuldig met onze eindgebruiker(s) en documenteren deze volgens de bovenstaande criteria. Ook de werking van dashboards/rapportages leggen we hierin vast, zodat deze uitlegbaar zijn.
- Van leveranciers en IT-dienstverleners eisen we dat leveranciers zich ook houden aan wet- en regelgeving, waaronder ook de AVG, BIO/ISO27001/2 (beveiliging) en de AI-verordening.

Vraag 5: In de evaluatie datagedreven werken (bijlage 1, p.7) wordt aandacht gevraagd voor de zwaktes en de bedreigingen waarvoor de gemeente zich op dit terrein gesteld ziet. ***A)*** *In hoeverre is met de gevraagde budgetten rekening gehouden met deze uitdagingen? M.a.w. zijn de gevraagde budgetten toereikend om alle maatregelen die p.8 genoemd worden afdoende uit te voeren?* ***B)*** *Dat datagedreven werken geld kost, is evident. In hoeverre is er zicht op eventuele terugverdieneffecten door efficiencywinst.*

Antwoord:
A) De gemeente heeft bij het opstellen van de begroting rekening gehouden met risico's en kwetsbaarheden die zich kunnen voordoen bij datagedreven werken. Zo zijn er middelen gereserveerd voor beheersmaatregelen waaronder

informatieveiligheid, privacybescherming, continuïteit van systemen en opleiding van medewerkers. Daarnaast benutten wij de sterke punten en kansen om maatregelen te nemen voor kwetsbaarheden. Zo organiseren wij momenteel AI workshops en ICT-trainingen voor onze medewerkers waarmee wij werken aan kennisopbouw (AI-geletterdheid , informatiebewustzijn en digivaardigheden) om ervoor te zorgen dat medewerkers slim én verantwoord omgaan met dashboards, AI en andere technieken/ICT-systemen. Ook maken we gebruik van landelijke ondersteuning en samenwerking in de regio (Parkstad en andere gemeenten) voor kennisdeling, o.a. op het gebied van beleid en governance en het uitvoeren van pilots. De basis staat. Deze gaan wij verder uitbouwen. Voor zover wij momenteel kunnen voorzien zijn de gevraagde budgetten toereikend. Mochten zich ontwikkelingen voordoen die wij nu niet voorzien, dan zullen we hierover aan uw Raad rapporteren zodra wij die voorzien.
B) Het betreft hier vooral kostenbesparing, efficiency en waardecreatie. Een aantal voorbeelden: kortere doorlooptijden, vroeg signalering van (multi-)problematieken in het sociaal domein (vroegtijdige maatregelen of interventies kunnen escalatie en bezwaarprocedures voorkomen, wat overigens ook voor andere dienstverleningsprocessen geldt), meer grip op kosten en kwaliteit, gerichtere inzet van mensen en middelen, efficiëntere bedrijfsvoering, efficiënter onderhoud van de openbare ruimte, minder afhankelijkheid van externe adviesbureaus die dure statische rapporten opleveren voor beleidsontwikkeling vanwege inzichten uit eigen dashboards en data, zoals bij het dataportaal vrijetijdseconomie. Ook biedt datagedreven werken in combinatie met AI en de benodigde technologie de gemeente de mogelijkheid om sneller te kunnen anticiperen op crisissituaties of complexe vaak gemeente-overstijgende ontwikkelingen en vraagstukken die samenwerking in de regio vereisen. De omvang van de financiële opbrengsten kunnen wij op voorhand niet inschatten.

Vraag 6: Waarom is de status informatieveiligheid 2024 van Beekdaelen bij Waarstaatjegemeente.nl nog niet gepubliceerd? (Bij de meeste omliggende gemeenten is dit namelijk wel gedaan)

Antwoord:
Uw opmerking is correct. Voor toetsing van de informatieveiligheid bij de gemeente dient de gemeente jaarlijks diverse vragenlijsten in te vullen en verschillende gegevens voor diverse controles en audits aan te leveren aan diverse partijen waaronder de accountant, de auditor voor de ENSIA-audit en aanvullend voor specifieke audits (zoals Wpg, het DigiD-beveiligingsassessment, Suwinet-audit). Jaarlijks rapporteert de gemeente aan uw Raad over de resultaten van de overkoepelende ENSIA-audit. Uit efficiencyoogpunt is bewust ervoor gekozen om vooralsnog af te zien van de monitoring over informatieveiligheid op andere sites zoals waarstaatjegemeente.nl, zolang dit geen verplichte KPI is van onze programmabegroting (bijlage 8.13 Beleidsindicatoren van de Programmabegroting 2026).

Vraag 7: Wat is het ambitieniveau van de gemeente op het gebied van digitale dienstverlening?

Antwoord:
Graag verwijzen we naar de Dienstverleningsvisie 2024-2030 die het College op november 2023 heeft vastgesteld. Hierin zijn de volgende ambities vastgelegd: De gemeente Beekdaelen stelt zich ten doel om haar digitale dienstverlening zodanig in te richten dat deze voor iedere inwoner, ondernemer en partner toegankelijk, betrouwbaar en toekomstbestendig is. Ons uitgangspunt is: digitaal waar mogelijk, persoonlijk waar nodig. Onze ambitie is om inwoners regie te geven over hun eigen zaken met de gemeente, door zoveel mogelijk producten en diensten digitaal aan te bieden, met inzicht in de status van aanvragen en persoonlijke gegevens. Tegelijkertijd blijft maatwerk en persoonlijk contact beschikbaar voor wie dat nodig heeft, zodat niemand wordt uitgesloten. De gemeente investeert in een omnichannel klantreis, waarbij inwoners het kanaal kiezen dat bij hen past: digitaal, telefonisch, schriftelijk of fysiek. De gemeente zorgt voor begrijpelijke communicatie, eenvoudige procedures en een hoge mate van transparantie. Privacy, veiligheid en digitale toegankelijkheid zijn randvoorwaarden. De gemeente monitort continu de kwaliteit van de gemeentelijke dienstverlening via servicenormen, klanttevredenheid en datagedreven sturing. Waar nodig stuurt de gemeente bij. De gemeente investeert structureel in vaardigheden van medewerkers, het verbeteren en vernieuwen van processen en systemen. Met deze visie brengt de gemeente Beekdaelen haar digitale dienstverlening op een niveau dat past bij de verwachtingen van de samenleving en de eisen van deze tijd, met blijvende aandacht voor menselijke maat en inclusiviteit.

Vraag 8: Hoe wapent Beekdaelen zich tegen eventuele veiligheidsrisico's die vergaande automatisering met zich mee brengt? Veel informatie wordt opgeslagen in de cloud, in de meeste gevallen op servers van Amerikaanse aanbieders. Leden van de Tweede Kamer hebben onlangs (schriftelijke vragen d.d. 13 november 2025) hun bezorgdheid uitgesproken over de privacy van Nederlanders nu een Amerikaans bedrijf mogelijk de gegevensopslag van DiGiD en MijnOverheid door een bedrijfsovername in handen krijgt.

Antwoord:
Wij delen de zorgen van de Tweede Kamer en volgen nauwlettend de nieuwsberichten. Wij nemen informatieveiligheid en privacy uiterst serieus en treffen structureel toetsbare maatregelen om de risico's van automatisering en cloudopslag te beheersen. Waar nodig nemen wij afscheid van leveranciers of passen wij ons beleid, processen, leverancierscontracten en/of systemen aan om de privacy van onze inwoners te waarborgen. Wij zijn ons zeer bewust van de veiligheidsrisico's die vergaande automatisering en het gebruik van cloudopslag met zich meebrengen, zeker wanneer gegevens worden opgeslagen bij internationale (veelal Amerikaanse) aanbieders. Om veiligheidsrisico's te beheersen, nemen wij de volgende maatregelen:

- Wij leven de BIO (Baseline Informatiebeveiliging Overheid) strikt na en werken volgens de BIO-normen, die eisen stellen aan informatieveiligheid, risicobeheersing en privacy. Jaarlijks doorloopt onze gemeente controles en audits (accountantscontrole/EDP-audit, ENSIA, DigiD, Suwinet) om naleving te toetsen;

- Voorafgaand aan het gebruik van cloudoplossingen beoordelen wij welke data worden opgeslagen, wat de gevoeligheid is en welke risico's er zijn bij uitbesteding aan buitenlandse partijen;
- Wij kiezen maximaal mogelijk voor Europese of Nederlandse cloud leveranciers die voldoen aan de AVG en aanvullende Nederlandse wet- en regelgeving. Bij Amerikaanse partijen letten wij scherp op contractuele waarborgen, zoals dataopslag binnen de EU, en eisen wij transparantie over toegang tot data. De EU heeft dit jaar weliswaar nieuwe afspraken gemaakt met Microsoft waardoor de licentievoorwaarden verbeterd zijn, maar vanwege de Cloud Act kan de VS toegang eisen tot data, zelfs als die in Europa staat;
- Bij nieuwe systemen, uitbesteding of het koppelen van nieuwe databronnen die persoonsgegevens verwerken, voeren wij een Data Privacy Impact Assessments (DPIA) uit om privacy risico's in kaart te brengen en te mitigeren;
- Wij volgen de landelijke lijn van VNG, Rijksoverheid en de Autoriteit Persoonsgegevens. Ook volgen wij de recente zorgen in de Tweede Kamer over Amerikaanse overnames van cloud providers. Indien nodig nemen wij aanvullende maatregelen;
- Wij informeren uw Raad jaarlijks over de stand van zaken rond informatieveiligheid en eventuele risico's of incidenten.

Nagezonden vraag GL/PvdA:

Vraag 9: Wie controleert of de geleverde data niet gebaseerd zijn op nep-/ fakenieuws?

Antwoord:
Deepfakes (digitale vervalsingen van beeld, geluid en video) zijn aan de orde van de dag en cybercriminelen gaan steeds geraffineerder te werk. Wij investeren in workshops en trainingen voor onze medewerkers waarmee wij werken aan kennisopbouw (AI-geletterdheid , informatiebewustzijn en digivaardigheden) om ervoor te zorgen dat medewerkers slim én verantwoord omgaan met ICT-middelen. Daarnaast is de vakafdeling zelf verantwoordelijk om vanuit haar eigen expertise de kwaliteit van de geleverde data en digitaal gegenereerde informatie inclusief de hierbij vermelde bronnen te controleren op juistheid. Dit hebben wij vastgelegd in het beleidskader voor AI dat het College op 1 juli 2025 heeft vastgesteld en communiceren wij herhaaldelijk tijdens workshops en trainingen. Datakwaliteit is een belangrijk aandachtspunt. Voor de data die wij op ons dataplatform opslaan, maken wij gebruik van betrouwbare, gevalideerde databronnen zoals officiële (basis-)registraties en landelijke databronnen. Nieuwe databronnen toetsen we vooraf op herkomst, actualiteit, kwaliteit (juistheid, volledigheid, consistentie), veiligheid en privacybescherming. Informatie uit open bronnen gebruiken we uitsluitend als we deze kunnen verifiëren. Dashboard, rapportages en analyses worden intern gereviewd door vakspecialisten. Wij documenteren dashboards en rapportages. Hierin leggen we ook vast, welke databronnen gebruikt zijn en welke kwaliteitseisen hieraan worden gesteld.