Formulier voor het indienen van vragen voor de vragenweek

Naam: Roger Nijsten en Kyra Heitzer

Fractie: Progressief Beek

Vraag 1:

Voorgesteld om in 2026 een bestemmingsreserve Digitale Soevereiniteit en AI te vormen. Hiervoor wordt eenmalig een bedrag van € 400.000 vanuit de algemene reserve gestort en de financiële verwerking hiervan vindt plaats in de Slotrapportage 2026.

a. Wat is de huidige omvang van de algemene reserve
b. Wat is het effect van de onttrekking van € 400.000 daarop
c. Is er vooraf een indicatie te geven van het jaarlijks bestedingsritme binnen de looptijd 2026-2030, of kan het volledige bedrag ook in één jaar worden ingezet?

Antwoord:

a. De laatste definitief vastgestelde stand van de algemene reserve is € 16.907.000 per 31 december 2025. Dit is de stand vóór de bestemming van het positieve rekeningresultaat 2025. In 2026 zijn al verschillende mutaties op de algemene reserve besloten.

b. Door de storting wordt de algemene reserve € 400.000 lager en komt hetzelfde bedrag in de nieuwe bestemmingsreserve Digitale Soevereiniteit en AI. Uitgaande van de stand per 31 december 2025 gaat het om ongeveer 2,4%. De storting zelf verlaagt het totale bedrag aan reserves niet: het geld krijgt eerst een andere bestemming. Pas wanneer uit de bestemmingsreserve uitgaven worden gedaan, neemt het totale reservevermogen af.

c. Er is geen vast bedrag per jaar afgesproken. De € 400.000 is een maximumbedrag voor de hele periode 2026-2030 en wordt niet vooraf over de jaren verdeeld. Het uitgangspunt is niet om de reserve op te maken, maar om alleen geld uit te geven aan kansrijke en verantwoorde initiatieven. Niet-bestede middelen blijven in de reserve beschikbaar.

Vraag 2:

Hoe verhoudt het lopende project 'Toekomst ICT' (Onderdeel G Programma 6, Bestuur en Organisatie uit de programmabegroting 2026) zicht tot het nu voorliggende voorstel over Digitale soevereiniteit, verantwoorde AI en publieke innovatie?

Antwoord:

Het project Toekomst ICT en het voorliggende AI-kader hangen met elkaar samen, maar hebben een ander doel.

Toekomst ICT richt zich op de technische en organisatorische basis van de ICT. Het gaat onder meer om een sterkere regierol van de gemeente, professioneel leveranciersbeheer, de toekomstige ICT-omgeving en een moderne digitale werkplek. Voor deze ICT-transformatie is in de Programmabegroting 2026 een aparte incidentele investering van € 1 miljoen opgenomen.

Het voorstel over Digitale Soevereiniteit, Verantwoorde AI en Publieke Innovatie gaat vooral over de manier waarop Beek AI wil gebruiken: veilig, uitlegbaar, met menselijke controle en met grip op gegevens en leveranciers. De voorgestelde reserve van € 400.000 is bedoeld voor tijdelijke expertise, verkenningen en pilots, AI-kennis, de AI-dialoog en regionale samenwerking.

Er is dus geen sprake van twee keer betalen voor hetzelfde. Wel moeten de projecten goed op elkaar aansluiten. Keuzes over bijvoorbeeld hosting, toegang, beveiliging en leveranciers van AI moeten passen binnen de toekomstige ICT-inrichting. Als een AI-toepassing later structurele ICT-kosten veroorzaakt, worden die apart beoordeeld in de reguliere begroting.

Vraag 3:

Het voorstel beschrijft het uitgangspunt dat een dergelijke veilige AI-voorziening, binnen passende autorisatie-, privacy- en gebruikskaders, niet alleen voor medewerkers maar ook voor raadsleden beschikbaar wordt gesteld. Daarmee kunnen ook raadsleden op een verantwoorde manier ervaring op doen met AI en deze technologie benutten als hulpmiddel bij informatieverwerking en de voorbereiding van hun volksvertegenwoordigende, kaderstellende en controlerende werkzaamheden.

a. Welke autorisatie-, privacy- en gebruikskaders worden voorzien voor raadsleden bij toegang tot een voorziening als LAICA, wie stelt deze vast?
b. Hoe wordt de onafhankelijke controlerende positie van raadsleden ten opzichte van door de organisatie beheerde AI-tooling geborgd?

Antwoord:

a. Er is nog geen definitief gebruikskader voor raadsleden vastgesteld. Dat moet klaar zijn voordat een voorziening als LAICA breed aan raadsleden wordt aangeboden. Het kader moet in ieder geval regelen: persoonlijke toegang en autorisaties, welke gegevens wel en niet mogen worden gebruikt, de omgang met vertrouwelijke informatie, beveiliging en logging, bewaartermijnen, controle van AI-uitkomsten en de handelwijze bij incidenten.

De technische, privacy- en beveiligingseisen worden binnen de gemeente uitgewerkt met de betrokken deskundigen. Voor het gebruik door raadsleden moet de griffie nadrukkelijk worden betrokken. Dat onderdeel is nu nog niet uitgewerkt.

b. De onafhankelijke positie van de raad blijft het uitgangspunt. AI is alleen een hulpmiddel. Een raadslid blijft zelf verantwoordelijk voor zijn of haar politieke oordeel en kan altijd andere informatiebronnen gebruiken. De voorziening mag niet worden gebruikt om de inhoudelijke werkzaamheden van raadsleden te volgen of te sturen. Daarom zijn gescheiden accounts en rollen, duidelijke afspraken over toegang tot loggegevens en zo weinig mogelijk inhoudelijke inzage door beheerders belangrijk.

Vraag 4:

In het voorstel staat dat de raad structureel betrokken blijft bij de maatschappelijke en bestuurlijke keuzes rond AI;

Kan worden bevestigd dat hiermee wordt bedoeld dat gelet op de snelheid van de ontwikkelingen rondom Digitale Soevereiniteit en de inzet van AI de tussenevaluatie (2028) en eindevaluatie (2030) via een raadsbesluit lopen en niet uitsluitend als onderdeel van de planning- en controlcyclus wordt behandeld?

Antwoord:

De visie legt vast dat in 2028 een tussenevaluatie met de raad en de samenleving plaatsvindt. Deze evaluatie is de basis voor de keuzes vanaf 2029. In 2030 volgt een eindevaluatie. Die is de basis voor de besluitvorming over de periode na 2030.

Ze worden aan de raad voorgelegd en worden dus niet alleen als technische verantwoording in de planning- en controlcyclus behandeld.

Als uit een evaluatie volgt dat de richting, de spelregels, de looptijd of het financiële maximum moet veranderen, is opnieuw een besluit van de raad nodig. Voor een nieuw kader en nieuwe financiële ruimte na 2030 is eveneens een raadsbesluit nodig.

Vraag 5:

De visie beschrijft dat een verkenning stilgelegd moest worden omdat de leverancier de vereiste privacyafspraken weigerde te tekenen. Is aantoonbaar uitgesloten dat ingevoerde gegevens worden gedeeld met derden, waaronder buitenlandse overheden?

Antwoord:

Nee, dat kan niet in algemene zin voor iedere AI-dienst worden gegarandeerd. Dat moet per leverancier en per technische omgeving aantoonbaar worden gemaakt.

Voor gebruik met persoonsgegevens of vertrouwelijke gemeentelijke informatie moet vooraf duidelijk zijn waar de gegevens worden verwerkt, welke onderaannemers toegang kunnen hebben, of gegevens buiten de Europese Economische Ruimte terechtkomen, of gegevens voor training worden gebruikt, hoe lang gegevens worden bewaard en welke partijen toegang hebben. Ook moet worden gekeken naar de wetgeving waaronder een leverancier valt.

Voor LAICA of een andere structurele voorziening geldt dit ook. Voordat gemeentelijke persoonsgegevens of vertrouwelijke gegevens worden gebruikt, moeten de afspraken en de technische inrichting voldoende zekerheid geven. Als dat niet aantoonbaar kan, worden die gegevens niet in de toepassing verwerkt.

Vraag 6:

Spelregel 4 schrijft voor dat verkenningen plaatsvinden met testgegevens, openbare gegevens of geanonimiseerde persoonsgegevens.

a. Op welke wijze wordt geanonimiseerd en wie toetst of die anonimisering voldoende is?
b. Waar worden testgegevens opgeslagen en wie heeft daar toegang toe?

Antwoord:

a. De visie schrijft voor dat bij verkenningen alleen testgegevens, openbare gegevens of zorgvuldig geanonimiseerde persoonsgegevens worden gebruikt. De visie schrijft nog niet één vaste methode voor anonimisering voor.

Bij anonimisering moeten gegevens zo worden aangepast dat een persoon redelijkerwijs niet meer kan worden herkend. Dit kan bijvoorbeeld door namen en andere directe kenmerken te verwijderen en indirecte kenmerken te vervangen, samen te voegen of minder precies te maken. Daarna moet ook worden bekeken of personen niet via een combinatie van gegevens alsnog herkenbaar zijn. Alleen een naam vervangen door een nummer is pseudonimiseren; dan blijven het persoonsgegevens en blijft de AVG van toepassing.

De eigenaar van de toepassing is verantwoordelijk voor een goede aanpak. Bij persoonsgegevens worden de privacyfunctie en, waar nodig, de Functionaris Gegevensbescherming betrokken. De precieze Beekse werkwijze wordt nog verder vastgelegd in het AI-beleid.

b. De visie schrijft geen vaste opslaglocatie voor alle testgegevens voor. Testgegevens worden alleen opgeslagen in een vooraf goedgekeurde omgeving. Toegang wordt beperkt tot medewerkers en leveranciers die deze toegang voor de proef nodig hebben. Voor de proef met GovChat/LAICA wordt gewerkt aan een Azure-omgeving bij Solido. Voor de start moeten opslaglocatie, toegang, logging, bewaartermijn en verwijdering van gegevens duidelijk zijn vastgelegd. Persoonsgegevens en vertrouwelijke informatie worden niet in publieke of onbeheerde AI-diensten geplaatst.

Vraag 7:

Elke voorgenomen toepassing krijgt een proportionele risicoscan volgens de Europese AI-verordening.

a. Wie voert deze risicoscan uit?
b. Welke criteria bepalen wanneer een toepassing als hoog risico geldt en in het Algoritmeregister wordt opgenomen?
c. Wordt ook een IAMA uitgevoerd bij toepassingen, zo ja, op welk moment in het traject?

Antwoord:

a. De risicoscan wordt niet door één persoon alleen uitgevoerd. De initiatiefnemer of eigenaar van de toepassing levert de informatie aan. De werkgroep AI is het centrale punt voor aanmelding, toetsing en prioritering. Afhankelijk van het risico worden ook deskundigen op het gebied van privacy, informatiebeveiliging, recht, informatiebeheer en inkoop betrokken. De precieze taakverdeling wordt nog verder vastgelegd in de AI-governance.

b. De Europese AI-verordening kijkt vooral naar het doel waarvoor een AI-systeem wordt gebruikt en naar de mogelijke gevolgen. Een systeem kan bijvoorbeeld hoog risico zijn als het wordt gebruikt bij belangrijke publieke voorzieningen, personeelsbesluiten of andere situaties waarin fouten grote gevolgen kunnen hebben voor rechten of veiligheid. Het Nederlandse Algoritmeregister is breder. Daarin worden ook impactvolle algoritmen opgenomen, bijvoorbeeld als een algoritme invloed heeft op een besluit met rechtsgevolgen of op de manier waarop inwoners worden ingedeeld of benaderd.

c. Een IAMA (Impact Assessment Mensenrechten en Algoritmes) wordt niet automatisch bij iedere eenvoudige AI-toepassing uitgevoerd. De visie bepaalt dat een passende impactbeoordeling wordt gedaan als een toepassing mogelijk wezenlijke gevolgen voor inwoners heeft. Een IAMA is dan een mogelijk instrument. Het IAMA wordt zo vroeg mogelijk uitgevoerd, voordat een toepassing structureel wordt ingevoerd en voordat inwoners er gevolgen van kunnen ondervinden. Bij een grote wijziging van doel, gegevens of werking wordt de beoordeling zo nodig opnieuw uitgevoerd.

Vraag 8:

De visie noemt een "soevereine AI-assistent" op blz 16, die eventueel samen met andere overheden wordt ontwikkeld. Is een Europese of publiek beheerde leverancier beschikbaar die aan de technische eisen voldoet?

Antwoord:

Op dit moment is een concrete publieke en open route beschikbaar: GovChat-NL, met in Limburg de toepassing LAICA. Dit initiatief is ontwikkeld door de Provincie Limburg en is juist bedoeld om overheden meer grip te geven op gegevens, privacy en de eigen technische omgeving. Voor Beek wordt een proef voorbereid in een Azure-omgeving bij Solido, met ondersteuning bij de technische inrichting.

De proef moet aantonen of de oplossing in de praktijk voldoet aan de eisen van Beek. Daarbij wordt onder meer gekeken naar beveiliging, privacy, beheer, continuïteit, prestaties, kosten, gegevenslocatie en de mogelijkheid om later van leverancier of oplossing te wisselen. Pas daarna kan worden besloten over structureel gebruik.

Vraag 9:

Structureel ingevoerde toepassingen worden periodiek gemonitord op werking, publieke waarde en risico's.

a. Met welke technische middelen vindt deze monitoring plaats en hoe vaak?
b. Welke prestatie-indicatoren worden gebruikt om te meten of een AI-toepassing correct en onbevooroordeeld werkt?
c. Binnen welke termijn kan een toepassing tijdelijk worden stilgelegd bij een geconstateerd incident?

Antwoord:

a. De visie schrijft voor dat structurele AI-toepassingen worden gemonitord, maar schrijft niet voor alle toepassingen één technisch hulpmiddel of één vaste frequentie voor. Voor iedere structurele toepassing moet daarom vooraf een monitoringsplan worden gemaakt. Daarin kunnen bijvoorbeeld systeem- en beveiligingslogs, foutmeldingen, steekproeven, gebruikersfeedback, klachten, wijzigingen van de leverancier en controles van de uitkomsten worden opgenomen. De frequentie hangt af van het risico.

b. Ook de prestatie-indicatoren verschillen per toepassing. Mogelijke indicatoren zijn: het percentage juiste en onjuiste uitkomsten, het aantal correcties door medewerkers, fout-positieve en fout-negatieve uitkomsten, verschillen tussen relevante groepen, klachten, toegankelijkheid, beschikbaarheid, incidenten, doorlooptijd en aantoonbare publieke waarde. Voor de start wordt bepaald welke indicatoren voor die toepassing echt iets zeggen over kwaliteit en mogelijke vooringenomenheid.

c. De visie noemt geen vaste termijn in uren. Wel moet iedere structurele toepassing een mogelijkheid hebben om tijdelijk te worden stilgelegd of te stoppen. Bij een ernstig privacy-, beveiligings- of grondrechtenrisico moet dat direct kunnen. Voor ingebruikname worden daarom ook de escalatieroute, verantwoordelijke personen en de praktische mogelijkheid om de toepassing uit te zetten vastgelegd.

Vraag 10:

De visie beschrijft de beveiliging van zeer vertrouwelijke gegevens, zoals over jeugdzorg en schuldhulpverlening. Wie is verantwoordelijk bij een datalek die ontstaat door het gebruik van AI?

Antwoord:

Het gebruik van AI verandert de verantwoordelijkheid voor een datalek niet. De gemeente, of het bevoegde gemeentelijke bestuursorgaan, blijft volgens de AVG verantwoordelijk voor de persoonsgegevens waarvoor zij het doel en de manier van verwerking bepaalt. Een leverancier die gegevens voor de gemeente verwerkt, heeft als verwerker ook verplichtingen, maar neemt die verantwoordelijkheid niet over.

Bij een datalek moet de leverancier het incident zonder onnodige vertraging bij de gemeente melden. De gemeente onderzoekt het incident, beperkt de gevolgen en legt het incident vast. Als het datalek waarschijnlijk een risico oplevert voor betrokken personen, meldt de gemeente het in beginsel binnen 72 uur bij de Autoriteit Persoonsgegevens. Bij een hoog risico moeten ook de betrokken personen worden geïnformeerd.

Intern wordt het incident behandeld via de bestaande privacy- en informatiebeveiligingsprocedure, met de verantwoordelijke proceseigenaar en de betrokken privacy- en beveiligingsdeskundigen. In contracten met leveranciers worden daarnaast afspraken gemaakt over beveiliging, meldtermijnen, medewerking en eventuele aansprakelijkheid.