

AI en algoritmes beleid Gooise Meren

Uitgangspunten voor het gebruik binnen de gemeente

1. Inleiding

Artificial Intelligence (vanaf nu AI) is met een enorme opmars bezig. Tools als ChatGPT (OpenAI) en Copilot (Microsoft) maken het gebruik ervan voor iedereen toegankelijk. AI is gebaseerd op complexe algoritmes maar ook algoritmes in een bredere zin en zijn steeds meer vertegenwoordigd in de samenleving en in de gemeentelijke organisatie. Het biedt veel kansen maar brengt ook risico's en ethische dilemma's met zich mee.

Het doel van dit beleid is om kaders te stellen waarbinnen wij deze kansen kunnen benutten en dit op een verantwoorde, veilige en ethisch manier kunnen uitvoeren.

1.1 Aanleiding

- De Europese AI-act die vanaf augustus 2024 in werking is getreden.
- De snelle ontwikkelingen in de samenleving op het gebied van Generatieve AI (GenAI).
- De behoefte aan kaders voor het gebruik van AI binnen onze organisatie: wat willen we wel en wat niet?

1.2 Leeswijzer

Dit beleid van de gemeente beschrijft het gebruik van AI en Algoritmes. Er wordt een schets gemaakt van de context, waarin de belangrijkste trends en ontwikkelingen worden besproken, zoals de opkomst van Generatieve AI, de EU-regelgeving rondom AI en de verplichting tot transparantie over algoritmes binnen de overheid. Daarnaast wordt ingegaan op de communicatie van dit beleid binnen de gemeente en de relatie van dit beleid tot andere documenten, waaronder het programma digitalisering en beleidskaders zoals het strategisch IB&P- en I&A-beleid.

Vervolgens wordt in het kader hoofdstuk uitgelegd hoe de gemeente AI en algoritmes wil benutten. Het beleid richt zich op het veilig en verantwoord inzetten van deze technologieën, door te investeren in vaardigheden en kennis, collega's bewust te maken van de risico's, en passende AI-oplossingen te zoeken die voldoen aan wet- en regelgeving. Ook wordt het belang van transparantie benadrukt door het publiceren van impactvolle algoritmes in het algoritmeregister.

In de uitvoeringsstrategie wordt dieper ingegaan op de achtergrond en risico's van AI en algoritmes. De opkomst van Generatieve AI, evenals de risico's zoals datalekken, betrouwbaarheid van de output, en ethische kwesties. Maatregelen zoals bewustwordingstrainingen, juridische toetsen en het naleven van wetgeving worden beschreven. Het beleid legt ook uit hoe de gemeente de mogelijkheden van AI-tools beoordeelt, waarbij gebruiksvoorwaarden en beveiliging van data centraal staan.

Tot slot wordt het gebruik van algoritmes nader toegelicht, inclusief de risico's zoals black-box problematiek, fouten en inbreuken op privacy. Hieraan gekoppeld worden maatregelen en transparantie uitgewerkt, inclusief het gebruik van het algoritmeregister. Het beleid sluit af met een monitoring- en evaluatiestrategie, waarin jaarlijks de voortgang wordt beoordeeld door informatiemanagement en Team IB&P.

2. Context

2.1 Trends en ontwikkelingen

- Opkomst van Generatieve AI (GenAI)
- Regulering van AI (*Regulation - EU - 2024/1689 - EN - EUR-LEX*, z.d.) binnen de EU
- Transparant maken van (hoog risico) algoritmes binnen de overheid (*Handreiking Algoritmeregister*, 2023)

2.2 Communicatie en participatie

- Dit beleid wordt actief gecommuniceerd binnen onze gemeente op een voor de betreffende doelgroep passende wijze

2.3 Afhankelijkheden

- Nieuwe ontwikkelingen op het gebied van (Gen)AI worden aangestuurd en geïmplementeerd vanuit het programma digitalisering

- Strategisch IB&P Beleid
- I&A Beleid 2025 – 2029

3. Kader

Als gemeente willen wij gebruik maken van de kansen die AI en Algoritmes ons bieden. De gemeente wil dit op een veilige en verantwoorde manier, daarom:

- investeren we als gemeente in de AI-vaardigheden en kennis van onze medewerkers;
- maken we als organisatie onze medewerkers bewust van de risico's en geven ze handvatten mee;
- communiceren we dit beleid actief aan onze medewerkers (gezien de hoge impact van de technologie);
- zoeken we als organisatie naar passende AI-oplossingen welke voldoen aan wet- en regelgeving;
- identificeren we de risico-classificatie van (nieuwe) AI-toepassingen binnen onze IT-omgeving;
- publiceren we als transparante gemeente hoge impact algoritmes in het algoritmeregister.

4. Uitvoeringsstrategie



artificial
intelligence

4.1 Artificial intelligence (AI)

4.1.1 Achtergrond

AI bestaat al sinds de vorige eeuw, maar sinds de uitvinding van de zogenaamde Transformers (Wikipedia contributors, 2024d) nemen Large Language Models (LLM's) (Wikipedia contributors, 2024a) in 2022 een flinke stap vooruit wanneer ChatGPT uitkomt (Wikipedia contributors, 2024c).

Met deze Generatieve AI (GenAI) (Wikipedia contributors, 2024b) hebben we opeens de mogelijkheid om nieuwe content (tekst, video, foto en audio) op basis van een beschrijving (prompt) te genereren.

Naast de verschillende losstaande oplossingen die er zijn om deze Generatieve AI te gebruiken, hebben de grote Tech-bedrijven (Microsoft, Google, Apple) de strategie om deze Generatieve AI in hun producten te bouwen.

4.1.2 Risico's en maatregelen

#	Risico	Maatregel
1	Datalekken <i>Het lekken van (onbedoeld) vertrouwelijk informatie of persoonsgegevens.</i>	a) Bewustwording / Training <i>De gemeente zorgt voor voldoende bewustwording van de risico's van het gebruik van vertrouwelijke informatie of persoonsgegevens in AI-tools. Als gemeente bieden wij trainingen aan om de medewerkers te scholen in dit onderwerp.</i> b) Technische maatregelen <i>Persoonlijke data mag niet gedeeld worden. De gemeente neemt technische maatregelen om dit zoveel mogelijk te voorkomen of te signaleren.</i>
2	Betrouwbaarheid Output <i>Op dit moment wil GenAI nog wel eens hallucineren, waardoor de output niet altijd klopt.</i>	a) Bewustwording / Training <i>Bewustwording van de betrouwbaarheid van de output. De gemeente biedt trainingen aan om de medewerkers te scholen in dit onderwerp.</i>

3	Inbreuk op intellectueel eigendomsrecht <i>Bij GenAI is het niet altijd duidelijk waar de informatie vandaan komt, waarmee het model getraind is. Soms is dit onrechtmatig verkregen (zonder toestemming van de eigenaar).</i>	a) Bewustwording <i>Een medewerker kan niet altijd weten of gegenereerde tekst of beeld grotendeels overeenstemt met al bestaande (auteursrechtelijk beschermd) teksten en/of beelden van derden. Het is van belang dat een medewerker daar bewust van is en mee omgaat. Als gemeente bieden wij trainingen aan om de medewerkers te scholen in dit onderwerp</i>
4	Privacy <i>Verlies van controle over (persoons)gegevens.</i>	a) Bewustwording / Training <i>Bewustwording van de betrouwbaarheid van de output. De gemeente biedt trainingen aan om de medewerkers te scholen in dit onderwerp.</i> b) Voldoen aan wetgeving <i>Product/tool moet voldoen aan de EU/NL wetgeving. Zo wordt er o.a., indien dit noodzakelijk is, een DPIA uitgevoerd en de principes van Privacy by Design en - Default toegepast.</i>
5	Ethiek <i>AI kan discriminerende algoritmes bevatten, daarnaast zitten er vaak Amerikaanse normen die mogelijk afwijken van de lokale normen en waarden.</i>	Ethische toets <i>Doorloop een DEDA (de ethische data-assistent) (Schäfer et al., 2018) waardoor het helder moet worden of we als gemeente dit algoritme kunnen/moeten willen inzetten.</i>
6	Hoog Risico AI gebruik <i>AI kan discriminerende algoritmes bevatten, daarnaast zitten er vaak Amerikaanse normen die mogelijk afwijken van de lokale normen en waarden.</i>	IAMA <i>Bij het gebruik van hoog risico AI is het IAMA (impact assessment voor mensenrechten bij de inzet van algoritmen) verplicht. (Ministerie van Algemene Zaken, 2024)</i>

4.1.3 Toepasbaarheid

Als gemeente willen we de Generatieve AI tools omarmen, wanneer het onze collega's kan ondersteunen in hun processen of werkzaamheden. De verschillende Generatieve AI-tools worden niet uitgesloten van gebruik, zolang er maar:

1. Geen koppeling is met ons IT-landschap, of;
2. Een koppeling met ons IT-landschap is (bijvoorbeeld wanneer er gebruik wordt gemaakt van vertrouwelijke informatie, persoonsgegevens of bij integratie met systemen van de gemeente) de toepassing gecontracteerd is, of
3. een interne risicoafweging is gemaakt.

Goed om te weten

AI-tools uit landen met een offensief cyberprogramma (Nationaal Cyber Security Centrum) tegen Nederland worden nooit toegestaan.

Aanschaf en eisen AI-producten

Wanneer er een nieuw AI-product wordt aangeschaft dan wordt er eerst contact gezocht met de informatiemanager. Door middel van een risicoanalyse vanuit Team IB&P wordt beoordeeld welke eisen er nodig zijn om aan relevante wetgeving zoals de EU AI-Act, AVG, NIS2 en BIO te voldoen. Onderdelen uit deze wetgeving die specifiek voor AI-toepassingen extra aandacht verdienen zijn Security by design, Security by default, ISO-27001, ISO-24028 & ISO-25027. Gooise Meren hanteert hier een best effort principe waar zo veel mogelijk gebruik wordt gemaakt van gestandaardiseerde methodieken en (internationale) standaarden. Bij het afnemen van producten en diensten kan (afhankelijk van het risicoprofiel) door Gooise Meren worden verlangd dat de wijze waarop Security-by-design is vormgegeven inzichtelijk wordt gemaakt via een onafhankelijke (code)review of audit.

Ontwikkeling door Gooise Meren

Wanneer een AI-toepassing door Gooise Meren of in opdracht van Gooise Meren wordt ontwikkeld, moet deze aan dezelfde eisen voldoen als een gecontracteerde toepassing.



algoritmes

4.2 Algoritmes

4.2.1 Achtergrond

Een algoritme wordt gezien als een reeks instructies of regels om tot een resultaat te komen, we kunnen het ook wel vergelijken met een recept. Algoritmes zitten in praktisch alle software die wij als gemeente gebruiken.

Goed om te weten

Een AI is opgebouwd uit verschillende algoritmes, maar niet iedere algoritme is een AI. Dit is ook de reden dat we AI en algoritmes apart behandelen in dit beleid.

Interne ontwikkeling algoritmes

Binnen onze gemeente worden ook eigen algoritmes ontwikkeld. Deze algoritmes behandelen we op dezelfde manier als algoritmes die niet door onze gemeente zijn ontwikkeld.

4.2.2 Risico's en maatregelen

Risico	Maatregel
Black Box <i>Een toepassing met een complex algoritme kan een Black-box (ondoorzichtig) zijn, waardoor het niet duidelijk is wat er gebeurt door het algoritme.</i>	Ethische toets <i>De gemeente zal indien dit noodzakelijk is een DEDA (de ethische data-assistent) doorlopen ("Proces Dataproduct", 2024), waardoor het helder wordt of we als gemeente dit algoritme kunnen/moeten willen inzetten.</i>
Ethiek <i>Een algoritme kan discriminerende vooroordelen bevatten.</i>	Ethische toets <i>De gemeente zal indien dit noodzakelijk is een DEDA (de ethische data-assistent) doorlopen ("Proces Dataproduct", 2024), waardoor het helder wordt of we als gemeente dit algoritme kunnen/moeten willen inzetten</i>
Privacy <i>Wanneer algoritmes toegang hebben tot persoonsgegevens kunnen deze leiden tot schending van privacy wanneer ze niet goed beveiligd worden.</i>	Voldoen aan AVG <i>De gemeente zorgt ervoor dat de algoritmes voldoen aan de AVG (denk aan dataminimalisatie, gegevensanonimisatie/pseudonimisatie, beveiligingsmaatregelen).</i>
Fouten in algoritmes <i>Het kan voorkomen dat er fouten in algoritmes zitten, dit kan in het ergste geval resulteren in een verkeerd gemaakt besluit voor de burger.</i>	Correctie mogelijk maken <i>De gemeente zal ervoor zorgen dat de betrokkenen bij een (persoonlijk) besluit (welke gevolgen heeft voor hen) zich kunnen beroepen op "het recht op een menselijke blik". De gemeente moet dan een nieuw besluit nemen waarbij een medewerker (een mens) hun gegevens opnieuw moet beoordelen</i>

Adviescommissie Digitale Ethiek

Er wordt een Adviescommissie Digitale Ethiek in het leven geroepen, welke het college gevraagd en ongevraagd adviseert over het gebruik van nieuwe digitale technologieën (zoals algoritmen, AI en sensoren) in de Gemeente Gooise Meren. De commissie bestaat uit commissieleden met kennis en affiniteit op het gebied van (digitale) ethiek.

4.2.3 Toepasbaarheid

Als gemeente zijn we voor transparantie van het gebruik van algoritmes binnen de gemeente, dit brengen we ten uitvoer door gebruik te maken van het Algoritmeregister (*Handreiking Algoritmeregister*, 2023). In het algoritmeregister maken we onderscheid in de volgende te publiceren algoritmes:

1. Hoog-risico algoritme
2. Impactvol algoritme

Algoritmes die voldoen aan een van deze classificaties (*Handreiking Algoritmeregister, 2023*) publiceren wij als gemeente in het algoritmeregister (*Handreiking Algoritmeregister, 2023*).

5. Monitoring en evaluatie

5.1 Monitoring en evaluatie

- Iedere januari (of vaker indien nodig) wordt het AI en Algoritme bij Gooise Meren – beleid geëvalueerd door informatiemanagement en Team IB&P.

Literatuurlijst

Handreiking algoritmeregister (1.0). (2023). Geraadpleegd op 7 januari 2025, van <https://aionalgoritmes.pleio.nl/attachment/entity/f1a35292-7ea6-4e47-93fa-b3358e9ab2e0>

Ministerie van Algemene Zaken. (2024, 20 augustus). *Impact assessment mensenrechten en algoritmes*. Rapport | Rijksoverheid.nl. <https://www.rijksoverheid.nl/documenten/rapporten/2021/02/25/impact-assessment-mensenrechten-en-algoritmes>

Proces dataproduct. (2024). In *Engage*. Gemeente Gooise Meren. Geraadpleegd op 23 januari 2025, van <https://viewer.engageprocess.com/?did=9a1376a7-7a2f-40c5-87a5-3bd98a96770f&state=4>

Regulation - EU - 2024/1689 - EN - EUR-LEX. (z.d.). <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

Schäfer, M. T., Franzke, A., Utrecht Data School, & Universiteit Utrecht. (2018). *Handleiding Inventarisatie van ethische kwesties rond data projecten bij overheden* (D. Van Der Hoek & M. Krijgsman, Reds.). <https://deda.dataschool.nl/wp-content/uploads/sites/415/2022/11/DEDA-NL.handbook.V3.1.pdf>

Turk, K., Pol, N., De Graaf, D., Koops, S., Van Dijk, R., & Vereniging van Nederlandse Gemeenten. (2020). *Proeftuin actieve openbaarmaking*.

Wikipedia contributors. (2024a, oktober 19). *Large language model*. Wikipedia. https://en.wikipedia.org/wiki/Large_language_model

Wikipedia contributors. (2024b, oktober 20). *Generative artificial intelligence*. Wikipedia. https://en.wikipedia.org/wiki/Generative_artificial_intelligence

Wikipedia contributors. (2024c, oktober 21). *ChatGPT*. Wikipedia. <https://en.wikipedia.org/wiki/ChatGPT>

Wikipedia contributors. (2024d, oktober 21). *Transformer (deep learning architecture)*. Wikipedia. Geraadpleegd op 21 oktober 2024, van [https://en.wikipedia.org/wiki/Transformer_\(deep_learning_architecture\)](https://en.wikipedia.org/wiki/Transformer_(deep_learning_architecture))