

Informatienota voor de Gemeenteraad

Onderwerp: Verantwoord gebruik van AI-platform SafeGPT

Collegedatum: 17-03-2026

Kernboodschap

De Werkorganisatie Druten Wijchen (WDW) is gestart met een pilot met SafeGPT, een AI-platform dat medewerkers helpt bij het analyseren van informatie en het maken van teksten. In SafeGPT willen we ook gevoelige gegevens zoals persoonsgegevens gaan verwerken, om zo meer uit het platform te kunnen halen. Omdat het AI-beleid aan het einde van het tweede kwartaal is afgerond en ter besluitvorming aan de raad wordt aangeboden, is gekeken of onder bepaalde randvoorwaarden al gestart kan worden met verwerking van persoonsgegevens in SafeGPT. De conclusie is dat dit mogelijk is, wanneer er succesvol een Data Protection Impact Assessment (DPIA) wordt doorlopen.

Eerdere besluiten

Datum	Korte omschrijving eerder genomen besluit
24-06-2024	Antwoord op schriftelijke vragen 'transparant algoritmegebruik binnen de gemeente' (Z/24/243617)
27-03-2025	Informatienota algoritmes en AI (Z/25/278615)
25-09-2025	Informatienota schriftelijke vraag D66 over afhankelijkheid Microsoft (Z/25/303011)

Toelichting

We zien veel kansen in het benutten van AI-technologie door medewerkers. Zo worden processen efficiënter en worden de uitkomsten kwalitatief beter en consistent. De AI oplossingen die wij al hanteren voor gemeente Wijchen, staan vermeld in het [landelijke algoritmeregister](#).

Op regionaal Rijk van Nijmegen niveau, is gestart met een pilot met het AI platform SafeGPT. Het platform is centraal door iRvN aangeschaft voor de deelnemende gemeenten, voor de periode van een jaar. De WDW is ook gestart met een pilot met SafeGPT.

Het aanbieden van een gecontracteerde AI-oplossing zoals SafeGPT, zorgt er voor dat medewerkers geen ongewenste alternatieven gaan gebruiken. Denk aan gratis software als ChatGPT. Met mogelijke datalekken als gevolg, zoals in gemeente Eindhoven heeft plaatsgevonden. Met een gecontracteerde oplossing, hebben wij als WDW controle over de voorwaarden waartegen we de oplossing aanbieden aan gebruikers. Zo kunnen we op een verantwoorde manier met een aantal gebruiksscenario's piloten om de meerwaarde van dit platform voor gemeente Wijchen te ontdekken.

SafeGPT is een snel groeiend Nederlands bedrijf met al zo'n 80 gemeenten als klant. Het bedrijf richt zich voornamelijk op Nederlandse overheden en tot nu toe primair gemeenten. De data die zij verwerken staat op Europese servers. Digitale soevereiniteit staat bij dit bedrijf voorop. Hiermee onderscheiden zij zich van Amerikaanse 'big tech' leveranciers en verminderen wij onze afhankelijkheid van deze leveranciers. SafeGPT

voldoet aan de vereisten voor gegevensbescherming en informatieveiligheid volgens de wettelijke kaders en richtlijnen. Ingevoerde gegevens worden alleen verwerkt in de omgeving van SafeGPT en worden niet gebruikt om AI-modellen te trainen.

Op 27 maart 2025 is de informatienota 'algoritmes en AI' in uw raad behandeld. Hierin is aangegeven dat de WDW een AI-beleid zou ontwikkelen, voordat we in uw gemeente AI-oplossingen in gebruik nemen waarin gevoelige data verwerkt worden. Zodat verwerking op een verantwoorde manier kan plaatsvinden. Tot nu toe hebben we daarom alleen openbare gegevens verwerkt in AI-oplossingen. Het AI-beleid heeft echter vertraging opgelopen en wordt aan het einde van het tweede kwartaal afgerond en ter besluitvorming aan de raad aangeboden. En inmiddels willen we al wel aan de slag met verwerking van gevoelige gegevens in AI-oplossingen. Om te beginnen binnen het AI-platform SafeGPT. Maar alleen als dit verantwoord kan plaatsvinden. We zien dat dit verantwoord kan plaatsvinden, ook al zonder een vastgesteld AI-beleid. Mits er voorafgaand aan de verwerking van gegevens succesvol een DPIA wordt uitgevoerd.

Wettelijke kaders

Bij het gebruik van generatieve AI-oplossingen kan sprake zijn van risico's, zoals onbedoelde openbaarmaking van gegevens, onduidelijkheid over wat er met ingevoerde gegevens gebeurt en onjuiste of misleidende output. De AVG verplicht organisaties om een DPIA uit te voeren wanneer een nieuwe toepassing een hoog privacy risico kan opleveren.

Een DPIA staat voor Data Protection Impact Assessment, in het Nederlands: Gegevensbeschermingseffectbeoordeling (GEB). Een DPIA is een verplicht onderzoek bij verwerkingen met een hoog privacy risico waarmee in kaart wordt gebracht welke persoonsgegevens worden verwerkt, welke risico's dat kan opleveren voor mensen en welke maatregelen nodig zijn om die risico's te verkleinen.

Het is een wettelijk verplichte instrument om risico's per proces vooraf te beoordelen én te beheersen (artikel 35 AVG). Het AI-beleid, dat later aan uw raad wordt voorgelegd, beschrijft hoe deze wettelijke verplichting binnen de WDW en de gemeente Wijchen structureel wordt geborgd, waaronder de wijze waarop risico's worden beheerst, verantwoordelijkheden zijn belegd en hoe toezicht en evaluatie blijvend worden georganiseerd.

De verantwoordelijkheid voor naleving van de AVG ligt bij het college als verwerkingsverantwoordelijke. De Functionaris Gegevensbescherming (FG) houdt onafhankelijk toezicht en adviseert.

Daarnaast is op 1 augustus 2024 de Europese AI-verordening (AI Act) in werking getreden. Deze stelt eisen aan transparantie, risicobeheersing en toezicht bij het gebruik van AI. De gekozen werkwijze sluit hierop aan.

Wanneer kan SafeGPT worden gebruikt?

SafeGPT wordt momenteel geïmplementeerd in de vorm van een pilot, waarin we enkele usecases uitwerken. Wanneer dit gereed is, mogen bepaalde groepen medewerkers SafeGPT gebruiken voor specifieke werkzaamheden. Bijvoorbeeld voor het schrijven van teksten of het doorzoeken van teksten om tot antwoorden op vragen te komen. Vooralsnog worden enkel openbare gegevens ingevoerd.

Het invoeren van persoonsgegevens of andere gevoelige data is niet toegestaan zonder voorafgaande DPIA en verwerkersovereenkomst met de leverancier (SafeGPT).

Werkwijze en borging

We voeren altijd een verwerkersovereenkomst en DPIA uit, voordat persoonsgegevens in SafeGPT (of andere mogelijk toekomstige AI-oplossing) mogen worden verwerkt. De FG brengt hierover advies uit aan het college.

DPIA's worden periodiek herbeoordeeld en in ieder geval bij relevante wijzigingen in het proces of de toepassing. Na afloop van het eerste jaar wordt de pilot geëvalueerd. Dan wordt ook bepaald wat dit voor de DPIA betekent. Deze werkwijze sluit aan bij de eisen van de AVG, ENSIA/BIO en de AI-verordening (AI Act).

Standpunt van de FG

De FG geeft aan dat, vanuit haar onafhankelijke toezichthoudende rol, het ontbreken van vastgesteld AI-beleid op zichzelf geen belemmering vormt om DPIA's uit te voeren. Met een DPIA wordt de verwerking van persoonsgegevens in een AI-oplossing rechtmatig.

Gevolgen

1. Met deze werkwijze houdt de organisatie grip op de inzet van SafeGPT binnen de kaders van de AVG en AI-verordening, vooruitlopend op het vast te stellen AI-beleid.
2. De onafhankelijke toezichthoudende rol van de FG blijft gewaarborgd. De raad kan haar controlerende rol blijven uitoefenen doordat zij op verzoek inzicht krijgt in de uitkomsten van uitgevoerde DPIA's; niet openbare onderdelen van de DPIA zijn hiervan uitgezonderd.

Communicatie

- Wanneer wij SafeGPT in gebruik nemen, wordt deze oplossing ook in het algoritmeregister opgenomen. Zodat transparant is voor inwoners en de raad met welk doel en op welke wijze we deze oplossing gebruiken.
- Vanuit de WDW Academie worden trainingen en workshops georganiseerd over AI en het verantwoord gebruik van AI volgens de intern vastgestelde richtlijnen van de WDW. Hier gaan we onverminderd mee door. Hiermee blijven we voldoen aan de AI-verordening die vereist dat we de AI-geletterdheid van medewerkers op niveau houden.

Uitvoering of Vervolgstappen

Het AI-beleid wordt momenteel opgesteld en wordt naar verwachting aan het einde van het tweede kwartaal van 2026 ter vaststelling aan college en raad aangeboden. Het pilot project SafeGPT wordt ondertussen opgestart en loopt voor een jaar. Het wordt aan het eind van dit jaar intern geëvalueerd. Een opgestelde DPIA ten behoeve van de inzet van persoonsgegevens in SafeGPT is openbaar en opvraagbaar voor de raad.

Geheimhouding

Niet van toepassing