Beleid Generatieve AI

provincie Gelderland

Managementsamenvatting

Dit beleidskader biedt medewerkers, teams en leidinggevenden duidelijke afspraken voor verantwoord gebruik van generatieve AI binnen de provinciale taak en bedrijfsvoering. Het is het instrument waarmee de provincie invulling geeft aan de wettelijke AI-geletterdheidsverplichting uit de EU AI-verordening (art. 4, sinds 2 feb. 2025, gehandhaafd vanaf 2026).

Vier leidende beginselen

- De mens blijft aan zet: AI vervangt nooit menselijk oordeel of verantwoordelijkheid.
- Bescherming van mensen, rechten en gegevens staat voorop.
- Inzet moet aantoonbare publieke meerwaarde hebben.
- AI moet begrijpelijk en verantwoord te gebruiken zijn.

Kernafspraken

Toegestane tools: Microsoft Copilot Chat is de standaard, veilig binnen het M365-contract (geen modeltraining op onze data, verwerking binnen Europa). Publieke tools (ChatGPT, Claude, Gemini) zijn verboden voor werkinhoud; DeepSeek is uitgesloten op grond van rijksbeleid.

Verboden toepassingsgebieden (ongeacht de tool): geautomatiseerde besluitvorming zonder controle, profilering/monitoring van medewerkers of burgers, verwerking van bijzondere persoonsgegevens/BSN, Woo-gevoelige of bestuurlijk zeer gevoelige dossiers, politieke beïnvloeding.

Nieuwe AI-functionaliteit (aangeschaft of ingebouwd in bestaande software) wordt nooit automatisch geactiveerd: eerst beoordeling door I&A, Informatiebeveiliging, AI Compliance Officer en Privacy Officer, met vijf verplichte gegevenspunten (welke data, waar verwerkt, trainingsgebruik, bewaartermijn, rol in besluitvorming).

Derde partijen: dezelfde eisen gelden bij AI die leveranciers/samenwerkingspartners zelf inzetten; beoordeling loopt via het inkoopproces.

Doelbinding: AI wordt alleen gebruikt voor het doel waarvoor de leverancier het ontworpen heeft, om “function creep” en ongewenst aanbiederschap onder de AI-verordening te voorkomen.

Governance

Nieuwe rol: CAICO (Certified AI Compliance Officer): twee aangestelde medewerkers binnen het CIO Office die toezicht houden, meekijken bij pilots en de organisatiebrede juridische borging van de AI-verordening verzorgen. Verder heldere rolverdeling (CIO, Teammanager Innovatieteam, Beleidsadviseur AI, Privacy Officer, CISO, functioneel beheer, medewerkers) en risico-gestuurd toezicht: hoe hoger het risico, hoe uitgebreider de logging. Auditlogs worden nooit gebruikt om individuele medewerkers te beoordelen.

Overige thema’s

Non-discriminatie/bias-toetsing, verplichte transparantie (intern én extern, o.a. bij AI-gegenereerd beeld), en een breed opleidingsaanbod (e-learnings, AI Kampvuurtjes, Copilot-prompttraining, Moralis Machina).

Borging

Dit beleid is een levend document, dat we elke kwartaal bijstellen en evalueren op basis van technologische ontwikkelingen, wetswijzigingen, DPIA’s/audits/incidenten of bestuurlijke besluiten.

44726623 0016

Inhoud

	Inleiding	**4**
1	**Begrippen en context**	**6**
1.1	Wat is generatieve AI?	6
1.2	Relatie met de AI-verordening	7
1.3	Relatie met overige wet- en regelgeving	7
1.4	Speelveld en afhankelijkheden	8
2	**Beginselen**	**10**
3	**Uitgangspunten**	**11**
3.1	Menselijke autonomie en betrouwbaarheid	11
3.2	Voorwaarden voor goed AI-gebruik	11
3.2.1	Welke AI-toepassingen mag je gebruiken?	12
3.2.2	Waarvoor mag je AI niet gebruiken?	13
3.2.3	Nieuwe AI-toepassingen en AI-functionaliteit in bestaande software	14
3.2.4	Samenwerking met derden	16
3.2.5	Doelbinding en voorkomen van ongewenst gebruik	17
3.3	Gegevensgebruik en dataverantwoordelijkheid	18
3.3.1	Persoonsgegevens en gevoelige informatie	18
3.4	Kwaliteit, betrouwbaarheid en technische robuustheid	19
3.5	Experimenteren met nieuwe technologieën	19
3.6	Governance, toezicht en verantwoordelijkheid	20
3.6.1	Rollen	20
3.6.2	Toezicht en monitoring	21
3.6.3	Bewaren en vastleggen van AI-interacties	21
3.6.4	Governance in de praktijk	22
3.7	Transparantie en communicatie – intern	22
3.8	Transparantie en communicatie - extern	22
3.9	Gelijkheid, non-discriminatie en bias	23
3.10	Bewustwording en training	23
4	**Borging en doorontwikkeling**	**25**
	Naslagwerk	**26**

44726623 0016

Inleiding

Provincie Gelderland zet artificiële intelligentie (AI) steeds vaker in om het werk te ondersteunen en de publieke taak goed uit te voeren. AI biedt nieuwe mogelijkheden, maar vraagt ook om zorgvuldigheid. Wie AI verantwoord wil inzetten, moet weten welke ruimte er is, wie waarvoor verantwoordelijk is en welke aandachtspunten gelden voor bijvoorbeeld privacy, informatieveiligheid, toezicht en wet- en regelgeving. Dit beleidskader geeft daarvoor richting.

AI is een verzamelnaam voor verschillende technologieën. Generatieve AI is daar een specifieke vorm van. Deze technologie kan op basis van eenvoudige opdrachten bijvoorbeeld teksten, analyses, afbeeldingen en code maken. Daarmee ontstaan allerlei praktische mogelijkheden. Generatieve AI kan medewerkers helpen bij hun dagelijkse werk, bijdragen aan maatschappelijke opgaven en de fysieke leefomgeving, de samenwerking met andere overheden en partners ondersteunen en interne werkprocessen vereenvoudigen.

Tegelijkertijd vraagt het gebruik van generatieve AI om een kritische blik. Een AI-toepassing maakt antwoorden op basis van patronen in grote hoeveelheden gegevens. Dat betekent niet dat een antwoord automatisch juist of betrouwbaar is. AI kan informatie overtuigend presenteren terwijl die niet klopt. Ook kan een toepassing vooroordelen uit de gebruikte gegevens overnemen of een antwoord geven dat niet past bij de provinciale of politieke context. Bovendien is vaak moeilijk te zien hoe een AI-model precies tot een antwoord komt. Daardoor zijn de uitkomsten niet altijd eenvoudig te controleren.

De snelheid en het gemak waarmee medewerkers AI kunnen gebruiken, maken deze aandachtspunten extra belangrijk. Een fout antwoord kan bijvoorbeeld snel worden overgenomen in een advies, document of besluit. Verantwoord gebruik vraagt daarom niet om blind vertrouwen in AI, maar om medewerkers die weten wat een toepassing wel en niet kan, de uitkomsten kritisch beoordelen en zorgvuldig omgaan met de informatie die zij invoeren. Dit beleidskader biedt daarvoor de kaders en uitgangspunten.

De inzet van generatieve AI staat bovendien niet op zichzelf. AI maakt deel uit van een bredere digitale ontwikkeling binnen de provincie, en geeft onder andere invulling aan “slimmer georganiseerd” als een van de doelstellingen in de organisatieontwikkeling (roadmap organisatieontwikkeling). Daarbij gaat het ook om de manier waarop we met data omgaan, digitaal samenwerken, informatie beheren en terugvinden en informatie duurzaam bewaren. Goed AI-gebruik begint immers bij betrouwbare informatie en een organisatie die haar digitale basis op orde heeft.

Daarom staat dit beleidskader niet los van thema’s als data- en informatiebeheer, gegevenskwaliteit en digitaal samenwerken. AI is één van de bouwstenen van een organisatie die stap voor stap werkt aan verantwoorde, datagedreven en digitaal volwassen organisatie.

Afbakening

Dit beleidskader richt zich op het gebruik van generatieve AI binnen provincie Gelderland. Het beschrijft hoe medewerkers, teams en leidinggevenden van provincie Gelderland op een verantwoorde manier gebruikmaken van generatieve AI in hun dagelijkse werk.

Het gaat hierbij om generatieve AI-toepassingen die worden ingezet ter ondersteuning van provinciale taken en de bedrijfsvoering. Denk bijvoorbeeld aan het opstellen of verbeteren van teksten, het samenvatten van documenten en het genereren van ideeën.

44726623 0016

Dit beleidskader gaat niet over andere vormen van AI. Voor deze toepassingen kunnen aanvullende regels, technische richtlijnen en toetsingen nodig zijn, afhankelijk van de toepassing en de risico's die daarmee samenhangen. Denk bijvoorbeeld aan:

- Voorspellende AI, zoals modellen die verkeersdrukte, wegonderhoud of waterstanden voorspellen.
- Beeldherkenning, zoals het analyseren van satellietbeelden voor natuurbeheer of het herkennen van objecten op camerabeelden.
- Geautomatiseerde besluitvorming, zoals systemen die subsidieaanvragen of vergunningen geheel of gedeeltelijk automatisch toetsen of beoordelen.
- AI in kaart- en geo-informatiesystemen (GIS), zoals het automatisch classificeren van grondgebruik op basis van kaartgegevens.

Leeswijzer

Dit beleidskader is het strategische kader: het beschrijft de beginselen, kaders en verantwoordelijkheden voor het gebruik van generatieve AI binnen provincie Gelderland. Ga je zelf aan de slag met AI in je dagelijks werk? Raadpleeg dan ook de Handreiking voor gebruik van generatieve AI. Die geeft praktische, direct toepasbare richtlijnen en voorbeelden; dit beleidskader legt uit waarom die richtlijnen er zijn en binnen welke grenzen ze gelden.

Het document is als volgt opgebouwd:

- **Hoofdstuk 1** - Begrippen en context: wat generatieve AI is en hoe deze technologie zich verhoudt tot de Europese AI-verordening en overige relevante wet- en regelgeving, zoals de AVG en de Woo.
- **Hoofdstuk 2** - Beginselen: de vier leidende beginselen voor verantwoorde AI-inzet — menselijke regie, bescherming van mensen en gegevens, publieke meerwaarde en begrijpelijk gebruik.
- **Hoofdstuk 3** - Uitgangspunten voor generatieve AI: de concrete afspraken voor dagelijks gebruik. Dit hoofdstuk behandelt onder meer welke AI-tools en toepassingsgebieden zijn toegestaan (3.2), hoe we omgaan met persoonsgegevens (3.3), de governance en rolverdeling rond AI (3.6), en transparantie, non-discriminatie en training (3.7 t/m 3.10).
- **Hoofdstuk 4** - Borging en doorontwikkeling: hoe we het beleid periodiek evalueren en actueel houden.

Op basis van evaluaties wordt het beleid waar nodig aangescherpt, aangevuld of verduidelijkt. Mochten er vragen, opmerkingen of bezwaren zijn, mail dan naar [redacted].

44726623 0016

1 Begrippen en context

Dit hoofdstuk legt uit wat we binnen dit beleidskader verstaan onder generatieve AI, welke ontwikkelingen we verwachten en wat deze ontwikkelingen betekenen voor het gebruik van AI binnen provincie Gelderland.

Voor juridische vraagstukken en de toepassing van wet- en regelgeving gebruiken we de formele definitie van een 'AI-systeem' uit de Europese AI-verordening (AI Act). Wie meer wil weten over deze formele definitie, vindt in de AI-verordening de volledige tekst en toelichting.

In het kort
Generatieve AI ontwikkelt zich snel en biedt nieuwe mogelijkheden voor het werk van de provincie. Tegelijk brengt het gebruik ervan risico's en nieuwe afhankelijkheden met zich mee. Dit hoofdstuk legt uit wat generatieve AI is, welke wet- en regelgeving van toepassing is en hoe de provincie omgaat met ontwikkelingen in de AI-markt. Zo krijg je de belangrijkste context voor de uitgangspunten en afspraken in het volgende hoofdstuk.

1.1 Wat is generatieve AI?

Generatieve AI is een specifieke vorm van AI die zelfstandig nieuwe inhoud kan maken, zoals tekst, afbeeldingen, audio, video en computercode. In tegenstelling tot traditionele AI genereert deze technologie zelf nieuwe inhoud. Die inhoud kan soms nauwelijks te onderscheiden zijn van wat een mens heeft gemaakt.

Generatieve AI-systemen leren van grote hoeveelheden gegevens. Een gebruiker geeft vervolgens een opdracht, ook wel een prompt genoemd. Het systeem genereert op basis daarvan een antwoord. Dat antwoord is geen vaststaand feit of een 'waarheid', maar een statistisch waarschijnlijke uitkomst. Het systeem combineert patronen die het tijdens het leren heeft herkend tot nieuwe formuleringen, beelden of andere inhoud.

De ontwikkeling van een generatief AI-model verloopt in vijf hoofdfasen (Rathenau Instituut, 2023):

1. Dataverzameling: er wordt een grote hoeveelheid tekst, beeld en audio verzameld, vaak afkomstig van het internet.
2. Datacuratie: de verzamelde gegevens worden gefilterd en opgeschoond. Zo kunnen bijvoorbeeld dubbele of ongewenste gegevens worden verwijderd.
3. Training: het model leert patronen in de gegevens herkennen, bijvoorbeeld welke woorden vaak samen voorkomen. Zo leert het verbanden binnen taal, beeld of code te herkennen.
4. Afstemming: ontwikkelaars sturen het model verder bij, zodat het beter aansluit bij wat mensen verwachten. Extra training en feedback helpen het model om instructies beter op te volgen, veiliger te reageren en ongewenst gedrag te beperken.
5. Implementatie: het model komt beschikbaar in een toepassing of hulpmiddel. In deze fase regelen ontwikkelaars ook zaken als toegangsbeheer, privacy en informatiebeveiliging, zodat het model verantwoord kan worden gebruikt.

44726623 0016

Bekende toepassingen zijn AI-taalmodellen zoals Copilot, ChatGPT en vergelijkbare systemen. Via tekst kunnen gebruikers met deze systemen communiceren en ondersteuning krijgen bij uiteenlopende taken, zoals analyseren, samenvatten, schrijven en programmeren. Andere toepassingen richten zich bijvoorbeeld op het maken van afbeeldingen, muziek of spraak.

Het ontwikkelen van grote AI-modellen vraagt om enorme hoeveelheden gegevens, rekenkracht en investeringen. De kosten kunnen oplopen tot honderden miljoenen euro. Ook het dagelijks beschikbaar houden van zo'n model vraagt veel rekenkracht en geld. Hierdoor ligt de ontwikkeling van de grootste modellen vooral bij een beperkt aantal grote technologiebedrijven, zoals OpenAI, Google, Microsoft en Meta. Deze bedrijven werken daarbij ook met elkaar en met andere technologie-bedrijven samen. Zo investeert Microsoft in OpenAI en levert het samen met NVIDIA de benodigde rekeninfrastructuur.

Wil je meer weten over AI en hoe je er verantwoord mee kunt werken? Op geregelde momenten organiseren we laagdrempelige AI-Kampvuurtjes op de tribune. Daar kun je in een informele setting vragen stellen en ervaringen uitwisselen. Aanmelden kan via Gelderland Leert. Wil je je liever zelfstandig verdiepen? Via Gelderland Leert zijn ook verschillende e-learnings over AI beschikbaar.

1.2 Relatie met de AI-verordening

De Europese AI-verordening (Verordening (EU) 2024/1689, de 'AI Act') vormt het juridische fundament voor het verantwoord inzetten van AI binnen provincie Gelderland. De verordening stelt onder meer eisen aan transparantie, risicobeheersing en menselijk toezicht. Ook verplicht artikel 4 organisaties die AI-systemen gebruiken om ervoor te zorgen dat hun personeel en andere betrokkenen over voldoende kennis en vaardigheden beschikken om AI verantwoord te gebruiken. Deze verplichting geldt sinds 2 februari 2025.

Dit beleidskader geeft invulling aan deze verplichtingen binnen de provincie. Daarnaast zijn binnen het CIO Office twee medewerkers aangesteld als Certified AI Compliance Officer (CAICO). Zij ondersteunen de provincie bij de toepassing en naleving van de AI-verordening, bijvoorbeeld bij het indelen van AI-systemen naar risiconiveau en het beoordelen van AI-toepassingen aan de hand van wettelijke eisen.

Het beleidskader en de CAICO-rol vullen elkaar aan: het beleidskader geeft medewerkers, teams en leidinggevenden houvast bij het dagelijks gebruik van AI, terwijl de CAICO's zich richten op de organisatiebrede en juridische borging van de AI-verordening.

1.3 Relatie met overige wet- en regelgeving

Naast de AI-verordening moet het gebruik van AI binnen de provincie voldoen aan de bestaande wet- en regelgeving die van toepassing is op ons werk. Deze wetten zijn niet specifiek voor AI gemaakt, maar gelden ook wanneer we AI inzetten voor provinciale taken.

- **Algemene Verordening Gegevensbescherming (AVG):** beschermt persoons-gegevens en bepaalt hoe organisaties daarmee moeten omgaan. Je mag persoonsgegevens alleen invoeren in een AI-toepassing als dat volgens de provinciale regels en de geldende privacywetgeving is toegestaan.

44726623 0016

- **Wet open overheid (Woo):** regelt de openheid van de overheid en het recht van mensen om overheidsinformatie in te zien. Dit kan ook gelden voor informatie die met behulp van AI is gegenereerd of verwerkt.
- **Algemene wet bestuursrecht (Awb):** stelt regels aan besluiten van de overheid en vraagt onder meer om zorgvuldigheid, eerlijkheid en een goede onderbouwing. Dit is relevant zodra AI een rol speelt bij de voorbereiding of ondersteuning van besluiten.
- **Archiefwet:** regelt hoe overheidsinformatie moet worden bewaard, zodat belangrijke informatie toegankelijk en terug te vinden blijft. Ook documenten en andere informatie die met behulp van AI zijn gemaakt, kunnen onder deze bewaarplicht vallen.
- **Auteurswet:** beschermt werken van anderen en bepaalt onder welke voorwaarden je deze mag overnemen of gebruiken. Dit vraagt aandacht bij het gebruik van AI-gegenereerde teksten, afbeeldingen of code waarin bestaand materiaal is verwerkt.
- **Data Act:** bevat Europese regels over de toegang tot en het gebruik en delen van gegevens. De verordening moet bijdragen aan een eerlijkere toegang tot gegevens en een zorgvuldiger gebruik daarvan.
- **Europese Digitale Decade:** ook de ambities uit de Europese Digitale Decade zijn relevant. Daarin werken Europese landen aan een sterke, mensgerichte digitale samenleving en een economie waarin digitale technologie en data verantwoord worden ingezet.

Landelijk Algoritmeregister

Voor bepaalde AI- en algoritmetoepassingen geldt daarnaast een registratieplicht in het Landelijk Algoritmeregister. Overheden registreren hierin algoritmes die bijvoorbeeld invloed hebben op burgers of een rol spelen bij besluitvorming. Zo wordt inzichtelijk welke algoritmes overheden gebruiken, met welk doel en onder welke voorwaarden.

Gebruik je binnen je team of proces een AI-toepassing die geheel of gedeeltelijk besluiten voorbereidt of beïnvloedt? Stuur dan een e-mail naar [redacted] We bekijken dan samen of registratie in het algoritmeregister nodig is.

1.4 Speelveld en afhankelijkheden

De ontwikkeling van geavanceerde generatieve AI-modellen vraagt om grote investeringen in infrastructuur, rekenkracht en specialistische kennis. Daardoor ligt de ontwikkeling van deze modellen in belangrijke mate bij een beperkt aantal grote, vaak niet-Europese technologiebedrijven. Dit creëert afhankelijkheden op het gebied van technologie, data, rekenkracht en leveranciers. Die afhankelijkheden kunnen invloed hebben op onze digitale autonomie en keuzevrijheid als organisatie.

Provincie Gelderland wil deze afhankelijkheid van big tech, en van landen met waarden die niet aansluiten bij de onze, zo veel mogelijk beperken. Dit vraagstuk staat niet los van AI, maar maakt deel uit van de bredere digitale ontwikkeling van de provincie. Vanuit het CIO Office werken we daarom aan digitale autonomie, zodat de provincie ook op de lange termijn grip houdt op haar technologie, data en digitale voorzieningen.

Deze ambitie sluit aan bij de Nederlandse Digitaliseringsstrategie (NDS). Daarin werken Rijksoverheid, provincies, gemeenten en waterschappen samen aan een sterke digitale basis, waaronder een AI-infrastructuur met open taalmodellen uit Nederland en de Europese Unie, zoals GPT-NL. Provincie Gelderland volgt deze ontwikkeling en onderzoekt de mogelijkheden om dergelijke modellen te gebruiken zodra zij qua functionaliteit en veiligheid een volwaardig alternatief bieden voor bestaande toepassingen.

44726623 0016

Bij de inzet en ontwikkeling van generatieve AI letten we daarom in het bijzonder op:

- **Bewuste keuzes in leveranciers en oplossingen**, met oog voor afhankelijkheden op de lange termijn;
- **digitale autonomie,** met aansluiting bij Europese kaders en waarden;
- **een zorgvuldige balans tussen innovatie, risico's en publieke waarden.**

44726623 0016

2 Beginselen

In het kort
Deze beginselen vormen het kompas voor de manier waarop provincie Gelderland AI inzet. Ze helpen om keuzes te maken die passen bij onze publieke taak en publieke waarden. De mens blijft verantwoordelijk, we beschermen mensen en gegevens, AI moet aantoonbare meerwaarde hebben en het gebruik ervan moet begrijpelijk en verantwoord zijn.

Deze beginselen vormen het kompas voor verantwoorde inzet van AI binnen de organisatie. Ze gelden voor AI in brede zin, maar geven binnen dit beleidskader vooral richting aan het gebruik van generatieve AI. Ze sluiten aan bij hoe we als organisatie willen werken: lerend, toekomstgericht en met oog voor de samenleving waarin we werken.

AI ontwikkelt zich snel. Techniek, beleid en praktijk veranderen voortdurend en niet voor iedere situatie bestaan al duidelijke regels of werkwijzen. Juist dan helpen deze beginselen om richting te geven aan keuzes en afwegingen.

De beginselen zijn geen technische handleiding en ook geen checklist. Ze vormen een gedeeld uitgangspunt voor medewerkers, managers en projectteams. Bij iedere toepassing kunnen we daarmee dezelfde kernvragen stellen: *draagt deze inzet bij aan publieke waarden? Blijft de mens aan zet? Voorkomen we schade? En kunnen we uitleggen wat we doen en waarom?*

Zo maken de beginselen duidelijk vanuit welke grondhouding provincie Gelderland AI inzet. De beginselen luiden als volgt:



- **De mens (blijft) aan zet**
  AI ondersteunt het werk van mensen, maar neemt het menselijk oordeel en de verantwoordelijkheid niet over. Besluiten met impact op mensen nemen we altijd zelf. Medewerkers kunnen de inzet en uitkomsten van AI beoordelen, bijsturen en zo nodig stoppen.



- **We beschermen mensen, rechten en gegevens**
  Bij het gebruik van AI staan de bescherming van mensen, grondrechten, privacy, veiligheid en een zorgvuldige omgang met gegevens voorop. Technologische mogelijkheden zijn nooit een doel op zich en mogen niet ten koste gaan van publieke waarden.



- **AI heeft aantoonbare publieke meerwaarde**
  We zetten AI alleen in als dit bijdraagt aan onze publieke taak en aantoonbare maatschappelijke meerwaarde heeft. De toepassing moet passen bij het doel en de risico's die ermee samenhangen. Daarbij hebben we oog voor rechtvaardigheid en inclusie.



- **AI is begrijpelijk en verantwoord te gebruiken**
  We gebruiken AI alleen als medewerkers de werking en uitkomsten voldoende kunnen begrijpen voor de taak die zij uitvoeren. Ook moet duidelijk zijn welke rol medewerkers hebben bij het beoordelen en gebruiken van de uitkomsten. Zo blijft helder wie waarvoor verantwoordelijk is.

44726623 0016

3 Uitgangspunten

De uitgangspunten in dit hoofdstuk vertalen de algemene beginselen naar concrete afspraken voor het gebruik van generatieve AI (*vanaf nu: AI*) binnen provincie Gelderland. Waar hoofdstuk 2 beschrijft wat wij belangrijk vinden, maakt dit hoofdstuk duidelijk hoe we daar in de praktijk naar handelen.

In het kort
AI kan het werk van medewerkers ondersteunen, maar de mens blijft verantwoordelijk voor de keuzes en uitkomsten. Daarom stellen we voorwaarden aan zowel de AI-toepassingen die we gebruiken als de manier waarop we ze inzetten. Dit hoofdstuk beschrijft welke toepassingen zijn toegestaan, welke informatie je wel en niet met AI mag delen en voor welke doelen AI niet mag worden gebruikt.

3.1 Menselijke autonomie en betrouwbaarheid

AI ondersteunt het werk van medewerkers, maar neemt menselijke besluitvorming niet over. De mens blijft verantwoordelijk voor keuzes, oordelen en uitkomsten. Daarom beoordeelt een medewerker AI-uitvoer altijd voordat deze wordt gebruikt, gedeeld of verwerkt in een product, advies of besluit. Menselijk toezicht is geen formaliteit, maar een wezenlijk onderdeel van verantwoord gebruik.

Een goede beoordeling vraagt om voldoende kennis van het onderwerp. Je moet kunnen bepalen of de uitkomst klopt, volledig is en past bij het doel waarvoor je deze gebruikt. Heb je die kennis niet, dan kun je de uitkomst ook niet betrouwbaar beoordelen. Ben je bijvoorbeeld geen jurist, dan kun je door AI gegenereerde juridische informatie of een juridisch advies niet zelfstandig als correct beschouwen of gebruiken in je werk. Laat dit beoordelen door iemand met de juiste expertise. Hetzelfde geldt voor andere vakgebieden: gebruik AI-uitvoer niet buiten je eigen kennis en beoordelingsvermogen en schakel bij twijfel een collega in.

AI mag daarnaast niet worden ingezet op een manier die mensen misleidt, manipuleert of buitenspel zet. In ieder werkproces moet ruimte blijven om AI-uitvoer te corrigeren of te negeren en om het gebruik van AI te stoppen.

3.2 Voorwaarden voor goed AI-gebruik

Provincie Gelderland stelt Microsoft Copilot Chat beschikbaar als standaard AI-hulpmiddel voor algemeen en dagelijks gebruik binnen de beveiligde Microsoft 365-werkomgeving.

De provincie heeft hierover afspraken gemaakt met Microsoft via een interprovinciaal contract. Daarin staat onder meer dat onze gegevens niet worden gebruikt om de AI-modellen van Microsoft verder te trainen en dat onze gegevens binnen Europa worden verwerkt. Daarmee hebben we als organisatie meer zicht en grip op wat er met ingevoerde gegevens gebeurt dan bij openbare, niet-gecontracteerde AI-toepassingen zoals ChatGPT.

44726623 0016

In de handreiking staat hoe je AI op een goede en veilige manier gebruikt. Daarnaast bieden we een Copilot-prompttraining aan. Deze helpt je om de mogelijkheden van Copilot veilig en effectief te benutten. Ben je aan de slag met Copilot en heb je een functionele vraag, bijvoorbeeld over de werking of mogelijkheden van Copilot? Dan kun je terecht bij de servicedesk bedrijfsvoering. Zij kunnen helpen bij vragen over de functionaliteit en toepassing van Copilot in het dagelijks werk.

Heb je een vraag over de **regels, risico's of verantwoorde inzet van AI** binnen de provincie? Dan kun je terecht bij het CIO Office en de CAICO's, via 5.1.2i

Naast Copilot verkennen we andere AI-oplossingen. Zo onderzoeken we welke toepassingen passen bij verschillende soorten werkzaamheden en behoeften. Dit sluit aan bij de bredere lijn uit de Nederlandse Digitaliseringsstrategie, waarin overheden samenwerken aan minder afhankelijkheid van een beperkt aantal, veelal niet-Europese leveranciers. Op dit moment biedt Copilot een goede en veilige basis voor het merendeel van het dagelijkse werk.

In de volgende paragrafen beantwoorden we twee vragen die vaak door elkaar lopen: welke AI-toepassingen je mag gebruiken (3.2.1) en waarvoor je AI wel en niet mag inzetten (3.2.2). Daarna volgen de afspraken over AI die is ingebouwd in bestaande software (3.2.3), over samenwerking met externe partijen (3.2.4) en over het vasthouden aan het oorspronkelijke doel van een toepassing (3.2.5).

3.2.1 Welke AI-toepassingen mag je gebruiken?

Voor je werk gebruik je alleen AI-toepassingen die de provincie heeft goedgekeurd. Voor deze toepassingen heeft de provincie afspraken gemaakt met de leverancier. Zo weten we beter waar onze gegevens worden verwerkt en wat ermee gebeurt.

Copilot is daarvan de bekendste, maar niet de enige. De provincie koopt en beheert ook AI-toepassingen voor specifieke taken. Voorbeelden zijn software die persoonsgegevens in documenten kan anonimiseren en toepassingen voor *remote sensing*, waarbij beelden van satellieten, vliegtuigen of drones automatisch worden geanalyseerd. Voor deze toepassingen gelden de algemene uitgangspunten uit dit beleidskader, aangevuld met specifieke afspraken per toepassing en leverancier (zie 3.3.1).

Wat niet mag

Voer geen werkinhoud in bij openbare, niet-gecontracteerde AI-tools zoals ChatGPT, Claude of Gemini. Ook niet als je deze via de browser binnen de werkomgeving gebruikt. Het gaat bijvoorbeeld om:

- niet-openbare documenten en concepten;
- interne communicatie, zoals een (concept)mail;
- beleidsinhoud, adviezen en interne analyses;
- elke vorm van persoonsgegevens;
- vertrouwelijke of niet-openbare informatie;
- gegevens waaruit is af te leiden voor wie je werkt of waar het over gaat.

Bij deze toepassingen hebben we als organisatie onvoldoende zicht en garanties over het gebruik, de opslag en het eventuele hergebruik van ingevoerde gegevens. Daardoor kunnen we onvoldoende grip houden op onze informatie.

44726623 0016

Het gebruik van externe AI-transcriptietools, zoals Wispr en vergelijkbare toepassingen, voor werkgerelateerde gesprekken is niet toegestaan. Bij dit soort toepassingen gaat het namelijk niet alleen om AI, maar ook om het opnemen en verwerken van gesprekken. Daarin kunnen uitspraken van collega's, inwoners, partners of andere deelnemers voorkomen. Dat brengt niet alleen risico's mee voor privacy en informatiebeveiliging. Ook vertrouwen, verwachtingen en de manier waarop we als organisatie met elkaar en met gespreksinformatie omgaan spelen een rol. Het is daarom niet voldoende om zelf te beoordelen dat een gesprek geen gevoelige informatie bevat. Ook de andere deelnemers aan het gesprek worden door de opname en verwerking geraakt.

De organisatie werkt aan een veilige voorziening voor transcriptie binnen Teams, met duidelijke regels voor het gebruik daarvan. Tot die tijd mogen medewerkers niet op eigen initiatief externe AI-toepassingen gebruiken voor het uitschrijven van werkgerelateerde gesprekken.

Voor sommige AI-toepassingen geldt bovendien een volledig verbod op gebruik met provinciale apparatuur, ongeacht het doel waarvoor je de toepassing wilt gebruiken. Het gaat om toepassingen die op grond van wet- en regelgeving of rijksbeleid niet zijn toegestaan op overheidsapparatuur. Een voorbeeld is het Chinese DeepSeek, waarvoor veiligheidsrisico's rond gegevensopslag buiten de Europese Economische Ruimte een rol spelen. Deze toepassingen worden waar mogelijk technisch geblokkeerd. Een actueel overzicht van uitgesloten AI-toepassingen vind je op de SharePoint-pagina van Digitaal Samenwerken.

Wat wel mag: AI als persoonlijk hulpmiddel

Het verbod gaat over werkinhoud, niet over het feit dat je bij de provincie werkt of met werkzaken bezig bent. Er is ruimte om AI te gebruiken om je gedachten te ordenen, op je werk te reflecteren of een gesprek of vergadering voor jezelf voor te bereiden. Dat mag ook met een externe AI-toepassing, zolang je dit in algemene termen doet. Deel daarbij geen concrete werkinhoud, documenten, namen of vertrouwelijke informatie. Dit sluit aan bij de ambtseed en de bestaande afspraken over het delen van informatie met externen.

We vertrouwen hierbij op het goed zeemanschap van iedere medewerker: twijfel je of je iets kunt delen, deel het dan niet. Twijfel je of je een bepaalde AI-toepassing voor je werk mag gebruiken? We denken graag mee. Stuur een e-mail naar [redacted]

3.2.2 Waarvoor mag je AI niet gebruiken?

De vorige paragraaf ging over de vraag welke AI-toepassingen je mag gebruiken. Hier gaat het om een andere vraag: waarvoor mag je AI gebruiken? Met andere woorden: het toepassingsgebied.

Sommige vormen van AI-gebruik zijn niet toegestaan, ongeacht welke toepassing je gebruikt. Dat geldt dus ook voor een goedgekeurde en beveiligde toepassing als Copilot. Deze beperkingen beschermen de privacy, rechtsbescherming en menselijke autonomie van mensen en sluiten aan bij de eisen uit de Europese AI-verordening en de AVG.

Je mag AI niet gebruiken voor:
- geautomatiseerde besluitvorming of besluitvoorbereiding waarbij de output zonder controle wordt overgenomen;
- profilering, monitoring, beoordeling, rangschikking of selectie van medewerkers of burgers;
- analyse of voorspelling van emoties, intenties of gedrag van medewerkers of burgers;

44726623 0016

- verwerking of analyse van HR-dossiers, integriteitsdossiers, medische of strafrechtelijke gegevens;
- verwerking van bijzondere persoonsgegevens of het burgerservicenummer (BSN);
- gebruik in Woo-gevoelige, juridisch vertrouwelijke of bestuurlijk zeer gevoelige dossiers;
- politieke beïnvloeding, stemadvies of andere vormen van manipulatie in democratische processen.

Deze beperkingen gelden naast de afspraken uit paragraaf 3.2.1 over welke AI-toepassingen je mag gebruiken. Beide regels gelden dus tegelijk: ook met een goedgekeurde AI-toepassing mag je AI niet voor bovenstaande doeleinden inzetten.

Het niet naleven van deze afspraken kan gevolgen hebben. Toezichthouders kunnen bijvoorbeeld handhaven op grond van de AVG en de AI-verordening. Daarnaast kan onzorgvuldig gebruik de provincie schaden in haar relatie met inwoners, Provinciale Staten en de rechter.

Kom je een toepassing tegen waarvan je vermoedt dat die onder een van deze beperkingen valt? Meld dit dan via [redacted] 5.1.2i

3.2.3 Nieuwe AI-toepassingen en AI-functionaliteit in bestaande software

AI kan op twee manieren de organisatie binnenkomen. Soms schaffen we bewust een AI-toepassing aan voor een specifieke taak. In andere gevallen voegt een leverancier AI toe aan software die we al gebruiken. Denk aan een nieuwe module, een plug-in of een geautomatiseerde functie in een bestaande applicatie.

In beide situaties gelden dezelfde uitgangspunten. We willen weten welke gegevens de AI verwerkt, waar die verwerking plaatsvindt en wat er met de gegevens gebeurt. Het verschil zit vooral in het moment waarop we die vragen kunnen stellen. Bij de aanschaf van nieuwe software kunnen we vooraf eisen stellen en afspraken maken. Bij AI-functionaliteit in bestaande software komt de vraag vaak pas aan de orde wanneer een leverancier nieuwe mogelijkheden aankondigt.

De norm verandert daarmee niet; alleen de route ernaartoe verschilt.

Uitgangspunten

- **AI-functionaliteit wordt niet automatisch geactiveerd.** Nieuwe of ingrijpend gewijzigde AI-functionaliteit wordt eerst beoordeeld door I&A en de AI Compliance Officer, en, afhankelijk van de toepassing en risico's, door Informatiebeveiliging en de Privacy Officer.
- **AI gebruiken we alleen binnen de daarvoor aangewezen provinciale werkomgeving**, nadat duidelijk is welke gegevens worden verwerkt en welke risico's daarmee samenhangen.
- **AI-toepassingen moeten voldoen aan de AVG, de BIO2, AI-architectuur richtlijnen en dit AI-beleidskader**. Gebruiksgemak of standaardinstellingen van een leverancier zijn geen reden om hiervan af te wijken.
- **Medewerkers worden tijdig geïnformeerd** wanneer nieuwe AI-functionaliteit beschikbaar komt in software die zij gebruiken of wanneer een nieuwe AI-toepassing in gebruik wordt genomen.
- **De verantwoordelijke applicatiebeheerder registreert in de CMDB** of een applicatie AI-functionaliteit bevat of zelf een AI-toepassing is. Het CIO Office en I&A bewaken samen de actualiteit en volledigheid van dit overzicht.

44726623 0016

Wanneer weten we genoeg?

Om te kunnen bepalen of een AI-toepassing verantwoord kan worden gebruikt, moeten we in ieder geval weten:

- welke gegevens de AI verwerkt en of daar persoonsgegevens bij zitten;
- waar de verwerking plaatsvindt en welke andere partijen daarbij betrokken zijn;
- of gegevens worden gebruikt om AI-modellen te trainen of te verbeteren;
- hoe lang gegevens worden bewaard en of ze kunnen worden verwijderd;
- of de uitkomsten van de AI een rol spelen bij advisering of besluitvorming over inwoners, bedrijven of andere betrokkenen.

Bij de aanschaf van nieuwe software vertalen we deze punten naar duidelijke eisen en afspraken die passen bij de manier waarop we de software inkopen. Bij een aanbesteding nemen we de relevante eisen op in het Programma van Eisen. Waar passend gebruiken we deze ook bij de beoordeling van de aanbiedingen. Zo maken we vooraf duidelijk aan welke voorwaarden een oplossing moet voldoen en welke informatie nodig is om de aanbiedingen goed te kunnen beoordelen. De keuze voor een leverancier maken we volgens de regels van de betreffende inkoopprocedure en op basis van het geheel aan eisen en beoordelingscriteria.

De diepgang van de beoordeling hangt af van de risico's. Worden alleen openbare of niet-gevoelige gegevens verwerkt en heeft de AI geen invloed op besluitvorming? Dan kan een beknopte beoordeling volstaan. Gaat het om persoonsgegevens of interne informatie, dan kan een pre-DPIA nodig zijn en moet worden gekeken naar de afspraken over gegevensverwerking. Bij hoog-risicotoepassingen in de zin van de AI-verordening geldt het volledige beoordelingsproces, waaronder een DPIA, een use case card, opname in het Algoritmeregister en een expliciet besluit van de verantwoordelijke concernmanager. Voor de beoordeling van de gegevens sluiten we aan bij de geldende dataclassificatie.

Als een leverancier nog niet alles kan aanleveren

Bij de aanschaf van nieuwe software nemen we vooraf duidelijke eisen en voorwaarden op. In een aanbesteding vertalen we de gewenste informatie naar eisen en, waar passend, gunningscriteria die aansluiten bij de aanbestedingsregels. Een leverancier moet daarmee kunnen aantonen dat de aangeboden oplossing geschikt is en aan onze eisen kan voldoen. De keuze voor een leverancier maken we altijd op basis van het volledige pakket aan eisen en gunningscriteria, niet op basis van één afzonderlijk antwoord over AI.

Bij software die we al gebruiken, ligt dat anders. Een leverancier kan bijvoorbeeld nieuwe AI-functionaliteit toevoegen zonder dat alle informatie over de werking en gegevensverwerking direct beschikbaar is. Dat kan ook gebeuren wanneer de leverancier voor de AI-functionaliteit gebruikmaakt van een andere partij.

Zolang we onvoldoende zicht hebben op de gegevensstromen en risico's, stellen we de functionaliteit niet beschikbaar. I&A en de AI Compliance Officers leggen samen vast wat bekend is, welke informatie nog ontbreekt en welke risico's daaruit voortkomen. Vervolgens bepalen zij, samen met de verantwoordelijke voor de applicatie, welke vervolgstap passend is. Daarbij zijn drie routes mogelijk:

- de functionaliteit blijft voorlopig uit. Bij een eerstvolgende contractherziening of ander geschikt contactmoment vragen we de ontbrekende informatie alsnog op;
- de functionaliteit wordt beperkt beschikbaar gesteld, met passende maatregelen. Denk bijvoorbeeld aan gebruik met alleen openbare gegevens of door een afgebakende groep medewerkers;
- de functionaliteit wordt beschikbaar gesteld op basis van een expliciet en gemotiveerd besluit over het resterende risico.

44726623 0016

Een besluit over resterende risico's leggen we vast bij de registratie in de CMDB. Daarbij nemen we ook een moment op waarop we de situatie opnieuw beoordelen, bijvoorbeeld bij een contractherziening of wanneer de leverancier nieuwe informatie verstrekt. Zo blijft zichtbaar welke risico's we bewust hebben geaccepteerd en op basis waarvan.

3.2.4 Samenwerking met derden

Provincie Gelderland werkt regelmatig samen met organisaties en bedrijven die bij de uitvoering van een opdracht mogelijk AI gebruiken. Denk aan advies- en onderzoeksbureaus of uitvoerende partijen die bijvoorbeeld analyse, rapportage, transcriptie of andere vormen van ondersteuning leveren. Soms weten we vooraf dat een leverancier AI gebruikt, maar dat is niet altijd het geval.

Bij deze vorm van AI draait de toepassing bij een externe partij. We hebben niet direct zicht op de gebruikte technologie, terwijl onze gegevens er wel doorheen kunnen gaan en de uitkomsten onderdeel kunnen worden van ons werk. Daarom moeten we bij samenwerking met derden nagaan **of AI een rol speelt, hoe de leverancier die inzet en wat dit betekent voor onze gegevens en dienstverlening.**

De opdrachtgever binnen de provincie is hiervoor verantwoordelijk. Bij het aangaan van een opdracht beoordeelt de opdrachtgever welke wet- en regelgeving en welke eisen voor de betreffende dienstverlening gelden. Als AI een rol speelt of mogelijk kan spelen, neemt de opdrachtgever dit mee in de voorbereiding en afspraken met de leverancier.

Inkoop kan hierbij ondersteunen wanneer zij bij de opdracht betrokken is, bijvoorbeeld door relevante voorwaarden en eisen op te nemen in de inkoop-documenten of overeenkomst. Inkoop is echter niet bij iedere opdracht betrokken. Dat geldt bijvoorbeeld voor opdrachten die via een raamovereenkomst of als kleine opdracht tot stand komen.

Om ook in die situaties een goede basis te leggen, werken we aan een aanpassing van de Algemene Inkoopvoorwaarden. Daarin willen we algemene afspraken opnemen over het gebruik van AI en de verwerking van gegevens door leveranciers. Zo kunnen deze afspraken ook gelden wanneer Inkoop niet rechtstreeks bij een opdracht betrokken is. Bij grotere of risicovollere opdrachten kunnen aanvullende eisen worden opgenomen in het Programma van Eisen, de overeenkomst of andere inkoopdocumenten.

Afspraken met leveranciers en samenwerkingspartners

Bij samenwerking met derden gelden de volgende uitgangspunten:

- **Maak duidelijk of AI een rol speelt.** Ga bij het aangaan van een opdracht na of de leverancier AI gebruikt of kan gebruiken voor de uitvoering ervan. Vraag, passend bij de aard en omvang van de opdracht, welke AI wordt ingezet, welke gegevens daarbij worden verwerkt, waar die verwerking plaatsvindt en welke andere partijen daarbij betrokken zijn.
- **Maak duidelijke afspraken over gegevens.** Leg vast waarvoor gegevens mogen worden gebruikt, hoe lang ze worden bewaard en of ze worden gebruikt om AI-modellen te trainen of te verbeteren. Wanneer een leverancier persoons-gegevens namens de provincie verwerkt, maken we hierover passende afspraken, onder meer in een verwerkersovereenkomst.

44726623 0016

- **Beoordeel de uitkomsten voordat we ze gebruiken.** Analyses, rapportages, transcripties en andere resultaten die met behulp van AI tot stand zijn gekomen, worden inhoudelijk gecontroleerd voordat ze worden gebruikt voor advisering of besluitvorming. Ook wanneer een externe partij AI heeft gebruikt, blijft de provincie verantwoordelijk voor het uiteindelijke gebruik van de uitkomst.
- **Let ook op andere partijen die de leverancier inschakelt.** Een leverancier kan voor zijn dienstverlening gebruikmaken van bijvoorbeeld een cloudleverancier of een externe AI-dienst. Ook dan moeten we weten welke gegevens daarbij betrokken zijn en onder welke voorwaarden de verwerking plaatsvindt.
- **Stem het delen van gegevens en het uitbesteden van werkzaamheden vooraf af.** Maak duidelijk welke gegevens worden gedeeld, met welk doel, met welke partijen en onder welke voorwaarden. Voor vertrouwelijke informatie en persoonsgegevens gelden de daarvoor geldende geheimhoudings-, privacy- en beveiligingsafspraken.

De Algemene Inkoopvoorwaarden van provincie Gelderland vormen hiervoor het algemene kader. Daarin staan onder meer afspraken over het naleven van de AVG, passende technische en organisatorische maatregelen en het verwerken van persoonsgegevens in opdracht van de provincie. Deze voorwaarden zijn nog niet specifiek gericht op de risico's van AI. Daarom werken we eraan om AI ook structureel mee te nemen in de algemene inkoopvoorwaarden en, waar nodig, in de afspraken voor een specifieke opdracht.

Tot die tijd vormt dit beleidskader een aanvullend uitgangspunt voor medewerkers die opdrachten voorbereiden en voor de beoordeling van AI-gebruik door leveranciers en samenwerkingspartners.

3.2.5 Doelbinding en voorkomen van ongewenst gebruik

Voor alles wat hierboven staat geldt een belangrijk uitgangspunt: de provincie gebruikt AI-functionaliteit alleen voor het doel waarvoor de toepassing is ontworpen en beoordeeld. We breiden het gebruik dus niet zelfstandig uit naar andere doelen. Als een toepassing bijvoorbeeld is bedoeld om teksten samen te vatten, gebruiken we die niet zonder nieuwe beoordeling voor het beoordelen van personen of het nemen van besluiten.

Dit voorkomt wat ook wel *function creep* wordt genoemd: het geleidelijk gebruiken van een AI-toepassing voor steeds meer of andere doeleinden dan oorspronkelijk bedoeld. Dat gebeurt vaak niet met één bewuste keuze, maar stap voor stap. Juist daarom is het belangrijk dat we overzicht houden over welke AI-toepassingen we gebruiken en waarvoor.

Elke AI-toepassing registreren we in de CMDB en, waar nodig, ook in het Algoritmeregister. Per toepassing leggen we in ieder geval de risicoclassificatie, de verantwoordelijke afdeling en de betrokken leverancier vast. Voor AI-toepassingen met een hoog risico leggen we daarnaast de doelomschrijving en het toegestane gebruik vast in een *use case card*.

Het CIO Office en I&A houden toezicht op dit overzicht. Als het gebruik van een AI-toepassing verandert of niet meer aansluit bij de oorspronkelijke beoordeling, bekijken we opnieuw welke risico's en voorwaarden gelden. Zo nodig zetten we de toepassing tijdelijk stop totdat die nieuwe beoordeling is afgerond.

44726623 0016

3.3 Gegevensgebruik en dataverantwoordelijkheid

AI gebruiken vraagt om een zorgvuldige omgang met gegevens. Daarom moeten AI-toepassingen aansluiten bij de Algemene Verordening Gegevensbescherming (AVG) en bij de organisatiebrede afspraken over informatiebeheer en datagebruik[1].

1 Data Governance Wiki: SharePoint-pagina CDO team – CIO Office. Afspraken over de manier waarop we in onze organisatie met data en informatie omgaan zijn van toepassing op de volledige levenscyclus van gegevens: van verzameling en gebruik tot opslag en verwijdering.

3.3.1 Persoonsgegevens en gevoelige informatie

De AVG geldt ook wanneer we AI gebruiken. Dit beleidskader vult de bestaande privacyregels aan, maar vervangt ze niet. Er gelden voor AI geen uitzonderingen op de privacyregels.

Copilot: geen bijzondere persoonsgegevens

In Copilot voeren we geen bijzondere persoonsgegevens of BSN-nummers in. Bijzondere persoonsgegevens[2] krijgen onder de AVG extra bescherming. Het is belangrijk dat medewerkers deze gegevens kunnen herkennen. Ze kunnen ook voorkomen in gewone werkinhoud, bijvoorbeeld in een dossier over een medewerker, een inwoner of een strafrechtelijke situatie.

2 Zoals gegevens over gezondheid, ras of etnische afkomst, religieuze of politieke overtuigingen, en strafrechtelijke gegevens.

Commerciële AI-tools: geen persoonsgegevens

Bij werkgerelateerd gebruik van openbare, niet-gecontracteerde AI-toepassingen voeren we helemaal geen persoonsgegevens in. Het maakt daarbij niet uit of het om bijzondere of gewone persoonsgegevens gaat. De reden is dat de provincie met deze aanbieders geen afspraken heeft over de verwerking van onze gegevens. We hebben daardoor onvoldoende zicht en grip op wat er met de gegevens gebeurt. (zie paragraaf 3.2.1).

Let ook op minder zichtbare persoonsgegevens. Een document of e-mail kan bijvoorbeeld persoonsgegevens bevatten in de tekst, maar ook in metadata, zoals de naam van de auteur. Ook openbare informatie, bijvoorbeeld over Statenleden, mag je niet automatisch zonder beoordeling in een AI-toepassing invoeren.

Andere gecontracteerde toepassingen: afspraken per leverancier

Voor andere gecontracteerde AI-toepassingen leggen we vooraf vast welke gegevens medewerkers wel en niet mogen invoeren. Dit hangt af van de afspraken die de provincie met de leverancier heeft gemaakt en van de risico's van de toepassing.

Bij een nieuwe AI-toepassing brengen we vooraf de privacyrisico's in kaart met een pre-DPIA. Als daar aanleiding toe is, volgt een volledige DPIA. Zo weten we voordat een toepassing in gebruik gaat welke risico's spelen en welke maatregelen nodig zijn om die risico's weg te nemen of te beperken.

Twijfel je over het gebruik of de verwerking van persoonsgegevens? Neem dan contact op met de centrale Privacy Officer(s) of de privacyambassadeur[3] van jouw afdeling.

3 SharePoint pagina privacy officers

44726623 0016

3.4 Kwaliteit, betrouwbaarheid en technische robuustheid

Verantwoord AI-gebruik vraagt om meer dan een kritische gebruiker. Ook de toepassing zelf moet voldoende betrouwbaar en veilig zijn voor het doel waarvoor we haar gebruiken. We moeten kunnen begrijpen hoe een AI-toepassing in hoofdlijnen werkt en welke factoren van invloed kunnen zijn op de uitkomsten. Dat helpt om fouten, vertekening en andere ongewenste effecten tijdig te herkennen. Hoeveel inzicht en uitleg nodig is, hangt af van de toepassing en de risico's.

Daarnaast moet een AI-toepassing stabiel en veilig functioneren binnen het werkproces waarvoor we haar gebruiken. We houden daarbij ook rekening met onverwachte situaties en foutieve invoer. Daarom maken we bij iedere AI-toepassing een passende risicobeoordeling.

Hoe groter het risico, hoe zwaarder de eisen aan bijvoorbeeld testen, beveiliging, toezicht en controle. AI-toepassingen met een hoger risicoprofiel leggen we ook vast in de CMDB en, waar dat verplicht is, in het Algoritmeregister. Bij AI-toepassingen waarvoor dat vanuit de risico's of de AI-verordening nodig is, zorgen we bovendien voor een manier om het gebruik te onderbreken of de toepassing buiten werking te stellen wanneer zich ernstige risico's of ongewenste effecten voordoen.

3.5 Experimenteren met nieuwe technologieën

Nieuwe technologie leer je niet alleen kennen door erover te lezen of er beleid over te schrijven. Daarom heeft I&A een intern innovatieteam dat AI-pilots en andere experimenten begeleidt. Dat gebeurt gecontroleerd, met de juiste expertise en volgens een eigen innovatieproces. Een experiment begint bij een concreet vraagstuk uit de organisatie. Eerst brengen we het probleem goed in beeld. Daarna onderzoeken we of nieuwe technologie, zoals AI, daarbij kan helpen en welke oplossing het beste past.

Een pilot is een gezamenlijke inspanning. Collega's of teams die een vraagstuk aandragen, blijven tijdens de pilot betrokken. Zij brengen hun praktijkkennis in, testen de resultaten en denken mee over de vervolgstappen. De combinatie van inhoudelijke kennis en technische expertise maakt een experiment sterker en helpt voorkomen dat we technologie inzetten omdat het kan, in plaats van omdat het iets toevoegt.

Heb je een idee voor een experiment? Neem dan contact op via [redacted] 5.1.2i
Een idee is een waardevol vertrekpunt, maar niet ieder idee leidt automatisch tot een pilot of werkende toepassing.

44726623 0016

3.6 Governance, toezicht en verantwoordelijkheid

Verantwoord AI-gebruik vraagt om meer dan goede afspraken over technologie en gegevens. Het vraagt ook om duidelijkheid over wie waarvoor verantwoordelijk is, wie toezicht houdt en waar medewerkers terechtkunnen met vragen of twijfels. Governance zorgt ervoor dat AI niet op zichzelf komt te staan, maar onderdeel blijft van de reguliere manier waarop we ons werk organiseren en verantwoorden.

De verantwoordelijkheid ligt zo veel mogelijk daar waar het gebruik van AI plaatsvindt. Medewerkers zijn verantwoordelijk voor hun eigen gebruik, managers zorgen voor ruimte en ondersteuning binnen hun teams en proces-eigenaren zijn verantwoordelijk voor de toepassing binnen hun proces. Specialistische functies ondersteunen wanneer specifieke kennis of toetsing nodig is.

3.6.1 Rollen

Een verantwoorde inzet van AI vraagt om duidelijke rollen. Niet iedereen hoeft dezelfde kennis over AI te hebben. Wel moet duidelijk zijn wie verantwoordelijk is, wie ondersteunt en wanneer andere expertise nodig is.

Medewerkers
Medewerkers zijn verantwoordelijk voor het eigen gebruik van AI. Zij houden zich aan de afspraken uit dit beleidskader, beoordelen AI-uitkomsten kritisch en blijven zelf verantwoordelijk voor het werk waarin zij AI gebruiken. Bij twijfel over de toepassing, risico's of regels zoeken zij afstemming.

Teammanagers en concernmanagers
Managers zijn een belangrijke schakel tussen het beleid en de dagelijkse praktijk. Zij hoeven niet zelf alle kennis over AI te hebben, maar zorgen er wel voor dat er binnen teams ruimte is om het gebruik van AI te bespreken.

Dat betekent onder meer dat managers met medewerkers in gesprek gaan over hoe zij AI gebruiken, welke kansen zij zien en waar zij tegenaan lopen. Ook maken zij vragen en twijfels bespreekbaar en signaleren zij wanneer aanvullende ondersteuning of expertise nodig is.

Managers faciliteren medewerkers bovendien om zich te ontwikkelen in het verantwoord gebruik van AI. Zij zorgen waar nodig voor tijd, ruimte en passende ondersteuning en stimuleren medewerkers om ervaringen en vragen met elkaar te delen.

Proceseigenaren en opdrachtgevers
Proceseigenaren en opdrachtgevers zijn verantwoordelijk voor de inzet van AI binnen hun proces, product of opdracht. Zij zorgen dat het doel van de toepassing duidelijk is, dat de risico's in beeld zijn en dat passende maatregelen zijn getroffen. Bij een nieuwe of gewijzigde toepassing betrekken zij tijdig de relevante expertise.

CIO Office en CAICO's
Het CIO Office ontwikkelt en onderhoudt het beleidskader en ondersteunt de organisatie bij vraagstukken rond AI, digitalisering en digitale ethiek. De CAICO's ondersteunen specifiek bij de juridische borging en naleving van de AI-verordening. Zij adviseren onder meer over risicoclassificatie, registratie en de toepassing van wettelijke eisen.

44726623 0016

Privacy, informatiebeveiliging, juridisch en andere deskundigen
Specialistische functies brengen hun expertise in wanneer de aard of het risico van een AI-toepassing daarom vraagt. Denk aan privacy, informatiebeveiliging, juridische zaken, informatiebeheer en archivering. Zij adviseren vanuit hun eigen verantwoordelijkheid en werken waar nodig samen met het CIO Office, de CAICO's en de betrokken organisatieonderdelen.

De rollen vullen elkaar aan. Verantwoord AI-gebruik is daarmee geen taak van één afdeling of functie, maar een gezamenlijke verantwoordelijkheid waarbij iedereen weet wanneer hij of zij aan zet is en wanneer andere expertise nodig is.

3.6.2 Toezicht en monitoring

We houden zicht op het gebruik van AI binnen de organisatie. De manier waarop we dat doen, hangt af van het doel en het risico van de toepassing. Voor toepassingen met grotere risico's is meer toezicht, vastlegging en evaluatie nodig dan voor eenvoudig dagelijks gebruik.

AI-toepassingen worden geregistreerd volgens de binnen de provincie afgesproken werkwijze. Daarbij leggen we onder meer vast waarvoor de toepassing wordt gebruikt, wie verantwoordelijk is en welke risico's zijn vastgesteld. Bij toepassingen met een hoger risico kijken we ook naar de werking in de praktijk, de kwaliteit van de uitkomsten en eventuele incidenten.

Monitoring is niet bedoeld om medewerkers individueel op hun AI-gebruik te beoordelen. Het doel is om te kunnen zien of een toepassing nog steeds doet waarvoor deze is bedoeld, of risico's veranderen en of aanvullende maatregelen nodig zijn.

Wanneer AI tot een fout, incident of mogelijk onwenselijke uitkomst leidt, melden en behandelen we dit via de daarvoor geldende processen. Op basis van de ernst en oorzaak bepalen we welke vervolgstappen nodig zijn. Dat kan bijvoorbeeld betekenen dat een toepassing wordt aangepast, opnieuw beoordeeld of tijdelijk wordt stilgezet.

3.6.3 Bewaren en vastleggen van AI-interacties

Niet iedere interactie met AI hoeft afzonderlijk te worden bewaard. Of een AI-interactie onderdeel is van het formele werkproces hangt af van de manier waarop AI binnen dat proces wordt gebruikt. Wanneer een AI-interactie onderdeel vormt van de totstandkoming van een product, advies, besluit of ander werkresultaat, gelden de bewaartermijnen en regels die voor dat proces van toepassing zijn. In andere gevallen kan de interactie onderdeel zijn van het persoonlijke werk- en denkproces van een medewerker.

Voor AI-interacties in bijvoorbeeld Copilot werken we nog uit welke bewaartermijnen en praktische afspraken passend zijn. Daarbij kijken we onder meer naar de aard van de interactie, de rol ervan in het werkproces en de bestaande afspraken voor bijvoorbeeld e-mail en chat. Het uitgangspunt is dat gegevens niet langer worden bewaard dan nodig is voor het doel waarvoor ze zijn vastgelegd en dat medewerkers zorgvuldig omgaan met AI-interacties die informatie bevatten die onderdeel is van het provinciale werk.

44726623 0016

3.6.4 Governance in de praktijk

Goede governance ontstaat niet alleen door registratie, controle en beleid. Juist het gesprek in de organisatie is belangrijk. Medewerkers moeten laagdrempelig vragen kunnen stellen, managers moeten ruimte maken om ervaringen te bespreken en signalen uit de praktijk moeten terugkomen bij de mensen die het beleid en de ondersteuning ontwikkelen.

Daarom gebruiken we vragen, ervaringen en incidenten uit de organisatie om het beleid, de ondersteuning en de kennis over AI verder te ontwikkelen. Zo blijft governance aansluiten bij de manier waarop AI zich in de praktijk ontwikkelt.

De governance rond AI is daarmee een doorlopend proces: we maken afspraken, ondersteunen medewerkers, houden zicht op het gebruik en leren van wat er in de praktijk gebeurt.

3.7 Transparantie en communicatie – intern

Transparantie werkt twee kanten op. De provincie is open over waar en hoe we AI inzetten, en van medewerkers verwachten we hetzelfde. Gebruik je AI bij je werk, dan maak je dat duidelijk wanneer dat relevant is. Maak je bijvoorbeeld met AI een afbeelding voor intern gebruik, vermeld dan bij het beeld dat AI daarbij is gebruikt.

Gebruik je AI in je werk, dan blijf je zelf verantwoordelijk voor de inhoud. AI helpt je bij je werk, maar neemt je vakkennis en professionele oordeel niet over. Controleer daarom de uitkomsten voordat je ze gebruikt, deelt of verwerkt. Let daarbij niet alleen op feitelijke fouten, maar ook op ontbrekende informatie, onjuiste aannames en een antwoord dat niet past bij de context.

Niet iedere AI-toepassing werkt op een manier die we volledig kunnen doorgronden. Hoeveel inzicht en controle nodig zijn, hangt daarom af van de toepassing en de risico's. Op basis van de risicoclassificatie bepalen we welke uitleg nodig is en waar extra menselijke controle nodig blijft.

Het CIO Office helpt medewerkers om AI verantwoord te gebruiken. Dat doen we onder meer met dit beleidskader, de handreiking, AI Kampvuurtjes, trainingen en e-learnings. Heb je een vraag of loop je ergens tegenaan? Voor vragen over het dagelijks gebruik van AI kun je terecht bij de Servicedesk Bedrijfsvoering. Voor vragen over de regels, risico's of verantwoorde inzet van AI kun je contact opnemen met het CIO Office via [redacted]

3.8 Transparantie en communicatie - extern

Waar de vorige paragraaf ging over transparantie richting onze eigen organisatie, gaat het hier om transparantie richting de buitenwereld: hoe gaan we om met AI in de communicatie- en beelduitingen die inwoners, partners en andere externe partijen van ons te zien krijgen? We maken een deel van ons beleid over AI-gebruik openbaar via onze website. Zo kunnen inwoners en andere belanghebbenden zien waar de provincie AI inzet en welke uitgangspunten daarbij gelden.

44726623 0016

Ook in onze communicatie en beeldvorming zijn we duidelijk over het gebruik van AI. Met generatieve AI kunnen inmiddels beelden ontstaan die nauwelijks van echte foto's te onderscheiden zijn. Dat kan een vertekend beeld geven van de werkelijkheid. Betrouwbaarheid is een belangrijke waarde in onze communicatie. Daarom gebruiken we AI niet om fotorealistische beelden te maken van situaties die niet bestaan. Gebruiken we wel een door AI gegenereerd beeld, dan vermelden we dat duidelijk.

Bestaande beelden mogen we met AI bewerken als het beeld de werkelijkheid blijft weergeven. De afdeling Communicatie kan bijvoorbeeld een tijdelijk object of een voorbijvliegende vogel uit een foto verwijderen. Een windmolen, gebouw of andere wezenlijke onderdeel van de situatie verwijderen kan niet. De Richtlijnen voor het gebruik van Generatieve AI geven hiervoor verdere uitgangspunten. Daarin staat onder meer dat AI-gebruik in beeld waarheidsgetrouw moet zijn, dat we hierover transparant zijn en dat we rekening houden met auteursrecht. Deze richtlijnen zijn ook opgenomen in het communicatiehandboek.

Bij infrastructuurprojecten gebruikt de provincie regelmatig geanimeerde impressies, bijvoorbeeld om te laten zien hoe een kruispunt er na een herinrichting uit kan zien. Zulke beelden helpen inwoners en partners om zich een voorstelling te maken van toekomstige plannen. Omdat een impressie soms nauwelijks van een bestaande situatie te onderscheiden is, vermelden we bij iedere afbeelding duidelijk dat het om een impressie of visualisatie van het ontwerp of de toekomstige situatie gaat.

3.9 Gelijkheid, non-discriminatie en bias

AI kan leiden tot uitsluiting, ongelijke behandeling of vertekening. Dat risico ontstaat bijvoorbeeld wanneer de gegevens waarop een toepassing is gebaseerd geen goede afspiegeling vormen van de werkelijkheid, wanneer historische keuzes bestaande ongelijkheid versterken of wanneer een toepassing bepaalde groepen structureel benadeelt.

Daarom besteden we bij het ontwerpen, inkopen en gebruiken van AI expliciet aandacht aan deze risico's. We brengen mogelijke vormen van vertekening in kaart en wegen deze mee bij de beslissing om een AI-toepassing te gebruiken, voort te zetten of uit te breiden.

Kunnen we risico's op discriminatie niet voldoende beperken, dan gebruiken we de AI-toepassing niet of zetten we deze stop. Daarnaast volgen we de verboden uit de Europese AI-verordening. Zo gebruiken we AI niet voor het beoordelen of classificeren van personen op basis van bijvoorbeeld persoonlijkheid, moraliteit of sociale positie wanneer dit onder de verboden toepassingen van de verordening valt.

3.10 Bewustwording en training

Verantwoord gebruik van AI begint met kennis en een goed begrip van de mogelijkheden en beperkingen ervan. Daarom investeert de provincie in opleiding en ondersteuning van medewerkers. Wanneer we nieuwe of uitgebreidere AI-functionaliteiten beschikbaar stellen, zorgen we ervoor dat medewerkers passende uitleg of training krijgen. Dat kan een interne training zijn of instructie van de leverancier.

44726623 0016

Voor alle medewerkers zijn via Gelderland Leert verschillende e-learnings over AI beschikbaar, onder meer over de basis, data, ethiek en het gebruik van AI. Deze e-learnings geven een algemeen beeld van wat AI is, wat de technologie voor het werk kan betekenen en welke risico's en verantwoordelijkheden daarbij horen.

Daarnaast organiseert het CIO Office maandelijks AI Kampvuurtjes. Dit zijn korte en toegankelijke sessies waarin medewerkers op een laagdrempelige manier kennismaken met AI en de gevolgen daarvan voor hun werk. We bespreken bijvoorbeeld de basis van AI, praktische toepassingen binnen de provincie, publieke waarden en ethiek en het omgaan met risico's. De bijeenkomsten zijn bedoeld voor alle medewerkers, ongeacht functie of digitale vaardigheid.

Voor het schrijven van AI-opdrachten ("prompts") bieden we een Copilot prompttraining aan. Medewerkers leren daarin hoe zij opdrachten helder, doelgericht en veilig formuleren. De training gebruikt onder meer de promptgids, waarin de verschillende onderdelen van een goede AI-opdracht worden uitgelegd.

Het CIO Office kan daarnaast een teamsessie op maat verzorgen. Daarbij kunnen we samen kijken naar de mogelijkheden en risico's van AI binnen het werk van het team. Waar dat helpt, maken we een domeinspecifieke gids met praktische AI-opdrachten, voorbeelden en vaste formuleringen. Zo kunnen teams AI op een herkenbare, veilige en effectieve manier gebruiken.

Voor teams die vooral met elkaar in gesprek willen over de bredere gevolgen van AI bieden we Moralis Machina aan: een interactief spel over AI en ethiek. Met gesprekskaarten bespreekt het team verschillende situaties en dilemma's. Zo ontstaat ruimte om samen te onderzoeken wat generatieve AI betekent voor het eigen werk en welke keuzes daarbij passen. Het CIO Office kan het spel op aanvraag begeleiden.

Met dit aanbod werken we aan brede en duurzame AI-geletterdheid. Medewerkers krijgen daarmee niet alleen kennis over hoe AI werkt, maar ook handvatten om de technologie kritisch en verantwoord toe te passen.

We sluiten waar mogelijk aan bij landelijke ontwikkelingen en beschikbare kennis. Zo werken overheidsacademies zoals RADIO aan een gezamenlijk leeraanbod voor AI-geletterdheid vanuit de Nederlandse Digitaliseringsstrategie. Waar dit aanbod aansluit bij de behoeften van onze medewerkers, benutten we het ook binnen provincie Gelderland.

44726623 0016

4 Borging en doorontwikkeling

Samen vormen deze hoofdstukken het kader waarbinnen provincie Gelderland AI op een zorgvuldige, doelgerichte en verantwoorde manier inzet.

Dit AI beleid is een levend document; we evalueren het ieder kwartaal. Tijdens deze evaluatie wordt beoordeeld of het beleid nog aansluit bij de praktijk en bij actuele ontwikkelingen.

Aanpassing van het beleid vindt plaats wanneer daar aanleiding toe is, bijvoorbeeld door:

- Ontwikkelingen in AI-technologie;
- Nieuwe of gewijzigde wet- en regelgeving;
- Landelijke normen en kaders vanuit de Nederlandse Digitaliseringsstrategie, zoals de aangekondigde overheidsbrede normen voor AI-gebruik en de bijbehorende inkoophandreiking;
- Uitkomsten van DPIA's, audits of incidenten;
- Bestuurlijke besluitvorming over opschaling, beperking of stopzetting van AI-toepassingen.

Op basis van deze evaluaties wordt het beleid waar nodig aangescherpt, aangevuld of verduidelijkt. Mochten er vragen, opmerkingen of bezwaren zijn over de inzet van AI binnen provincie Gelderland, mail dan naar 5.1.2i
Dit geldt ook voor het aandragen van ideeën voor pilots, het melden van zorgen of twijfelgevallen, of het verzoek om ondersteuning bij verantwoord gebruik van AI.

44726623 0016

Naslagwerk

Onderstaand overzicht bevat relevante handreikingen, naslagwerken en ondersteuningsmiddelen die medewerkers helpen bij de praktische toepassing van dit beleid.

- Handreiking voor gebruik van generatieve AI: https://prvgld.sharepoint.com/sites/Dig_samenwerken/Paginas/Handreiking-AI.aspx
- Promptgids: https://prvgld.sharepoint.com/sites/Dig_samenwerken/Paginas/Promptgids.aspx
- Kampvuurtjes: https://gelderlandleert.mijnlms.nl/execute/catalog20211?order=default&categories%5B%5D=11
- Prompttraining: https://gelderlandleert.mijnlms.nl/execute/catdetails?eventid=3284
- Wiki Data: https://prvgld.sharepoint.com/sites/datagovernance/Paginas/Wikidata.aspx
- Wie-doet-wat privacy: https://prvgld.sharepoint.com/sites/privay_en_avg/Paginas/wie-doet-wat.aspx
- Use case card: https://prvgld.sharepoint.com/:w:/s/SAM-CIOOffice/IQAmLLWJNXbdTZefeMIv_x9KAa7aWlnmG2Hry7j_lVzEqhE?e=GFuFwa
- Dit beleidskader is gebaseerd op vereisten uit de Europese AI-verordening en de ALTAI assessment en passend binnen de strategie van de Digital Decade
- AI-verordening: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32024R1689
- ALTAI Assessment: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment
- Digital Decade: https://digital-strategy.ec.europa.eu/en/policies/digital-decade-policy-programme
- Dit beleidskader sluit ook aan bij de Nederlandse Digitaliseringsstrategie (NDS), waarin Rijksoverheid, provincies, gemeenten en waterschappen gezamenlijk prioriteiten stellen voor onder meer verantwoorde AI-inzet. Nederlandse Digitaliseringsstrategie: De Nederlandse Digitaliseringsstrategie (NDS) - Digitale Overheid.

Voor vragen, opmerkingen of bezwaren, mail naar 5.1.2i of neem contact met ons op: 5.1.2e (5.1.2e @gelderland.nl) en 5.1.2e (5.1.2e @gelderland.nl).

Bij het opstellen van dit beleidsdocument is gebruikgemaakt van generatieve AI, onder meer om teksten te herschrijven, te verduidelijken en te structureren. De inhoud, keuzes en eindverantwoordelijkheid liggen bij het CIO Office.
Practice what you preach.

44726623 0016

Provincie Gelderland
Markt 11
6811 CG Arnhem
Postbus 9090
6800 GX Arnhem
026 359 99 99
5.1.2i @gelderland.nl
www.gelderland.nl

26 000 039