

AI Beleid van het Gegevenshuis

1. Inleiding

Kunstmatige intelligentie (AI) is tegenwoordig niet meer weg te denken uit onze samenleving. Ook binnen onze organisatie zien we veel mogelijkheden om AI te gebruiken. Tegelijkertijd is het belangrijk dat we goed nadenken over de risico's, maatschappelijke gevoeligheden en onze verantwoordelijkheden bij het gebruik van AI.

Kunstmatige intelligentie (AI) omvat systemen en algoritmen die zelfstandig kunnen leren, redeneren en beslissingen nemen. Dit varieert van generatieve AI die teksten, beelden of data-analyses kan creëren, tot voorspellende modellen en besluitvormingssystemen. Deze technologieën bieden organisaties kansen om hun dienstverlening te verbeteren, administratieve lasten te verlichten en interne processen efficiënter en slimmer in te richten. Tegelijkertijd brengen ze risico's met zich mee, bijvoorbeeld op het gebied van privacy, veiligheid, discriminatie en transparantie.

Binnen het Gegevenshuis zijn we nog bezig met het ontwikkelen van een duidelijke visie en beleid voor het gebruik van AI, dit kost tijd. Dit document helpt bij het opstellen verder door ontwikkelen van het AI-beleid en mogelijke AI-toepassingen. Ook draagt dit bij voor meer bewustzijn binnen de organisatie over het gebruik van AI.

Voor het opstellen van dit beleid is de “overheidsbrede handreiking voor de verantwoorde inzet van generatieve AI” van de VNG als bron gebruikt

2. Doel en Toepassingsgebied

Dit beleid is van toepassing op:

- Alle vormen van generatieve AI die binnen de organisatie worden ingezet;
- Zowel individuele als projectmatige toepassingen;
- Externe leveranciers of partners die generatieve AI namens of voor de organisatie inzetten.

3. Uitgangspunten voor Verantwoord Gebruik

3.1 Transparantie

- AI-gebruik wordt zichtbaar gemaakt richting deelnemers en collega's.
- AI mag nooit zelfstandig juridische of beleidsbesluiten nemen.

3.2 Menselijke Regie

- AI ondersteunt medewerkers, maar neemt het werk of de verantwoordelijkheid niet over.
- Medewerkers blijven verantwoordelijk voor inhoudelijke en feitelijke controle van AI-uitvoer.
- Bij gebruik van AI is bronvermelding verplicht waarbij de bron herleidbaar moet zijn.

3.3 Veiligheid en Privacy

- Er mag geen vertrouwelijke bedrijfsinformatie en persoonsgegevens worden ingevoerd in AI-tools.
- Bij gebruik van AI met persoonsgegevens is altijd vooraf een DPIA* en IAMA* vereist.

3.4 Inclusiviteit en Rechtvaardigheid

- AI-toepassingen worden gecontroleerd op vooringenomenheid (bias) en discriminatie.
- Resultaten van AI moeten uitlegbaar zijn.

4. Toegestaan en Niet-toegestaan Gebruik

Toegestaan:

- Hulp bij het schrijven of redigeren van teksten;
- Genereren van ideeën of samenvattingen;
- Ondersteunen bij data-analyse;
- Beantwoorden van veelgestelde vragen met vooraf getrainde modellen;
- Inzetten van AI-agents voor het automatiseren van routinetaken of communicatie;
- Robotisering van interne processen om de uitvoeringscapaciteit te vergroten en foutgevoeligheid te verminderen.

Niet toegestaan:

- Verwerking van vertrouwelijke gegevens via openbare AI-tools;
- AI inzetten voor besluitvorming met juridische of financiële gevolgen;
- Ongecontroleerde of niet-gedocumenteerde inzet.

5. Organisatie en Verantwoordelijkheden

Dagelijks bestuur is eindverantwoordelijk voor het ontwikkelen van het AI-beleid, naleven van de wet- en regelgeving omtrent AI, verantwoord gebruik van AI binnen de organisatie en een actueel algoritmeregister.

De directie is verantwoordelijk voor het uitdragen en naleven van het AI-beleid en veilig en verantwoord gebruik daarvan. Daarnaast stellen ze middelen beschikbaar om bewustzijn te creëren en het naleven van de afspraken te bevorderen.

De projectleider is verantwoordelijk voor het toepassen van het beleid, het inwinnen van advies, het toepassen van in dit beleid beschreven procedure en het aanleveren van de benodigde informatie.

De Functionaris Gegevensbescherming (FG) en Privacy Officer (PO) adviseren over privacy risico's bij het inzetten van de AI-systemen en bij het verwerken van de persoonsgegevens.

De CISO en de ICT-business analist:

- Beoordelen AI-toepassingen op informatiebeveiliging
- Houden een actueel register (CMDB) bij van alle processen waarbij AI wordt toegepast.
- Adviseren en toetsen bij nieuwe toepassing toepassingen of pilots op ethische aspecten, zoals transparantie, non-discriminatie en verantwoord gebruik van data

6. Procedure voor Inzet van (Generatieve) AI

1. Bepaal het doel en de maatschappelijke meerwaarde;
2. Voer risicoanalyse uit (DPIA* of IAMA*);
3. Leg afspraken vast met leveranciers (inclusief datagebruik);
4. Documenteer het gebruik in het algoritmeregister;
5. Informeer en train betrokken medewerkers.

* DPIA (Data Protection Impact Assessment)

Verplicht bij verwerking van persoonsgegevens met een hoog risico. De DPIA brengt in kaart welke gegevens worden verwerkt, met welk doel, welke risico's dit met zich meebrengt voor betrokkenen, en welke maatregelen worden genomen om deze risico's te beperken.

* IAMA (Impact Assessment Mensenrechten en Algoritmes)

Aanbevolen bij AI-toepassingen die invloed hebben op burgers of medewerkers. De IAMA beoordeelt de impact op fundamentele rechten zoals non-discriminatie, transparantie, autonomie en menselijke waardigheid. Dit instrument is met name relevant voor overheidsorganisaties of publieke instellingen.

7. Relevante Wet- en Regelgeving

AVG (Algemene Verordening Gegevensbescherming): vereist DPIA bij verwerking van persoonsgegevens.

AI-verordening (EU): stelt eisen aan transparantie, risicoanalyse en informatievoorziening bij gebruik van generatieve AI.

Grondwet: borgt privacy, gelijke behandeling en toegang tot informatie.

Wet open overheid (Woo): vereist herleidbaarheid en openheid van besluitvorming.

Auteurswet: houdt rekening met herkomst van AI-content en auteursrechten.

8. Meldplicht en Evaluatie

- Incidenten worden gemeld bij de CISO of FG.
 - Het AI-beleid wordt jaarlijks geëvalueerd en geactualiseerd op basis van technologische en juridische ontwikkelingen.
-

Bijlage(n):

- Gedragsregels AI
- Checklist AI-inzet

Bijlage 1 – Richtlijnen AI

Kunstmatige Intelligentie (AI) helpt om werkzaamheden efficiënter uit te voeren, zoals het zoeken van informatie, schrijven van rapporten en analyseren van data. Het ondersteunt ons in ons werk.

We onderzoeken op dit moment hoe we AI het beste kunnen toepassen bij het Gegevenshuis en hoe we voldoen aan de Europese AI-act. Deze wet bepaalt hoe AI veilig en verantwoord moet worden ingezet, bijvoorbeeld door transparantie- en verantwoordingsplichten.

Steeds meer collega's gebruiken AI in hun werk. Daarom hebben we een korte handleiding gemaakt met richtlijnen voor veilig en verantwoord AI-gebruik, vooral bij het genereren van teksten.

1. Basisprincipes voor AI-gebruik

- Gebruik AI als ondersteuning, niet als vervanging.
- Blijf kritisch en controleer: AI kan fouten maken.
- Bescherm privacy: Voer geen persoonsgegevens of vertrouwelijke bedrijfsinformatie in AI-tools.
- Neem verantwoordelijkheid: Jij blijft eindverantwoordelijk voor je werk.
- Let ook op je voorkeuren, schrijfstijl, vragen die je stelt, bestanden die je uploadt. Alles wordt opgeslagen.
- Wees transparant: Als je volledig door AI gegenereerde teksten extern gebruikt, vermeld dit dan.

2. Veiligheidsrichtlijnen en risico's AI biedt voordelen, maar brengt ook risico's met zich mee. Houd hierbij rekening met het volgende:

Onjuiste Informatie.

- AI kan fouten maken of verouderde informatie geven.
- + Controleer de output en combineer deze met jouw kennis en betrouwbare bronnen.

Privacy en gegevensbescherming

- Invoer van persoonsgegevens kan leiden tot een datalek
- + Deel geen gevoelige informatie en houd je aan de AVG

Vooroordelen (BIAS)

- AI kan discriminerende of bevooroordeelde antwoorden geven
- + analyseer resultaten kritisch en neem nooit blindelings beslissingen op basis van AI

Verlies van controle

- AI mag nooit een beslissing volledig overnemen
- + Gebruik AI als hulpmiddel, niet als vervanger van je professionele oordeel. Zorg dat beslissingen uitlegbaar blijven

Juridische en ethische risico's

- Onjuist gebruik kan leiden tot klachten, juridische of reputatieschade.
- + Check altijd of AI-uitkomsten voldoen aan wet- en regelgeving. Vraag bij twijfel vraag de IT Business consultant of de privacy officer om advies.

3. Tips voor effectief gebruik van AI

- Stel duidelijke vragen en geef duidelijke opdrachten (zgn. prompts) Een goede prompt ontstaat door duidelijke richtlijnen zoals je rol, de doelgroep, het doel en de

structuur mee te geven, en AI kan daarbij als sparringpartner helpen om de prompt verder te verfijnen.

- Controleer de uitkomsten. Let op actualiteit, betrouwbaarheid en eventuele vooroordelen.
- Wees je ervan bewust dat je niet weet waar de gegevens die je ingeeft worden bewaard.

Met deze richtlijnen zorgen we ervoor dat AI een waardevolle en veilige ondersteuning biedt in ons werk.

Bijlage 2: Checklist Verantwoorde Inzet Generatieve AI

Toepassen vóór ingebruikname van AI-tools:

- Doel en maatschappelijke meerwaarde vastgesteld
- Risicoanalyse uitgevoerd (DPIA en/of IAMA)
- Privacyaspecten beoordeeld
- Technische en organisatorische maatregelen genomen
- Afspraken met leverancier over datagebruik, retentie, training
- Transparantie voor burgers geregeld
- Uitlegbaarheid van AI-uitvoer gegarandeerd
- Interne verantwoordelijken benoemd
- Documentatie opgenomen in algoritmeregister
- Medewerkers geïnformeerd en getraind