Verboden AI praktijken

Overzicht | SharePoint

Ook te vinden op SharePoint Digitaal Samenwerken klik hier

Van	CAICO, CIO Office, provincie Gelderland
Datum	September 2026
Status	Versie 1.0
Kaders	**Verboden AI mag niet worden gebruikt - Algoritmekader**, het geldende AI beleid

AI biedt veel nuttige mogelijkheden, maar kan ook worden ingezet op manieren die schadelijk zijn voor mensen, de samenleving en onze organisatie. Zo kan AI nieuwe en krachtige mogelijkheden bieden voor manipulatie, uitbuiting en sociale controle, maar ook leiden tot het onbedoeld delen van organisatie-informatie met derden. Dergelijk gebruik kan risico's opleveren voor onder meer menselijke waardigheid, privacy, autonomie, vertrouwen en de publieke waarden waarvoor wij als overheid staan. Ook de Europese AI-verordening verbiedt bepaalde AI-toepassingen die in strijd worden geacht met de waarden van de Europese Unie, waaronder eerbied voor de menselijke waardigheid, vrijheid, gelijkheid, democratie en de rechtsstaat. Hieronder staat daarom een overzicht van AI-gebruik dat binnen onze organisatie niet is toegestaan. Het grootste deel hiervan vloeit rechtstreeks voort uit de verboden en verplichtingen van de AI-verordening,

- **Werkinhoud delen met publieke, niet-gecontracteerde AI-tools**
  Het invoeren of delen van werkinhoud in publieke, niet-gecontracteerde AI-tools zoals ChatGPT, Claude of Gemini is niet toegestaan. Dit geldt niet alleen voor vertrouwelijke informatie of persoonsgegevens, maar ook voor bijvoorbeeld niet-openbare documenten en concepten, interne communicatie, beleidsinhoud, adviezen en analyses. Ook informatie die op zichzelf misschien niet vertrouwelijk lijkt, maar waaruit kan worden afgeleid voor wie je werkt of waar een dossier of vraagstuk over gaat, mag niet worden gedeeld. De provincie heeft bij deze publieke tools onvoldoende duidelijkheid en garanties over waar onze gegevens worden verwerkt, hoe ze worden opgeslagen en of ze worden hergebruikt. Daardoor hebben we als organisatie onvoldoende grip op wat er met onze informatie gebeurt. Voor werkgerelateerd gebruik mogen daarom alleen AI-toepassingen worden gebruikt die door de provincie zijn goedgekeurd en waarvoor passende contractuele afspraken met de leverancier zijn gemaakt.

- **Gebruik van externe AI-transcriptietools voor werkgerelateerde gesprekken**
  Het gebruik van externe AI-transcriptietools, zoals Wispr en vergelijkbare toepassingen, voor werkgerelateerde gesprekken is niet toegestaan. Bij AI-transcriptie gaat het namelijk niet alleen om het gebruik van een AI-tool, maar ook om het opnemen en verwerken van gesprekken waarin uitspraken van collega's, inwoners, partners of andere deelnemers kunnen voorkomen. Naast privacy- en informatiebeveiligingsrisico's spelen daarom ook vragen over vertrouwen, verwachtingen en de manier waarop we als organisatie met elkaar en met gespreksinformatie willen omgaan. Het is niet voldoende om zelf te beoordelen dat een gesprek geen gevoelige informatie bevat: ook de andere deelnemers aan het gesprek worden door de transcriptie geraakt. Daarom moet vooraf duidelijk zijn wanneer transcriptie passend is, wanneer deelnemers hierover geïnformeerd moeten worden en onder welke voorwaarden transcriptie mag plaatsvinden. De organisatie werkt aan een veilige en organisatiebrede voorziening voor transcriptie binnen Teams, inclusief heldere gebruiksregels. In de tussentijd mogen medewerkers niet op eigen initiatief externe AI-transcriptietools gebruiken voor werkgerelateerde gesprekken.

- **Gebruik van DeepSeek als generatieve AI-dienst voor werkzaamheden van de organisatie**
  Voor overheidsorganisaties gelden strenge eisen voor het verantwoord gebruik van generatieve AI, waarbij onder meer privacy, informatiebeveiliging, gegevensdoorgifte en digitale soevereiniteit moeten worden geborgd. DeepSeek is een Chinese AI-dienst waarbij deze risico's nadrukkelijk spelen. Het Rijk heeft daarom het gebruik van dergelijke niet-goedgekeurde generatieve AI-diensten binnen de overheid

aan banden gelegd. Dit betekent dat medewerkers DeepSeek niet op eigen initiatief mogen gebruiken voor werkgerelateerde doeleinden, bijvoorbeeld voor het invoeren, analyseren, samenvatten of genereren van informatie

Verder mogen de volgende AI-toepassingen niet gebruikt worden:

- Een AI-systeem dat gebruik kan gaan maken van subliminale technieken om mensen onbewust of bewust kunnen manipuleren, waardoor ze beslissingen nemen die ze anders niet zouden hebben genomen
- Een AI-systeem dat gebruik kan gaan maken van kwetsbaarheden van individuen of specifieke groepen, zoals leeftijd, handicaps of sociale/economische omstandigheden, om het gedrag van die personen aanzienlijk te verstoren, wat kan leiden tot aanzienlijke schade bij henzelf of anderen
- Een AI-systeem dat gebruikt kan worden om natuurlijke personen of groepen gedurende een periode te evalueren of te classificeren op basis van hun sociale gedrag of afgeleide persoonlijke kenmerken
- Een AI-systeem dat gebruikt kan worden voor risicobeoordelingen van natuurlijke personen om het risico op crimineel gedrag te voorspellen, gebaseerd op profilering of persoonlijkheidskenmerken (dit geldt niet voor AI-systemen die worden gebruikt om menselijke beoordelingen te ondersteunen, gebaseerd op objectieve en verifieerbare feiten die rechtstreeks verband houden met criminele activiteiten)
- Een AI-systeem dat gebruikt kan worden om databanken voor gezichtsherkenning aan te leggen of aan te vullen door willekeurige gezichtsafbeeldingen van internet of CCTV-beelden te scrapen
- Een AI-systeem dat gebruikt kan worden om emoties van een persoon op de werkplek of in het onderwijs af te leiden (dit is niet van toepassing als het gebruik van het AI-systeem is bedoeld voor medische- of veiligheidsdoeleinden)
- Een AI-systeem dat gebruikt kan worden om natuurlijke personen individueel in categorieën in te delen op basis van biometrische gegevens om ras, politieke opvattingen, lidmaatschap van een vakbond, religieuze of levensbeschouwelijke overtuigingen, seksleven of seksuele geaardheid af te leiden (dit verbod geldt niet voor het labelen of filteren van rechtmatig verkregen biometrische datasets, zoals afbeeldingen, op basis van biometrische gegevens, of voor categorisering van biometrische gegevens op het gebied van rechtshandhaving)
- Een AI-systeem dat gebruikt kan worden als een biometrisch systeem in de publieke ruimte voor identificatie op afstand in real-time, met het oog op de rechtshandhaving


AI