

AI Beleid Belastingssamenwerking West-Brabant

Het Dagelijks Bestuur van de Gemeenschappelijke Regeling Belastingssamenwerking West-Brabant;

gelezen:

het voorstel met boven aangehaald onderwerp;

gezien:

de beraadslagingen op voornoemde datum;

besluit:

Het bijgevoegde 'AI Beleid Belastingssamenwerking West-Brabant' vast te stellen.

Bij Belastingssamenwerking West-Brabant (BWB) zien wij kunstmatige intelligentie (AI) als een waardevolle technologie om onze dienstverlening te verbeteren, processen te ondersteunen en innovatie binnen de organisatie te stimuleren. Tegelijkertijd beseffen we dat de inzet van AI raakt aan belangrijke publieke waarden, zoals privacy, gelijke behandeling, transparantie en menselijke controle. Juist omdat wij werken voor en met inwoners, vinden we het essentieel dat AI binnen BWB verantwoord wordt toegepast.

In deze beleidsnotitie beschrijven we hoe we dat doen. Het beleid geeft richting aan het gebruik van AI binnen onze organisatie en benoemt de voorwaarden waaraan toepassingen moeten voldoen. We sluiten aan bij geldende wet- en regelgeving, ethische uitgangspunten en maatschappelijke verwachtingen. AI is geen doel op zich, maar het moet concrete meerwaarde hebben en passen binnen onze publieke taak.

Het beleid geldt voor alle AI-toepassingen binnen BWB, nu en in de toekomst. Dat geldt zowel voor intern gebruik (zoals generatieve AI, besluit ondersteunende systemen en tools als ChatGPT of Copilot) als voor toepassingen richting inwoners (zoals chatbots of voorspellende modellen). Ook software-robots (RPA), zelflerende algoritmen en experimenten met nieuwe AI-toepassingen vallen onder dit kader. Zo maken we duidelijke afspraken over het gebruik van AI en houden we zicht op wat het oplevert en wat de risico's zijn.

BWB sluit aan bij de brede definitie van AI zoals opgenomen in de Europese AI-verordening: systemen die met algoritmes en leertechnieken voorspellingen, aanbevelingen of beslissingen genereren die normaal gesproken van mensen komen. In de praktijk vallen daar ook modellen onder die teksten genereren, signaleren, classificeren of ondersteunen bij besluitvorming. Dit beleid is dus breed toepasbaar en richt zich niet alleen op specifieke technologie, maar op het geheel van AI-gedreven systemen in onze organisatie.

Kaders voor verantwoorde inzet van AI

Bij de inzet van kunstmatige intelligentie gaat BWB uit van publieke waarden en wettelijke verplichtingen. Deze uitgangspunten helpen ons om AI zorgvuldig en maatschappelijk verantwoord toe te passen. Ze vormen het toetsingskader bij het ontwerp van toepassingen met AI, de inkoop van AI-systemen en het gebruik ervan in de organisatie. Voor elke toepassing wegen we af of deze past binnen deze uitgangspunten, en of aanvullende maatregelen nodig zijn. We hanteren daarbij de volgende uitgangspunten:

1. AI is ondersteunend, nooit leidend
AI mag geen beslissingen nemen die inwoners direct negatief raken, zoals het afwijzen van een bezwaar of een verzoek om kwijtschelding. De menselijke maat blijft leidend: een medewerker is altijd eindverantwoordelijk.
2. Transparantie en uitlegbaarheid
De werking van AI moet voor collega's én inwoners begrijpelijk zijn. Dat betekent inzicht in hoe beslissingen tot stand komen, welke data gebruikt zijn, hoe het systeem functioneert en hoe mens en systeem samenwerken.
3. Geen discriminatie of vooringenomenheid
We accepteren geen discriminatie of onbedoelde vooringenomenheid. We toetsen vooraf en regelmatig of een AI-toepassing mensen in gelijke situaties ongelijk zou kunnen behandelen, bij-

- voorbeeld op basis van afkomst, geslacht of leeftijd. Indien nodig nemen we aanvullende maatregelen om dit te voorkomen.
4. **Privacy en gegevensverwerking (AVG)**
AI respecteert privacy: wij verwerken alleen gegevens die noodzakelijk zijn voor het doel, en zorgen voor anonimisering of pseudonimisering, tenzij dat niet uitvoerbaar is. Indien volledige dataminimalisatie niet mogelijk is, hanteren wij het beginsel van proportionaliteit en evenredigheid: de verwerking moet in verhouding staan tot het doel en zorgvuldig worden begrensd. We verwerken alleen gegevens binnen de kaders van de AVG. Persoonsgegevens worden uitsluitend verwerkt met een geldige grondslag. De Functionaris Gegevensbescherming (FG) adviseert hierbij.
 5. **Informatiebeveiliging (BIO)**
AI-systemen moeten voldoen aan de normen uit de Baseline Informatiebeveiliging Overheid (BIO). Dat betekent: vooraf risico's analyseren, goed toegangsbeheer regelen, en toezicht houden via logging en monitoring. De CISO adviseert hierover.
We zetten AI alleen in als de baten opwegen tegen de risico's. Toepassingen zonder duidelijke meerwaarde of met disproportionele impact op privacy, veiligheid of uitvoerbaarheid worden niet ingezet. Daarnaast gebruiken we nooit AI-diensten die onze input of data gebruiken voor eigen training. Alleen in uitzonderlijke gevallen, met onze uitdrukkelijke schriftelijke toestemming, mag een model getraind worden op BWB-data.
 6. **Voorkeur voor Europese aanbieders**
Bij gelijke geschiktheid kiezen we voor Europese dienstverleners die uitsluitend gebruikmaken van in Europa gehoste diensten. Zo beperken we afhankelijkheid van grote commerciële platforms en vermijden we risico's van aanbieders uit landen met een offensief cyberprogramma. Alleen als een platform voldoet aan onze eisen voor privacy, veiligheid en transparantie, kan hiervan worden afgeweken.
 7. **Milieu-impact en duurzaamheid**
AI vergt veel energie. Daarom vragen we leveranciers om inzicht in het energieverbruik en geven we de voorkeur aan duurzame, efficiënt gehoste oplossingen. Medewerkers gebruiken AI bewust en alleen wanneer het echt functioneel iets oplevert, bijvoorbeeld tijdswinst of kwaliteitsverbetering.
 8. **Ethische toets bij maatschappelijke impact**
Toepassingen die vermoedelijk invloed hebben op inwoners of publieke waarden zoals gelijke behandeling, privacy, transparantie en menselijke controle worden vooraf ethisch getoetst. We kijken dan naar aspecten als rechtvaardigheid, autonomie, menselijke waardigheid en duurzaamheid. Alleen als deze toets positief is, gaan we verder met de toepassing.

Gebruik van AI in de organisatie – richtlijnen voor medewerkers

Medewerkers van BWB mogen AI gebruiken als hulpmiddel in hun werk, zolang zij zich houden aan een aantal duidelijke spelregels. AI kan bijvoorbeeld helpen bij het herschrijven van teksten, het samenvatten van openbare documenten of het genereren van ideeën. Tegelijkertijd zijn er risico's, zoals privacy, datalekken of misleidende output. Daarom gelden de volgende richtlijnen:

Wat mag en wat niet?

☑	Gebruik alleen AI-hulpmiddelen die zijn toegestaan en vermeld staan op het BSN-intranet. Gebruik geen andere AI-tools, ook niet via privéapparaten naast je werk-laptop. Zogenaemde 'schaduw-AI' is niet toegestaan.
⊘	Voer nooit persoonsgegevens of vertrouwelijke informatie in bij een AI-tool. Denk hierbij aan namen, BSN's, dossiernummers, e-mailadressen of interne documenten.
☑	Gebruik AI voor het herschrijven van teksten, brainstormen of samenvatten van openbare of niet-vertrouwelijke informatie.
☑	Gebruik AI als inspiratiebron. Jij blijft altijd verantwoordelijk voor de inhoud. Controleer dus kritisch de uitkomsten en pas deze zo nodig aan.
☑	Vraag, zeker bij juridische of beleidsmatige onderwerpen, naar de bronvermelding van het antwoord. AI genereert geen gegarandeerd juist antwoord, maar een inschatting op basis van patronen. Twijfel je aan de inhoud? Geef feedback in het systeem of raadpleeg een collega.
☑	Meld het als je AI hebt gebruikt bij het opstellen van een werkproduct. Bijvoorbeeld in een e-mail aan collega's of in een begeleidende notitie.
⚠	Let op auteursrechten. AI kan teksten genereren op basis van bronnen waarop auteursrecht rust. Voorkom dat je teksten één-op-één overneemt en controleer altijd of hergebruik verantwoord is.

☑	Laat AI-teksten voor inwoners altijd op taalniveau B1 opstellen. Zo zorgen we ervoor dat onze communicatie begrijpelijk blijft voor iedereen.
↘	Gebruik AI bewust. AI-systemen, zeker voor het maken van afbeeldingen, verbruiken veel energie. Gebruik deze functies alleen als er een functionele reden is, zoals tijdswinst of duidelijkere communicatie.
?	Bij twijfel: overleg. Weet je niet zeker of iets mag of verstandig is? Bespreek het met je leidinggevende, de Functionaris Gegevensbescherming of de CISO.

Ondersteuning

Wij ondersteunen medewerkers bij het verantwoord gebruik van AI. In het Teams-kanaal Artificial Intelligence (AI) kun je vragen stellen, ervaringen delen en tips uitwisselen. Indien nodig organiseren we verdiepende sessies of bieden we aanvullende ondersteuning.

Inkoop en gebruik van AI door externe partijen

AI wordt niet alleen binnen de organisatie toegepast. Ook externe partijen zoals softwareleveranciers, ingehuurd specialisten of controlemedewerkers kunnen AI inzetten bij het uitvoeren van werkzaamheden voor BWB, bijvoorbeeld voor data-analyse, tekstverwerking of advisering.

Om te voorkomen dat ons beleid wordt omzeild via uitbesteding, gelden ook voor deze externe partijen duidelijke spelregels. Hun inzet van AI moet altijd passen binnen de kaders van dit beleid.

Daarom stellen wij de volgende eisen:

- ✓ **Meldplicht vooraf:** de externe partij geeft vooraf aan of en hoe AI zal worden ingezet;
- ✓ **Inzicht in de toepassing:** er wordt uitgelegd welk AI-systeem wordt gebruikt, op welke gegevens het werkt en wat het doel is van de inzet;
- ✓ **Schriftelijke verklaring:** de partij verklaart schriftelijk dat geen persoonsgegevens of organisatiegegevens van BWB worden gebruikt voor training van AI-modellen, en dat deze beperking technisch is afgedicht;
- ✓ **Aantoonbare naleving van dit beleid:** de toepassing voldoet aantoonbaar aan de uitgangspunten op het gebied van privacy, uitlegbaarheid, veiligheid en duurzaamheid zoals vastgelegd in dit AI-beleid.

Deze voorwaarden zorgen ervoor dat uitbesteding niet leidt tot verlies van controle of tot risico's die wij intern niet zouden accepteren. Het ligt dan ook voor de hand om deze afspraken op te nemen in de overeenkomst met de betreffende partij.

Organisatie, toetsing en doorontwikkeling

Om AI op een verantwoorde manier te kunnen inzetten, is niet alleen beleid nodig, maar ook structuur en continu toezicht. Binnen BWB is daarom geregeld hoe nieuwe toepassingen worden getoetst, hoe we ruimte bieden voor gecontroleerde experimenten en op welke manier het beleid wordt geëvalueerd en waar nodig aangepast.

Werkgroep AI

Binnen BWB wordt een werkgroep AI ingericht. Deze bestaat uit een vertegenwoordiger van het MT, de Functionaris Gegevensbescherming (FG), de Chief Information Security Officer (CISO), de informatiemanager en de innovatieadviseur. De werkgroep is het centrale coördinatiepunt voor AI binnen de organisatie en ziet toe op de toepassing van dit beleid in de praktijk.

Nieuwe toepassingen

Nieuwe AI-toepassingen worden altijd vooraf gemeld bij de FG of de CISO. Dit geldt voor zowel interne voorstellen van medewerkers als voor toepassingen die door leveranciers worden ingebracht. De werkgroep AI beoordeelt deze toepassingen vooraf op risico's en randvoorwaarden. Daarbij wordt onder andere gekeken naar:

- de werking en uitlegbaarheid van de toepassing;
- het gebruik van gegevens;
- beveiligingsmaatregelen;
- ethische aspecten;
- de omgeving waarin AI wordt toegepast (bij voorkeur afgeschermd of gecontroleerd);
- en de risicocategorie volgens de Europese AI-verordening (AI Act): onaanvaardbaar, hoog, beperkt of minimaal risico.
- Alle goedgekeurde AI-toepassingen worden opgenomen in het interne algoritmeregister van BWB.

Ruimte voor experiment

We erkennen het belang van leren en experimenteren. AI-toepassingen kunnen pas goed worden beoordeeld als ze in de praktijk zijn uitgetest. Daarom maken we ruimte voor gecontroleerde pilots, waarbij AI op beperkte schaal wordt getest – bijvoorbeeld binnen een afgebakende werkomgeving, met fictieve gegevens of binnen een geselecteerd team.

Voor deze experimenten gelden dezelfde uitgangspunten als voor structurele inzet. Ze worden vooraf afgestemd met de werkgroep AI en moeten voldoende zicht geven op werking, gegevensgebruik, beveiliging en mogelijke maatschappelijke gevolgen. Op deze manier bouwen we gecontroleerd ervaring op, zonder onaanvaardbare risico's.

Jaarlijkse evaluatie

De technologische ontwikkelingen rond AI gaan snel. Daarom evalueert de werkgroep AI dit beleid minimaal één keer per jaar. Signalen uit de organisatie, maatschappelijke trends, nieuwe wetgeving of opgedane ervaringen kunnen aanleiding zijn om het beleid aan te passen. De werkgroep neemt hierin het initiatief en betreft waar nodig het MT en andere relevante onderdelen van de organisatie.

Aldus vastgesteld op 24 oktober 2025

Het Dagelijks Bestuur van de Gemeenschappelijke Regeling Belastingen West-Brabant

de secretaris,

M.S.A. van Leeuwen

Plaatsvervangend directeur

de voorzitter,

drs. K. van den Berg

Toelichting op het AI-beleid

Onderstaande toelichting licht een aantal van de eerder genoemde uitgangspunten verder toe. Hiermee maken we inzichtelijk waarom deze kaders belangrijk zijn voor BWB en hoe ze zich vertalen naar de praktijk.

Geen discriminatie of vooringenomenheid

AI-systemen nemen zelf geen standpunten in, maar worden getraind met data die afkomstig is van mensen en bronnen waarin (onbewuste) vooroordelen kunnen voorkomen. Daardoor bestaat het risico dat AI in gelijke situaties toch ongelijk behandelt bijvoorbeeld op basis van afkomst, geslacht of leeftijd. BWB accepteert dit niet. We toetsen daarom vooraf en regelmatig of AI-toepassingen risico's op ongelijke behandeling met zich meebrengen. Als zulke risico's zich voordoen, nemen we maatregelen, bijvoorbeeld door aanvullende monitoring, het aanpassen van dataselectie of het uitsluiten van bepaalde variabelen.

Informatiebeveiliging

Bij AI is het niet altijd duidelijk waar data wordt verwerkt en opgeslagen, zeker bij systemen van externe leveranciers. Daarom is informatiebeveiliging bij AI extra belangrijk. BWB stelt als eis dat risico's vooraf worden geanalyseerd, dat toegang goed is geregeld (inclusief rollen en rechten), en dat het gebruik van AI-systemen wordt gemonitord via logging. De CISO adviseert over deze maatregelen. Zo voorkomen we dat gevoelige informatie onbedoeld toegankelijk of uitlegbaar wordt.

Voorkeur voor Europese dienstverleners

AI-systemen draaien vaak op servers in het buitenland. Hierdoor hebben we weinig tot geen controle over wat er met data gebeurt zeker bij aanbieders uit landen met andere wetgeving of minder waarborgen. Zo bepaalt Amerikaanse wetgeving dat gegevens op Amerikaanse servers, of van Amerikaanse leveranciers, beschikbaar kunnen worden gesteld aan de Amerikaanse overheid, ook als de data in Europa is opgeslagen. Sommige aanbieders, zoals Microsoft Azure of OpenAI, bieden weliswaar contractueel aan om data binnen de EU te houden en niet voor training te gebruiken, maar vallen alsnog onder Amerikaanse wetgeving. Daarom geldt bij BWB het uitgangspunt dat we géén gevoelige of herleidbare informatie verwerken via zulke platforms, tenzij er aanvullende juridische en technische maatregelen zijn getroffen.

Bij voorkeur kiezen we voor Europese dienstverleners die uitsluitend gebruik maken van in Europa gehoste diensten. Zo blijven we binnen de Europese wet- en regelgeving en borgen we datasoevereiniteit, autonomie en transparantie. Aanbieders uit landen met een offensief cyberprogramma, zoals

Rusland, China of Iran, worden uitgesloten. Daarmee beschermen we onze organisatie tegen digitale inmenging, spionage en misbruik van publieke infrastructuur en bewaken we de belangen van onze inwoners.

Milieu-impact en duurzaamheid

AI verbruikt veel energie, vooral bij het trainen van grote modellen. Zo wordt geschat dat de training van een model als ChatGPT circa 500 ton CO₂ uitstoot en 700.000 liter water verbruikt. Zelfs een kort gesprek met AI of het genereren van een afbeelding kost relatief veel energie. Omdat leveranciers hier vaak geen transparante informatie over geven, vragen wij nadrukkelijk om inzicht in de milieu-impact van AI-toepassingen. We geven de voorkeur aan energiezuinige systemen en duurzaam gehoste oplossingen. Medewerkers gebruiken AI bewust en alleen wanneer het functioneel meerwaarde heeft.

Bronnen, referenties en wetgeving.

Voor deze beleidsnotitie zijn vele bronnen geraadpleegd, waaronder beleidsstukken van andere overheden, diverse publicaties en wetgeving. Ook is gebruik gemaakt van kunstmatige intelligentie ter inspiratie en bij het redigeren van de notitie. Met name de volgende bronnen zijn hierbij van belang geweest:

- AVG (Verordening (EU) 2016/679)
- AI Act (Verordening (EU) 2024/1689)
- Wet open overheid
- BIO 2022
- Overheidsbrede visie generatieve AI 2024
- Handreiking generatieve AI 2025 (VNG/Rijk)
- Richtlijnen Autoriteit Persoonsgegevens en IBD
- [Dit zijn de onzichtbare kosten van AI - Kennisnet](#)
- Gebruikte AI-tools: ChatGPT Enterprise (model 4.0) en Perplexity.ai