Gemeente & OCMW Kortenberg
Policy inzake artificiële intelligentie (AI)

Inhoudstopgave

Art. 1 – Doelstellingen en omvang van het AI-beleid

Art. 1.1 – Definitie van AI

Binnen onze organisatie wordt kunstmatige of Artificiële Intelligentie (verder: AI) gedefinieerd als het gebruik van geavanceerde algoritmen, technologieën en software/tools om taken uit te voeren die normaal gesproken menselijke intelligentie vereisen.

AI-systemen/technologie/tools/software/oplossingen kunnen data analyseren, beslissingen nemen of aanbevelingen doen met een zekere mate van autonomie, waardoor ze processen kunnen optimaliseren en waardevolle inzichten kunnen bieden.

Het personeelslid neemt er kennis van dat dit beleid geen statisch gegeven is, maar onderhevig is aan wettelijke veranderingen en wijzigende voorwaarden.

Het personeelslid wordt op de hoogte gebracht van deze wijzigingen via de gangbare communicatiekanalen in het bestuur. De laatste geactualiseerde versie wordt steeds via 'Infomail' verstuurd. Deze is voor gemeente/OCMWpersoneel beschikbaar via intranet en voor het onderwijspersoneel via de schooldirecteur en/of op Smartschool.

Ingeval een bepaling van dit beleid of een gedeelte daarvan nietig zou bevonden worden, worden de overige bepalingen van het beleid daardoor niet automatisch nietig. Deze blijven hun geldigheid behouden.

Art. 1.2 – Doelstellingen van het AI-beleid

Artificiële intelligentie stelt mensen in staat efficiënter en effectiever te werken. Elke toepassing van AI binnen onze organisatie moet in functie staan van de opdrachten van het lokaal bestuur en de dienstverlening naar onze doelgroepen.

Dit beleid spitst zich toe op generatieve AI gezien dit momenteel de meest gebruikte AI-toepassingen zijn binnen de lokale besturen. Generatieve AI is een vorm van AI die gebruik maakt van deep learning (complexe patronen in grote hoeveelheden data leren kennen) en is gericht op de creatie van nieuwe content zoals bv. teksten, audio, afbeeldingen, etc.

Het AI-beleid van onze organisatie is ontwikkeld om de volgende doelstellingen te bereiken:

- De efficiëntie van onze bedrijfsprocessen verhogen
- Innovatie binnen onze producten en diensten stimuleren
- De kwaliteit van onze dienstverlening aan 'klanten' verbeteren
- Datagestuurde besluitvorming ondersteunen
- Kostenbesparingen realiseren door automatisering van routinetaken
- Klantervaringen personaliseren en verbeteren
- Fraudedetectie en risicobeheer versterken
- Voorspellende analyses uitvoeren voor betere planning en voorraadbeheer
- Energieverbruik verminderen en duurzaamheidsdoelen te ondersteunen
- Productkwaliteit verbeteren door anomaliedetectie
- Menselijke fouten minimaliseren in kritieke processen
- Snellere en nauwkeurigere financiële rapportages genereren
- De efficiëntie van wervings- en selectieprocessen verhogen
- Markttrends en consumentengedrag beter voorspellen en analyseren
- Onderhoudswerkzaamheden optimaliseren door predictief onderhoud
- Naleving van regelgeving verbeteren door automatische monitoring en rapportage

- Interne kennisdeling en samenwerking bevorderen door AI-gestuurde kennismanagementsystemen

Art. 1.3 – Toepassingsgebied

Het AI-beleid is van toepassing op alle afdelingen en processen binnen onze organisatie (inclusief de gemeentelijke basisscholen) waar AI-technologieën kunnen worden ingezet om de doelstellingen, zoals hierboven beschreven, te ondersteunen.

Dit beleid geldt voor alle medewerkers en afdelingen en diensten die betrokken zijn bij de ontwikkeling, implementatie, het beheer en het gebruik van AI-systemen binnen de organisatie.

Externe partners en leveranciers die AI-oplossingen leveren aan de organisatie worden ook geacht te voldoen aan de richtlijnen van dit beleid.

Deze policy is ook van toepassing op derden, zelfstandigen, vrijwilligers, stagiairs en tijdelijke werkkrachten wanneer zij gebruikmaken van AI in hun werkzaamheden ten aanzien van de organisatie.

Art. 2 – Regelgeving

VERORDENING (EU) 2024/1689 VAN HET EUROPEES PARLEMENT EN DE RAAD van 13 juni 2024 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144, en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (**Verordening Artificiële Intelligentie**).

VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (**Algemene Verordening Gegevensbescherming**).

Art. 3 – Verantwoordelijkheid en toerekenbaarheid

Onze organisatie erkent dat het gebruik van AI-technologieën verantwoordelijkheden met zich meebrengt. De organisatie streeft ernaar dat de vele mogelijkheden van AI kunnen worden benut en tegelijkertijd de schade ten gevolge van onbetrouwbaarheid en privacyschending kan worden voorkomen. Daarom zijn de volgende maatregelen van kracht:

- **Toerekenbaarheid:** indien een AI-systeem een fout maakt of leidt tot ongewenste uitkomsten, wordt de verantwoordelijke partij geacht snel en doeltreffend te handelen om de situatie te corrigeren.

  Er worden mechanismen ingevoerd om de bron van fouten te identificeren en ervoor te zorgen dat vergelijkbare problemen in de toekomst worden voorkomen.

- **Menselijke tussenkomst:** waar nodig, moet er altijd een mogelijkheid zijn voor menselijke tussenkomst om beslissingen van AI-systemen te herzien of te corrigeren.

  AI-systemen mogen geen onbeperkte autonomie hebben in het nemen van beslissingen die een significante impact hebben.

Art. 4 – Richtlijnen

Art. 4.1 – Standaard richtlijnen

Hieronder bieden we richtlijnen voor de evaluatie, goedkeuring, en het gebruik van AI-tools binnen de organisatie.

Het spreekt voor zich dat AI-tools die worden gebruikt door medewerkers voldoen aan de eisen met betrekking tot eerlijkheid en transparantie, verantwoordelijkheid en toerekenbaarheid, privacy- en gegevensbescherming, en non-discriminatie.

- Wees steeds kritisch: begrijp dat AI-systemen gebaseerd zijn op patronen en gegevens. Vertrouw de resultaten niet blindelings.
- Bescherm (persoons)gegevens: deel nooit gevoelige (persoons)gegevens met AI-tools.
- Zorg voor menselijke supervisie: laat een mens de resultaten valideren voordat je beslissingen neemt op basis van AI. Beschouw de output van (generatieve) AI als een half-afgewerkt product waar je nog je eigen vakkennis en beroepservaring dient aan toe te voegen.
- Let op voor mogelijke vooroordelen: controleer of AI-resultaten eerlijk en onbevooroodeeld zijn.
- Wees transparant: geef bij gegenereerde teksten of beelden aan dat generatieve AI werd gebruikt. Breng ook je leidinggevende op de hoogte als je generatieve AI gebruikte. Indien je een beeld volledig overneemt van AI dat moet dit vermeld worden.
- Houd rekening met de milieu-impact: generatieve AI verbruikt veel energie, gebruik het enkel als het een meerwaarde oplevert.
- Blijf leren: houd je kennis over AI up-to-date door opleidingen te volgen en met je collega's te praten over je goede en slechte ervaringen.
- Houd professioneel en persoonlijk gebruik van generatieve AI strikt gescheiden: om generatieve AI te gebruiken dient je je te registreren met een e-mailadres. Respecteer een strikte scheiding tussen je professioneel en privé-gebruik. Als je een werk e-mailadres gebruikt om je te registreren, mag het wachtwoord dat je daarbij opgeeft niet hetzelfde zijn als een wachtwoord dat je al gebruikt om in te loggen op systemen van de organisatie.
- Gebruik veilige systemen: gebruik alleen veilige en betrouwbare systemen. Vraag zo nodig raad aan de ICT-dienst of de DPO.

In onderstaande lijst[1] kan er teruggevonden worden welke AI-toepassingen al dan niet gebruikt mogen worden in onze organisatie en in welke mate er ook aandachtspunten zijn bij het gebruik.

Naam toepassing	Aandachtspunten	Toegelaten	Verboden
Copilot desktop Windows 11 (gratis)	Indexeert alle gegevens die je uploadt en verwerkt deze voor commerciële marketingdoeleinden	• Openbare documenten zonder persoonsgegevens	• Vertrouwelijke documenten • Documenten met persoonsgegevens • Beveiligingsinformatie
Bing chat (gratis)	Indexeert alle gegevens die je uploadt en verwerkt deze voor commerciële marketingdoeleinden	• Openbare documenten zonder persoonsgegevens	• Vertrouwelijke documenten • Documenten met persoonsgegevens • Beveiligingsinformatie
Chat GPT (gratis)	Indexeert alle gegevens die je	• Openbare documenten zonder persoonsgegevens	• Vertrouwelijke documenten • Documenten met

[1] Opgelet: via ICT en intranet kan je steeds de meest recente lijst raadplegen.

	uploadt en verwerkt deze voor commerciële marketingdoeleinden		persoonsgegevens • Beveiligingsinformatie
Gemini (gratis)	Indexeert alle gegevens die je uploadt en verwerkt deze voor commerciële marketingdoeleinden	• Openbare documenten zonder persoonsgegevens	• Vertrouwelijke documenten • Documenten met persoonsgegevens • Beveiligingsinformatie
Deepseek (gratis)	Verboden	• Verboden	• Verboden
Microsoft Copilot (betalend)	Niet ondersteund door de organisatie	• Verboden	• Verboden

Wanneer je als medewerker een AI-systeem wenst te gebruiken dat niet werd opgenomen in de lijst met toegelaten AI-systemen, moet dit met de ICT en de DPO besproken worden en moet hiervoor uitdrukkelijke toestemming worden verkregen. Volg hiertoe de richtlijnen voor de aankoop van software. De organisatie kan het AI-systeem vervolgens toevoegen aan de lijst met toegelaten AI-systemen, dan wel vermelden op de lijst met uitgesloten systemen.

Het bestuur behoudt zich het recht voor om op elk ogenblik de toegang tot bepaalde systemen te verbieden.

Art. 4.2 – Beveiligingsrichtlijnen

Alle medewerkers moeten volgende richtlijnen volgen bij het gebruik van AI-tools:

- **Bescherming van vertrouwelijke gegevens**: het uploaden of delen van vertrouwelijke, eigendomsrechtelijke of door regelgeving beschermde gegevens is zonder goedkeuring niet toegestaan. Dit geldt voor gegevens van burgers, medewerkers en partners. Wanneer je per ongeluk gevoelige gegevens invoert in een AI-systeem, spreken we van een gegevenslek. Hiervoor dient de DPO te worden ingelicht via gdpr@kortenberg.be zodat we de schade kunnen beperken en afhankelijk van de impact voor de betrokkenen aangifte doen bij de autoriteiten.
- **Data privacy:** medewerkers moeten voorzichtig zijn met het delen van alle (ook niet-vertrouwelijke) informatie en zichzelf afvragen of ze comfortabel zouden zijn met het openbaar maken van deze gegevens. Bij twijfel mag geen data worden geüpload of gedeeld in AI-tools.
- **Toegangscontrole:** medewerkers mogen geen toegang tot AI-tools buiten de organisatie verstrekken zonder voorafgaande goedkeuring. Dit omvat het delen van inloggegevens of andere gevoelige informatie met derden.
- **Naleving van beveiligingsbeleid**: medewerkers dienen dezelfde beveiligingsrichtlijnen toe te passen als voor andere gegevens bekomen binnen de functie, zoals het gebruik van sterke wachtwoorden, het up-to-date houden van software, en naleving van het beleid voor gegevensopslag en -verwijdering.

Art. 4.3 – Voorbeelden van gepast gebruik

Kan ik generatieve AI gebruiken om e-mails of mededelingen op te stellen?

Ja, afhankelijk van de context kan je generatieve AI gebruiken ter ondersteuning van het opstellen van e-mails of mededelingen die geen persoonlijke of gevoelige informatie bevatten. Je kan vragen om een eerste aanzet voor die e-mail of mededeling te genereren, in een bepaalde stijl (formeel, professioneel, gemoedelijk, …) door op te lijsten welke punten zeker behandeld moeten worden en je kan die aanzet dan zelf verder personaliseren. De inhoud die je ingeeft, waarop de generatieve AI zich zal baseren om die e-mail of mededeling te genereren, mag geen persoonlijke, bedrijfsgevoelige of andere beschermde informatie bevatten.

Kan ik generatieve AI gebruiken om inhoud te schrijven voor publieke communicatie?
Ja, je kan inhoud (tekst en beelden) voor persmededelingen, webposts en sociale media aanmaken met generatieve AI. Wees wel voorzichtig, je bent er altijd verantwoordelijk voor dat deze inhoud accuraat, duidelijk, onpartijdig en onbevooroordeeld is. Je moet er ook voor zorgen dat de resultaten betrouwbaar zijn, gezien het potentiële bereik en de impact van publieke communicatie. Verzeker je er van dat je de nodige toestemmingen hebt voor het reproduceren, aanpassen of publiceren van materiaal van derden en dat de inhoud niet in strijd is met de wetten op intellectueel eigendom. Je moet het publiek ook informeren over elk significant gebruik van generatieve AI bij de productie van inhoud. Je kan eventueel aan de inhoud toevoegen "Een deel van deze inhoud is opgesteld met behulp van …. Alle feiten, cijfers en verklaringen zijn door de schrijver gecontroleerd op juistheid."

Kan ik generatieve AI gebruiken om mezelf te informeren over een bepaald onderwerp?
Ja, generatieve AI kan worden ingezet als onderzoeksinstrument om achtergrondinformatie te verzamelen over een onderwerp dat betrekking heeft op jouw beleidsterrein en waarmee je niet vertrouwd bent. Let echter wel op dat de vragen die je stelt niets onthullen over een nog niet publiek bekende bedoeling van de overheid, of wijzen op een bepaald overheidsbelang. Voordat je deze gegenereerde informatie gebruikt, moet je alle feiten die de generatieve AI vermeldt, verifiëren met andere betrouwbare bronnen waarnaar kan worden verwezen of die kunnen worden geciteerd.

Art. 5 – Training en opleiding

Training vormt de kern van ons AI-beleid. Alle medewerkers volgen een verplichte AI-basistraining, terwijl gespecialiseerde opleidingen beschikbaar worden gesteld voor diegenen die direct met AI werken.

We streven naar doorlopende ontwikkeling op het gebied van AI, waarbij resultaten worden geëvalueerd en succesvolle afronding van trainingen wordt erkend middels certificering.

Art. 6 – Privacy en gegevensbescherming

Privacy en gegevensbescherming zijn fundamenteel voor het vertrouwen in AI-technologieën.

Onze organisatie verplicht zich tot de volgende maatregelen:

- Alle AI-systemen binnen de organisatie moeten voldoen aan de geldende wet- en regelgeving met betrekking tot privacy en gegevensbescherming, zoals de Algemene Verordening Gegevensbescherming (GDPR) en de EU AI act.
- Alleen de minimale hoeveelheid persoonsgegevens die noodzakelijk is voor het doel van de AI-toepassing mag worden verzameld en verwerkt.
- Waar mogelijk worden persoonsgegevens geanonimiseerd of gepseudonimiseerd om de privacy van individuen te beschermen. We implementeren maatregelen om te voorkomen dat geanonimiseerde gegevens kunnen worden teruggeleid naar specifieke individuen.
- Gegevens die worden gebruikt voor AI-toepassingen moeten worden beschermd door robuuste beveiligingsmaatregelen, zoals encryptie en toegangscontrole, om ongeautoriseerde toegang, verlies of manipulatie te voorkomen.

Wat moet je doen als je denkt dat er een privacyrisico is bij het gebruik van AI?
Neem onmiddellijk contact op de de DPO via gdpr@kortenberg.be. Identificeer de bron van het risico, waar nodig via ondersteuning van de ICT-dienst, en zorg ervoor dat het systeem tijdelijk niet wordt gebruikt totdat het risico is beoordeeld.

Wat gebeurt er als ik per ongeluk gevoelige gegevens in een AI-systeem invoerde?
Dit is in principe een gegevenslek volgens de privacywetgeving. Hiervoor dient de DPO via gdpr@kortenberg.be te worden ingelicht zodat we de schade kunnen beperken en afhankelijk van de impact voor de betrokkene(n) aangifte doen bij de autoriteiten.

Kan ik generatieve AI gebruiken om niet-beslist beleid te formuleren?
Nee, je kan generatieve AI wel gebruiken om te helpen bij onderzoek tijdens de beleidsontwikkeling, maar je kan ze niet gebruiken om (nieuw) beleid te formuleren, te verduidelijken of te interpreteren. De inhoud die je hiertoe dient in te geven kan immers bedoelingen/ideeën/intenties onthullen die nog niet publiekelijk bekend zijn.

Art. 7 – Samenwerking met externe partijen

Bij samenwerking met externe partijen voor AI-projecten selecteert onze organisatie partners op basis van hun technische expertise, ethische en duurzame praktijken, en hun vermogen om onze strategische doelen te ondersteunen.

De selectie omvat een zorgvuldige evaluatie van hun ervaring, eerdere use cases, technische bekwaamheid, sector-specifieke kennis en de aangeboden technologie en diensten.

Art. 8 – Menselijke controle en toezicht

Medewerkers moeten zich bewust zijn van de beperkingen van AI en altijd hun eigen oordeel gebruiken bij het interpreteren en opvolgen van aanbevelingen/antwoorden/content die door AI zijn gegenereerd. AI-systemen zijn bedoeld om de besluitvorming van mensen te ondersteunen, niet om deze te vervangen.

Art. 9 – Sancties

Overtredingen van deze AI-policy kunnen leiden tot disciplinaire maatregelen zoals beschreven in het arbeidsreglement. De sanctie zal afhangen van de ernst van overtreding. Gelet op het belang van een correcte toepassing van deze richtlijnen, begrijpen de medewerkers dat elk gebruik van Artificiële Intelligentie waarbij deze richtlijnen ernstig geschonden worden, een zware fout kan uitmaken die aanleiding kan geven tot een ontslag om dringende reden.

Daarnaast kunnen de tuchtsancties worden opgelegd zoals voorzien in het arbeidsreglement.

Art. 10 – Contactgegevens

Voor alle vragen rond AI kan het personeelslid terecht bij de ICT-dienst (ICT@kortenberg.be) of de DPO (gdpr@kortenberg.be).

Elektronisch ondertekend op 6/11/2025 door Leen Ceuppens, algemeen directeur

Elektronisch ondertekend op 6/11/2025 door Alexander Rillaerts, voorzitter raad voor maatschappelijk welzijn