VERA
VLAAMS-BRABANT

HET IS MOGELIJK IN MERCHTEM

AI - Richtlijnen voor het lokaal bestuur Merchtem

1. Inleiding

Artificiële intelligentie (AI) helpt medewerkers sneller en efficiënter werken. Het bestuur wil deze technologie verstandig, veilig en transparant inzetten.
Dit document geeft duidelijke richtlijnen voor het gebruik van AI-toepassingen binnen het lokaal bestuur, met aandacht voor privacy, kwaliteit, auteursrecht en de Europese AI Act.

De richtlijnen richten zich in het bijzonder op **generatieve AI** (zoals Copilot), omdat dit vandaag de meest gebruikte vormen zijn binnen lokale besturen.

We willen dat je generatieve AI op een veilige manier kunt gebruiken zonder risico op schade door onbetrouwbaarheid of privacy-schendingen. Daarom bieden we je deze richtlijnen aan.

2. Definities

2.1 Kunstmatige intelligentie (AI)

Overkoepelende term voor technologie die complexe taken uitvoert die normaal menselijke intelligentie vragen.

2.2 Algoritmen

Reeksen instructies die gegevens verwerken of automatische beslissingen ondersteunen. Ze vormen de basis van alle software, inclusief AI-systemen.

2.3 Machine Learning (ML)

Een vorm van AI waarbij systemen leren uit gegevens, patronen herkennen en beslissingen nemen zonder menselijke tussenkomst.

2.4 Deep Learning

Een techniek binnen ML die neurale netwerken gebruikt om complexe patronen te herkennen in grote hoeveelheden data.

2.5 Generatieve AI

AI die nieuwe inhoud creëert: tekst, audio, beelden, video, code, enz.

2.6 Large Language Models (LLM's)

Generatieve AI-modellen die tekst begrijpen en genereren, zoals Microsoft Copilot en ChatGPT.

2.7 Andere AI-vormen die geen LLM zijn

- Beeldherkenning (bv. beveiligingscamera's)
- Zelfrijdende systemen (bv. sensorgestuurde voertuigen)
- **…**

3. Richtlijnen

De Europese Artificial Intelligence Act (AI ACT) bepaalt de regels voor de inzet van AI in de EU. Als je AI wil toelaten in je organisatie, dan is de regel dat je een AI-training moet voorzien voor je medewerkers.

De gemeente Merchtem kiest er voor om heel voorzichtig om te springen met AI gestuurde systemen. Generatieve AI is toegelaten mits het strikt naleven van de richtlijnen.

Voor de medewerkers van de gemeente Merchtem werd gekozen om enkel Microsoft Copilot toe te laten en dan nog enkel binnen de eigen tenant "merchtem.be".

Voor de AI-act valt een chatbot onder beperkt risico.

De GDPR is wel van toepassing zodra persoonsgegevens worden verwerkt.
Dit betekent o.a.:

- Geen persoonsgegevens invoeren in AI-systemen.
- Mogelijke datalekken melden aan de DPO.

Als je Microsoft Copilot wil gebruiken, dan moet je verplicht een opleiding volgen.

4. Basisprincipes bij het gebruik van Copilot

4.1 Slechte input = slechte output

Denk goed na over de input die je aan de chatbot geeft. Een chat met een eerste input die al veel informatie bevat, is beter dan in één chat input na input te geven. Bij meerdere inputs na mekaar heb je meer kans op 'hallucineren'.

4.2 Wees kritisch

AI bouwt op patronen en heeft geen broncontrole.
Het systeem kan verkeerde informatie geven of onnauwkeurige of verzonnen feiten genereren.

Dubbelcheck en controleer de gegenereerde output vooraleer je die gebruikt.

4.3 Bescherm persoonsgegevens

- Zet geen privacygevoelige gegevens of bedrijfskritische informatie in Copilot.
- Ook geen documenten met privacygevoelige informatie uploaden.

4.4 Let op voor vooroordelen

AI werkt met gemiddelden. Dit kan leiden tot discriminatie (bv. meer mannelijke CV's geeft voorkeur aan mannen).

4.5 Zorg voor menselijke supervisie

Voeg zelf nog waarde toe: door de gegenereerde inhoud te verbeteren en te verfijnen bewijs je dat de inhoud van jou komt. Laat Copilot niet autonoom beslissen.

Beslissingen blijven **altijd** de verantwoordelijkheid van de medewerker.

4.6 Gebruik veilige systemen

Gebruik enkel deze tool: Copilot binnen de 'merchtem.be' tenant.
Het gebruik van ChatGPT en andere chatbots is verboden binnen het lokaal bestuur.

4.7 Transparantie

Vermeld bij AI-gegenereerde tekst of beelden dat AI werd gebruikt.

4.8 Milieu-impact

Generatieve AI verbruikt veel energie.
Gebruik het enkel wanneer het effectief een meerwaarde biedt.

4.9 Blijf leren

De technologie verandert snel. Het bestuur voorziet opleidingen en updates.

4.10 Copilot is een hulpmiddel

Copilot kan een ondersteuning zijn maar jijzelf blijft de PILOOT en draagt de verantwoordelijkheid.

5. AI-toepassingen binnen het lokaal bestuur

5.1 Microsoft Copilot (versie binnen licentiemodel MS Office 365)

- Je moet aangemeld zijn met je persoonlijk account.
- Werkt binnen de eigen Microsoft-tenant.

- Informatie blijft binnen de tenant.
- Informatie wordt geëncrypteerd opgeslagen.

Toegelaten:

- Samenvattingen, herwerkingen van teksten via een bijlage, tekst rechtstreeks in de prompt, via een URL,...
- Opstellen en verbeteren van briefwisseling
- Zoekopdrachten
- ...

Verboden:

- Privacygevoelige gegevens

5.2 Andere chatbots zoals ChatGPT, Deepseek of de gratis versie van Copilot

- Verboden

5.3 overzicht toepassingen

Naam toepassing	Aandachtspunten	Toegelaten	Verboden
Microsoft Copilot (betalend)	Indexeert alle gegevens waar je toegang toe hebt binnen de organisatie	• Samenvattingen • Zoekopdrachten • Herstructuren • Brieven schrijven • ...	• Besluitvoering • Gevoelige persoonsgegevens Artikel 9 en 10 GDPR
Microsoft Copilot (gratis)	Indexeert alle gegevens en verwerkt deze voor commerciële marketingdoeleinden	• Verboden	• Verboden
Chat GPT (gratis of betalend)	Indexeert alle gegevens en verwerkt deze voor commerciële marketingdoeleinden	• Verboden	• Verboden
Gemini (gratis)	Indexeert alle gegevens en verwerkt deze voor commerciële marketingdoeleinden	• Verboden	• Verboden
Deepseek (gratis)	Verboden	• Verboden	• Verboden

6. Veelgestelde vragen

Hoe weet ik of ik persoonsgegevens invoer?
Als iemand direct of indirect identificeerbaar is (naam, adres, telefoon, dossiernummer, gedrag, stemgeluid ...).

Wat moet ik doen bij een mogelijk privacy-risico?
Stop onmiddellijk met de verwerking en meld het aan de dienst ICT of je DPO.

Mag AI gebruikt worden voor geautomatiseerde besluitvorming?
Nee, er moet altijd menselijke controle zijn.

Wat als ik per ongeluk gevoelige gegevens invoer in een AI-tool?
Dan is dit mogelijk een datalek.
De DPO moet geïnformeerd worden.

Wordt het AI-gebruik gelogd?
Bij de Copilot-versie die wij gebruiken zijn er logbestanden voorzien.

7. Contact en ondersteuning

Bij vragen over:

- AI-gebruik
- privacyrisico's
- DPIA-verplichtingen
- juridische beperkingen
- nieuwe AI-initiatieven

Neem contact op met de **Data Protection Officer (DPO)** of de **ICT-dienst**.

Bronnen: VERA