1. Onze opmerkingen en aandachtspunten

1.1 Intellectuele eigendom en auteursrechten

Input-risico: als je documenten uploadt in de Custom GPT, moet je over de rechten beschikken om dat materiaal te gebruiken voor AI-verwerking. Het uploaden van auteursrechtelijk materiaal van derden zonder licentie kan worden gezien als een inbreuk op de intellectuele eigendom.

Output: momenteel geldt in de Europese Unie dat AI-genereerde content in principe niet auteursrechtelijk beschermd is omdat menselijke creativiteit ontbreekt. Dit betekent dat je de output vaak niet juridisch zal kunnen beschermen tegen kopieën door concurrenten. Hierbij stippen wij graag al even aan dat eindredactie van de draft van de AI ervoor zou kunnen zorgen dat je toch genoeg creativiteit kunt aantonen om de output auteursrechtelijk beschermd te zien. Verder in dit advies halen we nog een reden aan om zeker voor voldoende eindredactie te voorzien (zie AI Act).

Inbreuken: Als je Custom GPT teksten genereert die te veel lijken op een bestaand werk, ben jij als eindverantwoordelijke/gebruiker in principe aansprakelijk voor die inbreuk.

1.2 Privacy en GDPR

Het gebruik van persoonsgegevens in je Custom GPT komt niet zonder gevolgen. Er zijn een aantal punten die je daarbij in het achterhoofd moet houden en waar nodig moet je actie ondernemen.

Gebruik geen bijzondere (gevoelige) persoonsgegevens of bedrijfsgeheimen als input bij de Custom GPT (of eender welke AI je zou gebruiken).

Voor de verwerking van (gewone) persoonsgegevens, bijvoorbeeld klantenreviews, heb je een rechtsgrond nodig, wat voor contentcreatie vaak toestemming zal moeten zijn. Zorg er dus voor dat vooraleer je persoonsgegevens via AI verwerkt, je daar de nodige toestemming voor hebt van de betrokkene.

Daarnaast zal het gebruik van persoonsgegevens in de Custom GPT vaak een nieuwe verwerking zijn, je moet deze dan ook correct opnemen in je privacy policy en dataregister.

Indien het gebruik van de persoonsgegevens in het AI-systeem een impact heeft op de privacy van je werknemers of klanten, kan het ook zijn dat je een DPIA moet uitvoeren. Een DPIA of Data Protection Impact Assessment moet je vooraf uitvoeren om de risico's in kaart te brengen zodat je organisatorische of technische maatregelen kan nemen die de risico's mitigeren. Dit is verplicht indien de verwerking waarschijnlijk een hoog privacyrisico oplevert. Dit is alleszins het geval wanneer je werkt met strafrechtelijke gegevens of op grote schaal gevoelige persoonsgegevens verwerkt.

1.3 AI Act

Het trainen en inzetten van een Custom GPT voor contentcreatie valt onder de Europese AI Act. Hoewel contentcreatie in principe niet als "hoog risico" wordt beschouwd, gelden er wel belangrijke regels, met name op het gebied van transparantie en auteursrecht.

Eén van de kernpunten is transparantie. Je bent in principe verplicht om duidelijk te maken dat content door AI is gegenereerd. Dit geldt zeker als je content publiceert die bedoeld is om het publiek te informeren over zaken van openbaar belang (zoals nieuws of opiniestukken).
Hierbij komen we graag terug op de eindredactie. Indien je de output van de Custom GPT beschouwd als een draft die je daarna verder afwerkt en aanpast, moet je er in principe niet bij vermelden dat de tekst werd gegenereerd door AI. Dit ligt anders indien het gaat om deepfakes. Als je de GPT gebruikt om beeld of geluid te maken dat echt lijkt (bijvoorbeeld een AI-stem van een werknemer) en dus een deepfake creëert, moet je dit expliciet vermelden.

Als gebruiker van OpenAI ben jij de *deployer*. Dit betekent dat jij verantwoordelijk bent voor hoe de AI in de praktijk wordt ingezet, de input die je geeft en de output die je publiceert.

Op het vlak van auteursrechten, stelt de AI Act strenge eisen voor het gebruik van auteursrechtelijk beschermd materiaal. Zoals eerder vermeld moet je er dus voor zorgen dat je enkel input geeft waarvoor jij ook effectief de rechten hebt.

Als laatste aandachtspunt vermelden we AI-geletterdheid. Het is verplicht onder de AI Act om als bedrijf te zorgen voor een bepaald niveau van AI-geletterdheid bij je medewerkers. Zorg er dus voor dat de persoon die werkt met de Custom GPT begrijpt hoe de tool werkt, wat de beperkingen zijn (bv. hallucinaties) en hoe ze de output kunnen controleren. Stel ook een interne AI policy op waarbij richtlijnen, informatie en afspraken omtrent AI-gebruik worden vastgelegd.

1.4 Menselijk toezicht

Indien je de Custom GPT koppelt aan de Facebook API moet je ervoor zorgen dat menselijke controle behouden blijft. Dit is noodzakelijk om na te gaan of de AI output niet ingaat tegen wettelijke bepalingen of schadelijke content bevat. De persoon die de menselijke controle uitoefent, moet de content daadwerkelijk begrijpen én controleren. Ook hier is de eindredactie weer van belang. Zoals in de handleiding al wordt aangestipt, is menselijke controle én goedkeuring hier heel belangrijk.

1.5 Enkele to do's:

- Voeg waar nodig een disclaimer toe aan je content: "gegenereerd met behulp van AI".
- Controleer telkens of je alle rechten hebt op de input voor de Custom GPT.
- Stel een intern AI-beleid op voor werknemers en leidt hen op omtrent AI-gebruik.
- Gebruik zeker een Enterprise versie van ChatGPT om ervoor te zorgen dat de data niet gebruikt wordt om het basismodel van OpenAI te trainen.