FØYEN

Hvordan bruke generativ KI og samtidig sikre personvern og redusere juridisk risiko

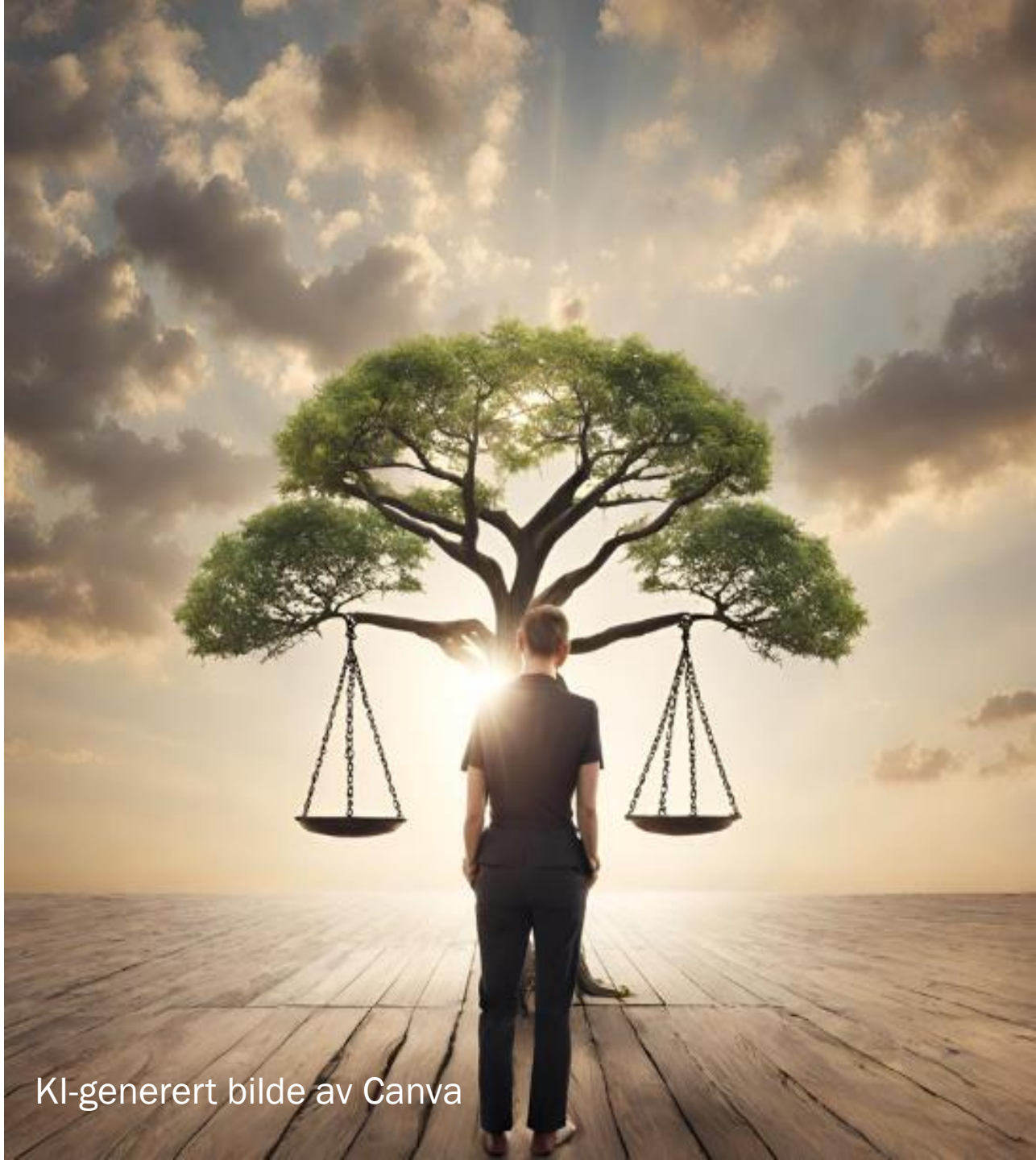
Camilla Gjersem,
Advokatfullmektig

FØYEN

Hvordan navigere i det juridiske landskapet ved bruken av kunstig intelligens

1. Eksisterende generelle og teknologinøytrale lover og regler som treffer bruken av algoritmer på store mengder data, blant annet
    - Diskrimineringslovgivning
    - Opphavsrett
    - Erstatningsrett og kontraktsrett
    - Ansvarlighet, mm.
    - Personvernlovgivningen
    - Lovfestet taushetsplikt, forretningshemmeligheter
    - Etiske problemstillinger

2. Kommende regelverk, AI Act, og internasjonale retningslinjer



KI-generert bilde av Canva

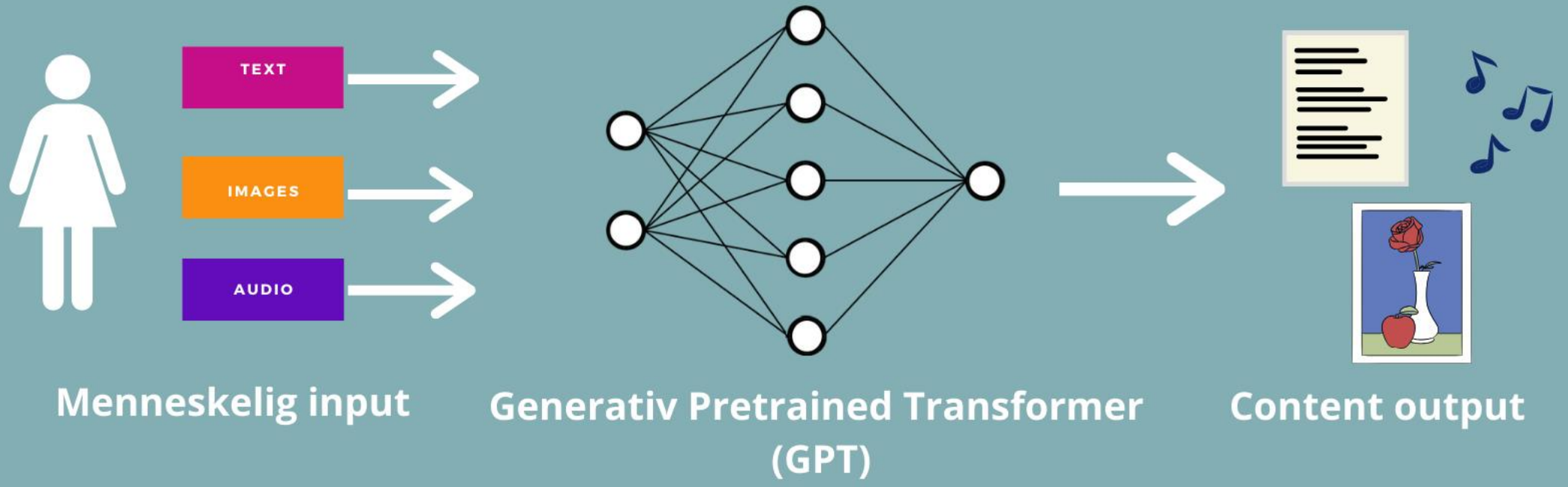
FØYEN

Personvernrettslige problemstillinger:

- Kan personopplysninger brukes til å trene opp KI-modeller? Hvilket lovgrunnlag?
- **Har brukerne kontroll over egne personopplysninger? Kan KI-leverandøren bruke dine personopplysninger til å forbedre KI-modellen?**
- Hvordan sikre at beslutninger knyttet til KI-generert innhold ikke fører til urettferdige, uetiske og diskriminerende resultater?

Bilde generert av Canva Design ved hjelp av KI

Kan KI-leverandøren bruke personopplysninger til å forbedre språkmodellen?



FØYEN

Kan LLM-modellen bruke dataene dine (samtaleloggene) til å trene/utvikle modellen?

LLM-modell	Vilkår (T&C)	Kan dine data brukes til å trene modellen?	Mulighet til å opt-out	Beskyttet delvis
ChatGPT (OpenAI)	Terms of use, Content "Our use of content", "Opt out"	Ja	Ja, mulighet til å optout	ja
ChatGPT Business (OpenAI)	Business terms 3 Content, 3.2 "Our obligation for Customer Content"	Nei		
(OpenAI plugin)	Plugins and Actions Terms, 2. "Plugins b and c" / Enterprise privacy at OpenAI	OpenAI kan ikke det, men er mulig å opt-in, men kommer an på tredjepartsvilkår	Kommer an på	
Gemini AI / Google AI studio	Gemini API Additional Terms of Service, Content License and Data Use	Ja	Nei	Nei
Google -Gemini for Enterprise	Service Specific Terms AI/ML services 17. "training restriction"	Nei		
Microsoft Azure	Microsoft terms of use	Nei		
xAI	Terms of use "6. xAI's Rights"	Ja	Ikke tillatt for europeiske brukere	

Oppsummering: store variasjoner, men bedriftens data er gjerne beskyttet ved Enterprise-versjoner
(sist oppdatert 04.mars 2024)

FØYEN

Viktigheten av å etablere interne retningslinjer

- Privatbruker vs. virksomhetsbruker
- Bruker KI-leverandøren dine data til å trene modellen? Opt-out muligheter?
- Etabler interne retningslinjer som et organisatorisk tiltak
- Er KI-modellen en chatbot eller en integrert KI-assistent?

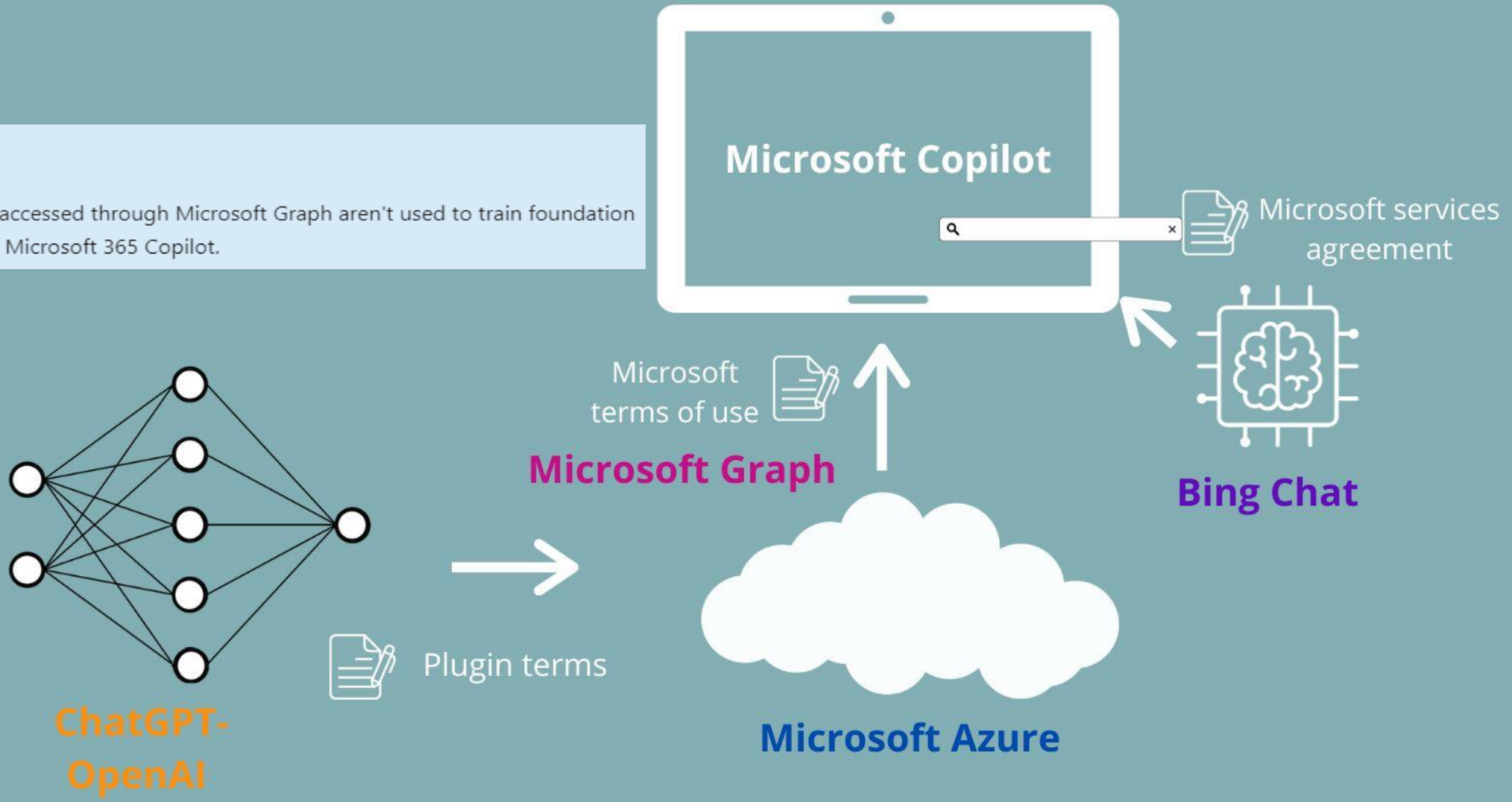
To help with quality and improve our products, human reviewers may read, annotate, and process your API input and output. Google takes steps to protect your privacy as part of this process. This includes disconnecting this data from your Google Account and API key before reviewers see or annotate it. **Do not submit sensitive, confidential, or personal information to the Services.**

(Gemini API Additional Terms of Service, Content License and Data Use)

Eksempel: innebygd KI-assistenten - Microsoft Copilot

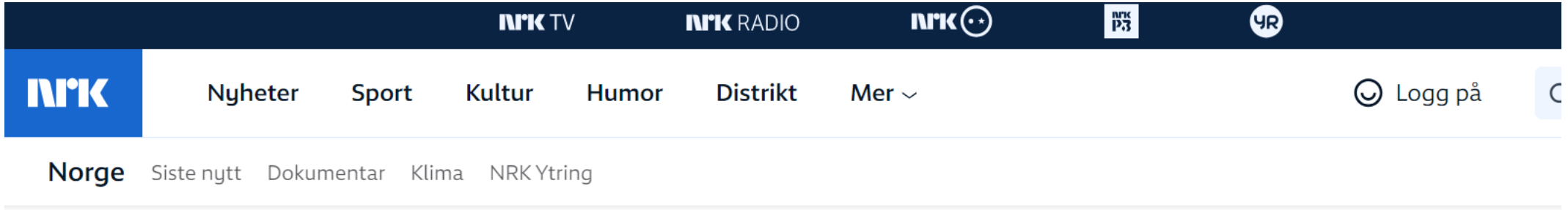
Important

Prompts, responses, and data accessed through Microsoft Graph aren't used to train foundation LLMs, including those used by Microsoft 365 Copilot.



FØYEN

NAV-saken og betydningen av tilgangskontroller



Datatilsynet gir 20 millioner i bot til Nav

Datatilsynet har funnet 12 lovbrudd knyttet til personvern hos Nav, og mener de bevisst har brutt loven. Nå kommer kravene om oppvask fra Stortinget.

FØYEN

Praktiske tips

- Vurder kontraktsvilkårene. Hvilke garantier om beskyttelse gir KI-leverandøren?
- Foreta personvernkonsekvensvurderinger (DPIA)
- Etabler tekniske og organisatoriske tiltak basert på den konkrete risikoen (interne retningslinjer knyttet til bruken og tilgangskontroller)

FØYEN

Takk for meg

Camilla Gjersem
Advokatfullmektig

Kontaktinfo:

camilla.gjersem@foyen.no

Tlf: + 47 46 61 00 28

Legg meg til på LinkedIn via denne QR-koden:

LinkedIn: https://www.linkedin.com/in/camilla-gjersem/