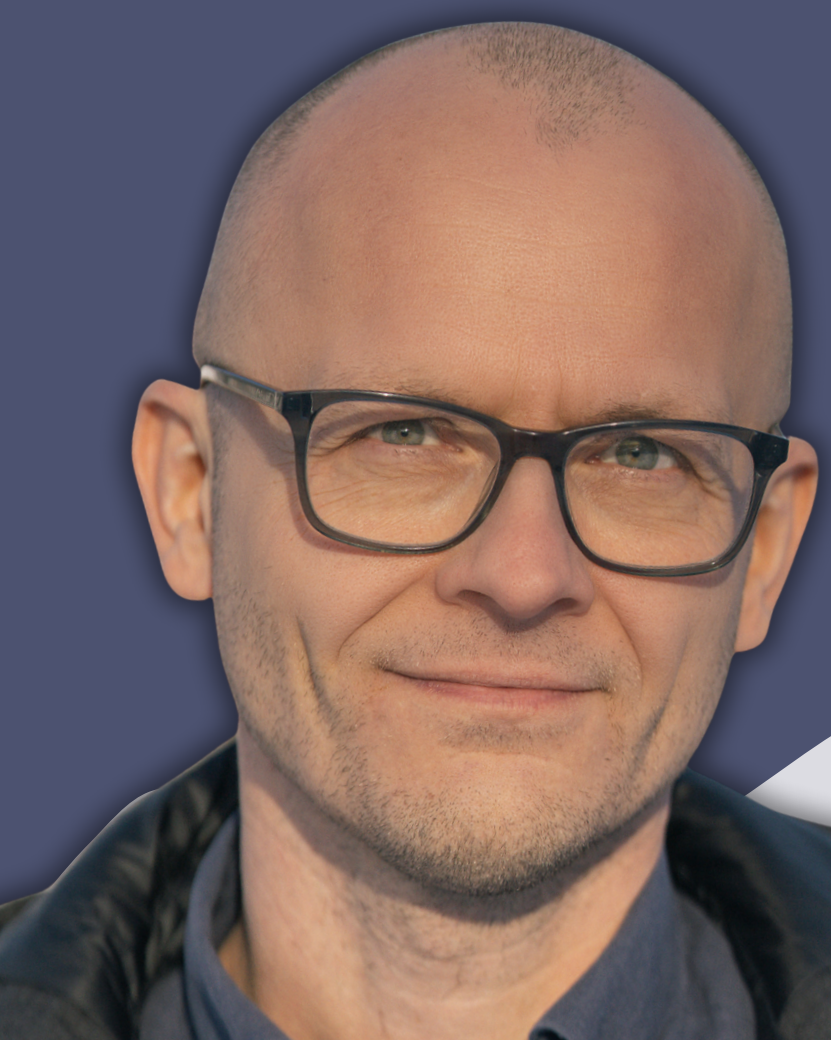
Solfi

Hva er egentlig...

AI Act?

Rundt 25% av virksomheter i Norge rapporterer å benytte seg av kunstig intelligens. Hva blir konsekvensene når den nye EU forordningen om AI trer i kraft i 2026?



John Arthur Berg
Teknolog og rådgiver

Kort forklart, det er en

Produkt-sikkerhetslov

AI Act er relevant for varer og tjenester der kunstig intelligens benyttes.

Loven forbyr **skadelig/farlig** AI. Det stilles strenge krav til risikostyring, kvalitets-kontroll og dokumentasjon for **risikofylt** bruk.

Det skal være tydelig at AI benyttes når det kan ha betydning for sluttbruker.

Loven regulerer ikke harmløs bruk av AI.

Erstatter dette GDPR?

Nei.

GDPR vil i høyeste grad være relevant når man benytter persondata i AI-tjenester. Etterlevelse av GDPR **må** allerede i dag være på plass når virksomheter implementer kunstig intelligens.

AI Act er bygget på samme lest som GDPR og harmoniserer med prinsippene for behandling av persondata.

Arg! Skjønner ikke EU viktigheten av AI, er ikke dette bare en snubletråd for Europeisk innovasjon?

EU er smertelig klar over at andre stormakter ligger foran i AI-kappløpet. Men det ville blitt håpløst om hvert enkelt medlemsland skulle lage sitt eget lovverk.

Her får man en felles regulering i Europa, og kanskje nok markedsmakt bak loven til å påvirke store teknologileverandører.

EU forsøker å insentivere til **mer** utvikling av AI i Europa, men uten at det går på bekostning av individets friheter.

Solfi

Risikobasert kategorisering

Graden av regulering bestemmes av risiko for brukere a produktet.

Risiko	Regulering
Uakseptabel	Forbudt
Høy	Strengt regulert
Begrenset	Krav til åpenhet om bruk av AI
Ubetydelig	Uregulert

Risiko for hva?

Risiko for liv og helse, eller at EU-borgeres grunnleggende rettigheter krenkes.

Det høres kanskje komplisert ut, men det er hva de fleste av oss har i ryggmargen. Ytringsfrihet, personvern, likhet for loven, likestilling, eiendomsrett, rett til utdanning osv.

I ryggmargen vår ja, men ligger det i AI algoritmen?

Eksempel på kategorisering

Risiko	Eksempel (ikke fullstrendig)
Uakseptabel	Manipulerende AI, “social scoring”, skadevare. Gjenkjenning av følelser på arbeidsplass eller skole. Biometrisk kategorisering av sensitive karaktertrekk.
Høy	Sikkerhetskomponenter, kritisk infrastruktur, opptak til / karaktersetting i utdanning, sosiale ytelser, lån- og kredittvurderinger, ansettelsesforhold.
Begrenset	Chatbots i kundeservice, tekstroboter.
Ubetydelig	NPC i spill, spam-filtre.

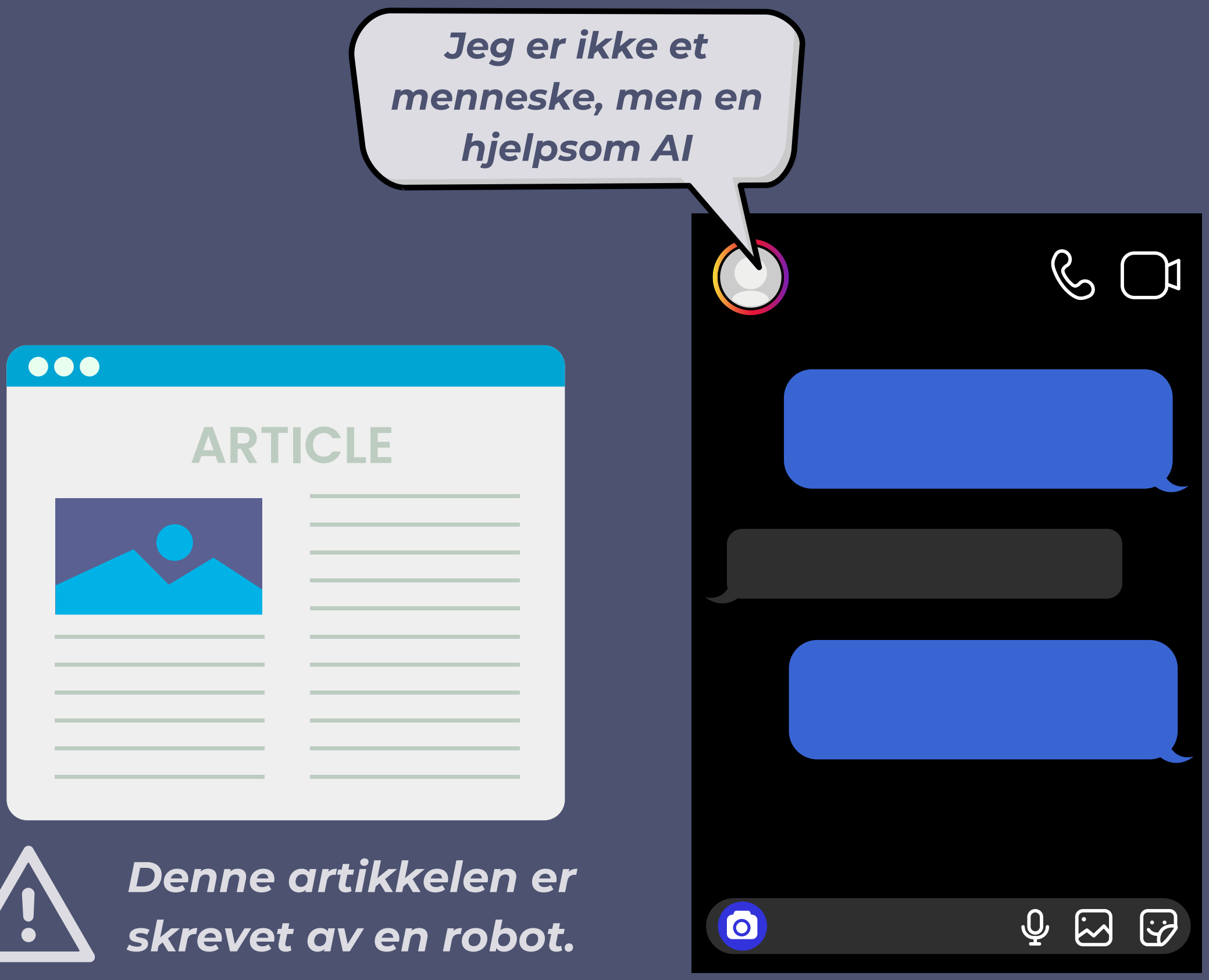
Krav ved høy risiko

- Risikostyringssystem og risiko-mitigering
- Høy kvalitet i datasett som benyttes for å trene AI
- Logging og sporbarhet
- Menneskelig overvåkning
- Detaljert dokumentasjon som kan benyttes til å vurdere etterlevelse
- Omfattende informasjon til sluttbrukere
- Samsvarsvurdering*

* Mange produkter er i dag allerede omfattet av krav til samsvarsvurdering i egen lovgivning. Der det ikke eksisterer slike krav må det gjennomføres en egen samsvarsvurdering.

Krav ved begrenset risiko

Hvis ikke allerede åpenbart, så kreves det åpenhet om at brukere samhandler med en AI og ikke et menneske.



Denne artikkelen er skrevet av en robot.

Hva med Chat-GPT og generativ AI?

Eksplosjonen i generativ AI har vært en hodepine for EU-kommisjonen og har komplisert forhandlingene om ny lov.

Det er enighet om at “General AI systems” må følge åpenhetsprinsippene i reguleringen og må vedlikeholde teknisk dokumentasjon om modellen. De må også forklare hvordan de følger EU sitt lovverk om opphavsrett.

For “General AI” som har stor innvirkning, så etableres det i realiteten en ny risikokategori, “**Systemrisiko**”. Se neste side!

“Systemrisiko”

Hvilke modeller faller i kategorien?

- Der EU bestemmer det (kan ankes)
- Hvis det ble benyttet mer enn 10^25 FLOPS med datakraft på å trene modellen.

Slike modeller vil få ytterligere krav knyttet til evaluering av modellen og risiko. Alvorlige hendelser må rapporteres og rettes. Det er også krav knyttet til sikring av løsningen og infrastruktur.

*10^25 FLOPS tilsvarer rundt tusen NVIDIA A100 skjermkort som arbeider i over 1 år, totalt forbruk rundt 3,5 GWh strøm. Det er **få** selskaper dette er relevant for*

Hvordan forberede seg?

Hvis du bygger eller bruker AI:

1. EU’s AI Act kommer fra 2026, men GDPR gjelder for AI som benyttes i dag. Start med å sikre etterlevelse av GDPR.
2. Bygger du AI løsninger? Basert på din produktstrategi, finn ut hvilke risikokategori du kan havne i.
3. “Hør risiko” vil bli strengt regulert. Selskaper som ikke har prosesser for å jobbe med regulatorisk etterlevelse bør starte å forberede seg **nå**.
4. For den mindre risikofylte bruken, vær åpen og ærlig om hvordan AI benyttes.

Solfi kan AI og compliance!

Ønsker du støtte og råd i hvordan implementere AI uten å bryte GDPR? Lurer du på hva fremtiden vil bringe av krav til kvalitetssystemer? Eller vil du bare ha en sparringspartner for hvilke muligheter og trusler AI åpner opp for din virksomhet?

John Arthur Berg

+47 930 53 088

Solfi

Vi hjelper vekstbedrifter å skalere