Retningslinjer for brug af kunstig intelligens (AI)

Revisionshistorik

Version	Dato	Beskrivelse af ændringer	Udført af	Godkendt af
1.0	26-03-2024	Oprettet	NIF	Sikkerhedsteamet
2.0	05-01-2026	Større ændringer foretaget i alle afsnit samt tilføjelse af afsnit om de registreredes rettigheder, lovmedholdelighed og sikkerhedsforanstaltninger	NHM	Sikkerhedsteamet

Indhold

Formål 1

Offentligt tilgængelige AI-værktøjer 2

Interne AI-løsninger 2

AI til beslutnings- og sagsunderstøttelse 4

Brug af AI-genererede resultater 4

Definition af kunstig intelligens 5

Relation til andet dokumentation:

- Retningslinjer for databehandleraftaler og tilsyn
- Retningslinjer for dataklassifikation og -opbevaring
- Ansatte kan på TRYK finde vejledning om korrekt og sikker brug af generativ AI.

Formål

Disse retningslinjer fastslår Jammerbugt Kommunes overordnede regler for anvendelse af kunstig intelligens (herefter AI) med henblik på at sikre, at overholdelse af relevant lovgivning, herunder databeskyttelseslovgivningen, forvaltningsretlige regler, sektorspecifik lovgivning og AI-forordningen.

Retningslinjerne omfatter brug af følgende værktøjer:

- Offentlige tjenester med AI (især generativ AI): Det vil sige AI-værktøjer, som sælges/udbydes af en ekstern leverandør typisk på internettet, hvor løsningen enten stilles til rådighed gratis eller mod betaling, og hvor løsninger typisk vil gøre brug af data, som er frit tilgængelige på internettet. Et eksempel på dette kan være ChatGPT og Copilot. Med eksterne løsninger er det typisk ikke muligt at lave databehandleraftaler, som regulerer leverandørers anvendelse af de data, som brugere indtaster i løsningen.
- Interne AI-løsninger, som enten er integreret i fagsystemer som funktionalitet/modul, eller selvstændige AI-løsninger, og hvor kommunen enten selv har udviklet eller har indkøbt løsningen via eksterne leverandører. Her er anvendelsen afgrænset til data,

som behandles og reguleres af kommunen på kommunens netværk eller i kommunens cloud-løsninger. Et eksempel er en ekstern, tilkøbt løsning, der anvender AI til automatisk fakturering i kommunens økonomisystem.

Offentligt tilgængelige AI-værktøjer
Ved brug af offentlige AI-tjenester (fx ChatGPT og den offentlige version af Copilot (ikke business-versionen)), som ikke er reguleret af en databehandleraftale med Jammerbugt Kommune, er det ikke muligt at vide, hvordan de data, man indtaster eller uploader i AI-løsningen, behandles, eller hvem de deles med. Det kan ikke udelukkes, at AI-værktøjerne anvender indtastede data til egne formål, fx til at forbedre værktøjet eller i nogle tilfælde at videregive til andre parter.

Ansatte i Jammerbugt Kommune må derfor *ikke* skrive, indtale eller lægge billeder ind i en ekstern, offentligt tilgængelig kunstig intelligens AI-tjeneste, som kan indeholde:

- **Personoplysninger af nogen art**. Hverken almindelige, fortrolige eller følsomme oplysninger. Der må heller ikke behandles personoplysninger, som er offentligt tilgængelige. Reglen inkluderer bl.a. navne, adresser, CPR-numre eller andre oplysninger, der kan kobles til personer. Dvs. også oplysninger, der ikke umiddelbart fremstår som en personoplysning, men som kan anvendes til at identificere en fysisk person, fx en persons jobfunktion, udseende eller lignende.

- **Forretningskritiske informationer, fortrolige oplysninger eller anden intern kommunal information,** som er fortrolige, eller som kan misbruges. Det er bl.a. sags- og budgetoplysninger, interne referater, strategiarbejde, økonomiske nøgletal, organisatoriske overvejelser, samarbejdsinformationer herunder også tredjepartsinformationer som fx leverandøroplysninger, andre myndigheders data mm.

Det vil sige, at persondata eller fortrolige og forretningskritiske data ikke må behandles i offentlige AI-løsninger.

Hvis en ansat enten tilsigtet eller utilsigtet behandler personoplysninger af nogen art i et offentligt AI-værktøj, vil der være tale om et sikkerhedsbrud.

Det er ikke tilladt at logge ind i offentligt tilgængelige AI-løsninger ved brug at sin kommunale it-bruger eller andre arbejdsrelaterede it-kontooplysninger, da det i værste fald kan medføre, at disse kontooplysninger bliver kompromitteret. I Copilot anvendes dog ens it-bruger som loginmetode grundet central opsætning af kommunens Microsoft-konti.

Interne AI-løsninger
Det er tilladt at udvikle, indkøbe og anvende AI-løsninger, som integreres direkte i fagsystemer som funktionalitet/modul, eller selvstændige AI-løsninger, som kommunen enten selv har udviklet eller indkøbt via eksterne leverandører.

Lederen af den pågældende afdeling, som beslutter sig for at udvikle eller indkøbe løsningen, er ansvarlig for at sikre, at gældende lovgivning overholdes, samt at vurdere, hvorvidt nytteværdien står mål med omkostningerne ved at udvikle, implementere og drifte systemet. Det er muligt at få sparring og vejledning herom ved at kontakte

Digitaliseringsafdelingen.

Sikkerhedsrådgiveren skal altid orienteres om overvejelserne for ibrugtagning af AI-løsninger, så det sikres, at der indgås databehandleraftaler, hvor det er nødvendigt. Sikkerhedsrådgiveren sørger desuden for at opdatere kommunens tværgående oversigt over anvendte AI-løsninger.

Hvis det planlægges, at AI-løsningen skal behandle personoplysninger, skal lederen være særligt opmærksom på følgende punkter:

- Lovhjemmel: Der skal altid identificeres en hjemmel til behandling af personoplysninger ved brug af AI-teknologi. Som regel vil kommunens hjemmel være myndighedsudøvelse (art. 6, stk. 1, litra e og art. 9, stk. 2, litra g), hvor der udover den databeskyttelsesmæssige lovhjemmel skal findes et supplerende hjemmelsgrundlag i særlovgivningen, fx beskæftigelsesloven, folkeskoleloven mv. Når kommunen agter at udvikle eller indkøbe nye AI-løsninger, vil der være tale om en vurdering af hjemmelsgrundlaget fra gang til gang, som skal foretages forinden af kommunens DPO.
    - *Særligt for brug af AI-teknologi til håndtering af borgerrettede myndighedsopgaver:* Efter Datatilsynets praksis kan være behov for et klart og direkte supplerende nationalt retsgrundlag til drift af AI-løsninger, hvis behandlingen er direkte og indgribende overfor borgeren, fx en afgørelse eller aktivitet. Læs mere herom i afsnittet 'Brug af AI til beslutnings- og sagsunderstøttelse'.
- Oplysningspligt: Der stilles krav om, at de registrerede informeres eksplicit om brugen af AI-teknologi til behandling af deres personoplysninger. Ønsker man at anvende AI-teknologi til behandling af personoplysninger i tidligere eller aktuelle personsager, skal lederen derfor sikre sig, at der gives en ny oplysningsskrivelse til de registrerede.
- De registreredes rettigheder i øvrigt: AI-løsninger skal ligesom andre it-løsninger kunne håndtere anmodninger fra de registrerede, ligesom det skal være muligt at håndtere klager. Herunder skal det være muligt at imødekomme en anmodning om ret til indsigt eller ret til sletning i AI-løsninger.
- Risikovurdering og konsekvensanalyse: Der skal ligesom for andre it-systemer, som behandler personoplysninger, udarbejdes en risikovurdering. Datatilsynet har i deres vejledning om AI vurderet, at brug af AI er forbundet med sandsynlighed for høj risiko for de registrerede, hvorfor der som udgangspunkt skal udarbejdes en konsekvensanalyse, inden AI-løsninger påbegynder behandling af personoplysninger – også i udviklings- og testfasen.
- Uddannelse: Der er indført lovpligtige krav til uddannelse i AI-færdigheder for medarbejdere, der arbejder direkte i AI-systemer. AI-kompetencer skal tilpasses den enkeltes rolle og kan omfatte:
    - Teknologisk forståelse: Hvordan AI-systemer fungerer og er opbygget.
    - Praktisk anvendelse: Evnen til at bruge AI-systemer korrekt og effektivt.
    - Etisk og juridisk forståelse: Kendskab til risici, ansvar, datasikkerhed og konsekvenser for samfund og individ.

AI til beslutnings- og sagsunderstøttelse
Der stilles særlige krav til, at kommunen skal kunne identificere et klart og direkte supplerende nationalt hjemmelsgrundlag, hvis der anvendes AI til beslutnings- og sagsunderstøttelse i myndighedsudøvelse. Derfor skal der kunne findes en direkte hjemmel til brug af AI-teknologi i særlovgivningen, før AI-teknologi må anvendes til beslutnings- og sagsunderstøttelse.

Kommunen har i forlængelse af ovenstående udfordringer besluttet, at AI-teknologi må ikke anvendes til (hel/delvist) automatiske afgørelser. AI-teknologi må derimod gerne anvendes til behandling af personoplysninger i forbindelse med beslutnings- og sagsunderstøttelse, hvis der ud fra en risikobaseret vurdering træffes tilstrækkelige tekniske og organisatoriske sikkerhedsforanstaltninger, herunder bl.a. at brugerne skal være instruerede i at kvalitetssikre outputtet.

Beslutnings- og sagsunderstøttelse defineres ikke ud fra en binær model, hvor en proces enten er eller ikke er beslutnings- og sagsunderstøttelse. Derimod skal det vurderes fra proces til proces, hvor stor en rolle AI-teknologien spiller i afgørelsessager. Herunder skal det vurderes, hvor indgribende afgørelsen er for borgeren, hvilke konsekvenser en forkert afgørelse kan få, hvor stor risikoen er for fejl, samt hvor mange borgere der kan blive berørte. Disse overvejelser bør indgå i risikovurderingen af en AI-løsning.

Hvis AI-teknologi anvendes til behandling af andre datatyper (dvs. ingen personoplysninger), er den leder, som ibrugtager/bestiller løsningen ansvarlig for at sikre, at der foretages en vurdering af potentielle konsekvenser ved fejl, og hvorvidt det er muligt at opdage eventuelle fejl. En AI-løsning, som behandler vandforureningsdata, og hvor fejl i outputtet ikke opdages, kan fx potentielt medføre væsentlige konsekvenser fx miljø, klima og natur.

I forvaltningslovens §24 er der beskrevet et princip om gennemsigtighed, hvor offentlige myndigheder skal kunne redegøre for, hvilke hovedhensyn og kriterier der er lagt vægt på i skønsvurderinger. Dette princip bliver udfordret ved brugen af generativ AI ved sagsunderstøttende funktionalitet i afgørelsessager, da kompleksiteten af generativ AI gør det svært at forstå, hvordan et output faktisk bliver dannet. Det er derfor vigtigt at overveje, om det er muligt at vise borgere, hvilke kriterier AI-teknologien har lagt vægt på, hvis den på nogen måde er anvendt til at foretage en skønsvurdering i en afgørelsessag. En god tommelfingerregel er, at man overfor en udefrakommende ikke-teknisk person i overordnede træk skal kunne forklare, hvordan AI-teknologien er nået frem til sit resultat.

Brug af AI-genererede resultater
Den enkelte medarbejder, som anvender AI-løsningen, har ansvaret for fagligt at vurdere det pågældende resultat og at udvise sund fornuft. Det skyldes, at AI genererer svar baseret på mønstre i data og ikke på reel forståelse, og derfor kan resultaterne indeholde fejl, være upræcise eller mangle nuancer.

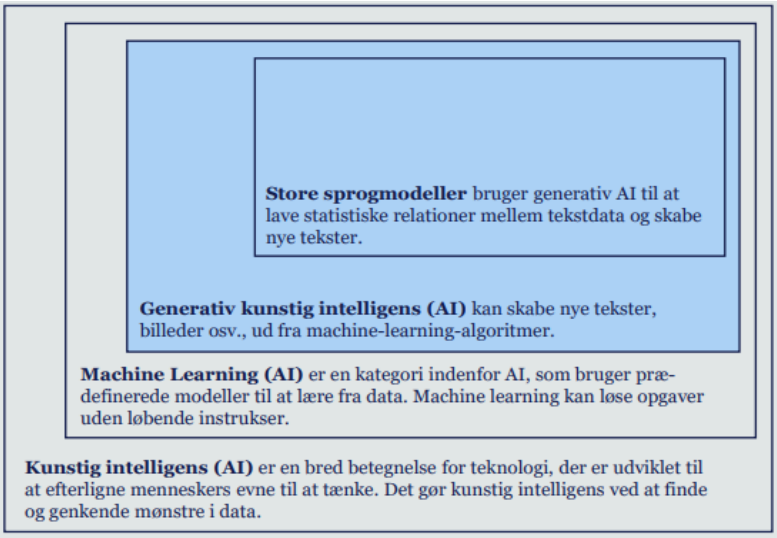
Medarbejdere skal være opmærksomme på algoritmiske bias og falsk information, da svar fra en generativ AI kan undlade vigtige forhold. Generativ AI laver sine svar ud fra sandsynlighed og ikke ud fra fakta. Fx kan der være indbygget køns- eller racemæssige bias

i genererede billeder og tekster.

Da generativ AI bygger på eksisterende indhold, kan der genereres resultater, der sammenstykker elementer fra indhold, som kan være beskyttet af ophavsret, varemærker, patenter mv. Hvis man fx beder AI om at skrive en tale, kan man risikere, at dele af talen stammer fra tekst på internettet, som er beskyttet af ophavsretten. Der foregår flere retlige stridigheder, som på sigt vil kunne danne præcedens vedrørende immaterialret og generativ AI. Det kan derfor være relevant at undersøge, hvilke kilder AI-løsningen har sammenstykket sit resultatet ud fra, hvis det er muligt. AI-genererede billeder kan dog altid anvendes, da disse ikke er omfattet af ophavsret (copyright).

Definition af kunstig intelligens

Kunstig intelligens (AI) udspringer af datalogi og handler om modeller og algoritmer, som kan udføre opgaver, der normalt kræver menneskelig intelligens. Meget forenklet er systemer baseret på AI, herunder f.eks. på maskinlæring, systemer, der igennem genkendelse af mønstre og sammenhænge i datasæt kan udlede konklusioner og anvende disse i fremtidige analyser.



Figur 1: Typer af kunstig intelligens (kilde: KL)

AI anvendes typisk til opgaver som:

- Datadrevet læring (f.eks. maskinlæring): AI-modeller lærer mønstre og sammenhænge ud fra store datamængder, og systemet forbedrer sig selv over tid baseret på data
- Problemløsning og beslutningsunderstøttelse
- Sprogforståelse og -generering, typisk sprogmodeller som ChatGPT og Copilot
- Planlægning og automatisering

Generativ AI er en gren af kunstig intelligens, der kan producere tekst, billeder, lyd og andet indhold ved at analysere store mængder data. Den genererer output, der ligner det, den er trænet på – men uden at forstå indholdet. Selvom det kan virke kreativt, er det i virkeligheden en avanceret form for mønstergenkendelse.