Sortland kommune

Retningslinjer for «Bruk av kunstig intelligens (KI)» i Sortland kommune

Innhold

1 Formål og virkeområde 3

1.1 Formål 3

1.2 Målgruppe (hvem omfattes av retningslinjene) 3

1.3 Forhold til øvrige interne styringsdokumenter 3

2 Hva er KI? 3

3 Overordnede prinsipper for bruk av KI 4

4 Godkjente og ikke godkjente KI-verktøy 5

4.1 Godkjente verktøy, dette kan du bruke 5

4.2 Ikke godkjente verktøy 5

5 Informasjonssikkerhet og personvern 5

6 Rolle- og ansvarsfordeling 6

7 Opplæring og kompetanseheving 6

8 Risiko- og sikkerhetsvurderinger (ROS / DPIA) 6

9 Avvik, brudd og konsekvenser 7

10 Revisjon og gyldighet 7

Vedlegg: 8

Sensitive personopplysninger er: 8

Sensitive virksomhetsopplysninger kan være: 8

1 Formål og virkeområde

1.1 Formål

Formålet med dette dokumentet er å

- Sikre at alle ansatte bruker KI-verktøy på en etisk, sikker og lovlig måte.
- Klargjøre hvilke regler og rutiner som gjelder for daglig bruk av KI.
- Bidra til at personvern, datasikkerhet og kommunens verdier ivaretas i all bruk av KI.

1.2 Målgruppe (hvem omfattes av retningslinjene)

Retningslinjene gjelder for alle ansatte i kommunen, samt innleid personell og eksterne leverandører. Det omfatter også øvrige som utfører arbeid på, eller har tilgang til kommunens systemer.

1.3 Forhold til øvrige interne styringsdokumenter

Dette dokumentet skal ses i sammenheng med Sortland kommunes øvrige interne styringsdokumenter innen;

- Kommunedelplanen samfunnsdel
  Hovedmål 3: Bærekraftig utvikling og samfunnsrobusthet
  Hovedmål 4: En handlekraftig og koordinert kommuneorganisasjon
- Digitaliseringsstrategi — ref. Endelig versjon - Digitaliseringsstrategi 2026 - 2029.docx)
- IKT sikkerhet
- Personvern

2 Hva er KI?

Kunstig intelligens (KI) er teknologi som gjør det mulig for maskiner å utføre oppgaver som normalt krever menneskelig intelligens, som å forstå språk, lære av erfaring og ta beslutninger.

Vi har flere typer KI;

- Smal KI (Narrow AI) – Dette er KI som er laget for en spesiell oppgave, f.eks. chatbots, ansiktsgjenkjenning eller anbefalingssystemer. Dette er den mest vanlige formen for KI i dag.

- Generativ KI – er KI som kan skape nytt innhold, som tekst, bilder, video eller kode. Det kan generere menneskeliknende svar på spørsmål og kommandoer i naturlig språk. Eksempler: ChatGPT, Copilot, Gemini.

- Maskinlæring (ML) – er en metode der KI lærer fra data for å forbedre seg over tid og som brukes til prediksjoner, mønstergjenkjenning og automatisering.

- Dyp læring (Deep Learning) – er en avansert form for maskinlæring som bruker nevrale nettverk. Dette brukes i talegjenkjenning, bildeanalyse og komplekse beregninger.

- Prediktiv analyse – er KI som analyserer historiske data for å forutsi fremtidige hendelser. Eksempel: Prognoser for ressursbehov eller vedlikehold.

Disse retningslinjene omhandler bruk av generativ kunstig intelligens. Sortland kommune har valgt å benytte Microsoft Copilot som sin løsning. Valget er gjort fordi Sortland har en gjeldende avtale med Microsoft, og fordi løsningen er vurdert som trygg når det gjelder datasikkerhet, kontroll og personvern. Informasjon som legges inn i Copilot via kommunens Microsoft-konto, behandles i tråd med Microsofts sikkerhetsstandarder og brukes ikke til videreutvikling av språkmodellen.

3 Overordnede prinsipper for bruk av KI

- KI skal støtte, ikke erstatte menneskelige vurderinger.
    - Ikke bruk KI til å ta beslutninger som i betydelig grad påvirker innbyggere og/eller ansatte

- Kun godkjente KI-verktøy kan brukes i arbeidssammenheng.

- KI-generert innhold skal alltid kvalitetssikres av menneske.
    - Husk at KI er en maskin, ikke et menneske, som også kan ta feil. Vær kildekritisk!

- Etikk, likebehandling og innbyggernes rettigheter skal ivaretas.
    - Ikke del personlig informasjon som personopplysninger om ansatte og innbyggere
    - Ikke del sensitiv informasjon, se vedlegg
    - Ikke del brukerinformasjon, som påloggingsinformasjon og passord.

- Transparens: ansatte skal synliggjøre når KI har vært brukt.
    - Vær transparent og si fra om når du bruker en KI-generert tekst, bilde, kode eller annet.
    - Vær nøye med å merke innhold som du har brukt generativ KI til å lage. F.eks «*Deler av dette dokumentet er utarbeidet med støtte fra generativ KI (Microsoft Copilot). Innholdet er kvalitetssikret av forfatteren»* eller «*Tekstutkastet ble generert ved hjelp av Microsoft Copilot og bearbeidet av forfatteren»*

4 Godkjente og ikke godkjente KI-verktøy

4.1 Godkjente verktøy, dette kan du bruke

- Microsoft Copilot, når du er logget inn med Sortland kommune bruker.
- Sikt KI-assistent, når du er logget inn med Feide-bruker.
- KI-funksjoner i kommunens fagsystemer, der dette allerede er en del av løsningen

4.2 Ikke godkjente verktøy

Alle andre KI-verktøy er ikke godkjent i jobbsammenheng

Eksempler:

- Lime inn saksdokumenter i ChatGPT
- Bruke KI til å foreslå vedtak som går direkte til innbygger
- Bruke KI-verktøy du har privat konto på i jobbsammenheng

Et KI-verktøy kan bare brukes i arbeid hvis det enten:

- Står på listen over godkjente verktøy, eller
- er vurdert og fått en egen godkjenning etter gjeldende rutiner.

Nye KI-verktøy må godkjennes i tråd med kommunens IKT- reglement, SK - Compilo

5 Informasjonssikkerhet og personvern

- Informasjon som inneholder sensitive data eller taushetsbelagt informasjon skal ikke behandles eller legges inn i KI verktøy. GDPR artikkel 9 og personopplysningsloven § 6-10 regulerer behandlingen av denne type data.

- All KI-bruk skal følge kommunens IKT sikkerhetspolicy.

6 Rolle- og ansvarsfordeling

- Kommunedirektør – Har det overordnede ansvar for at retningslinjene følges jfr. delegeringsreglement.
- Systemeier – Har ansvar for faglig oppfølging av KI-verktøy og rutiner
- IKT-avdeling – Har ansvar for teknisk drift, sikkerhetskontroller og godkjenning av KI-verktøy før bruk. IKT-avdelingens «godkjenning» er ment som en del av en felles vurderingsprosess, ikke en beslutning alene. Godkjenning innebærer teknisk og sikkerhetsmessig vurdering, i samarbeid med systemeier og personvernombud.
- Personvernombud – Gir råd og vurderer personvernkonsekvenser, inkludert behov for DPIA (personkonsekvensvurdering)[1]
- Ledere – Sikrer opplæring av ansatte og følger opp at retningslinjene praktiseres i avdelingen.
- Ansatte – Skal bruke KI-verktøy på en måte som er i tråd med retningslinjene og kommunens regelverk.

7 Opplæring og kompetanseheving

Ansatte som skal ta i bruk Copilot skal gjennomføre minst ett av punktene nedenfor;

- KS sine sikkerhetsfilmer[2]
- Digital Norway tilbyr gratis digitale læringsprogram[3] om kunstig intelligens i tre versjoner, tilpasset ulike målgrupper.
- Glasspaper.no tilbyr også opplæring i KI.

8 Risiko- og sikkerhetsvurderinger (ROS / DPIA)

- ROS-analyse må gjennomføres når nytt system, modul eller funksjon med KI skal anskaffes. DPIA må i tillegg gjennomføres i system der en behandler sensitive personopplysninger. Kravet gjelder også mindre KI-funksjoner i eksisterende systemer dersom bruken kan påvirke dataflyt eller personvern.
- Systemeier vurderer hvilke data som behandles og behov for ROS/DPIA, med støtte fra personvernombudet, som gir råd og kvalitetssikrer vurderingen.

[1] DPIA står for personvernkonsekvensvurdering, og er en sjekk for å sikre at vi ikke setter personvernet i fare før vi tar i bruk nye løsninger.
[2] Sikkerhetsfilmene - Intranett
[3] Læringsprogram om kunstig intelligens

9 Avvik, brudd og konsekvenser

- Avvik meldes i Compilo (kommunens kvalitet- og avvikssystem). Avvik der personsensitivt er på avveie eller mistenkes på avveie, skal meldes til datatilsynet, i tråd med prosedyren Varsling til Datatilsynet ved sikkerhetsbrudd - Compilo

10 Revisjon og gyldighet

- Retningslinjene skal gjennomgås og revideres minst en gang per år.
- Revisjonsansvarlig med myndighet til å gjøre endringer er leder ved IT avdeling.

Vedlegg:

Sensitive personopplysninger er:

- opplysninger om rasemessig eller etnisk opprinnelse
- opplysninger om politisk oppfatning
- opplysninger om religion
- opplysninger om filosofisk overbevisning
- opplysninger om fagforeningsmedlemskap
- genetiske opplysninger
- biometriske opplysninger (når behandlingsformålet er å entydig identifisere noen)
- helseopplysninger
- opplysninger om seksuelle forhold

Sensitive virksomhetsopplysninger kan være:

- opplysninger som påvirker sikkerhet
  - sårbarhets- og risikoanalyser
  - informasjon om beredskapsplaner
  - kritisk infrastruktur (vann, avløp, strømnett, skolebygg og IT-infrastruktur)
  - tilganger, passord og interne systemarkitekturer
- opplysninger som kan skade kommunen økonomisk eller strategisk
  - kontraktsforhandlinger
  - anskaffelsesdokumenter før offentliggjøring
  - intern økonomirapportering, revisoranmerkninger
  - utkast til politiske beslutningsunderlag før de er offentlige
- Taushetsbelagte opplysninger etter forvaltningsloven - kan gjelde både:
  - Enkeltpersoner
  - bedrifter (konkurransesensitive opplysninger)
  - fagforeninger