Råd vid intern kommunikation om användning av AI-baserade chattbotar

Den 30 november 2022 lanserades den AI-baserade chattboten ChatGPT av OpenAI som en prototyp. OpenAI är ett företag vars målsättning är att säkerställa att artificiell generell intelligens (AI-system) som är smartare än människor ska gynna hela mänskligheten. Den 14 mars 2023 släppte OpenAI en betydligt förbättrad version som exempelvis kan skriva programkod, musik, sagor, poesi, sångtexter och dessutom spela spel och svara på frågor. Det har uppmärksammats att den nya versionen kan klara provet för en juristexamen i USA. Utvecklingen går väldigt fort och flera IT-aktörer lanserar nu avancerade produkter baserat på den här typen av modell, i form av såväl generella som specifika tillämpningar.

Det kan uppstå frågor om de AI-baserade chattbotarna i relation till myndigheternas verksamhet, såväl i myndighetens relation till målgrupperna som hur den här typen av lösningar används inom organisationen. Chattbotarna bygger på stora språkmodeller (Large language models – LLMs) som potentiellt skulle kunna användas av myndigheterna för att utveckla sina egna tillämpningar, vilket skulle kunna ge betydande effekter.

Användningen av AI-baserade chattbotar är ett relativt outforskat område. Flera av eSams medlemmar har kommunicerat internt om hur medarbetarna ska förhålla sig till att använda den här typen av digitala tjänster. Syftet med den här promemorian är att erbjuda ett stöd och inspiration för budskapsformulering när organisationen ska kommunicera internt. Förslagen bygger på ett sammandrag av flera myndigheters internkommunikation.

Användning av AI-baserade chattbotar

Den tekniska utvecklingen av digitala tjänster som baseras på artificiell intelligens (AI) går för närvarande mycket snabbt och användningsområdena blir allt fler, det innebär möjligheter för myndigheter men det medför också risker.

Nu finns många tjänster som är baserade på Artificiell Intelligens (AI), till exempel AI-baserade chattbotar och bildgenereringstjänster. Det är potentiellt kraftfulla verktyg där man behöver förstå konsekvenserna vid användandet.

ChatGPT är en chattbot som har växt snabbare än någon annan digital tjänst och som har blivit populär inom arbetslivet. Den kan bland annat besvara faktafrågor, författa texter på olika språk och förklara och skriva kod. Den är en av flera AI-baserade chattbotar som tillhandahålls fritt på internet, en annan är Bing.

Allt fler ser möjligheter med att använda AI på området språkförståelse i arbetet. Det finns möjligheter med den nya tekniken och det är viktigt att följa med i utvecklingen och lära oss mer. Användningen av ny teknik uppmuntras, eftersom det är outforskad mark behöver användningen ske med eftertanke. Användandet av den nya tekniken kan medföra risker för myndigheter varför det är viktigt att vid användandet ha med sig aspekter som informationssäkerhet, trovärdighet, jämställdhet och opartiskhet.

Generellt om användning

- Använd AI-baserade chattbotar på ett etiskt och respektfullt sätt, undvik olämpligt språk och olämpliga ämnen.
- Tänk på att använda AI-baserade chattbotar som ett komplement till ditt arbete, snarare än att förlita dig helt på den.
- Du kan ställa väldigt öppna frågor till AI-baserade chattbotar som inte kan kopplas till myndigheten.
- Den här typen av chattbot använder det som matas in för att lära sig mer. Gör en allmän lämplighetsbedömning av vad du skriver in. Även om enskilda ord och uttryck framstår som harmlösa kan det t.ex. gå att kartlägga myndighetens kommande planer, strategier och beslut utifrån vad du väljer att söka på. Utifrån inmatad information kan tjänsterna generera nya svar på frågor från andra användare.

Information

- Avstå från att dela intern information med den AI-baserade chattboten eftersom informationen kan spridas. Med intern information menas all typ av information som är olämplig att publicera på myndighetens externa webbsida.
- När du skriver in uppgifter i AI-baserade chattbotar så innebär det att du lämnar ut information. Skriv därför **inte** in känslig eller konfidentiell information, såsom personuppgifter eller uppgifter som omfattas av sekretess. Personuppgifter är alla uppgifter som kan identifiera en person; Namn, personnummer, registreringsnummer och så vidare. Myndigheten saknar grund i dataskyddsförordningen för sådan personuppgiftsbehandling.
- Mata **inte** in intern kod, källkod, lösenord eller annan intern information i tjänsten.

Hantering av resultat

- Granska kritiskt och kontrollera de resultat som den AI-baserade chattboten producerar eftersom de kan vara ofullständiga eller felaktiga. Framför allt bör du kontrollera att svaren från den AI-baserade chattboten är korrekta, rimliga och följer myndighetens värdegrund och interna styrning. Det är viktigt att kontrollera källor och referenser.
- Tänk på att du alltid är ansvarig för det arbete du utför. Den som använder resultat från en AI-baserad chattbot ansvarar för det på samma sätt som om det producerats på egen hand.

Transparens

- Vi redovisar vår eventuella användning av AI-baserade chattbotar helt öppet. Det betyder att vi delar med oss av våra erfarenheter och berättar om, när och hur vi har använt oss av verktyget i vårt arbete.

Risker

- Meddela din chef om du upptäcker felaktigheter eller missbruk av AI-baserade chattbotar så att vi kan hantera de situationerna och förbättra användningen av AI-verktyget.
- Tänk på att det är förknippat med ökade risker att dela, använda eller ladda hem länkar, dokument, makron och kod, eller att använda AI för att generera kod.

- De här verktygen levereras ofta av utländska företag som molntjänster. Samma lagar och regler gäller därför vid användning av AI-baserade chattbotar som för andra typer av molntjänster.