

ANVÄNDNING AV GENERATIV AI I KOMMUNER

– gemensamt framtagna riktlinjer

Version 0.9, uppdaterad 26 april 2024.



Innehållsförteckning

Bakgrund och syfte	3
Nyttan av generativ AI	4
Ansvarsfull användning av generativ AI	5
AI Act	5
GDPR	5
Data och sekretess	6
Krav på förklarbarhet och spårbarhet	7
Likabehandlingsprinciper	8
Praktisk information	9

Bakgrund och syfte

Under det gångna året har utvecklingen av artificiell intelligens (AI) tagit stora framsteg, och teknikens påverkan på vårt arbetslandskap blir allt mer påtaglig.

AI bygger på att datorsystem tränar på stora mängder data och lär sig utföra olika sorters uppgifter som underlättar vardagen för oss människor. På kort tid har det som kallas generativ AI – en form av AI som har förmågan att skapa nytt och unikt innehåll, såsom text, bilder, ljud och video – tagit fart, med en växande popularitet för generativa verktyg som ChatGPT, Google Gemini, och Microsoft Copilot. Som med all teknik finns det risker med dessa avancerade AI-verktyg, som också har potentialen att öka effektiviteten och kapaciteten av medarbetare.

Generativ AI, blir en alltmer central komponent även i kommunernas digitalisering och utgör en pusselbit för att klara utmaningarna som den demografiska utvecklingen för med sig. Sveriges alla 290 kommuner står inför samma frågeställningar, och detta dokument syftar till att kraftsamla kring detta högaktuella ämne och då undvika att hjulet uppfinns gång på gång. I detta dokument hoppas vi kunna besvara frågor som: hur ska vi ta till oss den snabba utvecklingen av generativ AI? Vad kan, får och bör vi göra med generativ AI i våra verksamheter?

Dokumentet, som bygger på gediget arbete kring frågan i kommuner runt om i Sverige: Lund, Kungsbacka, Jönköping, Helsingborg, Höör, och Uddevalla, med flera, syftar också till att komplettera kommunens befintliga policydokument kring informationssäkerhet och digitalisering – och gör således inga anspråk på att vara heltäckande kring dessa frågor.

Dokumentet är bearbetat av kommunkollegor i Malmö, Lund, Helsingborg, Höör och Skurup i April 2024, och sammanställs och delas av AI Swedens södra nod, som organiserar företag, regioner, kommuner, och andra aktörer att tillsammans ta tillvara möjligheterna med tillämpad AI – till gagn för hela vårt samhälle och enligt parollen “Invest together, share with many”.

Nyttan av generativ AI

DIGG, myndigheten för digital förvaltning, har uppskattat att den årliga besparingen i offentlig sektor med användningen av AI skulle kunna uppgå till 140 miljarder kronor, cirka 6% av den totala offentliga budgeten. Offentlig sektor har således en skyldighet att bidra till att öka användningen av välfärdsteknik för att möta gemensamma samhällsutmaningar. Här kan generativ AI utgöra ett sätt att göra detta. Samtidigt är det extra viktigt att som offentlig aktör nyttja AI på ett ansvarsfullt sätt.

Med hjälp av generativa AI-verktyg, och dess förmågor att skapa bilder, ljud och andra uttryck som efterliknar världen, finns det nu större möjligheter att effektivisera och på andra sätt förbättra olika processer.

Samtidigt är det viktigt att komma ihåg att generativ AI inte är ett sätt att helt ersätta mänskliga medarbetare, utan att det bör ses som ett samarbetsverktyg. Generativa verktyg är inte autonoma system som arbetar på egen hand, och medarbetarens expertis och insikter är fortsatt avgörande för hur innehållet som verktygen genererar kan och ska användas.

Hur funkar det egentligen?

Generativ AI bygger på statistik och sannolikhet, snarare än intuitiv förståelse. Generativa modeller tränas på stora mängder data, som texter eller bilder, och lär sig att skapa innehåll som liknar det innehåll som de har tränats på. En generativ modell har alltså inte en verklig förståelse för innebörden av det innehåll den producerar, utan agerar snarare på en förutsägelse av vad som är mest troligt baserat på tidigare mönster i data. Vid textgenerering kan det till exempel handla om vilket ord som kommer näst i en mening och vid bildgenerering kan det handla om vilka pixlar som ska angränsa varandra. Denna sannolikhetsbaserade process är central för att förstå hur generativa modeller fungerar och hur de skiljer sig från mänsklig kreativitet och förståelse.

Ansvarsfull användning av generativ AI

Det finns en enorm potential i användningen av generativ AI. Därför är det också viktigt att generativ AI nyttjas på ett ansvarsfullt sätt för att säkerställa att dess tillämpningar inte orsakar skada eller orättvisa. Det är alltid individen som ansvarar för användningen av AI-verktyg på arbetsplatsen, och hur dessa resultat distribueras. Ansvaret gäller även om du köper ett system, och det går således inte att "skylla på leverantören."

Detta dokument grundar sig i de lagar, förordningar och regler som kommunens anställda redan lyder under. Förtroende, transparens och informationssäkerhet är några viktiga vägledande aspekter, och EU:s AI-förordning lägger ytterligare ett lager ovanpå detta. Utöver juridiska övervägande behöver varje verksamhet göra egna moraliska och etiska övervägande för att säkerställa att implementering är i linje med verksamhetens värdegrund.

En ansvarsfull användning av av generativ AI gäller för alla medarbetare i kommunen; all anställd personal, privata utförare och förtroendevalda, som i det här dokumentet benämns som användare.

Användare av generativa AI-verktyg behöver tänka på:

- Generativa AI-tjänster utgör arbetsverktyg och den som använder dessa är personligen ansvarig för resultatet.
- Ha alltid som rutin att granska, rätta och vid behov rapportera felaktigheter i den information som produceras vid användning av den generativa AI-tjänsten som används.
- Var särskilt noga med vilken information som hanteras så att integritet och säkerhet upprätthålls.
- Publika verktyg får bara användas med information som klassas som öppen, t.ex. sådant som publiceras på öppet åtkomliga hemsidor.
- Avvikelser, felaktigheter eller missbruk skall inrapporteras i kommunens ordinarie kanaler för incidentrapportering för informationssäkerhet och dataskydd.

AI Act – världens första lag för användning av AI

Under 2023 blev EU först i världen med en lagstiftning som syftar till att reglera utvecklingen och användningen av AI. Lagen som går under namnet *AI Act*, ska säkerställa att AI-system som används inom Europa är säkra, transparenta, spårbara, ickediskriminerande, och miljövänliga. Man slår också fast att AI-system bör övervakas av människor, snarare än skötas automatiskt – för att förhindra eventuella skadliga effekter.

För generativ AI innebär lagstiftningen bland annat att:

- Innehåll behöver märkas upp så att det framgår att det har genererats av AI
- Systemet behöver vara utformat så att det förhindrar att olagligt innehåll genereras
- Sammanfattningar av upphovsrättsskyddade data som används för utbildning ska offentliggöras

Hur lagstiftningen påverkar befintliga AI-tjänster återstår att se, när det här dokumentet skrivs är det ännu en liten stund kvar till att lagstiftningen helt träder i kraft.

[Läs mer: Artificiell intelligens | Europaparlamentet](#)

GDPR

Dataskyddsförordningen (GDPR) stärker allas våra rättigheter som medborgare i EU och hjälper var och en att ta kontrollen över hur ens personuppgifter används. GDPR ska också tillämpas i användningen av generativ AI, och användare av generativ AI måste ta hänsyn till de grundläggande principerna i dataskyddsförordningen. Principerna gäller för all behandling och kan sägas vara kärnan i dataskyddsförordningen. Principerna innebär bland annat att den personuppgiftsansvariga bara får samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål, inte ska behandla fler personuppgifter än vad som behövs för ändamålen och ska radera personuppgifter när de inte längre behövs. Rådgör gärna med dina kollegor eller din organisations dataskyddsombud om användningen av ett särskilt Generativ AI-verktyg om du känner dig osäker. [Läs mer: EU:s regler för skydd av personuppgifter | Europeiska kommissionen](#)

Data och sekretess

Vid användningen av generativa verktyg som är allmänt tillgängliga är det viktigt att komma ihåg att den data som matas in till verktyget, beroende på licens, oftast lagras av de olika tjänsteleverantörerna. Användningen av känslig information innebär därför en risk för oavsiktlig delning mot tredje part, vilket leder till förlust av konfidentialitet.

Idag erbjuds företagslicenser hos flera av de större generativa verktygen, som t.ex. ChatGPT Enterprise, Google Gemini Enterprise, och Microsoft Copilot. Till exempel är det många kommuner som använder Microsoft 365 och på så sätt har tillgång till Microsoft Copilot med kommersiellt dataskydd. Den kommersiella versionen av Copilot lagrar inte data och sparar inte heller chatthistorik, och är lika säker att använda som till exempel Outlook och Teams. Läs mer: [Copilot Privacy and Protections](#) | [Microsoft Learn](#)

Innan införskaffandet av företagslicens på något verktyg är det viktigt att läsa igenom dess villkor för användning. För dig som ansvarar för att köpa in nya tjänster och system är en bra riktlinje att välja leverantörer som du kan få ett personuppgiftsbiträdesavtal (PUB-avtal) med. Läs mer: [Allmänt om personuppgiftsbiträdesavtal, PUB-avtal](#) | [Sveriges kommuner och regioner](#)

Beakta följande punkter vid användning av generativa tjänster:

- **Följ GDPR – dela inte persondata**

Tänk på att det finns mer information än namn som kan göra att det går att identifiera en person: adresser, telefonnummer, arbetsplats, utbildning, och så vidare. Även röst, ansikte och andra biometriska uppgifter kopplat till en person kan vara känsliga att använda. Det är därför viktigt att vara försiktig och tänka igenom vilken information som delas för att skydda integriteten och säkerheten för både dig och andra.

- **Dela inte uppgifter som är känsliga eller omfattas av sekretess**

Offentlighets- och sekretesslagen (OSL) gäller, vilket innebär att du inte får samköra data mellan förvaltningar i olika nämnder hur som helst. Använd därför "sunt förnuft" – är informationen externt publicerad och öppet tillgänglig på internet är det troligtvis okej att mata in som en input till en AI.

Krav på förklarbarhet och spårbarhet

För att säkerställa transparens är det viktigt att kunna förstå och förklara hur beslut fattas av olika AI-system. I dagsläget är det inte tillåtet att använda generativ AI för att fatta viktiga beslut. Det innebär att du inte får be ett generativt verktyg att ta ställning till information i ett ärende, till exempel om en ansökan om insatser och bidrag ska beviljas eller inte. Det är viktigt att verktyget du använder kan förklara varför det gett det svar som det har gjort, ett krav som också EU-lagstiftningen ställer på kommande verktyg.

Likabehandlingsprinciper

Likabehandlingsprinciper är avgörande för att säkerställa att AI-system inte leder till diskriminerande eller orättvisa resultat genom att hantera och minimera eventuella fördomar eller partiskhet i data och algoritmer. Olika modeller är tränade på olika data och kommer, liksom människor, vara partiska på olika sätt. Det är viktigt att vara medveten om detta, då du som individ bär ett personligt ansvar att följa likabehandlingsprinciperna i din användning av olika generativa verktyg.

Praktisk vägledning

Som ett komplement till detta dokument har en användarguide för praktisk användning av generativ AI tagits fram. *Användarguide: för dig som vill utforska generativ AI i kommunal verksamhet* syftar till att ge praktisk vägledning till dig som är nyfiken på att använda generativ AI i den kommunala verksamheten.

I användarguiden finns bland annat mer information om hanteringen av AI-genererad text och bild.