HEDEMORA KOMMUN	STYRDOKUMENT	Sida 1(6)
	Datum 2024-11-28	**Omfattning** Kommunkoncernen
	Giltighet fr o m 2025-02-05	**Publicering** Författningssamlingen

Godkänt/antaget av	**Dokumentägare**	Dokumentansvarig
Kommundirektör 2025-02-05	Stabschef	Kommunikatör

Riktlinje för användning av stora språkmodeller (LLM) och generativ AI i Hedemora kommunkoncern

Dok. Kategori:	Riktlinje
Stadie:	Beslutad
Gallring:	Bevaras
Kort beskrivning:	Denna riktlinje anger ramarna för hur medarbetare i Hedemora kommunkoncern får använda sig av stora språkmodeller och generativ AI i tjänsten.

Ursprungligt beslutsdatum	**Ursprungligt diarienummer**	**Bör revideras senast**	**Skapad av**
2024-02-05	KS456-24 005	Vid behov, med årlig översyn	Kommunikatör Anders Olofsson och utredare Oksana Lukina
Revideringar (datum, §)	**Vad revideringen avsett**	**Diarienummer vid revidering**	**Ändrad av**

Riktlinje för användning av stora språkmodeller (LLM) och generativ AI i Hedemora kommunkoncern

Denna riktlinje gäller hela kommunkoncernen i Hedemora kommun. Med Kommunen nedan menas Hedemora kommun inklusive helägda kommunala bolag.

Bakgrund och avgränsningar

AI bygger på att datorsystem tränar på stora mängder data och lär sig utföra olika sorters uppgifter som underlättar vardagen för oss människor. Under de senaste åren har utvecklingen av artificiell intelligens (AI) tagit stora framsteg. Inte minst gäller det så kallad generativ AI – en form av AI som har förmågan att skapa nytt och unikt innehåll, såsom text, bilder, ljud och video – med verktyg som ChatGPT, Google Gemini, och Microsoft Copilot.

Dessa verktyg har potentialen att öka effektiviteten och kapaciteten hos användaren, men som med all teknik finns det också risker att vara medveten om och beakta.

Syftet med detta dokument är att ange ramarna för säker och ansvarsfull användning av generativa AI-tjänster inom Kommunen, med fokus på att skydda personlig integritet, skydda Kommunens informationstillgångar och att upprätthålla förtroendet för Kommunens användning av ny teknik.

Det kan finnas andra typer av AI-verktyg som används i Kommunen för vissa specifika ändamål. Detta dokument berör endast generativ AI, och då främst stora språkmodeller (Large Language Models, LLM), som är tränade på omfattande textdata för att förstå och generera (efterlikna) mänskligt språk.

Vad kan, får och bör vi göra med generativ AI i våra verksamheter?

Användning av generativ AI – vem ansvarar?

Det finns en enorm potential i användningen av generativ AI. Därför är det också viktigt att generativ AI nyttjas på ett ansvarsfullt sätt. Det är alltid individen/varje medarbetare som ansvarar för en ansvarsfull användning av AI-verktyg på arbetsplatsen, och hur dessa resultat distribueras och/eller lagras. Med medarbetare i Kommunen menas all anställd personal, privata utförare och förtroendevalda.

Detta dokument grundar sig i de lagar, förordningar, föreskrifter och styrdokument som Kommunens medarbetare redan lyder under. Förtroende, transparens, offentlighetsprincipen, personuppgiftshantering och informationssäkerhet är några viktiga vägledande aspekter som måste tas hänsyn till, och EU:s AI-förordning lägger ytterligare ett lager ovanpå detta.

Tillgängliga AI-tjänster

Copilot Webb

Det finns flera versioner av Copilot: Webb, Work och Pro. Det finns också en version som är inbyggd i Microsofts webbläsare Edge. Detta kan verka förvirrande, särskilt som det egentligen inte framgår vilken version man faktiskt använder. Som medarbetare i Kommunen räcker det dock att du vet att:

1. **Du ska bara använda Copilot som inloggad med ditt tjänstekonto i Microsoft 365.**
2. **Som inloggad kommer du inte åt någon annan version än Copilot Webb.**

Copilot Webb är den enda AI-tjänst som du har officiell tillgång till som medarbetare i Kommunen. Den finns som app (program) via Microsoft 365-portalen. Du kan också spara en genväg till den webbaserade versionen av appen Copilot i valfri webbläsare.

När du är inloggad med ditt tjänstekonto följer Copilot de säkerhetsinställningar och den säkerhetspolicy som Hedemora kommun satt upp för övriga program i Microsoft 365, så som Word, Outlook, PowerPoint och Teams. Den information du delar i Copilot sparas endast hos Kommunen i Kommunens molntjänst och används inte för att ”lära upp” Copilot. Du måste därför säkerställa att du är INLOGGAD med ditt tjänstekonto, när du använder dig av Copilot. Observera att du ändå måste följa de rutiner och användningsregler som specificeras längre fram i detta dokument.

Copilot är ett kraftfullt verktyg som kan vara en bra hjälp för många av Kommunens medarbetare. AI-teknikens förmåga att hantera och analysera stora datamängder på kort tid gör det möjligt för verksamheterna att frigöra resurser till mer kvalitativt arbete. Genom att fungera som en digital assistent kan Copilot effektivisera arbetsprocesser, förkorta ledtider och utveckla nya arbetssätt för Kommunens tjänster.

Andra versioner av Copilot

Om du har du en privat prenumeration på Microsoft 365, med egen inloggning, så har du även då tillgång till en app med namnet Copilot, men den versionen, som formellt heter Copilot Work, får inte användas för information och frågor som ägs av och rör Kommunen, eftersom det som delas här sparas på Microsofts servrar. Detsamma gäller versionen Copilot Pro.

Det finns även en version av Copilot som är inbyggd i webbläsaren Edge, men eftersom det finns säkerhetsrisker med den versionen har vi valt att stänga av den på Kommunens datorer.

Andra AI-verktyg

Du får inte dela information (texter, dokument, bilder) som ägs av och rör Kommunen med

andra AI-verktyg, som ChatGPT eller Google Gemini. Den data som matas in till dessa verktyg lagras oftast hos de respektive tjänsteleverantörerna. Användningen av personuppgifter och sekretesskyddad information innebär i sådana fall en risk för oavsiktlig och/eller olaglig delning mot tredje part.

Rekommendationen är att du helt avstår användning av andra AI-verktyg än Microsoft Copilot på enheter som ägs av Kommunen, såsom datorer, ipads, mobiltelefoner. Det gäller också när du använder andra enheter än Kommunens i Kommunens nätverk.

Säkerhet

Den version av Copilot som du har tillgång till, som medarbetare i Kommunen och inloggad med ditt Microsoft 365-konto, kommer inte åt något material, som epost, chattar, dokument, kontakter, kalendrar, filer eller appar på din tjänstedator, ipads, mobiltelefoner eller Kommunens servrar och nätverk. Så länge du är inloggad med ditt tjänstekonto så har Copilot endast tillgång till den information (text, bilder, dokument) som du matar den med.

För att du som medarbetare ska kunna få möjlighet att använda Copilot måste Kommunen kunna säkerställa viss säkerhetsnivå. Det är därför viktigt att du följer nedanstående användningsregler.

Användningsregler

Här är fem grundläggande regler att följa när du använder generativ AI i din tjänst:

- Använd inga andra AI -verktyg än Copilot, INLOGGAD med ditt Microsoft 365-konto från Hedemora kommun.

- Du ansvarar för den information du matar in till AI-verktyget.

- Du ansvarar för hur resultatet från AI-verktyget används. Du måste alltid faktagranska och rätta den information som den generativa AI-tjänsten producerar. Detta för att säkerställa att den information som skapas är korrekt och aktuell.

- GDPR gäller. Det är därför viktigt att du efterlever GDPR när du arbetar med AI-verktyg. Dela inte persondata om dig själv eller andra med AI-verktyget.

- Dela inte konfidentiell information (särskilt skyddsvärda och känsliga personuppgifter, sekretesskyddad information inklusive säkerhetsklassificerad information) med AI-verktyget. Om hantering av personuppgifter är nödvändigt, får alltså endast harmlösa/normala personuppgifter hanteras. Tänk på att harmlösa personuppgifter kan bli känsliga om du aggregerar (kombinerar) information, det vill säga att om du lägger in harmlösa personuppgifter i ett AI-verktyg kan resultatet vid en aggregering bli

känslig och ska då hanteras som sådan.

Du är ansvarig

Alla som använder AI-system inom Kommunen har ansvar för att hantera dessa på ett lagligt, säkert och hållbart sätt. Det innebär att du som användare är ansvarig för resultaten, noggrann hantering av data, och rapportering av fel och incidenter. Hållbar AI innebär att användarna på ett ansvarsfullt sätt beaktar etiska och samhälleliga risker med att använda AI. AI-användningen ska präglas av respekt för människors integritet, rättssäkerhet och jämlikhet.

Användaren kan inte överlåta sin yrkesmässiga bedömning till Copilot, eller annat AI-system. Du ansvarar själv för den färdiga texten, vare sig du fått hjälp helt eller delvis av AI.

En grundregel, för att undvika att man råkar dela konfidentiell information, är att aldrig kopiera text från ett annat system in i Copilot. Det går bra att förbereda en text i Word, och ta hjälp av Copilot, för att sedan klistra in texten i det andra systemet.

Användning av öppet tillgänglig information

Använd "sunt förnuft" när du använder en AI-tjänst. Om informationen är externt publicerad och öppet tillgänglig på internet är den troligtvis okej att använda som input till i Copilot. Ta alltid hänsyn till de immateriella rättigheterna, som upphovsrätt, patenträtt, varumärkesrätt, firmarätt. Offentlighetsprincipen och offentlighets- och sekretesslagen (OSL) gäller. Det innebär bland annat innebär att du inte får samköra data mellan nämnder och/eller kommunala bolag hur som helst. Du måste hela tiden beakta sekretess och vad det kan innebära att upprätta allmänna handlingar.

Intern information som endast finns på interna system, som intranät, får inte delas.

Källkritik

Granska alltid svar från AI-tjänster för att säkerställa att informationen är korrekt och lämplig. AI-genererade svar och material ska alltid ses som utkast och bearbetas vidare innan publicering eller användning i officiella sammanhang. Det är alltså en förutsättning att du själv är insatt i det material du matar AI-tjänsten med, för att kunna upptäcka eventuella felaktigheter i svaret.

När man använder Copilot och liknande verktyg är det lätt att få känslan att de är intelligenta och tänkande. Så är det inte. Tekniken är utformad för att generera text som låter rimlig, vilket gör det lätt att missta den för fakta. Stora språkmodeller kan ibland hallucinera, ljuga eller hitta på saker. *Hallucination* kallas det när en stor språkmodell presenterar felaktig information med gott självförtroende trots att de inte står att finna i data.

Det är därför viktigt att du har vetskapen om att du inte ska använda Copilot som en sökmotor

och att du ALLTID måste kvalitetssäkra svaren.

Upphovsrätt och märkning

Vid användning av AI-genererade bilder eller texter ska upphovsrättsregler följas. Om bilder används som är helt eller delvis skapade med AI ska detta anges, för att undvika förvirring eller missförstånd.

AI-genererad media (till exempel bilder, film, musik)

Det är möjligt att skapa bilder med hjälp av Copilot och annan generativ AI. Kommunen ska dock aldrig använda dessa i något offentligt material, som trycksaker, sociala medier eller hemsida. Det samma gäller för all annan form av AI-genererad media. Inom Kommunen ska Copilot endast användas för att redigera, skapa och bearbeta text.

Krav på förklarbarhet och spårbarhet

Det är inte tillåtet att använda Copilot eller annan 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. 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.