



TÖREBODA

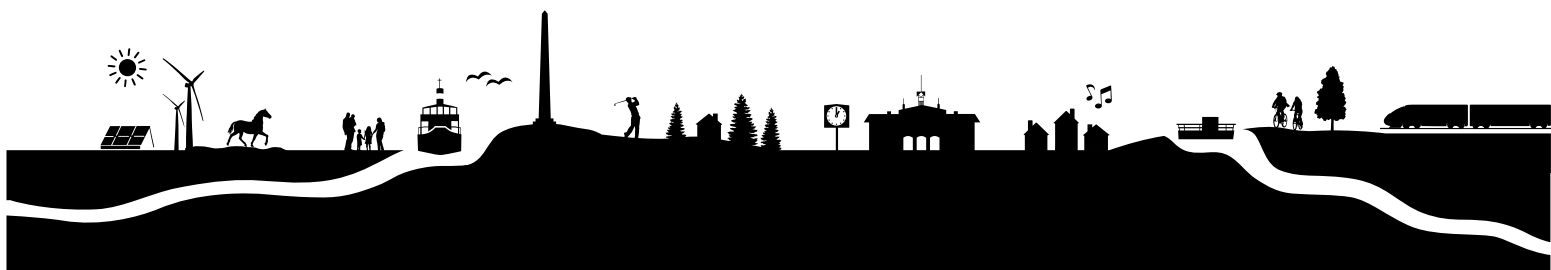
Riktlinje för användning av AI

Beslutande insats: Kommunfullmäktige

Beslutsdatum (inklusive revideringar): 2026-02-23

Dokumentansvarig: Informationssäkerhetsstrateg

Diarienummer: KS 2025/528



Innehåll

Inledning	3
Syfte och mål	3
Mål	4
Om AI	4
Grundläggande etiska principer för AI-användning	4
Likabehandling.....	4
Öppenhet, riskavvägning och rättssäkerhet	4
Ansvar vid användning av AI	5
Integritet och säkerhet (informationssäkerhet).....	5
Ansvar kring personuppgifter i AI (dataskydd).....	5
Ansvar för användare av AI	6
Regler för användning av AI-tjänster	6
Anpassade generativa AI-tjänster.....	6
Copilot webb.....	7
Utvecklad agent i Copilot.....	7
Co-pilot i arbetet.....	8
Allmänt tillgängliga generativa AI-tjänster (öppna AI-tjänster)	9
Utbildning av användare.....	9
Utveckling och inkludering av AI i andra IT-tjänster	10
Revision och uppföljning.....	10

Riktlinje för användning av AI

Denna riktlinje tydliggör vilka AI-tjänster som får användas inom Töreboda kommun och de kommunala bolagen och ger riktlinjer för hur folkvalda, anställda och kontrakterad personal ska förhålla sig när de interagerar med AI.

Riktlinjen ger stöd i vilka krav vi ska ställa när AI utvecklas internt och externt hos leverantörer.

Inledning

AI och speciellt generativ AI kan användas för många olika uppgifter och i det administrativa arbetet kan AI bidra till att skapa enklare, bättre och snabbare processer. Denna möjliga effektivisering kan i sin tur skapa utrymme att omfördela kapacitet till områden där det behövs fler medarbetare. AI-tjänster är kraftfulla verktyg som kan hjälpa till och underlätta inom många av kommunens verksamhetsområden och därmed ett viktigt stöd i kommunens digitalisering.

För att kunna använda AI-tjänster i kommunens processer krävs att det sker med hänsyn till den information som hanteras med hjälp av AI samt gällande författningar, exempelvis Dataskyddsförordningen som reglerar hantering av personuppgifter.

En framgångsfaktor för att lyckas nyttja potentialen i AI är en ökad kunskap om dess förmågor, öka organisationens digitala mognad och minimera obefogade rädslor hos användarna. Det sker genom att uppmuntra till egen omvärldsbevakning och nyfikenhet, erbjuda kompetenshöjande insatser och genomföra olika utforskande verksamhetsprojekt med AI som en komponent.

Syfte och mål

Syftet med denna riktlinje är att tydliggöra hur kommunen och de kommunala bolagen ska förhålla sig till användning av AI. Genom riktlinjen tydliggörs förhållningssätt och grundläggande principer för AI-användning.

Riktlinjen omfattar anpassade generativ AI-tjänster, exempelvis Co-pilot i kommunens M365 och allmänt tillgängliga generativa AI-tjänster.

Riktlinjen kompletterar kommunens informationssäkerhetsriktlinje och riktlinje för hantering av personuppgifter och därtill tillhörande styrdokument och vägledningar.

Mål

Kommunens medborgare, näringsliv och föreningar ska alltid känna sig trygga med att kommunen hanterar deras uppgifter och ärenden på ett ansvarsfullt och säkert sätt. Därför har kommunen upprättat en riktlinje för AI-användning.

Om AI

Töreboda kommun är utforskande och nyfiken på att utveckla arbetssätt med hjälp av ny teknik och ser därför stora möjligheter med AI.

Under de senaste åren har AI fått en allt större betydelse inom olika yrkessektorer, särskilt genom framväxten av generativ AI. Generativ AI bygger på maskininlärning, där stora mängder data samlas in, analyseras och används för att generera svar eller slutsatser baserade på de frågor som ställs.

Med generativ AI menas den typ av artificiell intelligens som skapar nytt innehåll från användarens instruktioner. Det kan exempelvis skriva texter och generera bilder, men också om att sammanfatta dokument, översätta mellan olika språk och skriva programkod. Ju mer kvalitativ information som matas in, desto bättre resultat kan genereras. Ett exempel är Co-pilot som kommunen har tillgång till via M365, andra öppna generativa AI-tjänster är exempelvis ChatGPT och Google Gemini med flera.

Grundläggande etiska principer för AI-användning

De nya möjligheter som generativ AI ger ska utforskas på ett ansvarsfullt sätt genom att väga in följande grundläggande etiska principer för hur kommunen tillämpar AI.

Likabehandling

AI-tjänster ska utformas så att alla individer och grupper behandlas rättvist och jämlikt. Detta innebär att AI-tjänster inte ska diskriminera, utesluta eller skada/missgynna någon på grund av deras identitet, bakgrund eller andra liknande omständigheter. AI-tjänster ska respektera människans värdighet och mångfald och främja social rättvisa och mänskliga rättigheter.

AI-tjänster ska utformas så att de är tillgängliga och inkluderande för alla individer och grupper. Detta innebär att de ska vara användarvänliga, begripliga och lyhörda för användarnas gensvar och synpunkter. AI-tjänster ska vara kulturellt och kontextuellt lämpliga och tillgodose användarnas behov, förmågor och preferenser. De ska möjliggöra deltagande och samarbete mellan användare.

Öppenhet, riskavvägning och rättssäkerhet

Det är viktigt att medvetandegöra risker som ny teknik kan medföra, men också ha insikt i de möjligheter och nyttor som dessa erbjuder. Eventuella risker ska alltid ställas i relation till den potentiella nyttan som användandet av AI kan medföra. Detta innebär att utvärdering och riskavvägning ska ske systematiskt i digitaliseringsprocessen, så införandet av AI-tjänster alltid sker med god medvetenhet om risker, konsekvenser och effekter.

AI-tjänster ska vara transparenta och förståeliga. Detta innebär att det ska finnas tydlig och meningsfull information om deras syfte, funktion och drift. Det ska finnas begripliga och relevanta förklaringar till AI-tjänsters åtgärder och resultat.

AI-tjänster ska vara tillförlitliga och säkra. Detta innebär att AI-tjänster ska fungera som avsett, utan att orsaka skada eller störningar. AI-tjänster ska vara robusta, motståndskraftiga och anpassningsbara till förändrade förhållanden och användarbehov. AI-tjänster ska därför testas och verifieras med avseende på driftssäkerhet, prestanda, kvalitet och noggrannhet i linje med den fastslagna ambitionen för respektive verksamhetsområde.

Ansvar vid användning av AI

Integritet och säkerhet (informationssäkerhet)

Användning av AI förutsätter riskmedvetenhet och adekvat hantering av information. Varje verksamhet ansvarar för att all informationsbehandling görs i enlighet med gällande författning och kommunens styrdokument och anvisningar, exempelvis Riktlinje för informationssäkerhet.

Ansvar kring personuppgifter i AI (dataskydd)

Kommunens nämnder och de kommunala bolagens styrelser är personuppgiftsansvariga när personuppgifter används i AI och ska säkra och följa upp att behandling av personuppgifter sker i linje med gällande lagstiftning och kommunens styrande dokument, exempelvis Riktlinje för hantering av personuppgifter.

Enligt dataskyddsförordningen ska behandling av personuppgifter var dokumenterad i registerförteckningen innan behandlingen får påbörjas. Med behandling avses exempelvis insamling, sammanställning och lagring. Samtidigt får personuppgifter som behandlas med ett ändamål inte behandlas med annat ändamål utan att samtliga registrerade fått information om det nya ändamålet. Behandling som ske i strid med ovanstående kallas otillåten ändamålsglidning. Användning av personuppgifter kan vara tillåten men kräver en designad AI-agent, ett styrt arbetssätt och att behandlingen dokumenteras i aktuell

registerförteckning. En designade AI-agent kan exempelvis utvecklas med hjälp av Copilot.

Om personuppgifter behandlas i en designad AI-tjänst så uppstår oftast ett tillkommande ändamål, effektivitet, som ska dokumenteras i nämndens registerförteckning. Laglig grund kan exempelvis vara allmänt intresse.

Ansvar för användare av AI

En förutsättning för användning av AI i tjänsten är att den sker i linje med gällande lagstiftning och kommunens styrdokument samt i övrigt sker på ett lagligt, hållbart, välvägt och förtroendeingivande sätt.

Användare är de folkvalda, anställda, eller inhyrd personal inom kommunen och de kommunala bolagen, som använder AI.

Följande ska alltid ligga till grund för användning av AI-tjänster inom kommunens verksamheter:

- Användaren ansvarar för de uppdrag som begärs av en AI-tjänst.
- Användaren ansvarar för den information som den delar med en AI-tjänst.
- Användaren ansvarar för hur den använder resultatet från en AI-tjänst. När användaren producerar något med stöd av en AI-tjänst ansvarar användaren för att granska och rätta eventuella fel innan materialet används.
- Användaren ska alltid rapportera eventuella avvikelser, fel eller missbruk enligt kommunens incidentprocess för informationssäkerhet och dataskydd.

Regler för användning av AI-tjänster

Anpassade generativa AI-tjänster

Anpassade AI-tjänster som är anskaffad, skapad eller införd specifikt för kommunens behov och i enlighet med kommunens säkerhetskrav. Copilot ingår som standard i kommunens M365 och designade agenter kan skapas baserat på denna. I dessa generativa AI-tjänster är det användaren eller utvecklaren (av den designade agenten) som aktivt väljer vilken information som delas med Copilot.

Även kommunens elever använder M365 och har därmed tillgång till en version av Copilot. Verksamhetsområdet Barn, utbildning och kultur ska ha interna rekommendationer för hur AI används i skolan.

Copilot webb

Användning av Copilot webb ska ske med följande som utgångspunkt:

1. Information som klassas som öppen exempelvis dokument med **känslighetsetikett 0. Öppen** får delas.
2. Information som klassas som intern exempelvis dokument med **känslighetsetikett 1. Intern får under vissa förutsättningar delas.** Om informationen innehåller personuppgifter så få dessa **inte** delas i Copilot.
3. Information som klassas som begränsad tillgänglig exempelvis dokument med känslighetsetikett **2 Begränsad får under vissa förutsättningar delas.** Om informationen innehåller personuppgifter så få dessa **inte** delas med den generella Copilot.
4. Information som klassas som Extra skyddsvärd exempelvis dokument med **känslighetsetikett 3 Extra skyddsvärd** samt information som är hemlig enligt OSL får **aldrig** delas i Copilot.

Notera att personuppgifter endast får användas i anpassade AI-tjänster om behandlingen är strukturerad, identifierad, har laglig grund och behandlingen är upptagen i nämndens registerförteckning. Vid osäkerhet dela eller efterfråga aldrig personuppgifter via en AI-tjänst.

Utvecklad agent i Copilot

Användning av en utvecklad agent i Copilot ska ske med följande som utgångspunkt:

1. Information som klassas som öppen exempelvis dokument med **känslighetsetikett 0. Öppen** får delas.
2. Information som klassas som intern exempelvis dokument med **känslighetsetikett 1. Intern får under vissa förutsättningar delas.**

Om informationen innehåller personuppgifter ska AI-behandlingen vara upptagen i personansvarigas registerförteckning.

3. Information som klassas som begränsad tillgänglig exempelvis dokument med känslighetsetikett **2 Begränsad får under vissa förutsättningar delas**. Om informationen innehåller personuppgifter så ska AI-behandlingen vara upptagen i personansvarigas registerförteckning.
4. Information som klassas som Extra skyddsvärd exempelvis dokument med **känslighetsetikett 3 Extra skyddsvärd** samt information som är hemlig enligt OSL får **aldrig** delas i Copilot.

Notera att personuppgifter endast får användas i utvecklade agenter om behandlingen är strukturerad, identifierad, har laglig grund och behandlingen är upptagen i nämndens registerförteckning. Vid osäkerhet dela eller efterfråga aldrig personuppgifter via en AI-tjänst.

Co-pilot i arbetet

Licensen Copilot i arbetet är ett tillägg mot kostnad som kan göras för enskilda användare. Copilot i arbetet medför att AI-tjänsten "ärver" användarens gällande behörighet till information inom samtliga funktioner i M365 och med det kommer några utmaningar:

1. Användaren kan inte ta ett aktivt ansvar för vad som delas med AI-tjänsten utan ansvaret kommer indirekt att vila på de som beviljar användarens behörighet till olika delar av M365, och
2. om användaren har tillgång till personuppgifter, vilket är mycket vanligt förekommande i kommunens verksamheter, uppstår otillåten ändamålsglidning¹ och verksamheten behandlar personuppgifter i strid mot dataskyddsförordningen.

På grund av ovanstående gäller följande **regler för licensen Copilot i arbetet**:

- Du som tilldelats licensen Copilot i arbetet får **inte** aktivt söka efter personuppgifter eller sammanställa personuppgifter via Copilot.
- Licensen Copilot i arbetet får endast tilldelas efter behov och främst till administrativa befattningar.

För att använda den utökade Co-pilot licensen ska även andra lämpliga och proportionerliga tekniska säkerhetsåtgärder vidtas för att undvika otillåten ändamålsglidning.

Allmänt tillgängliga generativa AI-tjänster (öppna AI-tjänster)

Allmänt tillgängliga generativa AI-tjänster är de som är tillgängliga för vem som helst exempelvis via Internet eller en mobil app, exempelvis ChatGPT, Google Gemini och många andra.

Information som delas i dessa "öppna" AI-tjänster används ofta för träning av AI-tjänsterna och samtidigt är risken hög att information delas utanför Sverige eller EU. När dessa "öppna" AI-tjänster är gratis är anledningen att leverantören i stället drar nytta av den information som delas i tjänsten och återanvänder den.

Användning av allmänt tillgängliga AI-tjänster ska undvikas eftersom all information som delas med dessa kan betraktas som röjd till omvärlden.

Om allmänna tillgängliga AI-tjänster ändå används så har användaren ett personligt ansvar för att detta endast sker under följande förutsättningar:

- Personuppgifter, känsliga personuppgifter, uppgifter som omfattas av sekretess och/eller annan känslig information får **aldrig** delas,
- Användare ska utbildas i riskerna vid användning av dessa "öppna" AI-tjänster,
- Användare ska även vara välbekanta med vad personuppgifter är, och
- Användare får enbart dela annan information än personuppgifter som klassas som öppen (etikett 0. Öppen).

Notera att de inloggningsuppgifter som tilldelas av kommunen får **inte** användas för att skapa konton i allmänt tillgängliga generativa AI-tjänster.

Utbildning av användare

Utbildning av användare ska göras innan AI-tjänster används av verksamheten. Utbildningen ska minst omfatta:

- Användarens ansvar vid användning av AI-tjänster
- Riskerna vid användning av AI-tjänster
- Behandling av personuppgifter i relation till AI-tjänster

En kommungemensam utbildning kring AI-tjänster ska tas fram, men även verksamhetsspecifik utbildning ska tas fram av respektive verksamhet när användning av AI-tjänster införs i specifika verksamhetsprocesser.

AI-utbildningen ska ingå i kommunens introduktionsutbildning.

Utveckling och inkludering av AI i andra IT-tjänster

Innan kommunen utvecklar egna AI-tjänster ska den aktuella information som ska behandlas i den nya tjänsten klassas och en riskanalys kring behandlingen ska genomföras, så krav och risker för exempelvis personuppgifter eller annan känslig information åtgärdas innan AI-tjänsten driftsätts. AI-tjänsten ska även registreras i kommunens AI-register. Ta kontakt med informationssäkerhetssamordnare eller informationssäkerhetsstrateg för att få stöd innan avtal tecknas med leverantörer.

Många IT-leverantörer överväger idag hur AI kan inkluderas i deras IT-tjänster. I de fallen där leverantörer genom extern drift har åtkomst till kommunens information får leverantörerna endast träna sina nuvarande eller kommande AI-funktioner på kommunens information efter uttryckligt tillstånd från informationsägaren. Innan ett sådant tillstånd ges skall informationsägaren genomföra eller uppdatera klassning av informationen som leverantören vill använda samt genomföra en riskanalys för att i första hand säkerställa att samtliga krav och risker kring behandling av personuppgifter enligt dataskyddsförordningen efterlevs. I andra hand att krav och risker kring annan känslig information åtgärdas.

Revision och uppföljning

Denna riktlinje ska revideras minst vart fjärde år eller vid behov.

Efterlevnad av riktlinje ska följas upp vartannat år via enkät till användarna.