



Riktlinje för hantering av information i AI-tjänster

<u>Diarienummer</u> 2025/74	<u>Fastställd av</u> Kommunstyrelsen	<u>Datum för fastställande</u> 2025-08-26
<u>Dokumenttyp</u> Riktlinje	<u>Dokument gäller för</u> Alla nämnder och helägda bolag	<u>Giltighetstid</u> Tills vidare
<u>Revideringsansvarig</u> Kommunstyrelsen	<u>Revideringsintervall</u> Vart fjärde år	<u>Reviderad datum</u>
<u>Dokumentansvarig (funktion)</u> Säkerhetschef	<u>Uppföljningsansvarig</u> Respektive nämnd och bolag.	<u>Uppföljning</u> Inom ramen för intern kontroll och revision.



1 Syfte

Utvecklingen inom AI (Artificiell intelligens) innebär förändrade förutsättningar för kommunens verksamheter. Genom AI förstärks förmågan att utföra komplexa uppgifter och hantera stora mängder data vilket ger goda förutsättningar för ökad effektivitet. Samtidigt medför utvecklingen på AI-området att hotaktörers förmåga ökar.

Denna riktlinje syftar till att vägleda medarbetare och förtroendevalda för laglig och säker användning av tjänster som innehåller AI. Genom riktlinjen tydliggörs ansvaret för informationshantering vid användning av AI-tjänster.

2 Riktlinje

2.1 Grundläggande principer

- Användning av AI-system innebär oftast att information matas in i systemet, vilket ställer krav på användarens hantering av informationen. För att säkerställa att informationen hanteras på ett korrekt och säkert sätt ska all information som hanteras vara klassad. Klassningen ska vara gjord i enlighet med kommunens klassningsmatris och utgör grunden för hur informationen får lagras, bearbetas och delas.
- Oavsett vilket AI-system som används så gäller att medarbetaren/den förtroendevalda ansvarar för den information som matas in i AI-systemet. Motsvarande gäller för hur resultatet från AI-systemet används.
- Avvikelser, felaktigheter eller missbruk ska inrapporteras i kommunens ordinarie kanaler för incidentrapportering för informationssäkerhet och dataskydd.
- Var restriktiv och tänk igenom syftet innan upphovsrättsskyddat material matas in i ett AI-system. Det är inte tydligt i lagstiftning och praxis om det är tillåtet eller otillåtet att mata in upphovsrättsskyddat material i ett AI-system. Många gånger är det användaren, och inte leverantören av systemet som gör sig skyldig till upphovsrättsbrott om det skulle visa sig att det är olagligt.

2.2 Att använda AI-system

- Det är inte tillåtet att mata in personuppgifter, sekretessbelagd information eller annan känslig information i AI-system som är allmänt tillgängliga på internet.
- För AI-tjänster som är allmänt tillgängliga på internet gäller de användarvillkor som accepteras när systemet används. Därför får allmänt tillgängliga AI-system endast användas för öppen information, klass 0 enligt kommunens klassningsmatris.
- Ge aldrig ett allmänt tillgängligt AI-system åtkomst till information på din enhet eller direktåtkomst till ditt konto i annan tjänst.



- När kommunen anskaffar AI-system ställs krav på systemet utifrån skyddsbehovet hos den information som ska hanteras i systemet. Därför kan det vara tillåtet att i vissa AI-tjänster hantera information som kategoriserats i högre klasser enligt kommunens klassningsmatris. Vilka förvaltningsövergripande AI-system som är godkända för hantering av olika informationsklasser framgår på intranät.
- Den som beslutar om att använda AI ansvarar för att tydligt kommunicera när och hur AI används i verksamheten. Om svar, texter, bilder, video eller ljud är automatiskt genererade av AI, ska det alltid framgå, särskilt när det finns en risk för att innehållet kan förväxlas med verkliga händelser eller personer.
- Kontrollera alltid resultat från AI-system innan de används.
- Ett AI-system ska aldrig tillåtas att fatta helt självständiga beslut – mänsklig kontroll ska vara ett givet moment i dessa fall.

2.3 Anskaffa och införa AI-system

Anskaffning och införande av AI-system ska följa det regelverk som gäller vid den ordinarie anskaffningsprocessen för system och regleras inte i denna riktlinje.

3 Definitioner, hänvisningar och avgränsningar

3.1 Definitioner

Artificiell intelligens, är en gren inom datavetenskap som fokuserar på att skapa system och program som kan utföra uppgifter som normalt kräver mänsklig intelligens. Detta inkluderar saker som att förstå språk, lösa problem, lära sig från data, och fatta beslut.

AI-system – med ordet “system” avses appar, programvaror samt andra digitala tjänster och verktyg. Med “AI-system” avses system innehållande större eller mindre inslag av artificiell intelligens (AI).

Ett allmänt tillgängligt AI-system är ett AI-baserat system eller verktyg som är öppet för användning av allmänheten via exempelvis webbläsare, appar eller molntjänster – utan särskilda krav på avtal, behörighetsstyrning eller autentisering. Systemet är inte utvecklat eller upphandlat av kommunen och är inte informationsklassat enligt kommunens riktlinjer för informationssäkerhet.

Med personuppgifter avses all slags information som på något sätt kan hänföras till en fysisk person som är i livet. Exempel på personuppgift kan vara namn, bilder, ip-adress, anställningsnummer med mera.



3.2 Hänvisningar

Viss information kan omfattas av sekretess. Vilken typ av information som hos myndigheter ska omfattas av sekretess regleras i offentlighets- och sekretesslagen.

Lag om informationssäkerhet för samhällsviktiga och digitala tjänster hanterar krav på säkerhet i nätverk och informationssystem inom utpekade sektorer. Utöver lagen finns förordning om informationssäkerhet för samhällsviktiga och digitala tjänster och ett antal föreskrifter från Myndigheten för samhällsskydd och beredskap (MSB). Cybersäkerhetslagen föreslås ersätta lag om informationssäkerhet för samhällsviktiga och digitala tjänster under 2025.

Genom dataskyddsförordningen (GDPR) och där tillhörande lagar skyddas människor mot att deras personliga integritet kränks vid behandling av personuppgifter. Förordningen innehåller också regler om vilka tekniska hjälpmedel och säkerhetsåtgärder som behöver vidtas vid hantering av personuppgifter.

AI-förordningen reglerar utveckling, tillhandahållande och användning av AI. AI-system regleras med en riskbaserad modell där vissa användningsfall ska förbjudas och annat tillåts med restriktioner och krav i form av bland annat tillsyn och registrering.

Kommunfullmäktige har antagit en säkerhetspolicy som anger inriktning och ramar för kommunens säkerhetsarbete. Därtill finns ytterligare riktlinjer, råd och anvisningar inom informationssäkerhetsområdet. Denna riktlinje bör läsas vid sidan om dessa.

4 Ansvar och uppföljning

Kommunstyrelsen ansvarar för att leda, samordna och utveckla kommunens strategiska informationssäkerhetsarbete.

Varje nämnd och bolagsstyrelse är ytterst ansvarig för informationssäkerheten, inklusive personuppgiftsansvarig, inom sitt verksamhetsområde. Vid behov kan varje nämnd och styrelse besluta om mer detaljerade anvisningar inom ramen för denna riktlinje.

Ansvar för informationssäkerheten följer det ordinarie verksamhetsansvaret. Detta innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet.

Kommunstyrelseförvaltningens säkerhetsenhet och kanslienhet fungerar som stöd i arbetet med informationshantering medan utvecklingsavdelningen stöttar vid digitalisering och verksamhetsutveckling med hjälp av AI. Serviceförvaltningens IT-enhet bistår med stöd gällande IT-säkerhet.

Dataskyddsombudet och övriga som arbetar specifikt med personuppgiftsbehandlingar, t ex personuppgiftssamordnarna, fungerar som stöd i arbetet avseende information innehållande personuppgifter. Ombudets roll är också att kontrollera att dataskyddsförordningen (GDPR) följs inom organisationen.



En bärande princip i GDPR är ansvarsskyldighet. Det innebär att kunna visa att man har kontroll på att hanteringen av personuppgifter är i linje med skyddskraven. Vid riskfylld hantering är det särskilt viktigt att ha regelbunden uppföljning på att skyddet håller måttet. Det går även i linje med AI-förordningens bestämmelser om löpande övervakning och monitorering av att AI-lösningen fungerar som den ska. Särskilda krav ställs på den ansvarige vad gäller dokumentation för att kunna påvisa ansvarsskyldighet och regelefterlevnad.

Varje medarbetare och förtroendevald ansvarar för att följa gällande styrdokument för informationssäkerhet samt rapportera informationssäkerhetsrelaterade brister och incidenter.