Kungsbacka

Regler för AI

Dokumentegenskaper:	Titel: Regler för AI
Beslutad av:	Digitaliseringschef, 2024-12-02
Gäller från:	2024-12-02
Ansvarig förvaltning:	Kommunstyrelsens förvaltning
Kontakt:	Kungsbacka direkt 0300-83 40 00 | info@kungsbacka.se Kungsbacka kommun, 434 81 Kungsbacka www.kungsbacka.se

Regler för AI

1 Inledning

Artificiell intelligens (AI) är ett område som väcker allt större intresse och påverkar vårt samhälle på många sätt.

I Kungsbacka kommun är vi nyfikna och vågar effektivisera och utveckla våra arbetssätt med hjälp av ny teknik. Samtidigt måste vi vara ansvarsfulla när vi utforskar de nya möjligheter som tekniken ger oss. För alla nya teknologier måste vi vara medvetna om riskerna, och samtidigt ha insikt om de möjligheter de erbjuder oss.

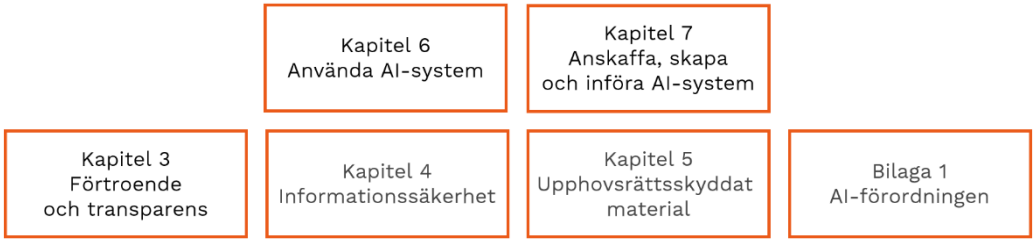
Du uppmuntras att vara nyfiken på den ny tekniken och att prova den på ett klokt sätt. På samma sätt som med alla digitala system är du ansvarig för ditt eget handlande när du använder AI-system.

- Du har ansvar för den information som du matar in i ett AI-system
- Du har ansvar för hur du använder resultatet från ett AI-system

Reglerna i det här dokumentet syftat till att göra dig som medarbetare trygg i hur du kan använda AI i ditt arbete. Reglerna grundar sig till stor del i de lagar, förordningar och regler som kommunen, dess chefer och medarbetare redan lyder under.

Förtroende, transparens och informationssäkerhet är några viktiga aspekter. EU:s AI-förordning lägger ytterligare ett lager ovanpå detta. Vissa regler i detta dokument handlar om system som är högrisk eller förbjudna enligt AI-förordningen. Vad det är framgår av *bilaga 1 AI-förordningen – sammanfattning*.

Reglerna gäller för alla medarbetare i Kungsbacka kommun.



Kapitel 3,4, 5 och bilaga 1 utgör grunden för reglerna i kapitel 6 och 7

Kapitel 2 innehåller definitioner av begrepp som används i dokumentet.

Kapitel 3, 4 och 5 handlar om förtroende och transparens, informationssäkerhet och upphovsrätt, områden som utgör grunden för reglerna i de efterföljande kapitlen.

Kapitel 6 innehåller regler kring hur du får använda ett AI-system i ditt dagliga arbete.

Kapitel 7 innehåller regler som handlar om att anskaffa, skapa eller införa ett AI-system.

Bilaga 1 innehåller en sammanfattning av de viktigaste reglerna i AI-förordningen.

2 Definitioner

Artificiell intelligens (AI) - Ett AI-system är ett maskinbaserat system som, för uttryckliga eller underförstådda ändamål, utifrån de indata det tar emot drar slutsatser om hur man genererar utdata, t.ex. förutsägelser, innehåll, rekommendationer eller beslut som kan påverka fysiska eller virtuella miljöer.

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). Om det specifikt handlar om generativ AI är detta utskrivet.

Generativ AI – AI-system som kan skapa nytt material baserat på enkla instruktioner eller exempel kallas för generativ AI, eller skapande AI. Det finns en stor mängd AI-baserade datorprogram, system och IT-tjänster som genererar nytt material i form av till exempel text, bild, video och programmeringskod. Många av dem är tillgängliga via internet för allmänheten.

Allmänt tillgängliga AI-system – AI-system som är tillgängliga för vem som helst att använda t.ex. via webbsida eller via en app. Allmänt tillgängliga AI-system är inte anskaffade, skapade eller införda specifikt för kommunens behov och är därför inte heller granskade av kommunen.

Öppen information – information som är tillgänglig för alla utan några begränsningar.

Leverantör – enligt AI-förordningen är en leverantör den som utvecklar ett AI-system, släpper ut ett AI-system på marknaden eller tar ett AI-system i bruk under eget namn eller varumärke.

Känsliga personuppgifter – uppgifter om ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening, hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter och biometriska uppgifter som entydigt identifierar en person.

Särskilt skyddsvärda personuppgifter – uppgifter som på grund av sin karaktär är extra viktiga att skydda, även om de inte definieras som känsliga personuppgifter i Dataskyddsförordningen. Personnummer, vissa uppgifter om ekonomiska förhållanden, omdömen och värderingar av en person såsom social förmåga, inlärningsförmåga och liknande, provresultat, resultat av personlighetstester och annan information som ligger nära den privata sfären är exempel på extra skyddsvärda personuppgifter.

3 Förtroende och transparens

I Sverige finns det ett högt förtroende för offentlig sektor. För att bevara eller stärka förtroendet när offentlig sektor använder AI måste AI användas på ett ansvarfullt sätt, med stöd av välutvecklade processer, ett systematiserat arbetssätt och med god dokumentation.

Kommunens verksamheter måste alltid följa den lagstiftning som gäller. I verksamhet som är lagstyrd behöver man analysera om det man tänkt göra är lagligt innan man börjar använda AI-systemet.

För att upprätthålla förtroendet för offentlig sektor finns det i Sverige bestämmelser som ger rätt till insyn.

Sverige har med offentlighetsprincipen ett väl utvecklat system för transparens inom offentlig sektor. En förutsättning är att allmänna handlingar ska diarieföras eller hållas ordnade så att de kan begäras ut. Därför måste det övervägas om det skapas nya allmänna handlingar genom användning av AI-systemet och hur de i så fall ska lagras och diarieföras.

Enligt förvaltningslagen är det ett krav att en myndighet ska motivera sina beslut och förklara vad som gjort att myndigheten nått sin slutsats. Därför behöver varje verksamhet som använder ett AI-system på ett sätt som påverkar kommunens invånare eller brukare kunna förstå och förklara sitt AI-systems inre funktioner på en lämplig nivå. Utmaningen ligger i att ett AI-system kan bestå av tusentals, eller till och med miljontals, numeriska värden, värden som AI-systemet lär sig under dess träningsfas. Det är därför ofta inte möjligt, ens för den som utvecklat systemet, att förklara exakt hur systemet når en viss slutsats. Därför kan det i vissa sammanhang vara olämpligt att använda AI av det skälet.

En verksamhet som använder ett AI-system på ett sätt som påverkar kommunens invånare eller brukare behöver kunna förstå och förklara sitt AI-systems inre funktioner.

Det är i dagsläget inte lämpligt att använda AI-system för att helt automatisera beslut i ärenden.

En verksamhet som använder ett AI-system behöver ta ställning till om AI-systemet skapar nya allmänna handlingar och hur de i så fall ska lagras och diarieföras.

Se även ”Automatisera lagligt – handbok i automatisering av ärendehandläggning och beslut”

4 Informationssäkerhet

I de flesta fall kräver användningen av ett AI-system att du matar in någon form av information i AI-systemet. Kommunens information är en av våra viktigaste tillgångar. Vår information omfattas av lagstiftning som rör bland annat personuppgiftsbehandling och sekretesskydd. Det finns även annan information som kan leda till skada om den sprids på fel sätt. Kommunens information ska vara informationsklassad och hanteras i system som är godkända utifrån informationsklassen. Det gäller även AI-system.

När kommunen anskaffar eller utvecklar system kan vi ställa krav på systemet utifrån den information som ska hanteras i det. Det kan inte kommunen när det gäller allmänt tillgängliga system som var och en kan använda. Där gäller i stället de användarvillkor du accepterar när du använder systemet.

Du bör vara medveten om *hur* AI-systemet och dess leverantör kan komma åt och använda den information som du matar in i systemet. Du måste veta om leverantören garanterar att den information som du matar in i AI-systemet inte används för att träna systemet, eller om det finns risk att den information som du matar in återanvändas i svar som ges till andra användare. Eftersom det innebär att den kan spridas helt öppet.

Nedan kan du läsa om vad som gäller för behandling av personuppgifter, sekretessbelagd information och annan känslig information i AI-system.

Allmänt tillgängliga AI-system får enbart användas för öppen information.

Hanteringen av personuppgifter och sekretessbelagd information omfattas av lagregler som måste följas. Det gäller även vid användning av AI-system.

Se även "Regler för informationssäkerhet för medarbetare och förtroendevalda"

4.1 Personuppgifter

Att mata in personuppgifter i ett AI-system är att behandla personuppgifter. All behandling av personuppgifter ska följa de grundläggande principerna i GDPR. Det finns information om de grundläggande principerna på Insidan bland sidorna om dataskydd. Om och hur principerna uppfylls måste analyseras *innan* AI-systemet används för den tänkta behandlingen. Eftersom AI är en ny teknik ska det i de flesta fall också göras en konsekvensbedömning enligt GDPR innan personuppgifter används i ett AI-system. För att ta ställning till om en konsekvensbedömning behövs, görs en så kallad *tröskelanalys.* Om det inte har gjorts en analys av behandlingen utifrån GDPR är det olagligt att mata in personuppgifter i ett AI-system. Dataskyddskontakten på din förvaltning ska alltid kontaktas innan personuppgifter behandlas på ett nytt sätt.

När det gäller allmänt tillgängliga AI-system saknas tillräckliga möjligheter för kommunen att kontrollera leverantörens behandling eller säkerhet.

Allmänt tillgängliga AI-system levereras ofta som molntjänster av utländska företag. Samma lagar och regler gäller vid användning av AI-system i molnet som för andra typer av molntjänster.

Innan personuppgifter matas in i ett AI-system måste det göras en tröskelanalys och eventuell konsekvensbedömning av behandlingen enligt GDPR.

Personuppgifter får inte matas in i allmänt tillgängliga AI-system.

Se även: "Dataskyddsombudens råd inför användning av AI"

4.2 Sekretess

Enligt offentlighets- och sekretesslagen får information som omfattas av sekretess inte *röjas* för utomstående. När information delas med en IT-leverantör, till exempel genom att laddas upp i en molntjänst, är informationen röjd. Om informationen är krypterad på ett sådant sätt att leverantören inte kan göra den läsbar är den dock inte röjd. Det är dock mycket svårt att kryptera på ett sätt som leverantören inte kan avkryptera. Att röja sekretessbelagd information är bara tillåtet om det finns en sekretessbrytande bestämmelse.

Om du röjer sekretessbelagda uppgifter genom att mata in dem i ett AI-system kan det vara straffbart enligt brottsbalken som *brott mot tystnadsplikten*.

För att avgöra om det är tillåtet att mata in sekretessbelagda uppgifter i ett AI-system behöver det göras en teknisk och juridisk analys.

Mata aldrig in sekretessbelagd information i ett AI-verktyg som inte har analyserats och konstaterats vara säkert för sådan information.

Sekretessbelagd information får inte matas in i allmänt tillgängliga AI-system.

4.3 Annan känslig information

Annan känslig information är till exempel information som, om den kommer i fel händer, riskerar skada individer, grupper av individer eller kommunen i allmänhet. Det kan röra sig om information från interna möten eller preliminära bedömningar i olika ärenden. Allmänt tillgängliga AI-system som använder inmatad information för att träna systemet, kan ta med din information i svar till andra användare. Det vill säga: den information som du matar in riskerar att göras tillgänglig för andra.

Mata aldrig in annan känslig information i ett AI-verktyg som inte har analyserats och konstaterats vara säkert för sådan information. Annan känslig information får inte matas in i allmänt tillgängliga AI-system.

5 Upphovsrättsskyddat material

Det är inte tydligt i lagstiftning och praxis om det är tillåtet eller otillåtet att mata in upphovsrättsskyddat material i ett AI-system. Det kan vara tillåtet enligt ett undantag i 2 kap 15a § upphovsrättslagen, men det är inte rättsligt prövat.

I de användarvillkor som man godkänner när man använder ChatGPT och Copilot anges att man själv ansvarar för att inte bryta mot någon annans upphovsrätt. Det innebär att det är du själv, och inte leverantören av systemet som gör sig skyldig till upphovsrättsbrott om det skulle visa sig att det du gör strider mot upphovsrätten. Var därför försiktig och tänk igenom om du verkligen behöver mata in upphovsrättsskyddat material. Andra system kan ha andra villkor.

Det kan vara bra att veta att författningar (som lagar, förordningar och föreskrifter), beslut av myndigheter och yttranden av myndigheter inte omfattas av upphovsrätt.

En annan fråga som inte är rättsligt klarlagd är om bilder och texter som genererats av AI skyddas av upphovsrätt eller ej.

Du som använder generativ AI för att skapa material har med största sannolikhet inte upphovsrätt till bilden eller texten, utan det står andra fritt att använda bilden som de vill. Men det här är inte heller rättsligt klarlagt ännu.

De som tillhandahåller systemet har troligtvis inte heller upphovsrätt till innehåll som genererats. Av användarvillkoren till ChatGPT och Copilot framgår dessutom att företagen bakom de tjänsterna inte gör anspråk på upphovsrätt till innehållet som du skapat, utan det står dig fritt att använda materialet som du vill.

Tillhandahållare av generativa AI-system tar dock inte ansvar för om det resultat som generas är väldigt likt ett upphovsrättsskyddat verk. Eftersom modellerna är tränade på material från internet kan resultaten bli väldigt likt en bild eller text som är vanlig på internet. Av användarvillkoren till både Copilot och till OpenAI (som tillhandahåller ChatGPT och Dall-E) framgår att du som användare är ansvarig om du använder AI-genererat material på ett sätt som strider mot någon annans upphovsrätt. Det innebär att om du sprider en AI-genererad bild eller text som är för lik någons upphovsrättsskyddade verk kan du begå ett upphovsrättsbrott och bli skadeståndsskyldig.

6 Att använda AI-system

Oavsett om AI-systemet som du använder är tillgängligt för allmänheten, är av typen generativ (skapande) AI eller om AI-systemet är anskaffat, skapat eller infört specifikt för kommunens behov så gäller två grundläggande saker:

Du har ansvar för den information som du matar in i AI-systemet (se kapitlet om informationssäkerhet).

Du har ansvar för hur du använder resultatet från AI-systemet.

6.1 Allmänt tillgängliga AI-system

I takt med teknikutvecklingen lanseras nya AI-system som görs allmänt tillgängliga för användning. Allmänt tillgängliga AI-system kan tillföra värde för kommunen genom att underlätta vissa arbetsuppgifter och effektivisera arbetet.

Utöver det som framgår i kapitlet om informationssäkerhet och upphovsrätt måste du även tänka på följande innan du använder ett allmänt tillgängligt AI-system:

Du som använder systemet accepterar de användarvillkor som gäller för systemet. Du personligen är ansvarig för att känna till och följa villkoren. Vid osäkerhet om användningen, fråga din närmaste chef eller dataskyddskontakten på din förvaltning.

Eftersom kommunen inte har något avtal med leverantören av allmänt tillgängliga AI-system finns det ingen möjlighet för kommunen att påverka eller få insyn i leverantörens användning av informationen i AI-systemet. Det är du personligen som godkänner de villkor som gäller för systemet. Det är därför du personligen som tar ansvar för den information du lämnar ifrån dig och att leverantören använder informationen på det sätt som framgår av villkoren. Du använder alltså ett allmänt tillgängligt AI-system på egen risk och på eget ansvar.

Tänk på att det är svårt att veta exakt vad ett AI-system gör. Vad vet du om det AI-systemet som du tänkt att använda? Gör systemet det som du tänkt dig och uppfyller det de krav på kvalitet som krävs för uppgiften? Du personligen är ansvarig för resultatet. Ju mindre du vet om systemet, desto större risk tar du.

AI-baserade chattbotar levereras ofta av utländska företag som molntjänster. Samma lagar och regler gäller vid användning av AI-system i molnet som för andra typer av molntjänster.

Du som använder systemet accepterar de användarvillkor som gäller för systemet.

Du personligen är ansvarig för att känna till och följa villkoren.

Använd aldrig ett allmänt tillgängligt AI-system som stöd för beslutsfattande eller som en del av ärendehandläggningen.

Använd inte ett AI-system som är helt nytt eller kommer från en okänd avsändare i ditt arbete.

Ge aldrig ett allmänt tillgängligt AI-system åtkomst till information på dina enheter som arbetstelefon och dator.

Allmänt tillgängliga AI-system får enbart användas för öppen information.

Du får under inga omständigheter mata in personuppgifter, sekretessbelagd information eller annan känslig information i AI-system tillgängliga för allmänheten.

Du får inte använda allmänt tillgängliga AI-system för ändamål som är förbjudna eller högrisk enligt AI-förordningen.

6.2 ChatGPT

ChatGPT är varken informationsklassat eller konsekvensbedömt. Det tillhandahålls som en molntjänst som saknar möjligheter att få insyn i eller ställa krav på. Oavsett om du använder gratisversionen, har köpt betalversionen privat eller har fått tillgång till den via arbetsgivaren gäller reglerna för allmänt tillgängliga AI-system när du använder ChatGPT.

6.3 Microsoft Copilot

Microsoft Copilot är Microsofts digitala assistent med AI-teknik. Den är en del av kommunens Microsofts 365-miljö (M365) vilket innebär att den information du matar in i denna digitala assistent hanteras i Microsofts molntjänst på samma sätt som informationen i OneDrive eller Outlook. På samma sätt som med övriga produkter i M365 får känsliga personuppgifter, särskilt skyddsvärda personuppgifter och sekretessbelagda uppgifter inte behandlas i Microsoft Copilot.

När du använder Microsoft Copilot inloggad med ditt Kungsbacka kommun-konto räknas det *inte* som allmänt tillgängliga AI-system. I inloggat läge får du en ikon formad som en sköld. Om du inte är inloggad med ditt Kungsbacka kommun-konto gäller reglerna för allmänt tillgängligt AI-system.

Varje förvaltning måste ta ställning till i vilken mån det finns laglig grund för att behandla personuppgifter i Microsoft Copilot, och i så fall för vilka ändamål. (Den *tekniska* säkerheten för M365, och därmed också för Microsoft Copilot, är tillräcklig för att behandla personuppgifter som inte är känsliga eller särskilt skyddsvärda.)

Känsliga personuppgifter, särskilt skyddsvärda personuppgifter och sekretessbelagda uppgifter får inte behandlas i Microsoft Copilot.

Du får inte använda Microsoft Copilot för ändamål som är förbjudna eller högrisk enligt AI-förordningen.

Se även: ”Regler för hantering av information i Kungsbacka kommuns digitala samarbetsplattform Microsoft 365”

6.4 Använda resultatet från generativ (skapande) AI

AI-system som kan skapa nytt material baserat på enkla instruktioner eller exempel kallas för generativ AI, eller skapande AI. Du ansvarar för resultatet som AI-systemet har skapat, därmed måste du också kontrollera det.

Du behöver vara medveten om hur generativ AI skapar sitt resultat och att resultatet kan vilseleda. Det vill säga du behöver vara medveten om potentialen för felaktig information från dessa generativa AI-system.

De generativa AI-systemen är inte sökmotorer, de är däremot väldigt duktiga på att skapa nytt trovärdigt material utifrån dina instruktioner, till exempel att skapa ny text. För att skapa ny text använder sig det generativa AI-systemet av en språkmodell som, baserat på sannolikhet, beräknar vilket kommande ord som är mest troligt. De

generativa AI-systemen kan också erbjuda olika svar på samma fråga om den ställs mer än en gång, och de kan hämta sina svar från källor som du inte skulle lita på i andra sammanhang.

Att texten som det generativa AI-systemet har skapat ser trovärdig ut är inte samma sak som att den är faktamässig korrekt, att den har rätt tonalitet eller att den är fri från fördomar eller annan bias. Behandla alltid de resultat som dessa generativa AI-system producerar som ett utkast.

Du är alltid ansvarig för att texten är faktamässigt korrekt, har rätt tonalitet och är fri från fördomar och annan bias.

Du kan inte överlåta din yrkesmässiga bedömning till ett generativt AI-system.

Du ansvarar för texten som om du själv hade skrivit den.

7 Att anskaffa, skapa och införa AI-system

Att anskaffa eller skapa nya AI-system, eller att införa befintliga AI-system i nya verksamheter är en del i Kungsbacka kommuns digitaliseringsarbete och integreras med övrig styrning och utveckling i kommunen. Genom att vi anskaffar, skapar och inför AI-system enligt befintliga processer och metodiker säkerställer vi också att alla relevanta aspekter utreds.

När kommunen anskaffar eller själv skapar AI-system utvärderas systemets och leverantörens förmåga att skydda informationen. Det ställs också krav på funktioner och avtalsvillkor som säkrar kommunens kontroll över informationen.

En viktig del av processen är att säkerställa att AI-systemet är tillräckligt transparent och uppfyller de krav som behöver ställas utifrån tillämplig lagstiftning. Tillämplig lagstiftning kan vara den speciallagstiftning som gäller för verksamheten, offentlighets- och sekretesslagen, GDPR, förvaltningslagen, kommunallagen och lagstiftning om cybersäkerhet och EU:s AI-förordning.

Befintliga processer och metodiker anpassas kontinuerligt utefter ny teknik, direktiv och lagstiftning.

7.1 AI-system som är högrisk enligt AI-förordningen

Det ställs extra höga krav på högrisk AI-system enligt AI-förordningen. Därför är det viktigt att tidigt avgöra om det tänkta användningsområdet utgör högrisk eller inte.

När kommunen använder ett högrisk AI-system i sin verksamhet har kommunen rollen som *tillhandahållare* enligt AI-förordningen. Det innebär att det tillkommer krav, både som vi behöver ställa på leverantören, och som behöver uppfyllas av kommunen vid användningen av systemet.

När kommunen i stället skapar eller utvecklar ett högrisk-AI-system kan man komma att klassas som leverantör och då ställs ännu högre krav på oss. Bland annat krävs omfattande dokumentation, uppföljning och nya arbetssätt. Kungsbacka kommun har i dagsläget inte de resurser som krävs för att kunna leva upp till de krav som ställs på en *leverantör* enligt AI-förordningen. Kommunen ska därför inte skapa egna högrisksystem och därmed ta på sig rollen som leverantör av ett högrisk-AI-system.

Vid anskaffning av AI-system med hög risk behöver särskilda krav ställas på leverantören. Vid samarbeten om utveckling av AI-system med hög risk måste det

säkerställas att någon annan aktör än kommunen tar på sig rollen som *leverantör* enligt AI-förordningen. Se mer i bilaga 1.

Befintliga processer och metodiker för digitaliserings- och innovationsarbete gäller och ska användas, oavsett om den tänkta lösningen innehåller AI eller inte.

Ta alltid ställning till om AI-systemet är förbjudet eller kommer att klassas som högrisk enligt AI-förordningen. Bedömningen ska dokumenteras oavsett vad slutsatsen är. Vid osäkerhet, kontakta kommunjurist.

Om systemet klassas som högrisk kontakta digitaliseringsenheten.

7.2 Skapa AI-system i Power Platform

Det finns flera möjligheter att skapa eller utveckla egna AI-system. Power Platform som är en molnbaserad ”low-code” plattform från Microsoft och en del i vår M365-miljö ger möjligheter att skapa egna AI-system. Plattformen gör det lätt att komma i gång med att utforska AI i olika sammanhang samt att på ett enkelt sätt ta en idé till något som kan testas och utvärderas.

Plattformen innehåller många olika byggblock och fler AI-tekniker tillkommer i takt med teknikens utveckling. När man ska skapa ett AI-system med hjälp av Power Platform är det extra viktigt att välja information, tillämpning och behandling som är förenlig med reglerna i detta dokument.

Tänk på att det AI-system som du har skapat kanske inte är lämplig att skalas upp och tas i bruk i Power Platform om den inte är förenlig med reglerna i detta dokument. Din idé kan dock ligga till grund för utveckling i en annan plattform eller så måste den anpassas innan den kan skalas upp och tas i drift.

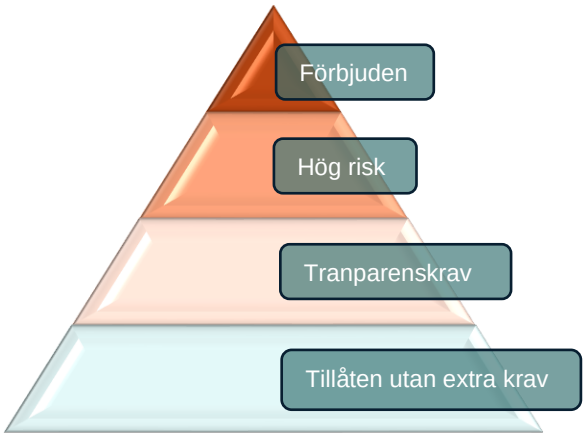
Du får inte använda verkliga personuppgifter, sekretessbelagd information eller annan känslig information när du laborerar med och testar AI-teknik i Power plattformen.

De lösningar du bygger i Power Platform får inte tas i drift utan att en bedömning har gjorts av lösningen enligt det som nämns ovan.

Du får inte använda Power Platform för ändamål som är förbjudna eller högrisk enligt AI-förordningen.

Bilaga 1 AI-förordningen - sammanfattning

EU har antagit en förordning som gäller för användning av AI. Förordningens syfte är att säkerställa att AI inte används på ett sätt som kan orsaka skada på människors liv och hälsa eller riskera våra mänskliga fri- och rättigheter. Den här bilagan innehåller en förenklad beskrivning av innehållet i AI-förordningen. För att veta exakt vad som gäller i en viss situation behöver man läsa förordningstexten eller ta hjälp av jurist. AI-förordningen finns publicerad här.



AI-förordningen utgår ifrån olika risknivåer. Vissa tillämpningar medför så stora risker att de är förbjudna. Andra kan medföra höga risker och omgärdas därför av ett omfattande regelverk som ska säkerställa att AI:n håller hög kvalitet och är säker. Vissa tillämpningar kan medföra risker om man inte är öppen med att AI-används, därför omfattas de av transparenskrav. Merparten är dock tillåtet utan några särskilda krav i AI-förordningen. AI-förordningen gäller parallellt med annan lagstiftning, därför kan det finnas andra bestämmelser som man måste följa när man tränar eller använder AI.

De flesta reglerna i AI-förordningen gäller för **leverantörer**. Leverantör enligt AI-förordningen är den som utvecklar ett AI-system, släpper ut ett AI-system på marknaden eller tar ett AI-system i bruk under eget namn eller varumärke. Om vi själva utvecklar ett AI-system måste vi alltså följa reglerna för leverantörer.

Det finns också regler som gäller för **tillhandahållare**. Det är en organisation som ianvänder AI-system i sin verksamhet, till exempel när kommunen har ett AI-system som används i arbetet av de anställda. Kommunen är då *tillhandahållare* medan de anställda är *användare.*

Förbjuden AI

De tillämpningar som är förbjudna i AI-förordningen får inte tillhandahållas på marknaden eller användas. De tillämningar som är förbjudna enligt AI-förordningen är:

- AI-system som använder subliminala tekniker för att omedvetet påverka människor och allvarligt påverka deras beteende på ett sätt som kan orsaka fysisk eller psykisk skada. Exempel: Ett AI-system som skickar omedvetna signaler till användare för att påverka deras val eller handlingar utan att de är medvetna om det.
- AI-system som utnyttjar sårbarheter hos specifika grupper, såsom barn eller personer med funktionsnedsättningar, för att påverka deras beteende på ett sätt som kan orsaka fysisk eller psykisk skada. Exempel: Ett system som riktar reklam till barn för att uppmana dem att köpa något de inte förstår konsekvenserna av.

- AI-system som används av offentliga myndigheter och för social poängsättning som kan leda till orättvis eller diskriminerande behandling av individer. Exempel: Ett system som betygsätter medborgares beteende och därmed påverkar deras tillgång till tjänster som utbildning eller sociala förmåner.
- AI-system som används för att förutse risken att någon ska begå brott enbart baserat på profilering, personlighetsdrag och egenskaper.
- AI-system som skapar eller fyller på databaser för ansiktsigenkänning genom oriktad “skrapning” av bilder från internet eller övervakningskameror.
- AI-system för känsloigenkänning på arbetsplatser och skolor, om det inte är av säkerhetsskäl eller medicinska skäl. Exempel: ett AI-system som utvärderar vilka medarbetare som är uttråkade och vilka som är energiska.
- AI-system som använder biometriska uppgifter för att kategorisera personer utifrån känsliga egenskaper som ras, kön, etnicitet, religion, politisk åskådning eller sexuell läggning. Exempel: Ett system som använder ansiktsigenkänning för att kategorisera personer utifrån etnisk tillhörighet eller religiösa attribut.
- Användning av AI-system för att identifiera personer i realtid genom biometrisk data på offentliga platser, om det görs av brottsbekämpande myndigheter. Det är dock tillåtet i mycket specifika situationer. Exempel: Att kontinuerligt övervaka och identifiera personer i en folkmassa genom ansiktsigenkänning på offentliga platser är förbjudet som utgångpunkt, men kan vara tillåtet för att stoppa terroristbrott.

Om du vill läsa förbuden i förordningstexten finns de i artikel 5.

Högrisk-AI

Vad reglerna innebär

Leverantörer

Det ställs höga krav på leverantörer av högrisk-system. Reglerna gäller kvalitet på data, loggning, effektiv mänsklig kontroll, riktighet, robusthet och cybersäkerhet. För att säkerställa att detta håller genom hela AI-systemets livscykel behöver leverantören ha ett riskhanteringssystem, ett kvalitetsstyrningssystem och ett system för att övervaka AI-systemet efter att det har släppts ut på marknaden. Allt detta ska också dokumenteras i en teknisk dokumentation som ska kunna visas upp för tillsynsmyndigheten – och en dokumentation som vänder sig till den som ska använda AI-systemet i sin verksamhet.

Dokumentationen som vänder sig till den som ska använda AI-systemet ska innehålla information som gör det möjligt att förstå vilken prestanda systemet har, i vilket sammanhang det ska användas och hur det ska användas för att ge ett korrekt resultat. AI-förordningen innebär alltså att vi får tillgång till viktig information när vi anskaffat ett AI-system som är högrisk.

Om vi själva utvecklar ett AI-system med hög risk, sätter vårt namn på ett AI-system med hög risk eller använder ett system som inte är godkänt som högrisk på ett högriskområde, måste vi uppfylla alla de krav som ställs på *leverantörer* av högrisksystem.

System som är högrisk enligt AI-förordningen ska genomgå ett förfarande för att visa att det följer förordningens krav, det ska också registreras och CE-märkas. Det är leverantören som ansvarar för detta.

Tillhandahållare

Det finns också krav som gäller för *tillhandahållare,* det vill säga för den som infört och använder AI-system med hög risk i sin verksamhet. Exempelvis behöver tillhandahållaren:

- Säkerställa att leverantören har gjort förfarandet för överensstämmelse.
- Använda och övervaka systemet enligt bruksanvisningen och agera om man upptäcker att systemet utgör en risk.
- Tilldela kompetent personal med uppgift att utöva mänsklig kontroll över systemet.
- Om man som arbetsgivare avser att använda ett högrisk-AI-system på arbetsplatsen ska förhandling ske med berörda fackliga organisationer och arbetstagarna ska informeras att de kommer att bli föremål för användning av AI-systemet.
- Om man använder högrisk-AI-system som fattar beslut eller hjälper till att fatta beslut som rör enskilda personer, ska man informera de personerna om det.
- Spara systemets loggar.
- Om man har kontroll över indata, se till att den är relevant och representativ för AI-systemets syfte.
- Göra konsekvensbedömning för dataskydd, och konsekvensbedömning för grundläggande rättigheter.
- Registrera vilket system man valt i en EU-databas.
- Samarbeta med berörda myndigheter.

Det här är högrisk-AI

Nedan återges de högrisktillämpningar som mest sannolikt blir aktuella för kommunen. Högrisktillämpningarna finns i bilaga III till förordningen.

Biometri

AI-system för biometrisk identifiering på distans. Undantag görs för system som enbart används för att verifiera en persons identitet.

AI-system som kategoriserar människor baserat på känsliga eller skyddade egenskaper, inklusive system som drar slutsatser om sådana egenskaper.

AI-system för att känna igen känslor.

Kritisk infrastruktur

AI-system som är avsedda att användas som säkerhetskomponenter i samband med förvaltning och drift av kritisk digital infrastruktur, vägtrafik eller i samband med tillhandahållande av vatten, gas, värme och el.

Utbildning och yrkesutbildning

AI-system som används för att avgöra antagning eller placering i utbildning på alla nivåer, inklusive yrkesutbildning.

AI-system som utvärderar läranderesultat, även när dessa används för att anpassa en persons lärandeprocess.

AI-system som bedömer vilken utbildningsnivå en person kan få eller kan komma att få tillgång till.

AI-system som övervakar och upptäcker otillåtet beteende vid prov.

Anställning, arbetsledning och eget företagande

AI-system som används för rekrytering och urval av personer, inklusive att publicera riktade jobbannonser, analysera ansökningar och bedöma kandidater.

AI-system som används för att fatta beslut om arbetsvillkor, befordringar, uppsägningar, fördelning av arbetsuppgifter baserat på beteende eller egenskaper, samt för att övervaka och utvärdera prestationer och beteenden på arbetsplatsen.

Tillgång till och åtnjutande av väsentliga offentliga tjänster och förmåner

AI-system som används av eller för offentliga myndigheter för att bedöma människors rätt till offentliga stöd, som vårdtjänster och försörjningsstöd, och för att bevilja, minska, dra tillbaka eller återkräva sådana stöd.

AI-system som används för att utvärdera och prioritera nödsamtal eller styra utsändning av larmtjänster som polis, brandkår och ambulans, samt för patientsortering vid akutsjukvård.

Annan högrisk-AI

Utöver dessa finns det högriskområden inom *tillgång till väsentliga privata tjänster* – som lån och försäkringar, *brottsbekämpning*, *migration, asyl och gränskontroll* samt *rättskipning och demokratiska processer*.

Det finns också en lista över produkter som behöver bedömas av en tredje part innan de släpps ut på marknaden, som hissar och leksaker. Om AI-systemet är en säkerhetskomponent i en sådan produkt är det också högrisk. Det rör sig dock om produkter där leverantörerna är vana vid att omfattas av lagstiftning om produktsäkerhet, och där vi som kommun redan idag behöver ställa krav på standarder och CE-märkning.

Transparenskrav

I ett fåtal specifika fall finns det transparenskrav kopplade till AI. För leverantörer innebär det att

- AI-system som ska interagera direkt med människor ska utformas så att man informeras eller förstår att det är ett AI-system som man interagerar med.
- Ljud, bild, video eller text som genereras ska märkas som artificiellt genererat.

För tillhandahållare innebär det att tillhandahållaren måste

- Informera berörda personer om man använder system för känsloigenkänning eller biometrisk kategorisering (och följa gällande EU-förordningar för personuppgifter).
- Upplysa om att innehåll som är en deepfake är artificiellt eller manipulerat.
    - Undantag: uppenbart konstnärligt, kreativt, satiriskt eller skönlitterärt verk
- Upplysa om att en text som publiceras för att informera allmänheten om frågor av allmänt intresse, har genererats eller manipuleras av AI.
    - Undantag om innehållet har granskats och kontrollerats av en människa, och en fysisk eller juridisk person har det redaktionella ansvaret