

AI-förordningen: Praktiska tips för dig som använder AI i din verksamhet på en A4-sida!

Användningen av AI ökar snabbt; men med det följer också behovet av reglering. EU har därför infört **AI Act** (eller ”AI-förordningen” på svenska). Förordningen trädde i kraft redan förra året, men implementeras successivt fram till 2026. Förordningen ställer bland annat krav på dig som använder AI i din verksamhet och träffar såväl storföretagen som den enskilda småföretagaren.

Har du koll på vad som gäller? Här ger vi dig fyra frågor (och en bonusfråga) som du bör ställa till dig själv!

Fråga 1: Är det AI?

Förordningen gäller för ”AI-system”. Det finns tre kriterier:

- Systemet fungerar med viss grad av **autonomi**, d v s systemet har viss *självständighet* eller *självbestämmande*.
- Systemet kan uppvisa **anpassningsförmåga efter införande**, d v s systemet kan *lära sig*.
- Systemet kan på grundval av indata **dra slutsatser om** hur utdata ska genereras för uttryckliga eller underförstådda mål, d v s systemet kan *förstå syftet* med exempelvis den fråga som matas in.

Fråga 2: Vilken roll har vi i AI-kedjan?

Vilka skyldigheter ni har är starkt förknippat med vilken **roll** som ni har i AI-kedjan. De tre vanligaste rollerna är:

- Konsument/anställd:** Har ingen särskild definition, men kan sägas vara den som ”exponeras” för AI-användningen.
- Tillhandahållare:** Den som *använder* ett AI-system i näringsverksamhet.
- Leverantör:** Den som *utvecklar* eller *släpper ut* ett AI-system på marknaden.

Andra aktörer som omfattas av AI-förordningen är distributör, importör och ombud.

VAR FÖRSIKTIG! Som **tillhandahållare** kan man bli ansvarig såsom **leverantör** om man till exempel sätter sitt eget varumärke på AI-systemet eller om man gör väsentliga ändringar av AI-systemet.

Fråga 3: Vilken risknivå gäller för vårt AI-system?

Enligt AI-förordningen finns det fyra risknivåer. Ni bör utvärdera vilken risk ert AI-system faller under.

- Oacceptabel risk** – förbjudna system; får aldrig användas! T.ex. ansiktsigenkänning i realtid på offentliga platser.
- Hög risk** – omfattande krav. T.ex. rekryteringssystem, kreditbedömningar eller utbildningsverktyg som styr betyg.
- Begränsad risk** – transparenskrav; det ska tydligt framgå att det är AI-genererat. T.ex. chatbotar eller ”deepfakes”.
- Minimal risk** – inga särskilda krav. T.ex. AI i spel eller spamfilter.

OMSTÄNDIGHETERNA ÄR VIKTIGA! En chatbot som används för kundservice i detaljhandel kan vara att betrakta som *begränsad risk*, medan en chatbot som används för att ge medicinska råd sannolikt är hög risk.

Fråga 4: Vilka skyldigheter har vi/Vilka åtgärder ska vi vidta?

Efter att ni besvarat de första tre frågorna följer den fjärde och kanske den viktigaste frågan: **Vilka skyldigheter har vi?** Här följer några exempel på vad ni bör göra:

- Utbilda personalen!** AI-förordningen ställer som **generellt krav** att de som använder AI ska ha *”tillräcklig AI-kunnighet”*.
- Dokumentera din bedömning av systemets risknivå:** För leverantörer är detta ett krav, men även andra aktörer har förmodligen nytta av att dokumentera den här typen av bedömning.
- Upprätta ett AI-register:** Håll koll på vilka AI-system er organisation använder.
- Ta fram en AI-policy:** Inget krav enligt AI-förordningen, men säkerställer att organisationen vet hur ni avser att använda AI.

Om ert AI-system är hög risk:

Då ställer AI-förordningen höga krav på användningen. Nedan är några exempel – men ni bör stämma av er regelefterlevnad med juridisk expertis!

- Upprätta teknisk dokumentation** enligt AI-förordningens föreskrifter.
- Spara loggar** enligt AI-förordningens föreskrifter.
- Gör en konsekvensbedömning** om hur AI-systemet kan påverka ex. grundläggande fri- och rättigheter.
- Inrätta ett **riskhanteringssystem**.
- Rapportera incidenter** till marknadskontrollmyndigheten.
- Följ alltid leverantörens anvisningar.**

(Offentlig aktör? Då får ni bara använda AI-system registrerade i EU:s databas)

För system med begränsad risk:

- Transparenskrav:** Det ska framgå att materialet är skapat av AI. (Men om materialet har genomgått ”mänsklig granskning” kan kravet falla bort).

GPAI (General Purpose AI, t.ex. ChatGPT):

- För *tillhandahållare* gäller (i dagsläget) inga särskilda krav utöver transparens på AI-skapat material och säkerställande så att systemet inte används för att producera olagligt innehåll.

Bonusfråga: Har vi koll på utvecklingen och annan lagstiftning?

Det finns mer lagstiftning än bara AI-förordningen att hålla koll på när ni använder AI i er verksamhet. Till exempel behöver ni följa GDPR, arbetsmiljölagstiftning samt respektera immaterialrättsliga rättigheter som exempelvis upphovsrätten.

De strikta kraven som följer av AI-förordningen gäller i dagsläget främst för högrisk-system. Men med den ständiga utvecklingen av AI är det viktigt att ni **håller koll på utvecklingen!** Är ni osäkra på AI-förordningens tillämpning? **Stäm av med juridisk expertis!**