



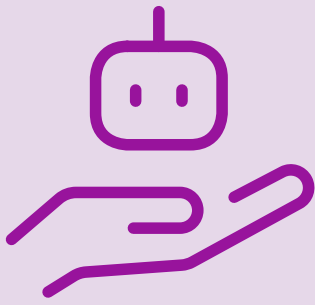
Workshop guide: Tenk nytt med AI Act

En praktisk veiledning med tips for hvordan du
kan bruke EUs AI Act til å utvikle bedre løsninger



Innhold

Introduksjon	3
Steg-for-steg guide til AI ACT	4
• Hva vil dere bruke AI til, og hvem skal det hjelpe?	4
• Hva vil dere oppnå, og hvordan vet dere at det virker?	4
• Er dette noe helt nytt, eller skal det forenkle noe dere allerede gjør?	5
• Hva forventer folk av løsningen, og hva kan gjøre dem skeptiske?	5
• Hva forventer folk av løsningen, og hva kan gjøre dem skeptiske?	6
• Hvilke data kommer AI-løsningen til å bruke eller lage?	6
• Hvilken modell/leverandør vil dere bruke, og hvorfor akkurat den?	7
• Hvilke lover og bransjekrav må dere ta hensyn til?	7
• Hvordan bygger dere tillit til løsningen?	8
• Hva er det verste som kan skje om noe går galt eller løsningen misbrukes?	8
Praktisk AI ACT vurdering	9
Kort AI ACT henvisning	10



EUs AI ACT

Skal dere lage en ny AI-løsning, kjøpe en AI-tjeneste eller bruke AI til å utvikle noe nytt? Da bør dere vurdere løsningen opp mot EUs forordning om kunstig intelligens, kjent som EU AI Act. I Norge omtales gjennomføringen som AI-loven. Nkom beskriver AI-loven som Norges gjennomføring av EUs AI Act, med mål om at AI skal utvikles og brukes på en trygg, ansvarlig og rettferdig måte.

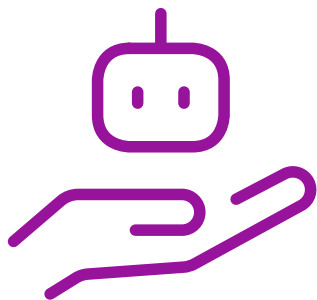
Heldigvis er det langt fra så byråkratisk og krevende som det høres ut. Faktisk er det noe du kan bruke til å skape bedre løsninger.

Sikkerhetsrådgiverne i Advania har satt sammen en liste med ti spørsmål som du kan ta i bruk.

Sett dere sammen, lag et dokument, og gå i gang. Og husk: Det er viktigere at dere diskuterer og vurderer, enn at svarene blir perfekte.

Bruk sjekklisten som en praktisk start på AI Act-vurderingen: Hvilken rolle har dere, hvilken risikokategori faller løsningen inn under, hvilke krav gjelder, og hvordan kan vurderingene dokumenteres på en enkel og etterprøvbar måte?





Guide

Hva vil dere bruke AI til, og hvem skal det hjelpe?

EU AI Act bygger på en risikobasert tilnærming. Det betyr at det først må vurderes hva AI-en brukes til, hvem som påvirkes, og hvor stor risiko løsningen kan skape. Loven beskriver fire risikonivåer: forbudt AI, høyrisiko-AI, begrenset risiko og minimal risiko. Jo større påvirkning løsningen kan ha på mennesker, rettigheter, sikkerhet eller samfunnsfunksjoner, desto strengere krav gjelder. Derfor er det viktig å være konkret på målgruppe, behov og brukssituasjon fra start.



Tips til utfyllingen: Vær konkret: Hvem får nytte av dette (eks. ansatte, kunder, ledelse), og hva er utfordringen eller behovet i hverdagen?

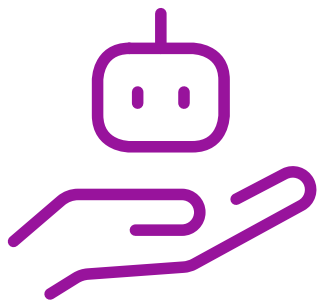
Hva vil dere oppnå, og hvordan vet dere at det virker?

AI Act legger vekt på at AI-systemer skal være trygge, robuste og fungere som forventet. For løsninger med høy risiko kan det være krav til risikostyring, testing, dokumentasjon, logging, kvalitet i data, menneskelig kontroll og oppfølging etter at løsningen er tatt i bruk. Også for løsninger med lavere risiko bør dere definere hva som er et godt resultat, hvordan kvaliteten skal måles, og hvordan feil skal oppdages og håndteres.



Tips til utfyllingen: Beskriv ønsket gevinst og effekt (eks. spare tid, færre feil, bedre service), og hvordan dere skal måle at det faktisk fungerer.





Er dette noe helt nytt, eller skal det forenkle noe dere allerede gjør?

AI Act skiller mellom ulike roller, blant annet den som utvikler eller tilbyr et AI-system, og den som tar det i bruk i egen virksomhet. Dette påvirker ansvar, dokumentasjon og oppfølging. Hvis dere utvikler, tilpasser eller setter en løsning på markedet, kan kravene bli mer omfattende enn om dere bare bruker et ferdig verktøy internt. Derfor bør dere tidlig avklare om dere er leverandør, bruker, importør, distributør eller bare intern bruker av en eksisterende løsning.



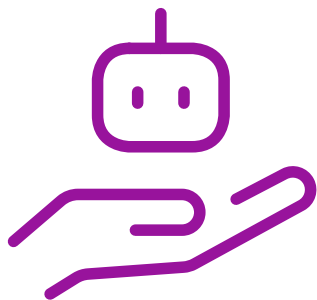
Tips til utfyllingen: Finn ut om dere skal bruke AI til å lage en ny tjeneste, forbedre noe dere har, eller avlaste en eksisterende oppgave.

Finnes det allerede noe som løser dette, og hvorfor er AI det beste valget?

AI skal ikke brukes bare fordi det er mulig. Regelverket bygger på prinsippet om at løsningen bør stå i forhold til behovet og risikoen. Derfor er det smart å vurdere om AI er den beste måten å løse problemet på. Den vurderingen gir ofte bedre prioriteringer, lavere kostnader og mindre kompleksitet. Samtidig blir det lettere å forklare beslutningen til både ansatte, kunder og ledelse.



Tips til utfyllingen: Se om konkurrenter eller andre verktøy gjør noe lignende, og forklar hvilken verdi AI gir som "vanlige" løsninger ikke gir.



Hva forventer folk av løsningen, og hva kan gjøre dem skeptiske?

AI Act inneholder egne krav til åpenhet for enkelte typer AI-systemer. Brukere bør forstå når de samhandler med AI, hva løsningen gjør, og hvilke begrensninger den har. Dette er særlig relevant for chatboter, anbefalingssystemer, AI-generert innhold og løsninger som kan påvirke beslutninger om enkeltpersoner. God merking, tydelig informasjon og realistiske forventninger bygger tillit og reduserer risiko for misforståelser.



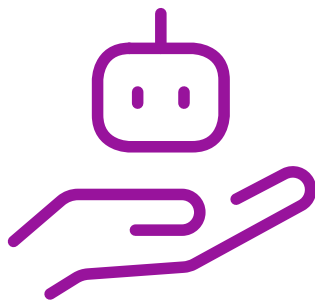
Tips til utfyllingen: Tenk på hva brukerne trenger for å føle seg trygge: at løsningen gir korrekte resultater, er lett å bruke, at de kan forstå prosessen og kontrollere resultatet, etc.

Hvilke data kommer AI-løsningen til å bruke eller lage?

Data er sentralt i AI Act, særlig for høyrisiko-systemer hvor krav til datakvalitet, relevans, sporbarhet og dokumentasjon kan bli viktige. Her bør dere forstå hvilke data som brukes, hvor de kommer fra, om de inneholder personopplysninger eller sensitiv informasjon, og hvordan kvalitet, eierskap, lagring og tilgang håndteres. Dårlige eller uklare data gir ofte dårlige resultater, uansett hvor god modellen er.



Tips til utfyllingen: Avklar tidlig om det gjelder personopplysninger, kundedata, økonomi, eller innhold dere eier (f.eks. dokumenter, kode, tekster, opphavsrett).



Hvilken modell/leverandør vil dere bruke, og hvorfor akkurat den?

Valg av modell og leverandør påvirker sikkerhet, datalagring, kontroll, dokumentasjon, ansvarsdeling og hvilke AI Act-krav som gjelder. Dere bør derfor gjøre en bevisst vurdering av leverandørens rolle, dokumentasjon, sikkerhetsnivå, bruksvilkår, databehandling og mulighet for innsyn eller kontroll. For generelle AI-modeller og tjenester kan det også være relevant å forstå hvilke forpliktelser leverandøren selv har etter AI Act.



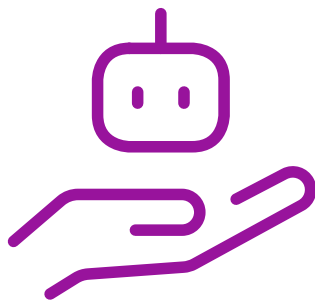
Tips til utfyllingen: Hva spiller inn på valget deres? Er det kvalitet, pris, sikkerhet, hvor data lagres, regler og krav, eller hvor mye kontroll dere trenger?

Hvilke lover og bransjekrav må dere ta hensyn til?

AI Act kommer ikke alene. Personvern, informasjonssikkerhet, opphavsrett, sektorregler og kontraktskrav gjelder fortsatt. I Norge skal AI Act gjennomføres gjennom AI-loven, og Nkom er gitt en sentral rolle i koordineringen av arbeidet. For enkelte sektorer, som helse, finans, utdanning, kritisk infrastruktur, rettspleie og offentlig sektor, kan løsningen falle inn under høyrisiko-kategorien. Da kan kravene til dokumentasjon, testing, risikostyring, tilsyn og oppfølging bli betydelig strengere.



Tips til utfyllingen: Gjør en god vurdering på hvilke lover og krav som gjelder både deres egen bransje, og markedet dere skal selge løsningen til.



Hvordan bygger dere tillit til løsningen?

AI Act legger stor vekt på ansvar, åpenhet og menneskelig kontroll. Det betyr ikke at alt må kvalitetssikres manuelt, men at noen må forstå løsningen, følge med på resultatene og kunne gripe inn ved behov. For høyrisiko-systemer kan menneskelig kontroll være et eksplisitt krav. I praksis handler dette om klare ansvarslinjer, rutiner for kvalitetssikring, opplæring, eskalering, hendelseshåndtering og dokumentert oppfølging.



Tips til utfyllingen: Forklar hvordan dere sjekker kvalitet, håndterer feil, og hvem som har ansvar, 'human-in-the-loop.'

Hva er det verste som kan skje om noe går galt eller løsningen misbrukes?

Dette er noe av kjernen i AI Act: å forstå og redusere risiko før problemer oppstår. Regelverket forbyr enkelte former for uakseptabel risiko, stiller strenge krav til høyrisiko-systemer, og krever åpenhet for flere løsninger med begrenset risiko. Dere trenger ikke forutse alt, men bør tenke gjennom hva som kan gå galt, hvem som kan bli påvirket, og hvilke tiltak som reduserer sannsynlighet og konsekvens. Målet er ikke å stoppe innovasjon, men å sikre at AI brukes trygt, rettferdig og ansvarlig.

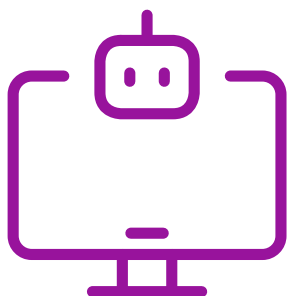


Tips til utfyllingen: Se for dere et "verste fall" (feil beslutninger, lekkasje, omdømmetap), og beskriv noen enkle tiltak som reduserer risikoen for at dette kan skje.

Praktisk AI Act-vurdering

For hver AI-løsning bør dere minst dokumentere: formål, målgruppe, risikokategori, datagrunnlag, leverandør/modell, mulige konsekvenser, nødvendige tiltak og hvem som eier løsningen og er ansvarlig for å følge den opp.

- Hvis løsningen kan påvirke mennesker, rettigheter, sikkerhet eller tilgang til viktige tjenester, bør dere vurdere om den kan være høyrisiko.
- Hvis brukeren samhandler med AI eller mottar AI-generert innhold, bør dere vurdere krav til merking og tydelig informasjon.
- Hvis løsningen bruker personopplysninger, kundedata eller konfidensiell informasjon, må personvern, informasjonssikkerhet og databehandleransvar vurderes samtidig.



Kort om AI ACT

EU AI Act er EUs felles og bindende regelverk for kunstig intelligens. Regelverket trådte i kraft i EU i august 2024 og skal gjennomføres i norsk rett gjennom AI-loven. Nkom beskriver formålet som å beskytte mennesker og grunnleggende rettigheter, legge til rette for trygg innovasjon og bygge tillit til digitale tjenester.

Regelverket er risikobasert. AI-systemer deles inn i fire hovedkategorier: forbudt AI, høyrisiko-AI, begrenset risiko og minimal risiko. For virksomheter betyr dette at man bør kartlegge AI-systemer, avklare rolle og ansvar, vurdere risikonivå, dokumentere vurderinger, sikre åpenhet overfor brukere og etablere nødvendig menneskelig kontroll. For høyrisiko-systemer må virksomheter forvente strengere krav til testing, dokumentasjon, risikostyring, tilsyn og oppfølging.

Vil du lære mer om AI i praksis?

Kontakt folkene bak AI i Advania.



Leo Eliassen
leo.eliassen@advania.no



Erik Stol Øyan
erik.oyan@advania.no



The tech company
with people at heart

