

DEN KOMPLETTE HÅNDBOKEN FOR NORSKE SMB-ER

AI Act i praksis

Fra kartlegging til kontroll — med referanser til KI-forordningen og norske tilsynsmyndigheter, skrevet uten unødvendig juridisk språk.

18 kapitler

Klar-til-bruk maler

Juni 2026

Om denne håndboken

Åpenhet om AI-bruk i denne boken

Denne håndboken er utarbeidet med betydelig hjelp fra KI-verktøy, og er gjennomgått og godkjent av Smartsona AS før publisering. Vi praktiserer dermed vår egen anbefaling fra kapittel 11 - at innhold som i hovedsak er AI-generert, bør merkes tydelig og tidlig, ikke gjemmes i et vilkår.

De fleste bedrifter trenger ikke flere artikler om kunstig intelligens. De trenger et sted å starte, og en logisk vei videre. Denne håndboken er bygget rundt den reisen en bedriftseier faktisk går gjennom - ikke rundt paragrafer.

Strukturen

Boken er delt i seks deler som følger en naturlig rekkefølge:

- Del I — Forstå rammene: hva regelverket faktisk sier, og når det gjelder.
- Del II — Kartlegg: finn ut hvilke AI-verktøy som faktisk er i bruk.
- Del III — Vurder og klassifiser: sett en farge eller risikokategori på det dere har funnet.
- Del IV — Konkrete tiltak: gjør noe med de fire områdene der AI oftest møter kunder og ansatte.
- Del V — Ansvar, dokumentasjon og opplæring: gjør arbeidet gjenfinnbart og forankret.
- Del VI — Handlingsplan: prioriter og hold det i gang.

Hvert kapittel er en mal i seg selv

Du trenger ikke lese boken fra perm til perm før du gjør noe. Der et kapittel inneholder et konkret skjema, en sjekkliste eller et oppslag du skal bruke direkte, er det merket med en blå rubrikk - slik finner du hjelpemiddelet raskt igjen, uten å lese forklaringen på nytt:

- MAL — et skjema du fyller ut med egne data (f.eks. AI-inventarlisten).
- SJEKKLISTE — punkter du går gjennom og krysser av (f.eks. AI Act Quick Check).
- OPPSLAG — en referansetabell du slår opp i (f.eks. risikonivåene).
- VERKTØY — et rammeverk du bruker i et møte eller en vurdering (f.eks. ansvarskartet).

Vil du ha redigerbare versjoner av malene?

Flere av malene finnes som egne, fyllbare Word- og Excel-filer. Send en e-post til post@smartsona.no, så sender vi deg redigerbare versjoner av de malene du trenger.

Hva denne boken ikke er

Dette er ikke juridisk rådgivning, og det er ikke en fullstendig juridisk fremstilling av KI-forordningen (EUs AI Act). Det er et praktisk utgangspunkt skrevet for ledere og eiere uten juridisk bakgrunn, med referanser til regelverket og norske myndigheters egne veiledninger der det er relevant - slik at du vet hvor du kan lese mer, og hva du bør spørre en jurist om hvis du er i tvil.

Regelverksstatus

EU vedtok i mai 2026 en politisk enighet om å forskyve flere frister for høyrisiko-AI. Del I, kapittel 2 gir en oppdatert og etterprøvbar tidslinje per juni 2026 - bruk den i stedet for eldre artikler du finner på nett.

Innhold

<u>Del I — Forstå rammene</u>	3
1. Hva er KI-forordningen, og gjelder den din bedrift?	3
2. Tidslinjen: hva gjelder når	4
3. Hvem fører tilsyn i Norge	5
<u>Del II — Kartlegg</u>	7
4. Start her: de fire spørsmålene	7
5. AI-inventarliste	8
<u>Del III — Vurder og klassifiser</u>	9
6. De fire risikonivåene	9
7. Rød-flagg-listen	10
8. Trafikklysmodellen	11
9. AI Act Quick Check	12
<u>Del IV — Konkrete tiltak</u>	14
10. Kundedialog og chatbot	14
11. Merking av AI-innhold	15
12. Markedsføring	17
13. HR og rekruttering	18
<u>Del V — Ansvar, dokumentasjon, opplæring</u>	20
14. Ansvarskart	20
15. Dokumentasjonsstruktur	21
16. Lær opp organisasjonen	22
<u>Del VI — Handlingsplan</u>	24
17. Prioriteringsliste	24
18. Hold det levende	24
<u>Vedlegg A — Ordliste</u>	26
<u>Vedlegg B — Referanser og videre lesning</u>	27
<u>Vedlegg C — Hvordan bruke denne boken internt</u>	28
<u>Vedlegg D — Om Smartsona AS</u>	29



DEL I

Forstå rammene

Hva regelverket faktisk sier, hvem det gjelder for, og når de ulike kravene trer i kraft.

DEL I — FORSTÅ RAMMENE

1. Hva er KI-forordningen, og gjelder den din bedrift?

EUs forordning om kunstig intelligens, KI-forordningen, internasjonalt kjent som *AI Act* (forordning (EU) 2024/1689), trådte i kraft 1. august 2024. Den er verdens første helhetlige regelverk for kunstig intelligens, og bygger på ett grunnprinsipp: Jo større risiko en AI-bruk utgjør for enkeltpersoner, desto strengere krav gjelder.

Norge er ikke EU-medlem - men er likevel omfattet

Som EØS-land er Norge forpliktet til å innlemme KI-forordningen i norsk rett. Regjeringen sendte forslag til en egen KI-lov på høring sommeren 2025, og loven er ventet å tre i kraft fra sensommeren 2026, omtrent samtidig med at hoveddelen av EU-regelverket begynner å gjelde. Det betyr at norske bedrifter ikke bør vente og se; forberedelsene bør være i gang allerede nå.

Det avgjørende spørsmålet er ikke størrelse

Det er lett å tro at slike regler først og fremst treffer store selskaper med egne compliance-avdelinger. I praksis avgjøres pliktene av hvordan AI brukes, hva den brukes til, hvem som påvirkes, og hvilken rolle virksomheten har i verdikjeden, ikke av bedriftens størrelse eller om den selv har utviklet AI-systemet.

Provider og deployer — to roller du bør kjenne

KI-forordningen skiller særlig mellom *provider* og *deployer*. En provider er virksomheten som utvikler eller setter et AI-system på markedet under eget navn. En deployer er virksomheten som bruker et AI-system i egen drift, med mindre bruken skjer rent privat.

For de fleste SMB-er er deployer-rollen den mest relevante.

Bruker virksomheten en chatbot, et generativt skriveverktøy, et HR-verktøy eller et system som rangerer saker, kandidater eller kunder, kan den få plikter selv om teknologien er utviklet av noen andre. I denne boken bruker vi derfor ordet «bruker» om deployer-rollen for å holde språket enkelt.

De fire risikonivåene - kort fortalt

KI-forordningen deler AI-bruk inn i fire kategorier etter risikoen for enkeltpersoner. De fleste vanlige bruksområder i en SMB, som interne produktivitetsverktøy og vanlig markedsføringstekst,

havner i de to laveste kategoriene. Del III i denne boken går gjennom alle fire i detalj, med konkrete eksempler.

- Uakseptabel risiko – forbudt uavhengig av hensikt, for eksempel sosial poengsum av personer.
- Høy risiko – strenge krav til dokumentasjon, kontroll og menneskelig oppfølging, for eksempel AI i rekruttering.
- Begrenset risiko – krav om åpenhet, for eksempel at en chatbot må opplyse at den er AI.
- Minimal risiko – ingen spesifikke krav etter AI Act, men generelt forsvarlig bruk gjelder fortsatt.

Usikker på hvor din bedrift står?

Kapittel 9 i denne boken («AI Act Quick Check») gir deg en konkret status på under 10 minutter.

DEL I — FORSTÅ RAMMENE · STATUS PER JUNI 2026

2. Tidslinjen: hva gjelder når

Mye av det som er skrevet om «fristen 1. august 2026», er allerede utdatert. I mai 2026 ble EU-institusjonene politisk enige om en pakke endringer, *Digital Omnibus for KI*, som forskyver flere frister for høyrisiko-systemer betydelig. Endringene venter fortsatt på formell vedtakelse og publisering, men den politiske enigheten er tydelig nok til at den bør legges til grunn i planleggingen nå.

Det som har skjedd og det som gjelder fra før

Dato	Hva gjelder fra denne datoen
1. august 2024	KI-forordningen trer i kraft i EU.
2. februar 2025	Forbudte AI-praksiser ble ulovlige, blant annet sosial poengsum og manipulerende teknikker. Generelle bestemmelser og AI-kompetansekravet i artikkel 4 gjelder også.
2. august 2025	Krav til AI for allmenne formål, GPAI, gjelder. Medlemslandene skal også ha utpekt nasjonale tilsynsmyndigheter.

Det som gjelder snart - og det som nå er forskjøvet

2. august 2026 — fortsatt en reell frist

Åpenhetskravene i artikkel 50 gjelder fra denne datoen som planlagt. Brukere skal få vite at de samhandler med AI, og visse typer AI-generert innhold skal merkes. Norges KI-lov er også ventet å gjelde fra denne perioden. Dette er den fristen som er mest relevant for de fleste SMB-er.

2. desember 2026 — utvidet frist for teknisk merking

Den tekniske plikten til maskinlesbar merking («vannmerking») av syntetisk innhold er forskjøvet fire måneder, fra 2. august til 2. desember 2026. Den grunnleggende åpenhetsplikten (at brukeren skal vite at det er AI) er ikke påvirket av denne forsinkelsen.

2. desember 2027 — høyrisiko-krav forskjøvet 16 måneder

Krav til frittstående høyrisiko-systemer, for eksempel i rekruttering og kredittvurdering, var opprinnelig satt til 2. august 2026. Etter avtalen fra mai 2026 er fristen nå 2. desember 2027, for å gi mer tid til at EU skal få på plass veiledning og tekniske standarder.

2. august 2027 / 2028 — sandkasser og produktintegret høyrisiko-AI

Kravet om at hvert land skal ha en regulatorisk KI-sandkasse, er forskjøvet ett år, fra 2026 til 2. august 2027. Høyrisiko-krav for AI innebygd i regulerte produkter, for eksempel medisinsk utstyr og maskiner, er forskjøvet fra 2027 til 2. august 2028.

Hva betyr dette i praksis for din bedrift?

Det som faktisk haster mot 2. august 2026 for de fleste SMB-er, er åpenhet og merking: om kundene vet at de snakker med AI, og om AI-generert innhold er tydelig merket. Det er nettopp dette kapittel 10 og 11 i boken dekker. En fullskala høyrisikovurdering har derimot fått mer tid enn mange tror. Det er likevel ingen god grunn til å vente med selve kartleggingen i del II, fordi den tar kort tid og er nyttig uavhengig av hvilken frist som gjelder.

Kildene for denne tidslinjen er listet i Vedlegg B. Fristene bygger på den politiske enigheten om Digital Omnibus for KI fra mai 2026, som ved skrivepunktet ventet på formell vedtakelse og publisering i EUs offisielle journal. Sjekk Vedlegg B for oppdaterte lenker før du legger en plan som bygger på en bestemt dato.

DEL I — FORSTÅ RAMMENE

3. Hvem fører tilsyn i Norge

KI-forordningen krever at hvert medlemsland, og hvert EØS-land, utpeker tilsynsmyndigheter. I Norge er ansvaret delt mellom flere etater som nå bygger opp et felles system.

① Nkom — nasjonal koordinerende tilsynsmyndighet

Rolle

Nkom, Nasjonal kommunikasjonsmyndighet, er utpekt som Norges koordinerende KI-tilsyn. Sammen med sektortilsynene skal etaten kontrollere at AI-systemer på det norske markedet brukes trygt og ansvarlig

② Datatilsynet — personvern og KI henger tett sammen

Rolle

Mange AI-bruksområder involverer personopplysninger, og Datatilsynet har derfor en sentral rolle der KI-forordningen og GDPR overlapper.

Datatilsynet har allerede utvidet veiledningen sin til å omfatte KI-forordningen, og har egne anbefalinger for personvernvennlig bruk av AI, se Vedlegg B

KI-forordningen erstatter ikke GDPR.

De to regelsettene må ofte leses sammen, særlig der AI-systemer behandler personopplysninger om kunder, ansatte eller jobbsøkere. En vurdering etter KI-forordningen fritar ikke fra plikter etter personvernregelverket, og omvendt.

③ Digdir — den regulatoriske sandkassen og «KI-Norge»

Rolle

Digitaliseringsdirektoratet koordinerer en regulatorisk KI-sandkasse i samarbeid med Nkom og Datatilsynet, samlet under satsingen KI-Norge. Sandkassen skal gi utvalgte virksomheter veiledning og et avgrenset vern mot overtredelsesgebyr mens de tester nye AI-løsninger.

④ Norsk akkreditering (NA)

Rolle

Norsk akkreditering har fått rollen som nasjonalt akkrediteringsorgan for KI-forordningen, og bygger videre på systemet som allerede brukes i norsk offentlig forvaltning.

Dette er regjeringens uttalte plan per skrivende stund. KI-loven er fortsatt på høring, ikke vedtatt lov, så det nøyaktige tilsynsbildet bør alltid sjekkes mot offentlige kilder før du legger det til grunn for en viktig beslutning, se Vedlegg B

Hva kan det koste å bryte reglene?

KI-forordningen artikkel 99 gir hjemmel for overtredelsesgebyr på opptil 35 millioner euro eller 7 prosent av global omsetning for de mest alvorlige bruddene, som forbudte praksiser, med lavere satser for andre brudd. Tallene er ikke ment som skremsel, men som en påminnelse om at dette er bindende regelverk, ikke en frivillig anbefaling. Det lønner seg derfor å starte kartleggingen i god tid.

Datatilsynets eget råd til virksomheter som tar i bruk AI-løsninger andre har bygget:

- ✓ Gjør en risikovurdering før systemet tas i bruk.
- ✓ Still krav til innebygd personvern.
- ✓ Gjør regelmessige tester.
- ✓ Gi brukerne god informasjon og veiledning.
- ✓ Sett dere inn i hvilke plikter som faktisk gjelder for dere.



DEL II

Kartlegg

Du kan ikke vurdere risiko for verktøy du ikke vet at dere bruker. Alt starter her.

DEL II — KARTLEGG

4. Start her: de fire spørsmålene

Hvis virksomheten ikke vet hvilke AI-verktøy som faktisk brukes, blir resten av arbeidet gjetning. Kartlegging er derfor ikke et administrativt tillegg, men grunnlaget for alle senere vurderinger. Det er bedre å få et ufullstendig første bilde raskt enn å vente på en perfekt oversikt som aldri blir laget.

Slik stiller du spørsmålene bedre

I stedet for å spørre: «Bruker vi AI?», bør du spørre mer konkret:

- Hvilke verktøy bruker salg, kundeservice, HR og markedsføring hver uke?
- Hvilke verktøy brukes til tekst, bilde, video, søk, analyse eller prioritering?
- Hvilke verktøy påvirker kunder, ansatte eller publisert innhold?
- Hvilke verktøy er tatt i bruk uten formell godkjenning?

Jo mer konkret kartleggingen er, desto lettere er det å skille mellom intern produktivitet og bruk som utløser tydeligere plikter

VERKTØY · De fire spørsmålene — ta dem inn i neste ledermøte og noter svarene direkte

① Hvilke AI-verktøy bruker vi faktisk?**Still spørsmålet slik**

Kan du liste dem opp akkurat nå - eller må du spørre noen?

② Hvem bruker dem?**Still spørsmålet slik**

Hvilke avdelinger eller personer bruker dem konkret, ikke «markedsføring» i sin helhet?

③ Hva brukes de til?**Still spørsmålet slik**

Og berører det kunder, ansatte, eller noe som publiseres utad?

④ Hvilken bruk er vi mest usikre på?

Still spørsmålet slik

Hvis dere måtte forklare denne bruken i morgen - hvor ville dere være mest usikre?

Disse spørsmålene virker enkle, men de avdekker ofte det viktigste først: skjult bruk, uklare formål, manglende ansvar og manglende oversikt over kundevendt bruk. Svarene leder deg videre til malen i neste kapittel.

DEL II — KARTLEGG

5. AI-inventarliste

En AI-inventarliste er den enkleste måten å gjøre AI-bruk synlig og håndterbar på. Målet er ikke å beskrive hele teknologistacken i detalj, men å få nok informasjon til å kunne prioritere videre arbeid. Denne malen finnes også som et eget, fyllbart Excel-ark, *AI-Inventarliste-Smartsona.xlsx*.

MAL • AI-inventarliste — registrer ett verktøy per rad, last gjerne ned Excel-versjonen for utfylling

Verktøy	Leverandør	Formål	Hvem bruker det	Krever oppfølging?
ChatGPT (Enterprise)	OpenAI	Utkast til kundesvar og markedstekst	Markedsføring, kundeservice	Ja - merkerutine
AI-rekrutteringsverktøy	Ukjent leverandør	Sortering av jobbsøknader	HR	Ja - bør vurderes nærmere

Tre regler for å få nytte av inventaret

- Registrer ett verktøy eller én tydelig bruk per rad.
- Skriv formålet konkret, ikke bare «AI» eller «effektivisering».
- Marker usikkerhet åpent og synlig; «usikker» er bedre enn å gjette.

Send listen til den som er ansvarlig for AI-styring, se kapittel 14, for en kvalitetssjekk. Usikre rader er nettopp de som bør prioriteres i del III.



DEL III

Vurder og klassifiser

Sett en farge eller risikokategori på det dere har funnet - før dere bruker tid på tiltak.

DEL III — VURDER OG KLASSIFISER

6. De fire risikonivåene

KI-forordningens fire nivåer er nyttige som en overordnet struktur, men de er ikke en ferdig fasit for hver enkelt situasjon. I praksis trenger de fleste SMB-er en første filtrering: Er dette sannsynligvis forbudt, potensielt høyrisiko, transparenspliktig, eller hovedsakelig internt og lavrisiko?

Dette er en forenklet, ikke-juridisk oversikt som hjelper deg å gjøre en første vurdering. Ved tvil eller høy risiko bør vurderingen kvalitetssikres nærmere; se Vedlegg B for Europakommisjonens egne retningslinjer.

OPPSLAG • De fire risikonivåene — bruk denne tabellen til å plassere hvert AI-verktøy

Risikokategori	Hva kjennetegner den?	Eksempel
Uakseptabel risiko	AI-bruk som er forbudt, for eksempel manipulerende teknikker, sosial vurdering av personer eller systemer som utnytter sårbare grupper.	Ikke relevant for de aller fleste vanlige bedrifter.
Høy risiko	AI som påvirker viktige beslutninger om enkeltpersoner, for eksempel ansettelse, kredittvurdering, tilgang til tjenester eller overvåking av ansatte.	AI-verktøy som rangerer jobbsøkere eller vurderer kredittverdighet.
Begrenset risiko	AI som har krav om åpenhet, altså at brukeren skal vite at de snakker med, eller blir påvirket av, AI.	Chatbot på kundeservice, AI-generert markedsinnhold.
Minimal risiko	Resten av AI-bruken, der det ikke gjelder spesifikke AI Act-krav, men hvor generelt ansvar for forsvarlig bruk fortsatt gjelder.	Interne produktivitetsverktøy uten direkte effekt på kunder eller ansatte.

«Minimal risiko» betyr ikke «ingen ansvar».

God intern kontroll, ansvar og bevissthet er fortsatt nødvendig, særlig hvis bruken senere flyttes ut mot kunder eller ansatte. For mange SMB-er vil hverdagsbruken havne i kategoriene begrenset eller minimal risiko. Det betyr at arbeidet ofte starter med oversikt, merking og intern styring, ikke med full høyrisiko-compliance.

DEL III — VURDER OG KLASSIFISER

7. Rød-flagg-listen

Noe AI-bruk er ikke bare risikabelt; det er forbudt, uavhengig av hensikt. Denne listen hjelper deg å kjenne igjen de tilfellene først, slik at du ikke bruker tid på å diskutere «hvor trygt er dette» når det egentlige spørsmålet er: «Er dette i det hele tatt lov?»

Artikkel 50 og opplæringskravet i artikkel 4 handler i stor grad om å gjøre vanlige AI-løsninger mer ansvarlige. Rød-flagg-listen handler om noe annet: å stoppe bruk som kan være prinsipielt eller rettslig uakseptabel fra starten.

SJEKKLISTE · Rød-flagg-listen — gå gjennom alle fem punktene for hvert AI-verktøy dere bruker

① Sosial poengsum / vurdering av personer

Kjennetegn	AI som rangerer eller gir mennesker en score basert på oppførsel, og bruker scoren til å gi eller nekte dem noe.
Eksempel	Et internt system som rangerer kunder eller ansatte etter «pålitelighet» og automatisk gir dem ulik behandling.
Hvorfor viktig	Dette er blant det regelverket forbyr direkte, uavhengig av om hensikten var god.

② AI som manipulerer eller utnytter sårbarhet

Kjennetegn	AI-bruk utformet for å påvirke beslutninger hos personer i en sårbar situasjon, på en måte de ikke ville valgt selv.
Eksempel	Markedsføring som målretter AI-genererte budskap mot personer i økonomisk nød for å presse frem et kjøp.
Hvorfor viktig	Forbudt uavhengig av om det «virker» kommersielt; hensikten endrer ikke regelen.

③ Biometrisk sanntidsovervåking uten klart grunnlag

Kjennetegn	Ansiktsgjenkjenning eller annen biometrisk identifisering av kunder eller ansatte i sanntid, uten et klart rettslig grunnlag.
Eksempel	Kameraer med ansiktsgjenkjenning som identifiserer enkeltkunder i butikk i sanntid.
Hvorfor viktig	Strengt regulert i de fleste sammenhenger, med svært høy juridisk eksponering uten vurdering.

④ AI som avgjør viktige ting om enkeltpersoner uten menneskelig kontroll

Kjennetegn	AI som avgjør beslutninger om ansettelse, kreditt, forsikring eller andre viktige tjenester, uten reell menneskelig vurdering.
Eksempel	Automatisk avslag på jobbsøknad eller lån basert kun på en AI-score.
Hvorfor viktig	Høyrisiko-bruk som krever dokumentasjon, kontroll og innsyn, se kapittel 6 og 15.

⑤ Emosjonsgjenkjenning av ansatte

Kjennetegn	AI som analyserer ansattes tonefall, ansiktsuttrykk eller «humør» for å vurdere engasjement eller ytelse.
Eksempel	Programvare som analyserer video eller lyd fra medarbeidersamtaler for å vurdere «engasjementsnivå».
Hvorfor viktig	Sterkt begrenset på arbeidsplassen, med få unntak, for eksempel sikkerhet eller medisin.

Oppsummert: Scorer dere mennesker, utnytter sårbarhet, overvåker biometrisk i sanntid, lar AI bestemme uten menneskelig kontroll, eller emosjonsanalyserer ansatte? Stopp og vurder det først, uavhengig av alt annet AI-arbeid.

DEL III — VURDER OG KLASSIFISER

8. Trafikklysmodellen

De fleste ledere trenger ikke en 40-siders juridisk analyse i første runde. De trenger en forståelig status som sier om virksomheten kan fortsette som før, må rydde opp snart, eller må stoppe og eskalere. En trafikklysmodell er nyttig, så lenge den brukes som en første operasjonell vurdering, ikke som endelig juss.

Rød

Kjennetegn	Avgjør noe viktig om en konkret person uten reell menneskelig kontroll, eller bruken ligger nær et forbudt mønster.
Krav / tiltak	Stopp videre bruk til det er vurdert nærmere. Innfør menneskelig kontroll eller hent inn ekstern vurdering. Rød betyr ikke «ulovlig», men at vanlig intern håndtering ikke er tilstrekkelig.
Eksempel	Automatisk avslag på jobbsøknader basert kun på en AI-score.

Gul

Kjennetegn	Berører kunder, ansatte eller publisert innhold, men utgjør ikke uten videre høy eller forbudt risiko.
Krav / tiltak	Merk innholdet eller interaksjonen tydelig. Dokumenter formål, ansvarlig person og risiko. Sett en revurderingsdato
Eksempel	En chatbot som svarer kunder uten å opplyse at det er AI.

Grønn

Kjennetegn	Verktøyet er internt, avgrenset og påvirker ikke enkeltpersoner direkte eller publisert informasjon på en måte som utløser særskilte krav.
Krav / tiltak	Grønn betyr fortsatt at virksomheten bør vite hva verktøyet er, hvem som bruker det, og hva det brukes til, ikke at det er fritatt fra oppfølging.
Eksempel	Et internt AI-verktøy som oppsummerer møtenotater for eget team.

Regelmotor — maks 5 enkle regler

Denne modellen er bevisst enkel. Basert på ja/nei-svar i et skjema kan fargen tilordnes automatisk, i denne rekkefølgen:

OPPSLAG · *Regelmotor for trafikklys — bruk i denne rekkefølgen for hvert AI-verktøy*

1	Brukes til beslutning om enkeltperson = ja og menneskelig kontroll = nei → rødt
2	Berører kunder eller ansatte = ja og merket/informert om AI = nei → gult
3	Ansvarlig person for systemet utpekt = nei → gult
4	Ingen av regel 1–3 slår inn og berører ikke kunder, ansatte eller innhold → grønt
5	Usikker på noe av dette → gult, til det er avklart

DEL III — VURDER OG KLASSIFISER

9. AI Act Quick Check

De ti spørsmålene under gir deg en rask statusvurdering: en tydelig grønn, gul eller rød status, pluss konkrete neste steg. Denne sjekken kan brukes i et ledermøte eller fylles ut individuelt før en felles gjennomgang. En interaktiv versjon finnes også på nettsiden www.smartsona.no/ai-act. Del gjerne med kollegaer.

SJEKKLISTE · AI Act Quick Check — fyll ut alle ti spørsmål før du leser av resultatet

#	Spørsmål	Ja	Nei	Usikker
1	Vet dere nøyaktig hvilke AI-verktøy som er i bruk, og hvem som bruker dem?	☐	☐	☐
2	Er det avklart hvem som har det interne ansvaret for AI-bruken?	☐	☐	☐
3	Hvis dere bruker AI i kundedialog: er det tydelig for kunden at det er AI?	☐	☐	☐
4	Bruker dere AI i beslutninger som påvirker enkeltpersoner?	☐	☐	☐
5	Er det innført rutiner for å merke AI-generert eller AI-assistert innhold?	☐	☐	☐
6	Har ansatte fått noen form for innføring i hva AI-verktøyene kan og ikke kan gjøre?	☐	☐	☐
7	Er det dokumentert hvilken risikokategori de ulike AI-verktøyene faller i?	☐	☐	☐
8	Har dere en rutine for å sjekke nye AI-verktøy før de tas i bruk?	☐	☐	☐
9	Vet dere hva leverandørene faktisk garanterer om systemene?	☐	☐	☐
10	Har ansatte et sted å melde fra om uventet eller feilaktig AI-bruk?	☐	☐	☐

Tips: spørsmål 2, 3, 4 og 7 veier tyngst. Et «nei» på disse bør senke statusen, selv om de andre svarene er gode.

Slik leser du resultatet

● Grønn (8-10 ja-svar)

God oversikt og kontroll. Neste steg: vedlikehold rutinene og gjør en enkel årlig gjennomgang.

● Gul (4-7 ja-svar)

Et godt stykke på vei, men med tydelige hull. Neste steg: tett de viktigste hullene først.

● Rød (0-3 ja-svar)

Lite oversikt over egen AI-bruk per nå. Neste steg: start med kartleggingen i kapittel 5.

En virksomhet kan ha mange ja-svar og likevel være sårbar hvis den ikke vet hvem som eier problemstillingen, eller hvordan kundevendt bruk faktisk foregår. Vekt derfor spørsmål om ansvar, kundedialog, personpåvirkning og opplæring ekstra tungt når du tolker resultatet.



DEL IV

Konkrete tiltak

Fire områder der AI oftest møter kunder og ansatte direkte - og der det er enkelt å komme i gang.

DEL IV — KONKRETE TILTAK

10. Kundedialog og chatbot

Hvis en bruker samhandler direkte med et AI-system, sier artikkel 50 at personen som hovedregel skal informeres om dette, med mindre det er åpenbart ut fra sammenhengen. Informasjonen skal gis tydelig og senest ved første interaksjon.

Det betyr at en virksomhet ikke bør gjemme denne opplysningen i vilkår eller en personvernerklæring. Den bør være synlig i selve kundereisen, i chatvinduet, i botens introduksjon eller i en tilsvarende tydelig melding.

MAL · Varseltekst for chatbot — velg ett av de tre forslagene og lim det rett inn

① Formell

Passer	Virksomheter med strengere tone, for eksempel finans, helse eller offentlig sektor.
Forslag	«Du kommuniserer nå med en AI-løsning. Svarene genereres automatisk og kan i enkelte tilfeller være ufullstendige. Du kan når som helst be om å bli satt over til en medarbeider.»

② Vennlig

Passer	De fleste forbrukerrettede nettsider og kundeservicechatter.
Forslag	«Hei! Du chatter med vår AI-assistent. Den gjør sitt beste for å hjelpe deg, men er ikke perfekt. Si bare ifra hvis du heller vil snakke med et menneske.»

③ Kort og stram

Passer	Der plassen er begrenset, for eksempel i en liten chat-boble eller på mobil.
Forslag	«Du chatter med en AI. Skriv «menneske» for å bli koblet videre.»

Fem praktiske krav for god chatbotstyring

- Opplys tidlig at brukeren samhandler med AI.
- Gi en enkel vei til menneskelig hjelp når det er relevant.
- Unngå å love mer presisjon enn løsningen faktisk har.
- Loggfør feil og avvik som grunnlag for forbedring.
- Vurder personvern parallelt hvis chatten behandler personopplysninger.

DEL IV — KONKRETE TILTAK

11. Merking av AI-innhold

Artikkel 50 skiller mellom flere typer transparensplikt. En viktig del gjelder AI-systemer som genererer eller manipulerer syntetisk lyd, bilde, video eller tekst, med krav til merking og deteksjon i bestemte situasjoner. AI-innhold er sjelden problemet; manglende merking er det ofte.

For SMB-er er det nyttig å skille mellom tre nivåer: at brukeren må forstå at AI er involvert, for eksempel i kundedialog; at visst innhold må merkes eller gjøres detekterbart der regelverket krever det; og at det finnes unntak, blant annet ved menneskelig redaksjonelt ansvar for tekst publisert om saker av offentlig interesse.

En enkel intern merkepolicy

① Merk alltid

Når

Når innhold er deepfake-lignende eller kunstig manipulert på en måte som kan villedde mottakeren.

② Vurder merking aktivt

Når

Når AI har generert mesteparten av publisert tekst, bilde eller video.

③ Dokumenter internt

Når

Når AI bare har vært et hjelpeverktøy for kladd, struktur eller språkjustering under tydelig menneskelig kontroll.

MAL · Merketekster — fem situasjoner, hver i tre toner, klar til å lime inn

① Generell merking (footer / informasjonsside)

Nøktern

Dette innholdet er helt eller delvis generert med AI.

Tydelig

Merk: Innholdet på denne siden er produsert med hjelp av AI.

Vennlig

Heads up - vi har brukt AI som en hjelpende hånd i dette innholdet.

② Artikkel / blogginnlegg

Nøktern

Artikkelen er skrevet med AI-assistanse og kvalitetssikret av redaksjonen.

Tydelig

AI-generert artikkel. Innholdet er gjennomgått og godkjent av et menneske før publisering.

Vennlig

Denne artikkelen ble skrevet sammen med AI - og lest gjennom av oss før du fikk den.

③ Bilde / illustrasjon

Nøktern

Illustrasjon generert med AI.

Tydelig

Dette bildet er AI-generert og ikke et fotografi av en reell situasjon.

Vennlig

Dette bildet er laget av AI – ikke et ekte foto.

④ Markedsføringstekst / annonse

Nøktern

Denne annonseteksten er utarbeidet med AI-støtte.

Tydelig

Merk: Teksten i denne annonsen er AI-assistert.

Vennlig

Litt AI-hjelp lå bak denne teksten - men budskapet står vi 100% bak.

⑤ Kort badge / ikon-tekst

Nøktern

AI-assistert innhold

Tydelig

Generert med AI

Vennlig

Laget med litt AI-hjelp.

Hvis virksomheten publiserer AI-generert eller AI-bearbeidet innhold utad, bør den ha en tydelig intern beslutning om når merking brukes, hvordan den brukes, og hvem som godkjenner dette. Selv der loven ikke krever synlig merking i alle tilfeller, er en dokumentert praksis ofte klokere enn tilfeldig håndtering.

DEL IV — KONKRETE TILTAK

12. Markedsføring

Markedsføring er et område der AI-bruk ofte glir fra intern effektivisering til reell risikopåvirkning uten at virksomheten merker overgangen. Et verktøy som begynte som hjelp til utkast, kan raskt brukes til personalisering, målretting eller generering av store volumer publisert innhold.

KI-forordningen er ikke den eneste rammen her. Markedsføring kan også reise spørsmål om forbrukerrett, personvern og tillit.

Spør derfor ikke bare: «Kan vi gjøre dette?», men også: «Hvordan vil dette fremstå for mottakeren?»

SJEKKLISTE · AI i markedsføring — gå gjennom alle fire områdene før en kampanje lanseres

① Tekst

Bør sjekkes	Er teksten AI-generert eller AI-assistert? Stemmer fakta, tall og referanser? Er tonen i tråd med merkevaren?
Vanlige feil	Publiserer AI-utkast direkte uten gjennomlesning. Lar AI finne på fakta eller kilder.
Praktisk tiltak	Innfør en fast regel: Ingen AI-tekst publiseres uten at et menneske har lest gjennom og godkjent den.

② Bilder

Bør sjekkes	Kan bildet oppfattes som et ekte foto av en reell person eller situasjon?
Vanlige feil	Bruker AI-bilder som ser ekte ut, uten merking.
Praktisk tiltak	Merk AI-genererte eller AI-manipulerte bilder tydelig, særlig der de kan forveksles med ekte fotografi.

③ Kundedialog

Bør sjekkes	Er det tydelig for kunden at de snakker med en AI-assistent?
Vanlige feil	Chatboten fremstår som et menneske uten å si noe.
Praktisk tiltak	Sørg for en tydelig velkomstmelding, se kapittel 10, og en enkel vei til et menneske.

④ Publisering / godkjenning

Bør sjekkes	Finnes det en fast godkjenningsrunde før innhold publiseres?
Vanlige feil	Innhold publiseres rett fra AI-verktøyet uten en mellomstasjon.
Praktisk tiltak	Sett en enkel regel: Alt AI-assistert innhold går gjennom én navngitt godkjenner.

Unngå: «AI-generert markedsføring er lovlig så lenge den merkes.»

Det er en for grov forenkling. Bedre formulering: AI-generert markedsføring krever vurdering av transparens, innholdskvalitet, eventuelt personvern og risiko for villedning. Merking kan være ett tiltak, men er ikke hele vurderingen.

Smartsona AS tilbyr fotograf til en rimelig pris som kan ta bilder som reduserer behov for AI-genererte bilder. Ta kontakt på post@smartsona.no

DEL IV — KONKRETE TILTAK

13. HR og rekruttering

HR er et av områdene der virksomheter raskt kan bevege seg nær høyrisiko-regimet. AI brukt til rangering, filtrering, vurdering eller prioritering av jobbsøkere krever langt større varsomhet enn et verktøy som bare hjelper HR med å skrive stillingsannonser eller oppsummere intervjunotater.

Det mest risikable er ikke alltid det mest avanserte systemet. Risikoen øker når AI reelt påvirker hvem som får en mulighet, hvordan mennesker vurderes, eller hvilke beslutninger som fattes om dem.

Tre enkle HR-regler

- Hvis AI påvirker utvelgelse, prioritering eller vurdering av kandidater, eskaler vurderingen.
- Hvis systemet fremstår som «rådgivende», men i praksis styrer beslutningen, behandle det som en reell risikofaktor.
- Hvis menneskelig kontroll bare er formell og ikke reell, er det ikke nok.

SJEKKLISTE • 10 HR-kontrollspørsmål — gå gjennom alle tre gruppene før et nytt AI-verktøy tas i bruk

Bruksområde

1	Brukes AI noe sted i rekruttering, screening eller intern personaladministrasjon hos oss?
2	Vet vi nøyaktig hvilke verktøy det gjelder, og hvem som bruker dem?

Påvirkning på mennesker

3	Påvirker verktøyet om en kandidat går videre i en ansettelsesprosess?
4	Påvirker verktøyet vurderinger av nåværende ansatte, for eksempel ytelse, forfremmelse eller oppsigelse?
5	Er det et menneske som faktisk kan overprøve det AI foreslår, i praksis?
6	Vet kandidater og ansatte at AI er involvert i vurderingen av dem?

Dokumentasjon og oppfølging

7	Har vi dokumentert hva systemet faktisk gjør, og hvilke data det bruker?
8	Har vi sjekket om systemet kan favorisere eller forskjellsbehandle bestemte grupper utilsiktet?
9	Vet vi hva vi gjør hvis en kandidat eller ansatt klager på en AI-påvirket vurdering?
10	Har vi avklart hvem internt som er ansvarlig hvis noe går galt?

Svarer du «nei» eller «usikker» på spørsmål 3-6, bør bruken vurderes nærmere før den fortsetter. Svarer du «nei» på 7-10, er det ofte det raskeste å rette opp i.

Unngå: «AI i HR er høyrisiko.»

Det er mer presist å skrive: Visse former for AI i HR og rekruttering kan falle inn under høyrisiko-reglene eller kreve særskilt vurdering, særlig når systemet påvirker vurdering, rangering eller beslutning om enkeltpersoner.



DEL V

Ansvar, dokumentasjon, opplæring

Gjør arbeidet gjenfinnbart og forankret - ikke avhengig av én person sitt minne.

DEL V — ANSVAR, DOKUMENTASJON, OPPLÆRING

14. Ansvarskart

AI-styring blir fort svak hvis «alle» egentlig har litt ansvar, men ingen har det operative eierskapet. De fleste SMB-er trenger ikke en stor komité. De trenger et enkelt ansvarskart, både internt i organisasjonen og i forholdet til leverandøren.

Minimumsroller internt

Rolle	Oppgave
Eier eller daglig leder	Setter retning og aksepterer risiko.
Fagansvarlig eller teamleder	Eier konkret bruk i sin del av virksomheten.
AI-ansvarlig koordinator	Holder oversikt over inventar, rutiner og revisjoner.
IT / sikkerhet / personvern ved behov	Bidrar ved databruk, tilgang og sikkerhet.

Den viktigste regelen er at hvert verktøy eller hver vesentlig AI-bruk bør ha én tydelig navngitt eier. Ikke «markedsavdelingen», men en faktisk person som kan svare på hvorfor verktøyet brukes, hvilke data som går inn, og hvilke kontroller som finnes.

VERKTØY • Ansvarskart for leverandørkjeden — bruk sammen med minimumsrollene over

① Leverandør — hva systemet er bygget for å gjøre

Ansvar	Sørge for at systemet er bygget, testet og dokumentert for det det faktisk skal brukes til.
Typiske feil	Mangelfull eller utdatert dokumentasjon. Ingen rutine for å varsle kunder når systemet endres.
Bør dokumenteres	Teknisk dokumentasjon, risikokategori, kjente begrensninger, rutine for oppdateringer.

② Innkjøper — hvorfor det tas inn i organisasjonen

Ansvar	Vurdere om verktøyet faktisk dekker behovet, og avklare hvem som blir intern eier etter innkjøpet.
Typiske feil	Kjøper inn verktøy uten å sjekke hva leverandøren faktisk garanterer.
Bør dokumenteres	Beslutningsgrunnlaget for innkjøpet, avtalevilkår, hvem som er intern eier.

③ Bruker — hvordan det faktisk brukes i praksis

Ansvar	Bruke verktøyet innenfor grensene som er satt, og melde fra hvis noe virker feil eller uventet.
Typiske feil	Limer sensitiv informasjon inn i åpne, offentlige AI-verktøy. Tar AI-svar for sannhet uten å sjekke.
Bør dokumenteres	Hvilke konkrete oppgaver verktøyet brukes til, og eventuelle avvik som er meldt.

DEL V — ANSVAR, DOKUMENTASJON, OPPLÆRING

15. Dokumentasjonsstruktur

Hvis vurderingen ikke er dokumentert, finnes den i praksis ikke. Mange virksomheter gjør faktisk en vurdering av AI-bruk, men den blir liggende i hodet til én person eller i en e-posttråd ingen finner igjen senere. Samtidig overkompliserer mange dokumentasjon: Målet er ikke en stor compliance-bok, men dokumentasjon som kan gjenfinnes, oppdateres og forstås.

En enkel dokumentpakke

- AI-inventar, kapittel 5.
- Trafikklys- eller risikovurdering per vesentlig bruk, kapittel 8.
- Kort notat om ansvarlig person, kapittel 14.
- Rutine for nye verktøy.
- Eventuell merkepolicy for kundedialog og publisert innhold, kapittel 11.
- Logg over revisjoner og endringer, selve dokumentasjonsloggen under.

Dette er nok i starten. Kommisjonens egen veiledning om AI-kompetansekravet i artikkel 4 peker på at tiltak skal tilpasses kontekst, kompetanse og bruk. Den samme tankegangen gjelder dokumentasjon: nok til å vise oversikt og ansvar, men ikke så tung at den aldri blir oppdatert.

MAL · Dokumentasjonslogg — registrer én vurdering per rad, last gjerne ned Excel-versjonen

De ni feltene

Et fyllbart Excel-ark, *Dokumentasjonsstruktur-Smartsona.xlsx*, følger denne strukturen. Her er et utfyllt eksempel:

Dato	Ansvarlig	System	Vurdering	Risiko	Status
2026-06-15	Kari Nilsen	ChatGPT (Enterprise)	Krever åpenhet ved publisering	Begrenset	Lukket
2026-06-15	Per Olsen	AI-rekrutteringsverktøy	Påvirker kandidater - krever vurdering	Høy	Under arbeid

Feltene i fullversjonen er: dato, ansvarlig person, systemnavn, formål, vurdering, risiko, tiltak, status og neste revisjon.

*Tips: **Skriv en konkret dato i «neste revisjon».** En kalenderpåminnelse er det som faktisk får revurderingen gjort, ikke bare en intensjon.*

DEL V — ANSVAR, DOKUMENTASJON, OPPLÆRING

16. Lær opp organisasjonen

Artikkel 4 krever at leverandører og brukere, «etter beste evne», sikrer et tilstrekkelig nivå av AI-kompetanse hos ansatte og andre som bruker eller opererer AI-systemer på deres vegne. Vurderingen skal ta hensyn til kunnskap, erfaring, opplæring og konteksten systemene brukes i.

Det betyr to ting som er viktige for SMB-er: Det finnes ikke ett obligatorisk kurs som passer alle, og opplæringen bør være rollebasert og praksisnær, ikke bare teoretisk.

Hva «tilstrekkelig nivå» kan bety i praksis

For en liten virksomhet kan et tilstrekkelig nivå være at ansatte:

- vet hvilke verktøy som er godkjent,
- forstår begrensningene i verktøyene de bruker,
- vet når de må eskalere,
- kjenner rutinene for kundedialog, publisering og personpåvirkning,
- og vet hvor de melder fra om feil eller uønsket bruk.

VERKTØY • Opplæringsplan — fem moduler, til sammen rundt 80 minutter

① Modul 1 — Hva er AI, og hva er det ikke?

Mål	Ansatte skal kunne forklare enkelt hva verktøyet faktisk gjør, og hvor grensene går.
Varighet	20 minutter

② Modul 2 — Hvilke AI-verktøy bruker vi, og til hva?

Mål	Ansatte skal vite hvilke godkjente verktøy som finnes, og hva de er ment for.
Varighet	15 minutter

③ Modul 3 — Grenser: hva bør vi ikke bruke AI til?

Mål	Ansatte skal kjenne igjen situasjoner der AI ikke bør brukes uten å spørre først.
Varighet	20 minutter

④ Modul 4 — Ansvar: hvem gjør hva?

Mål	Ansatte skal vite hvem de spør når de er usikre.
Varighet	10 minutter

⑤ Modul 5 — Merking og åpenhet

Mål	Ansatte skal vite når og hvordan AI-generert innhold skal merkes.
Varighet	15 minutter

Gjenta gjerne modul 3 og 5 årlig; grenser og merking er det som glemmes først. Spør «hva ville du gjort?» i stedet for å bare fortelle reglene. Oppdater opplæringen når nye verktøy tas i bruk, og dokumenter at innføringen faktisk er gjennomført.

Smartsona AS har tilrettelagte kurs på 2-4 timer med opplæring og bevisstgjøring av ansatte. Kursene har fokus på å løfte forståelsen av hva som er hjelpemiddelet og hva som er faresignalene i bruk av AI i bedrifter. Ta kontakt for mer informasjon.



DEL VI

Handlingsplan

Prioriter riktig, og hold systemet i gang etter at boken er lagt fra deg.

DEL VI — HANDLINGSPLAN

17. Prioriteringsliste

Det er sjelden nødvendig å løse alt på én gang. Bedrifter utsetter ofte dette arbeidet til det blir stress, men en god SMB-plan prioriterer det som gir mest kontroll raskest, i tre faser à 30 dager.

VERKTØY · 30/60/90-dagersplan — kryss av etter hvert som punktene er gjort

Først — de neste 30 dagene

- Lag et første AI-inventar, kapittel 5.
- Utpek ansvarlig person for de viktigste brukene, kapittel 14.
- Finn alle kundevendte AI-flater og vurder transparens, kapittel 10.
- Finn publisert AI-innhold og avgjør om merkepolicy trengs, kapittel 11.
- Kartlegg om AI brukes i HR, rangering eller beslutningsstøtte, kapittel 13.

Deretter — de neste 60 dagene

- Etabler en enkel rutine for nye AI-verktøy.
- Innfør grunnleggende AI-kompetanseopplæring, kapittel 16.
- Samle dokumentasjonen på ett sted, kapittel 15.
- Gjennomfør første trafikklysvurdering av de viktigste brukene, kapittel 8.

Så — de neste 90 dagene

- Revider høyrisiko-nære brukstilfeller, kapittel 6 og 7.
- Oppdater kontrakter eller leverandørspørsmål der det trengs.
- Evaluer chatbot- og publiseringspraksis.
- Sett fast revisjonsfrekvens, for eksempel halvårlig eller årlig.

DEL VI — HANDLINGSPLAN

18. Hold det levende

AI-styring er ikke et engangsprosjekt. Nye verktøy tas i bruk raskt, og gamle verktøy endrer funksjon eller får nye moduler som endrer risikobildet. Derfor bør virksomheten behandle AI-styring som en liten, levende kontrollsløyfe.

Den enkle kontrollsløyfen

1	Kartlegg ny bruk.
2	Klassifiser raskt.
3	Gjør nødvendige tiltak.
4	Dokumenter kort.
5	Revider når bruken endrer seg.

En enkel årlig rutine

- Kjør AI Act Quick Check, kapittel 9, på nytt minst én gang i året, eller når noe stort endres.
- Gå gjennom dokumentasjonsloggen, kapittel 15, og sjekk om noen «neste revisjon»-datoer har passert.
- Spør de fire spørsmålene fra kapittel 4 på nytt; svarene endrer seg ofte mer enn man tror.
- Følg med på Vedlegg B sine kilder for endringer i tidslinjen, spesielt rundt høyrisiko-fristene.
-

Hvis virksomheten klarer å holde denne sløyfen levende, har den i praksis kommet langt. Målet er ikke perfekt teori; målet er at virksomheten vet hva den gjør, hvem som eier det, og hva som må oppdateres når AI-bruken endrer seg.

Vil du ha hjelp til å sette dette i gang eller holde det i gang?

Smartsona AS hjelper SMB-er med en uavhengig AI Act Quick Check, skriftlige rapporter og løpende oppfølging. Gå inn på www.smartsona.no/ai-act for en rask sjekk.

Book en gratis 20-minutters gjennomgang: post@smartsona.no

Vedlegg A — Ordliste

KI-forordningen / AI Act — EUs forordning (EU) 2024/1689 om kunstig intelligens - det formelle navnet på regelverket denne boken handler om.

Provider / leverandør — Virksomheten som utvikler eller setter et AI-system på markedet under eget navn.

Deployer / bruker — Virksomheten som bruker et AI-system i egen drift, med mindre bruken er rent privat. De fleste SMB-er er «brukere», ikke «leverandører».

AI literacy / AI-kompetanse — Tilstrekkelig kompetanse til å forstå, bruke og håndtere AI i riktig kontekst (artikkel 4).

GPAI — AI for allmenne formål (General Purpose AI) - f.eks. store språkmodeller som kan brukes til mange ulike oppgaver.

Høyrisiko AI-system — AI som kan ha betydelig negativ innvirkning på menneskers grunnleggende rettigheter, f.eks. i rekruttering eller kredittvurdering.

Transparens — Krav om tydelig informasjon når AI brukes i bestemte sammenhenger (artikkel 50).

Deepfake — AI-generert eller manipulert innhold som kan gi et misvisende inntrykk av virkelighet.

FRIA — Konsekvensanalyse om grunnleggende rettigheter (Fundamental Rights Impact Assessment) - kreves for visse høyrisiko-systemer, og ligner en DPIA etter personvernregelverket.

DPIA — Vurdering av personvernkonsekvenser etter GDPR - relevant der AI-bruk involverer personopplysninger.

Regulatorisk sandkasse — Et avgrenset testmiljø der virksomheter kan prøve ut AI-løsninger med veiledning fra myndighetene, og et begrenset vern mot overtredelsesgebyr.

Nkom — Nasjonal kommunikasjonsmyndighet - Norges koordinerende tilsynsmyndighet for KI-forordningen.

Datatilsynet — Norges tilsynsmyndighet for personvern, med en sentral rolle der KI-forordningen og GDPR overlapper.

Digdir — Digitaliseringsdirektoratet - koordinerer bl.a. den regulatoriske KI-sandkassen og «KI-Norge».

Vedlegg B — Referanser og videre lesning

Denne boken bygger på offentlig tilgjengelige kilder per juni 2026. Regelverket er i bevegelse - bruk lenkene under til å sjekke om noe har endret seg siden denne utgaven ble skrevet.

EU-nivå

KI-forordningen (forordning (EU) 2024/1689), offisiell tekst — <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>

EU AI Act Service Desk — offisiell tidslinje for innføring — <https://ai-act-service-desk.ec.europa.eu/en/ai-act/timeline/timeline-implementation-eu-ai-act>

Norge

Datatilsynet — KI-forordningen på 1-2-30 minutter — <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2024/ki-forordningen-pa-1-2-30-minutter/>

Datatilsynet — Bruk og håndheving av kunstig intelligens — <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2025/bruk-og-handheving-av-kunstig-intelligens/>

Datatilsynet — Anbefalinger for godt personvern i utvikling og bruk av KI — <https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/kunstig-intelligens/anbefalinger/>

Datatilsynet — Regulatorisk sandkasse for KI — <https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/>

Datatilsynet — Ny lov om KI sendt på høring — <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2025/ny-lov-om-ki-sendt-pa-horing/>

Nkom — Regulatorisk sandkasse for KI — <https://nkom.no/ki/regulering/regulatorisk-sandkasse>

Regjeringen.no — Paving the way for safe and innovative use of AI in Norway — <https://www.regjeringen.no/en/whats-new/gjor-norge-klar-for-trygg-og-innovativ-ki-bruk/id3093081/>

Om fristene som ble forskjøvet i mai 2026 (Digital Omnibus for KI)

EU AI Act Implementation Timeline (artificialintelligenceact.eu) — <https://artificialintelligenceact.eu/implementation-timeline/>

Gibson Dunn — Postponed High-Risk Deadlines and Other Key Changes — <https://www.gibsondunn.com/eu-ai-act-omnibus-agreement-postponed-high-risk-deadlines-and-other-key-changes/>

Sidley — EU AI Act Transparency Obligations: Preparing for Compliance by 2 August 2026 — <https://datamatters.sidley.com/2026/06/24/eu-ai-act-transparency-obligations-preparing-for-compliance-by-2-august-2026/>

Disse lenkene var aktive da denne utgaven ble skrevet. Endrer en adresse seg, søk på sidetittelen hos den respektive myndigheten.

Vedlegg C — Hvordan bruke denne boken internt

Det enkleste er å bruke boken i tre møter, fremfor å lese den fra perm til perm:

Møte 1 Kartlegg verktøy og ansvar

Bruk

Kapittel 4, 5 og 14 - de fire spørsmålene, AI-inventarlisten og ansvarskartet.

Møte 2 Sett trafikklys og prioriter tiltak

Bruk

Kapittel 6-9 for å klassifisere, og kapittel 17 for å prioritere de neste 30/60/90 dagene.

Møte 3 Vedta dokumentasjon, opplæring og revisjonsrutine

Bruk

Kapittel 15, 16 og 18 - dokumentasjonsloggen, opplæringsplanen og den årlige rutinen.

En virksomhet som gjør dette godt, er ikke «ferdig» med KI-forordningen. Men den har flyttet seg fra uklarhet til styring - og det er det viktigste første steget.

Vedlegg D — Om Smartsona AS

Smartsona AS hjelper norske SMB-er å forstå og etterleve KI-forordningen uten juridisk tungspråk. Vi bygger et enkelt AI Act Quick Check-verktøy som gir status, risikovurdering og konkrete neste steg - og vi hjelper bedrifter gjennom hele veien fra kartlegging til dokumentasjon.

Klar for neste steg?

Book en gratis 20-minutters gjennomgang, eller send oss spørsmål om noe i denne boken.

post@smartsona.no

Et lite, frivillig bidrag

Har denne boken gitt deg eller bedriften din ny innsikt? Da setter Smartsona AS stor pris på et frivillig bidrag på kr 99,- - betalt til Vipps på 920 59 188 (QR kode) eller kontonummer 3606 27 54057.

Det er et ønske, ikke en forutsetning: du står fritt til å bruke hele boken og alle malene uten å betale noe. All støtte vil gå til utarbeidelse til ny-utvikling av gratis tjenester/informasjon



© Smartsona AS, 2026. Denne håndboken er et praktisk utgangspunkt og er ikke juridisk rådgivning.