



DEHN.

ADVOKATFIRMAET DEHN

Infoteamdagene 2026

Juridiske utfordringer med bruk av kunstig intelligens (KI) i ERP.

Advokat Grete Funderud Stillum

18.03.2026



DEHN
ADVOKATFIRMAET DEHN

Hvordan tenke «KI-jus»?

- Kunnskap om relevant jus
 - Grunnleggende kunnskap hos ledelsen og «alle» involverte
 - Advokat/jurist med dybdekunnskap som rådgiver og del av teamet
 - Gjennomgående endring: Fra tillatelse/konsesjon til egne dokumenterte vurderinger, ofte basert på risiko
- Plan for å fange opp, vurdere og oppfylle relevante juridiske krav i alle faser
 - Anskaffelse
 - Utvikling og implementering, ofte med endringer
 - Vedlikehold og drift, ofte med ny bruk og utvikling
- Hva som er rettslig relevant varierer ...
 - Rolle - leverandør eller kunde, eller begge deler
 - Datagrunnlag
 - Bruk
 - Sektor



Hovedfokus: «Vanlige private bedrifter som bruker KI i ERP»



KI-loven / AI Act.

- Hva og hvem?
 - Ikraft: EU 2024-27. Norge fra august 2026?
 - Sikre grunnleggende rettigheter og demokratiske verdier, særlig innen helse, utdanning, arbeidsliv, kritisk infrastruktur og retts håndhevelse
 - Virksomheter som utvikler, benytter eller videreformidler KI-systemer, med særregler for tilbydere av Generelle AI-modeller – GPAI (som ChatGPT)

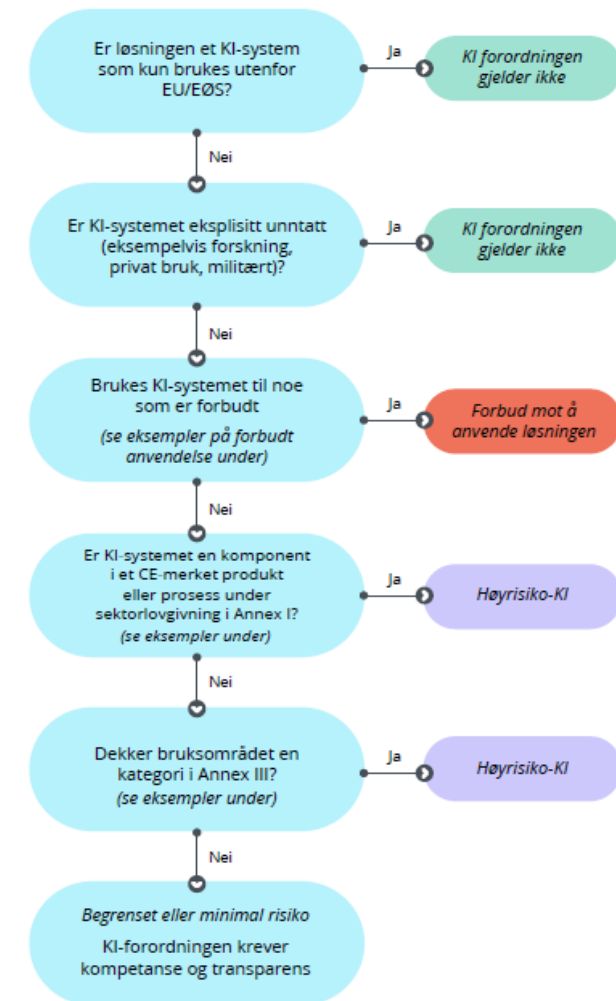
• Kravene i KI-loven beror på risikoklasse og rolle

• Risikoklasser - bruk:

Uakseptabel risiko (forbudt)
Høy risiko
Begrenset risiko
Minimal risiko

• Roller:

- Bruker (idriftsetter - deployer)
- Leverandør (provider)
 - Systemleverandør, og kanskje distributør, konsulent og kunde
 - Endret «tiltenkt bruk» basert på dokumentasjon fra leverandøren
 - Tilgjengelig for eksterne brukere/tredjeparter



Eksempler på forbudt anvendelse

1. Manipulerende KI
2. Utnyttelse av sårbare grupper
3. Sosial scoring
4. Prediktiv kriminalitetsvurdering ("pre-crime")
5. Masseskrapping til ansiktsgjenkjenning
6. Emosjonsgjenkjenning i arbeid og skole
7. Biometrisk kategorisering av sensitive egenskaper
8. Sanntids ansiktsgjenkjenning i det offentlige rom for politibruk

Eksempler på Annex I anvendelse

1. Maskiner
2. Leker
3. Biler og fritidsbåter
4. Heiser og kabelbaner
5. Radioutstyr / IoT
6. Verneutstyr
7. Medisinsk utstyr og diagnostikk

Eksempler på Annex III anvendelse

1. Biometrisk identifikasjon
2. Kritisk infrastruktur
3. Utdanning og kompetansevurdering
4. Arbeids- og personalforvaltning
5. Tilgang til viktige tjenester
6. Retts håndhevelse
7. Grensekontroll / migrasjon
8. Rettspleien & demokratiske prosesser

Bruken avgjør risikoklassen.

Vurder bruken og endringer i bruken:

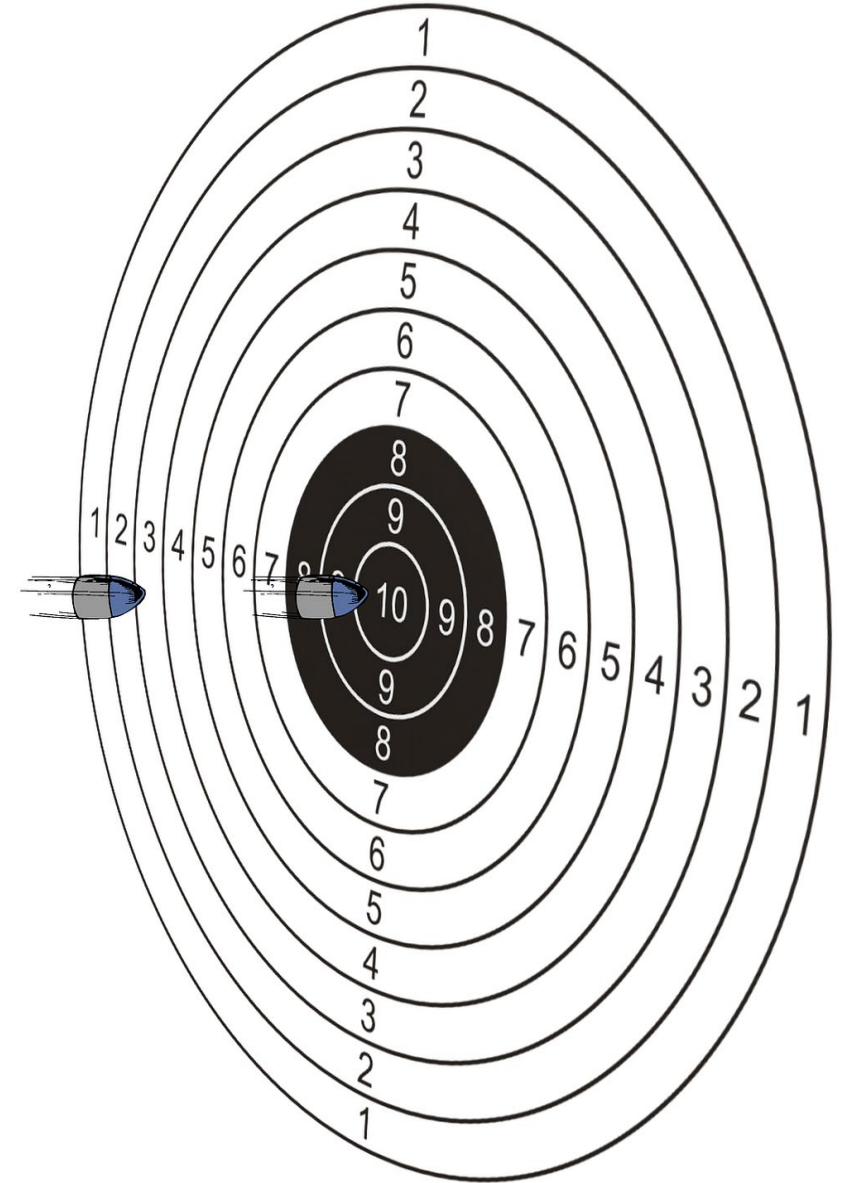
- Ikke et juridisk skille i KI-loven mellom AI-assistenter vs. AI-agenter
- Funksjonelle forskjeller påvirker pliktene - Hvilken risiko innebærer bruken?
- Systemdokumentasjon og interne retningslinjer for bruk

KI i forretningssystemer vil normalt ikke være forbudt eller høyrisiko, men kanskje:

- Sikkerhetskomponent i et Annex I-produkt, f.eks en maskin
- Annex III-funksjoner, unntatt bl.a. de som ikke utgjør en betydelig risiko for skade på fysiske personers helse, sikkerhet eller grunnleggende rettigheter, eller ikke påvirker utfallet av beslutningsprosesser.

Samme funksjonalitet kan kategoriseres ulikt - f.eks:

- Begrenset/ minimal risiko ved bruk til:
 - Lagerstyring
 - Etterspørselsprognoser og produksjonsplanlegging
 - Automatisk fakturahåndtering
- Høy risiko ved bruk til:
 - Vurdering av ansattes prestasjoner, beslutninger om oppsigelser eller forfremmelser
 - Automatisk rekruttering eller CV-screening



Krav til KI med begrenset/ minimal risiko (1).

- Oppfordring til frivillig etterlevelse av adferdsregler og etiske retningslinjer
- Vurderinger og dokumentasjon for alle KI-systemer/ funksjonalitet – krav 1
 - Risikokategoriseringen (basert på bruk)
 - Rolle
 - Tiltak for å redusere risiko
 - Unngå skyggesystemer...
- Åpenhet (Transparency) – krav 2
 - Brukere skal informeres om samhandling med et KI-system, med mindre det er åpenbart
 - KI-generert/manipulert dype forfalskninger av bilde-, lyd- eller video (deepfakes) skal merkes
 - KI-generert tekst «for å informere allmennheten» skal normalt merkes
 - Brukeren og den som blir berørt av beslutninger skal i mange tilfelle kunne få en forklaring på hvordan KI-systemet har bidratt til beslutningsgrunnlaget
 - Etiske og ev. avtalemessige tilleggskrav om å informere om når KI har spilt en vesentlig rolle, eller når det er relevant for kontekst og tillitt



Krav til KI med begrenset/ minimal risiko (2).

KI kompetanse for alle (AI Literacy) - krav 3

- Grunnleggende forståelse av hvordan KI-løsningen fungerer, hva den kan og ikke kan
- Kjennskap til hva som utgjør datagrunnlaget og integrasjoner, og om/ hvordan bruker kan berike datagrunnlaget
- Hvordan bruke løsningen forsvarlig, vurdere output kritisk, avdekke feil og bias, hvordan sikkerhet og ansvarlighet håndteres, vanlige feil og begrensninger
 - Retningslinjer for bruk
- Konkret vurdering av roller og teknologi
 - KI-assistent: Hvordan stiller gode spørsmål og gi instruksjer (promter)
 - KI-agent: Innblikk i konfigurering og grad av autonomi
- Løpende øvelse - opplæring
- Dokumenter kompetansevurderinger, og hvem som har mottatt opplæring i hva og når



Viktige tilleggskrav for Høyrisiko-KI – sjelden i ERP.

Krav	Beskrivelse
Risikovurdering og styring	Identifisere, vurdere og håndtere risiko knyttet til KI-bruken, inkludert risiko for helse, sikkerhet, personvern og grunnleggende rettigheter. Kontinuerlig prosess gjennom hele livssyklusen til KI-systemet.
Testing	Grundig testing før og under bruk for å sikre at de fungerer som tiltenkt og oppfyller krav til sikkerhet og pålitelighet.
Loggføring	Det skal føres tilstrekkelig logging av KI-systemets bruk og hendelser for å sikre sporbarhet og mulighet for etterkontroll.
Datakvalitet og -styring	Data brukt til trening og drift av KI må være av høy kvalitet, korrekt håndtert og i samsvar med personvernregler. Anonymisering og tilgangskontroll er viktige tiltak.
Åpenhet og informasjon	Brukere skal informeres om at de samhandler med KI-systemer, og KI-generert innhold skal merkes tydelig. Åpenhet om systemets funksjoner og begrensninger er påkrevd.
Menneskelig tilsyn	Mulighet for menneskelig tilsyn og kontroll ved beslutninger som påvirker enkeltpersoner.
Nøyaktighet	Passende nivå av nøyaktighet for å unngå feil og skjevheter som kan føre til diskriminering eller andre uønskede konsekvenser.
Robusthet	Systemene må være teknisk robuste og motstandsdyktige mot feil, uventede situasjoner og forsøk på manipulasjon.
Cybersikkerhet	Det skal implementeres tiltak for å beskytte KI-systemene mot cyberangrep, uautorisert tilgang og datalekkasjer.
Opplæring	Økt krav til opplæring.
FRIA?	Krav til Fundamental Rights Impact Assessment – FRIA for offentlige myndigheter og visse private virksomheter basert på sektor og bruk.



Personvern.

- Relevant dersom personopplysninger inngår i datagrunnlaget
 - Hva er en personopplysning? Fysiske personer som kunder, leverandører, ansatte og andre, inkl. kontaktpersoner. ID-bruk?
Ulike type personopplysninger: «ordinære» eller «særlige kategorier».
 - Behov for gode tilgangsreguleringer for KI-systemet
- Rolleavklaring:
 - Behandlingsansvarlig - felles behandlingsansvarlig - databehandler. Brukes data til systemtrening?
- Rettslig grunnlag (behandlingsgrunnlag) og formålsbegrensning
 - Eks: Samtykke, avtale, berettiget interesse som må dokumenteres
- Dataminimering og datakvalitet
- Informasjon – personvernerklæring for «alle»
- Automatiserte avgjørelser (KI-agenter mv)
 - Avgjørelser som har rettsvirkning eller i betydelig grad påvirker en person. Grensen mot anbefalinger.
 - Forbudt eller bare rett til å nekte? Uansett krav om behandlingsgrunnlag og informasjon.
 - Mulighet for overprøving
- Risikovurderinger
 - Et egnet tiltak for å oppnå et sikkerhetsnivå tilpasset risikoen
 - DPIA (personvernkonsekvensvurdering) må gjennomføres dersom bruk av KI-assistenten medfører høy risiko for enkeltpersoners rettigheter



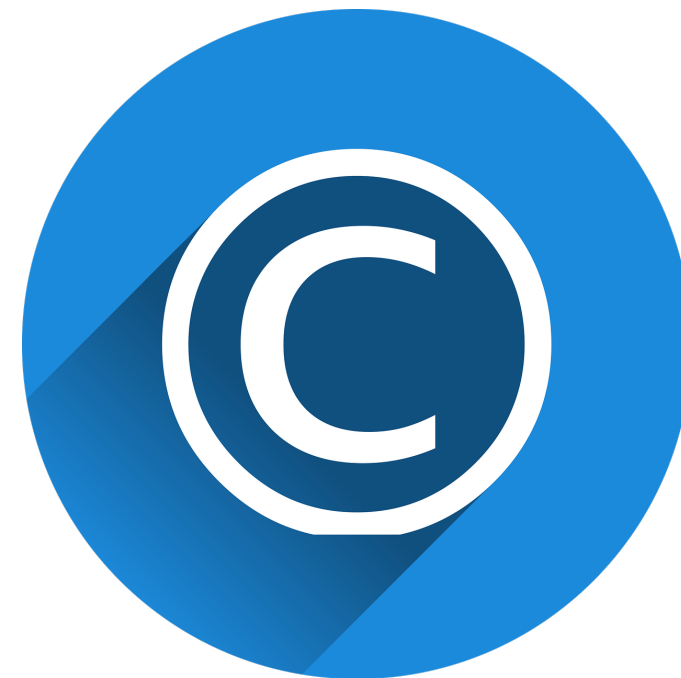
Personvern – leverandør.

- Databehandleravtale
 - Ramme for: type data, formål, sikkerhet, revisjon og dokumentasjon, bistand, lagringssted, bruk av underleverandører, endringer og sletting ved avslutning.
- Behandlingssted – lagring, support ved fjernaksess mv
 - Norge, EU
 - USA eller andre tredjeland
- Overføringsgrunnlag
 - Adekvansbeslutning – for noen land og for sertifiserte virksomheter i USA, Data Privacy Framework - DPF
 - SCC, BCR eller unntak i art. 49
 - Ekstra tiltak etter Schreems II: Kryptering, pseudonymisering
 - Dokumentert risikovurdering basert på type data og tiltak- TIA
- Exit-rett og strategi
 - Brudd på DBA eller bortfall av overføringsgrunnlag



Rettigheter til input og output .

- Datagrunnlag i KI-tjenesten og fra bruker
 - Opphavsrettslig beskyttet: Tekst, bilder, musikk, foto mv
 - Databasevern
 - Krever avtale, lisens eller annet rettslig grunnlag for bruk i KI
- Data fra KI:
 - Trening av KI-systemet? Bruk for andre kunder?
- Data Act – Dataforordningen
 - Gjelder (delvis) i EU, og blir norsk lov
 - Gir brukere rett til å få tilgang til, bruke og dele data generert av produkter de eier eller tjenester de bruker (IoT, industrielle systemer, m.m.)
 - Hovedsakelig ikke-personlige og data
 - GDPR gjelder parallelt
 - Tilbydere kan beskytte forretningshemmeligheter
 - Regler mot urimelige kontraktsvilkår og innlåsing
- EU GPAI Code of Practice - krav om rutiner for opphavsrett og transparens



Arbeidsrettslige forhold.

- «Alltid» personvern når personopplysninger om ansatte inngår i datagrunnlaget
 - Behandlingsgrunnlag og formålsbegrensning
 - Innsyns forskriften («e-post forskriften»): Begrenset mulighet til innsyn i eposter og annet elektronisk lagret materiale i personlige områder
 - Begrenset rett til overvåkning av ansatte – logger
 - Bevissthet rundt tilgangsstyring av KI-systemet som ofte «deler» brukers tilgang, men finner mye mer...
- Arbeidsmiljøloven og hovedavtalen i arbeidslivet
 - Medbestemmelse, informasjon og drøfting med tillitsvalgte ved innføring av nye teknologier som kan påvirke arbeidsmiljøet



Mer «KI-jus» - ikke uttømmende.

- Taushets-/konfidensialitetsplikt etter lov eller avtale
- Etske regler og bransjenormer, som kan bli kutyme
- Lover om produktansvar, produktsikkerhet, CE-merking
 - Ansvar for skade forårsaket av defekte produkter, sikkerhetskrav
 - Produksansvarsloven vil endres etter nytt EU Produktansvarsdirektiv
 - Teknologiske løsninger i kritiske systemer kan kreve sertifisering eller godkjenning
- Konkurranselovgivning feks ved innhenting og bruk av informasjon
- Sikkerhetsloven for virksomheter som håndterer nasjonal sikkerhet, kritisk infrastruktur og annen samfunns viktig informasjon
- Digital sikkerhetslov og sektorspesifikke regler, som f.eks DORO, krever cybersikkerhet og hendeshåndtering for kritiske tjenester
- Helse- og omsorgstjenester har omfattende krav til faglig forsvarlige helse- og omsorgstjenester og god pasientsikkerhet
- Offentlige virksomheter er underlagt forvaltningsloven, offentlighetsloven og arkivloven, med særlige krav ved bruk av KI



Juridiske sjekklister - primært for begrenset eller minimal risiko KI

- Prosjektoppstart
- Prosjektgjennomføring m/ veiledende eksempel på dokumentasjon
- Vedlikehold og drift
- Avtaleregulering

Disclaimer: Utgangspunkt for videre utvikling og tilpasning.

I alle fasene kan og bør vi bruke KI som assistent ved utarbeidelse og evaluering, men (kanskje) med informasjon om bruk av KI til de vi samarbeider med 😊



Prosjektoppstart av KI.

- Unngå unødige begrensninger!
 - Ønske om innovasjon og konkurrere med USA- eksperimentell tilnærming
- Kartlegg og spør leverandør / konsulent(er)
 - Avklar risikonivået
 - Klarlegg tiltenkt bruk (behovet) og vurder om det faller inn under forbudt eller høyrisiko KI
 - Vurder datagrunnlaget
 - Personopplysninger eller data m/begrensede rettigheter, og grunnlag for å bruke dataene
 - Innhent dokumentasjon på hvordan KI-funksjonen fungerer
 - Viktig utgangspunkt for vurderinger
 - Har leverandør/konsulent vurdert KI-lovens krav? Risikoklasse? Krav om sertifisering?
 - Ta høyde for endringer, ny bruk
 - Vurder behov/ ønske om kompetanse
 - Hvem bør ta ansvar for juridiske krav ved implementering, og senere oppdateringer?
Ulike typer juridisk kompetanse.
 - Avklar krav til sikkerhet og behandlingssted
 - Ønskelig og lovlighetsbegrensning?

Prosjektgjennomføring av KI.

- Plan, ansvars-/ oppgavefordeling for oppsett, konfigurasjon, tilpasning av KI
 - Hvem gjør hva, når? Husk faren for utilsiktede rolleendringer både etter KI-loven og GDPR
- Sikring av rett datatilgang m/ tilgangsstyring og grunnlag (personvern og annet)
- Sette opp sikkerhet og logging for å spore databruk, KI anbefalinger eller beslutninger og funksjon/ feil
- Testing med testcaser for å sikre rett risikoklassifisering og lovlig bruk
- Retningslinjer for bruk
 - Basert på systemets dokumentasjon, ev. etter videreutvikling/justering basert på planlagt bruk
- Bygging av kompetanse med plan for opplæring av alle
- Dokumentasjon
 - Sørg for teknisk og funksjonell dokumentasjon av valg og tilpasninger
 - Dokumenter hvordan kunden skal bruke systemet, datagrunnlag, kompetanse og opplæringsplan
 - Vurderinger av risiko og klassifiseringer av personvern, KI-loven og andre lovkrav. Ev. DPIA eller FRIA?
- Plan for vedlikehold og ny/ endret bruk
- Godkjenning og driftssetting/ aktivering av KI-funksjon, gjerne gradvis



Dokumentasjon av lav risiko - Fiktivt eksempel.

System: Infor LN - Prediktiv vedlikehold

Leverandør: xx

Produktbeskrivelse og bruksanvisning:

xxxx.x [Navn på produkt], xx[[lenke til produktbeskrivelse og bruksanvisning-ID](#)]

Implementert av: [Konsulentfirma], dato xx

Hva gjør KI-funksjonen?

Systemet analyserer sensordata fra produksjonsutstyr og predikerer når vedlikehold er nødvendig. Den bruker maskinlæring til å identifisere mønstre som indikerer slitasje eller feil.

Hvordan bruker vi det?

Vedlikeholdsteamet mottar varsler når systemet predikerer behov for vedlikehold. En tekniker vurderer alltid varselet før vedlikehold planlegges. Systemet tar ikke automatiske beslutninger. Vi har retningslinjer for bruk.

Hvilke data brukes?

Temperatur, vibrasjon, strømforbruk og driftstid fra produksjonsmaskiner. Ingen personopplysninger.

Risikovurdering:

Lav risiko - systemet påvirker ikke grunnleggende rettigheter. KI-systemet er ikke integrert i en maskin som omfattes av produktsikkerhetsregelverk (Annex I). Feil prediksjon kan føre til unødvendig vedlikehold eller utsatt vedlikehold, men ikke fare for liv/helse da menneskelig vurdering alltid gjøres.

Vår rolle: Idriftsetter. Vi bruker systemet i tråd med leverandørens produktbeskrivelse og bruksanvisning.

Kompetanse:

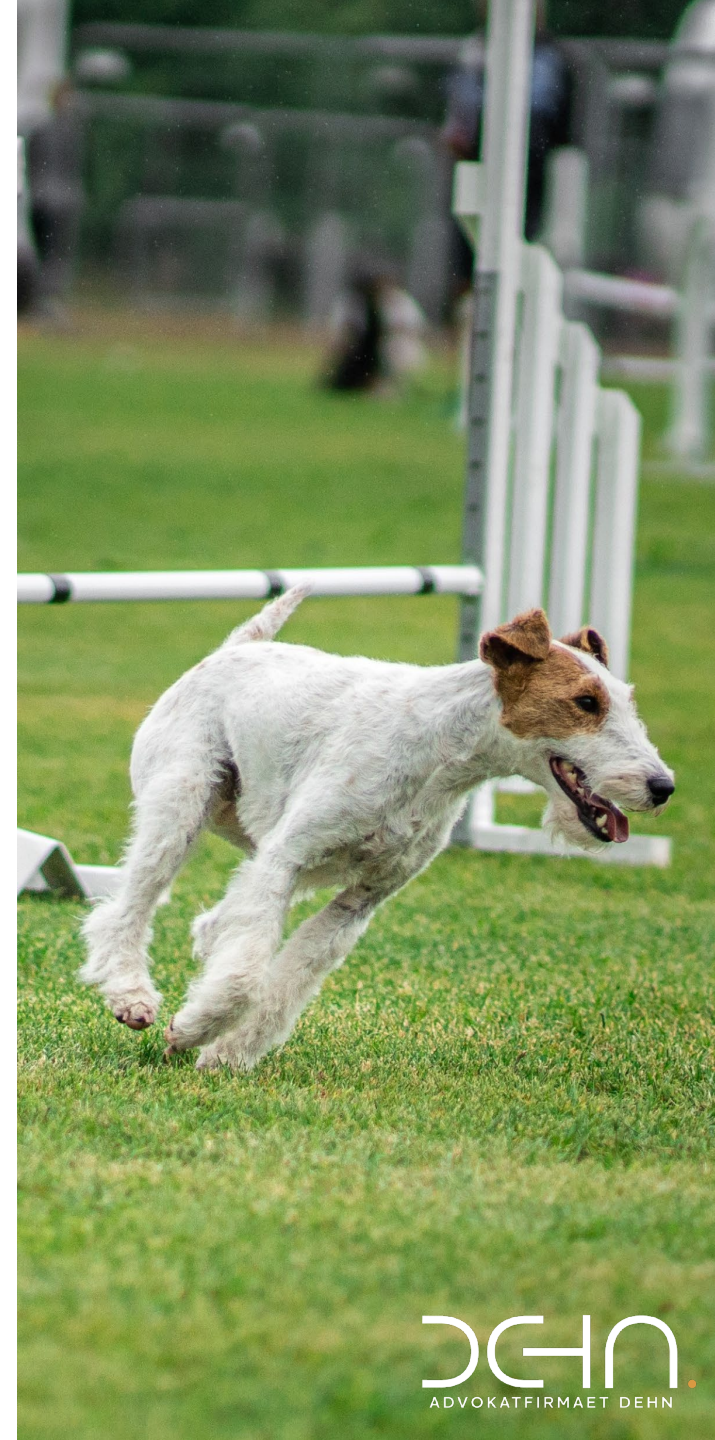
Vedlikeholdsteamet har fått opplæring i bruk, begrensninger og tolkning.

Det er rutiner for vurdering av varsler og menneskelig kontroll, samt jevnlig oppdatering av kompetanse ved endringer.

Ansvarlig: Produksjonssjef.

Vedlikehold av KI - evaluering.

- Overvåking av hvordan KI-systemet/ funksjonen fungerer
 - Logging av bruk
 - Sikring av nødvendig menneskelige tilsyn
- Endringer kan medføre behov for nye vurderinger og dokumentasjon
 - Ny funksjonalitet og endret bruk
 - Endrede lovregler, retningslinjer
- Løpende opplæring og inspirasjon for lovlig og best mulig bruk
- Retting av «feil» og kontinuerlig forbedring
- Rutine for rapportering av avvik, ev. til tilsynsmyndigheter
- Årlig/halvårlig systematisk gjennomgang, ev. revisjon
 - Avdekke endringer i bruk og lovverk
 - Vurdere behov for nye vurderinger og oppdatering av dokumentasjon
 - Vurdere behov for endring i avtaler



Avtaleregulering av KI.

- Egen avtale eller del av en avtale
- Krav til funksjon/ bruk, kvalitet og ytelse, sikkerhet, inkl. sikring mot bias, åpenhet og forklarbarhet. Angivelse av risikokategori(er) og datagrunnlag.
 - Teknisk og funksjonell dokumentasjon, bruksanvisning. Ev. samsvarserklæring og CE-merking .
- Rettigheter til teknologi, modeller, dokumentasjon, rapporter, generert data
- Rolleavklaring: Leverandør(er) vs. idriftsetter - RACI-matrise
 - Hvem vurderer og dokumenterer faktisk bruk, og ev. avvik fra leverandørens brukerbeskrivelse og ny vurdering av risikokategori(er), og behov for tiltak?
 - Hvem vurderer og dokumenterer datagrunnlag, personvern, sikkerhet, tilgangsstyring, logging og sletting?
 - Hvem identifiserer og vurderer andre juridiske krav enn KI-loven og personopplysningsloven?
 - Hvem sørger for retningslinjer for bruk og god kompetanse/opplæring av brukere?
- Tredjeparter og underleverandører
- Databehandleravtale og ev. overføringsgrunnlag
- Kostnadsstruktur og triggere
- Ansvarsforhold - begrensninger
- Kriterier for driftssetting?
- Endringer og leveranser etter driftssetting
- Exit-regulering



KI-assistenter i arbeidslivet – en praktisk guide

*Ekspertgruppen for ansvarlig innføring
og bruk av KI-assistenter*

Tips til mer kunnskap om «KI-jus».

- Dele usecases og vurderinger – inspirere og bli inspirert
- KI-assistenter i arbeidslivet – en praktisk guide «Regjeringens KI-veileder» fra 16.06.2025
 - <https://www.regjeringen.no/no/dokumenter/ki-assistenter-i-arbeidslivet-en-praktisk-guide/id3109040/>
- Digital Norway – artikler og kurs
 - <https://digitalnorway.com/>
- Høring – utkast til KI-loven m/norsk oversettelse av KI-forordningen (AI Act)
 - <https://www.regjeringen.no/no/dokumenter/3112327/id3112327/?expand=horingsnotater>
- The AI Act Explorer fra EU m/AI Act for søk, oppsummeringer, tidslinje, guider, artikler, compliance checker mv
 - <https://artificialintelligenceact.eu/ai-act-explorer/>
- Dansk Industri -Juridisk hjelp til bruk af AI
 - <https://www.danskindustri.dk/vi-radgiver-dig/virksomhedsregler-og-varktojer/ai/juridiske-ai-varktojer/>
- EU har varslet en Digital omnibus package med review of all existing tech legislation to ease the burden on companies by cutting for example reporting or transparency obligations i desember 2025
- Bransjeveiledninger ol

Takk for meg!

DEHN.
ADVOKATFIRMAET DEHN



Grete F. Stillum

Advokat MNA | Partner

☎ 990 90 710

✉ stillum@dehn.no

🌐 www.dehn.no

Advokatfirmaet Dehn .

Advokatfirmaet Dehn er Asker og Bærums største advokatfirma, og ble kåret til Årets Bedrift i Bærum 2024.

Vi holder til i Sandvika, med klienter over hele landet. Våre 24 advokater har bred erfaring innen både forretningsjus og privatjus. Vi tilbyr spesialisert juridisk bistand til bedrifter, privatpersoner og det offentlige, og jobber tett med våre klienter for å bidra til at de når sine mål.

Sentrale kompetanseområder:

- Selskapsrett og transaksjoner
- Eiendom og entreprise
- Forvaltning og offentlig rett
- Konkurs og restrukturering
- Kontraktsrett
- Tvisteløsning og prosedyre
- Immaterialrett (IPR) og markedsføringsrett
- IT, teknologi og digitalisering
- Arbeidsrett
- Personvern
- Arverett
- Barnerett
- Barnevern
- Familie- og skifterett
- Strafferett



DEHN

ADVOKATFIRMAET DEHN

Høy kompetanse • Tydelig rådgivning • Praktiske løsninger •