Poul Schmith
KAMMERADVOKATEN

AI-UDDANNELSEN

RESPONSIBLE AI GOVERNANCE & COMPLIANCE

Poul Schmith/Kammeradvokaten udbyder i samarbejde med DTU Compute uddannelsen Responsible AI Governance & Compliance. Uddannelsen klæder dig på til at kunne identificere og håndtere de centrale regler, problemstillinger og risici forbundet med udvikling og anvendelse af løsninger baseret på kunstig intelligens (AI). Det gælder bl.a. reglerne i databeskyttelsesforordningen (GDPR) og den nye AI-forordning om anvendelse af løsninger baseret på AI i praksis. Uddannelsen er relevant for alle, der arbejder med AI-løsninger og compliance i virksomheder eller hos offentlige myndigheder. Du undervises af førende eksperter på området, og undervisningen gøres levende gennem cases og konkrete værktøjer og skabeloner.

DIT UDBYTTE

Som deltager på uddannelsen opnår du følgende:

- Overblik og forståelse for de relevante regler for udvikling og anvendelse af AI-løsninger i praksis fra førende eksperter med erfaringer fra konkrete projekter.
- Kortlægning og viden om de centrale risici samt gode råd til, hvordan man kan håndtere dem.
- Træning i anvendelse af konkrete værktøjer og skabeloner, som du efterfølgende kan bruge i din egen organisation, f.eks. skabelon til konsekvensanalyse vedrørende databeskyttelse, kravkatalog m.v.
- Mulighed for sparring og faglig ajourføring på efterfølgende gratis event.
- Sparring og netværk med øvrige deltagere inden for området.

UDDANNELSE I TO NIVEAUER – FOR GENERALISTEN OG PRAKTIKEREN

Uddannelsen er opdelt i niveauerne 'Foundation' og 'Practitioner', og det er op til dig, om du ønsker begge niveauer, eller om du blot foretrækker et af dem.

Foundation-niveauet giver det nødvendige overblik over og forståelse for, hvad kunstig intelligens (AI) er, hvordan AI fungerer og kan anvendes til at skabe værdi i praksis samt de centrale regler i navnlig databeskyttelsesforordningen og AI-forordningen om ansvarlig anvendelse af AI-løsninger. Samtidig får du indblik i de centrale risici forbundet med brugen af AI-løsninger, og hvordan man kan håndtere disse på en effektiv måde.

Foundation er derfor relevant for bl.a. databeskyttelsesrådgivere (DPO'ere), personer der skal arbejde i en DPO-lignende rolle eller tæt sammen med en DPO, IT-ansvarlige IT-sikkerhedschefer (CIO/CISO), Compliance Officers, Legal Counsels, Contract Managers, andre jurister, rådgivere og informationssikkerhedsfolk samt udviklere, brugere og procesejere fra forretningen.

Practitioner-niveauet klæder dig på til at implementere konkrete compliance-tiltag i praksis, herunder implementering og vedligeholdelse af et Responsible AI Governance og Compliance-program, udarbejdelse af konsekvensanalyser (DPIA) og Fundamental Rights Impact Assessments i AI-projekter, implementering af Privacy by Design og by Default og grundlæggende AI-principper i AI-løsninger samt håndtering af kontraktuelle forhold ved anskaffelse af AI-løsninger.

Målgruppen for Practitioner omfatter bl.a. databeskyttelsesrådgivere (DPO'ere), personer der skal arbejde i en DPO-lignende rolle eller tæt sammen med en DPO, IT-ansvarlige, IT-sikkerhedschefer (CIO/CISO), Compliance Officers, Legal Counsels, Contract Managers eller andre jurister, rådgivere og informationssikkerhedsfolk.

I dette katalog kan du læse detaljeret om alle vores moduler på begge niveauer på uddannelsen.

OVERBLIK OVER UDDANNELSENS INDHOLD

Uddannelsen afholdes i følgende moduler:

MODUL	FOUNDATION	PRACTITIONER
Modul 1	Kunstig intelligens og anvendelsesområder i praksis.	Implementering og vedligeholdelse af et Responsible AI Governance og Compliance-program.
Modul 2	Overblik over de retlige rammer for brug af AI-systemer.	Udarbejdelse af en konsekvensanalyse (DPIA) og en Fundamental Rights Impact Assessment i et AI-projekt.
Modul 3	Betydningen af standarder og etiske retningslinjer.	Implementering af Privacy by Design og by Default og grundlæggende AI-principper i AI-løsninger.
Modul 4	Databeskyttelsesforordningens betydning for udvikling og anvendelse af AI-systemer.	Håndtering af kontraktuelle forhold ved anskaffelse af AI-løsninger.
Modul 5	Overblik over AI-forordningens regler.	
Modul 6	Risikostyring og menneskelig kontrol.	
Modul 7	AI & cybersikkerhed.	
Modul 8	AI til brug for automatiske, individuelle afgørelser og profilering.	
Modul 9	Håndtering af de registreredes rettigheder og oplysningsforpligtelser.	
Modul 10	Governance og egenkontrol samt håndhævelse og sanktioner.	

DETALJERED LÆRINGSMÅL OG UNDERVISNINGSINDHOLD FOR MODULERNE PÅ FOUNDATION OG PRACTITIONER.

Moduler på Foundation

MODUL 1 – *Kunstig intelligens og anvendelsesområder i praksis*

LÆRINGSMÅL/KOMPETENCER	UDDYBENDE BESKRIVELSE
Forstå, hvad kunstig intelligens (AI), herunder machine learning, er.	• De alment anerkendte definitioner af AI/machine learning, herunder fra OECD. • De grundlæggende karakteristika for AI/machine learning. • Svag/stærk AI og General AI (The Singularity). • Forskellen på AI og tilstødende teknologier såsom robotics og RPA.
Forstå og kunne kende forskel på de forskellige typer af AI-teknologier og -modeller.	• Regelbaserede modeller (ekspertsystemer). • Maskinlæring. • Supervised / unsupervised learning. • Neurale netværk / deep learning. • Statiske og dynamiske modeller. • Foundation models. • Generative AI. • General purpose AI.
Forstå AI-teknologistakken.	• AI-applikationer, platform, computerinfrastruktur. • Behovet for processorkraft.
Forstå, hvor og hvordan AI anvendes i praksis – use cases.	• Praktiske use cases. • Automated Decision Making (ansættelser, kreditvurderinger, forsikringspræmier, forvaltningsafgørelser m.v.). • Beslutningsstøtte (risikobaseret kontrol, svigbekæmpelse m.v.). • Service/vejledning (målrettet vejledning og service, målrettet markedsføring, produktanbefalinger m.v.). • Værktøjer (generative AI, talegenkendelse, billedgenkendelse, tekstgenkendelse, kildesøgning). • Cases fra myndigheder og virksomheder/AI-signaturprojekter. • Brugen af AI hos offentlige myndigheder, på det finansielle område og i sundhedssektoren.
Forstå milepælene i den historiske udvikling af AI-systemer og AI-megatrends.	• Tidlig udvikling fra 1950'erne og dannelsen af begrebet "AI". • Tidlige ekspertsystemer. • AI-somre og -vintre og gennembrud. • Seneste udviklinger (AI indbygget i cloudapplikationer, AI-megatrends m.v.).

MODUL 2 – *Overblik over de retlige rammer for brug af AI-systemer*

LÆRINGSMÅL/KOMPETENCER	UDDYBENDE BESKRIVELSE
Forstå, hvilke retsregler der typisk kommer i spil ved anvendelse af AI-løsninger.	• Overblik over det retlige landkort. • Databeskyttelsesforordningen (GDPR). • AI-forordningen. • Anti-diskriminationslovgivning. • Digital Services Act. • Immaterialretten (ift. IP-rettigheder). • Relevante regler om ansvar og produktansvar, herunder AI-liability directive.
Forstå betydningen af centrale dele af databeskyttelsesforordningen, når AI-løsninger behandler personoplysninger.	• Brugen af personoplysninger, anonyme og syntetiske data i AI-løsninger. • Betydningen af de grundlæggende principper. • Hjemmel til behandling af personoplysninger ved træning og anvendelse af AI-løsningen. • Pligten til databeskyttelse gennem design og gennem standard-indstillinger ved udvikling og anvendelse af AI-løsninger. • Pligten til at udarbejde en konsekvensanalyse vedrørende databeskyttelse (DPIA) ved brug af AI-løsninger.
Forstå og få et overblik AI-forordningens regler og pligter til brugere af AI-systemer.	• Anvendelsesområde, aktører og centrale definitioner. • Generelle principper for alle AI-systemer. • Den risikobaserede tilgang. • Forbud mod visse AI-systemer. • Kravene til brugere, der anvender høj risiko AI-systemer og foundation models. • Transparensforpligtelser. • Pligten til at udarbejde en Fundamental Rights Impact Assessment (FRIA). • Sanktioner for noncompliance og håndhævelse af reglerne.
Få et overblik over relevante internationale frameworks og ISO-standarder for AI-anvendelse.	• Standarders rolle i AI-forordningen. • Centrale ISO-standarder for anvendelse af AI-løsninger. • Centrale AI-risk management frameworks.
Få et overblik over væsentlige etiske principper og metoder for anvendelse af AI.	• Dataetiske principper for ansvarlig AI. • Ethics Guidelines for Trustworthy AI af EU AI High Level Expert Group.

MODUL 3 – *Betydningen af standarder og etiske retningslinjer*

LÆRINGSMÅL/KOMPETENCER	UDDYBENDE BESKRIVELSE
Få et overblik over relevante internationale frameworks og ISO-standar- der for AI-anvendelse.	• Standarders rolle i AI-forordningen. • Centrale ISO-standarder for anvendelse af AI-løsninger. • Centrale AI-risk management frameworks.
Få et overblik over væsentlige etiske principper og metoder for anvendelse af AI.	• Dataetiske principper for ansvarlig AI. • Ethics Guidelines for Trustworthy AI af EU AI High Level Expert Group.

MODUL 4 *- Databeskyttelsesforordningens betydning for udvikling og anvendelse af AI-systemer*

LÆRINGSMÅL/KOMPETENCER	UDDYBENDE BESKRIVELSE
Forstå betydningen af centrale dele af databeskyttelsesforordningen, når AI-løsninger behandler personoplysninger.	• Brugen af personoplysninger i AI-systemer, herunder udledte personoplysninger. • Anonyme og syntetiske data i AI-løsninger. • Betydningen af de grundlæggende principper. • Hjemmel til behandling af personoplysninger ved træning og anvendelse af AI-løsningen.

MODUL 5 *- Overblik over AI-forordningens regler*

LÆRINGSMÅL/KOMPETENCER	UDDYBENDE BESKRIVELSE

Forstå og få et overblik AI-forordningens regler og pligter til brugere af AI-systemer.	• Anvendelsesområde, aktører og centrale definitioner.
	• Generelle principper for alle AI-systemer:
	  • Responsible AI / Trustworthy AI
	  • Menneskelig kontrol og overvågning
	  • Teknisk robusthed og sikkerhed
	  • Databeskyttelse og data governance
	  • Transparens
	  • Diversitet, ikke-diskrimination og rimelighed
	  • Social and environmental well-being.
	• Den risikobaserede tilgang.
	• Forbud mod visse AI-systemer.
	• Kravene til brugere, der anvender høj risiko AI-systemer og foundation models.
	• Transparensforpligtelser.
	• Pligten til at udarbejde en Fundamental Rights Impact Assessment (FRIA).

MODUL 6 - *Risikostyring og menneskelig kontrol*

LÆRINGSMÅL/KOMPETENCER	UDDYBENDE BESKRIVELSE
Forstå og få et overblik over reglerne om risikostyring i forhold til anvendelse af AI-løsninger.	• Risikostyring og menneskelig kontrol. • Privacy by design/default i AI-løsninger. • Konsekvensanalyser vedrørende databeskyttelse (DPIAs). • Fundamental Rights Impact Assessments (FRIAs).
Forstå de typiske risici og konsekvenser for personer ved anvendelse af AI-løsninger.	• Gennemgang af taksonomi over typiske konsekvenser (privacy harms) for de registreredes rettigheder og frihedsrettigheder ved brug af AI-løsninger. • Gennemgang af taksonomi over typiske risici for de registrerede, der kan forårsage ovennævnte konsekvenser ved brug af AI-løsninger, herunder begrænsninger i AI's potentiale.
Forstå de typiske risici og konsekvenser for organisationer ved anvendelse af AI-løsninger.	• Gennemgang af taksonomi over typiske risici for organisationer ved anvendelse af AI-løsninger.
Forstå centrale tekniske og organisatoriske foranstaltninger, der kan bruges til at mitigere risiciene.	• Overblik over centrale risikostyringsstrategier. • Konkrete eksempler på organisatoriske og tekniske foranstaltninger, der kan mitigere risiciene.
Forstå pligten til og processen for at indtænke databeskyttelse m.v. i AI-løsningens design (privacy by Design/Default).	• Overblik over betydningen af reglerne om privacy by design/default ved udvikling og anvendelse af AI-løsninger. • Eksempler på Privacy Enhancing Technologies og centrale data og procesorienterede designprincipper.
Forstå, hvornår man skal lave en konsekvensanalyse vedrørende data- beskyttelse (DPIA) ved anvendelse af en AI-løsning, og hvad DPIA'en skal indeholde.	• Tærskel/triggeranalyse af, hvornår man skal lave en DPIA. • Indholdet af en DPIA.
Forstå, hvornår man skal lave en Fundamental Rights Impact Assessment (FRIA) ved anvendelse af en AI-løsning, og hvad FRIA'en skal indeholde.	• Tærskel/triggeranalyse af, hvornår man skal lave en FRIA. • Indholdet af en FRIA. • FRIA'ens sammenhæng med DPIA'en.

MODUL 7 - *AI & Cybersikkerhed*

LÆRINGSMÅL/KOMPETENCER	UDDYBENDE BESKRIVELSE
Forstå kravene til identifikation, evaluering og håndtering af risici forbundet med anvendelse af AI-løsninger.	• Kravene i GDPR til at udarbejde en risikovurdering vedrørende behandlingssikkerhed. • Kravene i AI-forordningen om robusthed og cyber security i løsningens livscyklus. • Øvrige relevante regelsæt om sikkerhed ved anvendelse af AI-løsninger (NIS2, DORA etc.).
Forstå metoder til risikoevaluering af beskyttede aktiver.	• Overblik over beskyttede aktiver. • Metoder til risikovurderinger, herunder fra ENISA og Digitaliserings-styrelsen. • Relevante kontroller.
Forstå typiske sikkerhedsmæssige risici og angrebstyper ved anvendelse af AI-løsninger.	• Gennemgang af risikotaksonomi over typiske trusler, herunder: • Manipulation af modellen. • Manipulation af datasets (”data poisoning”). • Inputs designet til at forårsage fejl i modellen (”adversarial examples”).
Forstå best practices samt tekniske og organisatoriske sikkerheds- foranstaltninger til at mitigere risiciene og sikre robusthed.	• Gennemgang af katalog over typiske sikkerhedsforanstaltninger, herunder: • Overvågning af input og output. • Styring af modeludvikling og -træning. • Penetrationstests. • Security-by-design og privatlivsfremmende teknologier. • Krav til logning. • Brug af gendannelsesplaner og backup-løsninger.

MODUL 8 - *Automatiske, individuelle afgørelser og profilering*

LÆRINGSMÅL/KOMPETENCER	UDDYBENDE BESKRIVELSE
Forstå, hvornår man anvender automatiske, individuelle afgørelser og profilering.	• Forskellen på fuldautomatiske afgørelser, brug af AI til beslutningsstøtte og profilering. • Eksempler inden for offentlig forvaltning, kreditvurderinger, behandling af jobansøgninger, markedsføring, vejledning, sundhedsområdet m.v. • At kunne forskel på profilering og statistisk analyse.
Forstå det skærpede hjemmelskrav ved anvendelse af automatiske, individuelle afgørelser og profilering.	• Skærpede krav til retsgrundlaget for fuldautomatiske afgørelser og profilering, herunder samtykke, kontrakt og lovhjemmel
Forstå pligten til at fastsætte passende foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder samt legitime interesser.	• Pligten til at fastsætte foranstaltninger, herunder mulighed for menneskelig indgriben m.v.
At kunne identificere og håndtere relevante typiske risici forbundet med brugen af automatiske, individuelle afgøreler og profilering.	• Identifikation og håndtering af risici såsom automatiseringspar- tiskhed, sikre menneskelig kontrol og indgriben, sikre transparens (forklarlighed) af resultatet af afgørelserne m.v.

MODUL 9 - *Håndtering af de registreredes rettigheder og oplysningsforpligtelser*

LÆRINGSMÅL/KOMPETENCER	UDDYBENDE BESKRIVELSE
Forstå oplysningspligten ved behandling af personoplysninger i AI-løsninger.	• Kravene til oplysningspligtens indhold ved behandling af person-oplysninger til træning og anvendelse af algoritmer. • Retten til oplysning om forekomsten af automatiske, individuelle afgørelser, ret til menneskelig indgriben og ret til at modtage menings fulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser.
Forstå GDPR's rettigheder for de registrerede i en AI-kontekst.	• Ret til ikke at være genstand for en automatisk, individuel afgørelse. • Rettigheder ved brug af profilering, herunder retten til at gøre indsigelse mod profilering. • Retten til indsigt, berigtigelse, sletning m.v. af træningsdata, input- og outputdata/udledte data.
Forstå AI-forordningens rettigheder for kunder/borgere.	• Retten til en forklaring på individuelle afgørelser. • Oplysningsforpligtelser om brug af AI-løsninger.

MODUL 10 - *Governance og egenkontrol samt håndhævelse og sanktioner*

LÆRINGSMÅL/KOMPETENCER	UDDYBENDE BESKRIVELSE
Forstå de væsentligste karakteristika ved et effektivt Responsible AI Governance & Compliance-program.	• Kunne fastslå, hvornår man er bruger, og hvornår man kan blive leverandør (og dermed underlagt langt skrappere krav end brugere), hvis man ændrer eller videreudvikler standardløsninger. • Identifikation af centrale interne og aktører og interessenter. • Fordeling af ansvar for programmets aktiviteter – compliance-tilgange.
Forstå kravene til udarbejdelse af relevante interne politikker og retningslinjer for anvendelse af AI-løsninger.	• Overblik over relevante interne politikker og retningslinjer for anvendelse af AI-løsninger.
Forstå kravene til uddannelse af medarbejdere vedrørende anven-delse af AI-løsninger.	• Kravene til uddannelse af medarbejdere, så de forstår, hvordan AI fungerer, reglerne for anvendelse af AI og de væsentligste risici forbundet hermed (AI literacy).
Forstå kravene til egenkontrol for overholdelse af reglerne om anvendelse af AI-løsninger.	• Kravene til og de centrale elementer i risikobaseret egenkontrol.
Forstå, hvilke myndigheder der fører tilsyn med reglerne.	• Overblik over tilsynsmyndighederne på området. • Datatilsynet og øvrige tilsynsmyndigheder.
Forstå tilsynsmyndighedernes håndhævelsesbeføjelser.	• Overblik over tilsynsmyndighedernes håndhævelsesbeføjelser, herunder retten til at udstede påbud, forbud og indgive politianmeldelse m.v.
Forstå sanktionsmulighederne for overtrædelse af reglerne samt mulighed for erstatning.	• Overblik over mulighederne for bøder og øvrig straf for overtrædelse af reglerne for offentlige myndigheder og virksomheder. • Mulighederne for at få erstatning for materiel eller immateriel skade.

Moduler på Practitioner

MODUL 1 - *Implementering og vedligeholdelse af et Responsible AI Governance og Compliance-program*

LÆRINGSMÅL/KOMPETENCER	UDDYBENDE BESKRIVELSE
At forstå de væsentligste skridt og forudsætninger ved implementering af et AI Governance og Compliance-program.	• Fastlæggelse af scope, målbillede og vision. • Identifikation af centrale interne og aktører og interessenter og deres roller. • Fordeling af ansvar for programmets aktiviteter – compliance-tilgange. • Fastlæggelse af fælles AI-terminologi. • Gode råd til at få succes med implementering af programmet.
At kunne fastsætte en effektiv egenkon-trolmekanisme til kontrol af, at reglerne overholdes.	• Krav til og best practices for at fastsætte en effektiv og risikobaseret egenkontrolmekanisme til kontrol af, at reglerne overholdes. • Typer af kontroller og frekvens heraf. • Sammenhæng til DPO'ens kontrol.
At kunne stille forslag til konkrete KPI'er og privacy metrics til evaluering og rapportering af complianceindsatsen.	• Eksempler på konkrete metoder, privacy metrics og modenheds målinger, der kan anvendes til at evaluere på og rapportere om complianceindsatsen over for centrale interessenter.

MODUL 2 - *Udarbejdelse af en konsekvensanalyse (DPIA) og en Fundamental Rights Impact Assessment i et AI-projekt*

LÆRINGSMÅL/KOMPETENCER	UDDYBENDE BESKRIVELSE
At kunne udarbejde en tærskel/trigger-analyse for at finde ud af, om der er krav om at lave en DPIA og en FRIA for at anvende en AI-løsning.	• Kriterierne og reglerne for, hvornår man skal lave en DPIA og en FRIA ved anvendelse af AI-løsninger. • Overvejelser om, hvorvidt man skal lave en DPIA/FRIA for både udviklings- og anvendelsesfasen. • Undervisningen sker med udgangspunkt i en case og skabelon til en tærskel/trigger-analyse, som udleveres på kurset.
At kunne udarbejde en DPIA og FRIA.	• Kravene til processen og metoden. • Identifikation af centrale stakeholders (DPO'en, CISO, domæneeksperter, forretningen etc.). • Kravene til indholdet af DPIA'en og FRIA'en. • Pligten til høring af de registrerede. • Pligten til høring af Datatilsynet. • Undervisningen sker med inddragelse af en skabelon til en DPIA og en FRIA, som udleveres på kurset.
At kunne foretage en risikovurdering af risici for de registrerede rettigheder og frihedsrettigheder samt fastsætte effektive tekniske og organisatoriske foranstaltninger til at håndtere disse risici.	• Identifikation af centrale og typiske risici forbundet med brug af AI-løsninger. • Risikomitigeringsstrategier og fastsættelse af effektive tekniske og organisatoriske foranstaltninger til at håndtere risiciene. • Undervisningen sker med inddragelse af et risikokatalog over typiske risici ved anvendelse af AI-løsninger med forslag til konkrete tekniske og organisatoriske foranstaltninger til at håndtere disse risici, som udleveres på kurset.
At kunne sikre rettidig ajourføring og vedligeholdelse af DPIA'en/FRIA'en.	• Regler om og metoder til at sikre rettidig ajourføring og vedligeholdelse af DPIA'en og FRIA'en, herunder når behandlingen af personoplysninger eller formålet med AI-løsningen ændrer sig.

MODUL 3 - *Implementering af Privacy by Design og by Default og grundlæggende AI-principper i AI-løsninger*

LÆRINGSMÅL/KOMPETENCER	UDDYBENDE BESKRIVELSE
At kunne stille konkrete forslag til privacy by Privacy by Design/ Default-strategier og principper ved udvikling og anvendelse af AI-løsninger.	• Dataorienterede og procesorienterede designprincipper og strategier. • Anvendelse af strategierne og principperne ved både egen udvikling og ved brug af standardløsninger. • Relevante tests og algoritmisk audit
At kunne stille konkrete forslag til implementering af Privacy Enhancing Technologies (PETs) ved udvikling og anvendelse af AI-løsninger.	• Anvendelse af PETs ved både egen udvikling og ved brug af standardløsninger, f.eks. brug af syntetiske data til træning, teknologier til at skabe transparens (Explainable AI), metoder til at undgå bias, federated learning, differential privacy og homomorfisk kryptering.
At kunne stille konkrete krav om ansvarlig AI til leverandører af udvikling af AI-løsninger samt kunne screene standard AI-løsninger for overholdelse af kravene (AI Audit).	• Kravstillelse af relevante krav om ansvarlig AI til udviklingsleverandører med inddragelse af et kravkatalog med krav og strategier til udvikling og anvendelse af AI-løsninger, som udleveres på kurset. • Screening af standard AI-løsninger for overholdelse af kravene med inddragelse af en skabelon til et AI Audit ved anskaffelse af AI-standardapplikationer, som udleveres på kurset.

MODUL 4 - *Håndtering af kontraktuelle forhold ved anskaffelse af AI-løsninger*

LÆRINGSMÅL/KOMPETENCER	UDDYBENDE BESKRIVELSE
Forståelse for relevante kontraktmæssige overvejelser ved anskaffelse af AI-løsninger.	• Redskaber til at håndtere AI-kontrakter i praksis. • Kravspecificering. • Metoder til tilsyn og kontrol med kontraktparten.
Forståelse for ansvaret for brugen af AI-løsninger og ansvarsbegrænsninger og garantier i kontraktgrundlaget.	• Ansvarsbegrænsninger, erstatningsbestemmelser og garantier.
Forståelse for relevante krav om IP-rettigheder i kontraktgrundlaget.	• Forslag og overvejelser vedrørende kontraktbestemmelser om beskyttelse af immaterialretligt beskyttet materiale, herunder software, (trænings)data og output.

TILMELD DIG UDDANNELSEN PÅ WWW.POULSCHMITH.DK/AI-UDDANNELSEN TILMELD →