

Opleiding : Generatieve AI, beheer van en toezicht op gebruik in bedrijven in de richting van verantwoord bestuur

AI-governance ontwikkelen / implementeren, LLM-toepassingen beveiligen

Praktijkcursus - 3d - 21u00 - Ref. LLN

Prijs : 2010 € V.B.

NEW

Deze cursus leidt deelnemers door de governance en controle van LLM's en generatieve AI. U leert hoe u het gebruik kunt beveiligen, auditen en controleren, intern beleid kunt definiëren en toezicht kunt houden op AI-projecten binnen een regelgevend en strategisch kader.

Pedagogische doelstellingen

Aan het einde van de training is de deelnemer in staat om:

- ✓ De belangrijkste principes van generatieve AI en de rol van LLM's identificeren.
- ✓ De risico's en gevolgen van het gebruik van LLM's in bedrijven analyseren.
- ✓ AI-governance opzetten, aangepast aan regelgevingskwesties.
- ✓ Intern beleid en handvesten ontwikkelen voor het gebruik van GenAI.
- ✓ Toezicht houden op en auditen van AI-projecten om naleving en ethiek te waarborgen.
- ✓ De geleidelijke implementatie van AI-governance in bedrijven sturen.

Doelgroep

DPO's, CISO's, compliance managers, data-, AI-, digitale en innovatiedirecteuren, IT-juristen, AI-projectmanagers.

DEELNEMERS

DPO's, CISO's, compliance managers, data-, AI-, digitale en innovatiedirecteuren, IT-juristen, AI-projectmanagers.

VOORAFGAANDE VEREISTEN

Geen technische vereisten. Kennis van regelgeving of auditkwesties wordt op prijs gesteld.

VAARDIGHEDEN VAN DE CURSUSLEIDER

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vakkennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

BEOORDELINGSMODALITEITEN

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, ...

De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

Voorafgaande vereisten

Geen technische vereisten. Kennis van regelgeving of auditkwesties wordt op prijs gesteld.

Opleidingsprogramma

1 Inzicht in generatieve AI en hoe LLM's werken

- Vereenvoudigde werking van LLM's (GPT, Claude, LLaMA, enz.).
- Belangrijkste toepassingen: chatbots, agents, generatie, extractie, co-pilots.
- Integratiearchitecturen: API's, RAG's, multi-agenten, LangChain, ontologieën.
- Interacties tussen LLM's en bestaande systemen.

2 Risicoanalyse en GenAI-regelgeving

- Vooroordelen, hallucinaties en vervalsingen.
- Instabiliteit en misinterpretatie.
- Vertrouwelijkheidsrisico's en datalekken.
- Afhankelijkheid van leveranciers en soevereiniteitskwesties.
- RGPD en implicaties voor generatieve AI.
- Europese AI-wet: verplichtingen en tijdschema's.

3 AI-governance en organisatorische structurering

- IA-commissie of ethische eenheid.
- Belangrijkste rollen: PO, DPO, CISO, Data Steward, Architect.
- Functioneel bestuur tussen bedrijf, IT, juridische afdeling en beveiliging.
- Communicatie en rapportage van AI-beslissingen.
- Methoden voor het integreren van governance in AI-projecten.

4 Intern beleid, toezicht en controleerbaarheid

- Handvesten voor het gebruik van GenAI tools (intern en extern).
- Beheer van aanwijzingen en gegenereerde inhoud.
- Menselijk toezicht op resultaten en processen.
- Vertrouwelijkheidsbeleid voor inkomende/uitgaande gegevens.
- Traceerbaarheid van beslissingen genomen door LLM's.
- Tools voor documentatie en technisch beheer: LangChain, PromptLayer, Trulens, MLflow.

Praktisch werk

Opstellen van een kader voor AI-gebruik in bedrijven. Groepswerk over het gebruiksbeleid voor een echte AI-casus. Identificatie van risico's, controlemechanismen en toezicht.

5 Evaluatie en controle van generatieve AI-projecten

- IA projectfiches.
- Use case classificatiematrix: risico, waarde, controle.
- Specifieke IADPIA.
- Ethische en sociale aanvaardbaarheidscriteria.
- Projectchecklists (RGPD, AI-wet, beveiliging).
- Go/no-go-proces of gecontroleerde inzet.

PEDAGOGISCHE EN TECHNISCHE MIDDELEN

- De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
- Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
- Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

TOEGANGSMODALITEITEN EN TERMIJNEN

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

TOEGANKELIJKHEID VOOR MINDERVALIDEN

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.

6 Beheer van gegevens, kennis en ontologieën

- Kwaliteit van invoergegevens: opschoning, beveiliging, verifieerbaarheid.
- Documentaire grondslagen en bronnen voor de RAG.
- Bedrijfsontologieën en kennisstandaardisatie.
- Semantische validatie en controle van informatiestromen.
- Prestatie-indicatoren voor ethiek en naleving.

Praktisch werk

Plan d'action de gouvernance IA Générative. Priorisation des actions à mettre en place dans l'entreprise. Structuration d'une gouvernance progressive. Alignement stratégique.

Data en plaats

KLAS OP AFSTAND

2026 : 16 maa., 22 juni, 21 sep., 30 nov.

PARIS LA DÉFENSE

2026 : 16 maa., 15 juni, 14 sep., 23 nov.