

Wahlweise als Inhouse-Seminar oder Webinar buchbar

# KI & Risikomanagement

## Lerne wie du typische Risiken im Umgang mit großen Sprachmodellen (LLM) identifizierst und mitigierst

### Zielgruppe

- ▶ Alle Branchen inkl. aller Personen und Funktionsträger im Unternehmen, die sich mit der Einführung und Nutzung von KI/ML befassen (Business, Innovation, IT, Marketing, Vertrieb, Personal, Datenschutz, Informationssicherheit, Recht etc.)

### Dauer

- ▶ Empfohlen als 1-tägiges Vor-Ort-Seminar oder Webinar

### Preis

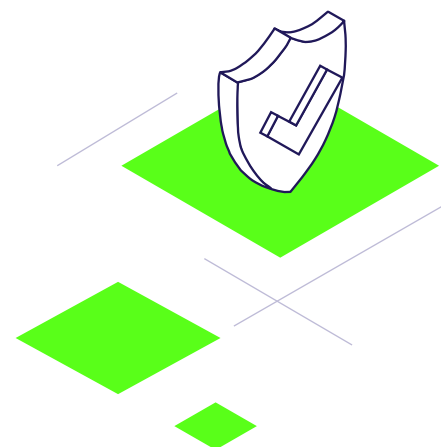
- ▶ EUR 800,- p. P. zzgl. MwSt., zzgl. Reisekosten bei Durchführung vor Ort. Mindestteilnehmerzahl 4 Personen. Bei kleineren oder größeren Gruppen Preis auf Anfrage.

KI und ML bieten enormes Potenzial – gleichzeitig entstehen neue **Risiken, die Unternehmen aktiv steuern** müssen. Neben etablierten Anforderungen aus Datenschutz, Informationssicherheit und Recht geraten besonders solche Risiken in den Fokus, die aus den Ergebnissen und Entscheidungen **großer Sprachmodelle (LLM)** hervorgehen, zum Beispiel rund um Fairness, Erklärbarkeit, Datenqualität, Urheberrecht oder Verzerrungen.

In unserem Seminar/Webinar arbeitet ihr mit unserer **praxiserprobten Risikoanalyse** entlang des gesamten **KI-Lebenszyklus**. So lernt ihr Risiken und passende **Mitigationsmaßnahmen** (technisch und organisatorisch) im Umgang LLMs systematisch zu identifizieren und wirksam zu beherrschen – vom Training über Reasoning und Operations bis zum Output.

Die Vorlage, die dabei entsteht, könnt ihr **unmittelbar für eure eigenen Vorhaben** nutzen – als praxistaugliches Arbeitsmittel für den Alltag und als Grundlage für eine professionelle **KI-Governance**.

So schafft ihr schnell mehr Sicherheit, mehr Klarheit und mehr **Digital Trust**.



**Besprich euren individuellen Bedarf in einem persönlichen Gespräch mit uns**



**Stephanie Knappe-Stauder**

T +49 6172 / 177 630

E [anfrage@microfin.de](mailto:anfrage@microfin.de)

# Inhalte



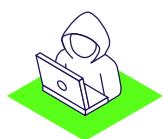
## Identifikation, Kategorisierung und Bewertung spezifischer LLM-Risiken

u.a. bzgl. Datenschutz, Erklärbarkeit, Fairness, geistiges Eigentum, Genauigkeit, Interaktion, Robustheit, Zuverlässigkeit etc.



## Beherrschung LLM-spezifischer Risiken als Aufgabe der IT-/KI-Governance

Integration KI-Risikomanagement in bestehende Governance-Strukturen mit Fokus auf Angemessenheit, Nutzen und Wirksamkeit



## Überblick, Erläuterung und Beispiel möglicher Mitigation spezifischer LLM-Risiken

wie z. B. Adversarial Attacks, Copyright Violation, Data Poisoning, Deepfakes, Drift, Knowledge Cutoff Jailbreaks, Prompt Injection etc.



## Sicherstellung unternehmensweiter Achtsamkeit im Umgang potenzieller LLM-Risiken

wie z. B. Aufklärung der LLM-Nutzer über (versteckte) Gefahren und Sensibilisierung für mögliche Risiken



## LLM-Risikovorsorge durch Umsetzung allgemeiner Vorgaben aus Gesetz und Regulatorik

wie z. B. aus KI-VQ, DSGVO, DORA, NIS-2 sowie ISO/IEC 23894:2023 etc.



## Startzusammenstellung LLM-spezifischer Risikoanalyse inkl. Mitigationsmaßnahmen

Muster-Vorlage entlang der Phasen im KI-Lebenszyklus zur Steuerung erkannter Risiken und Mitigationen

## Eure Trainer



**Sebastian Dosch**

Enabler |  
Principal Consultant



**Stefan Wendt**

Enabler |  
Managing Partner