

## **AI342 Informationssicherheit 24/7: KI-basierte Compliance-Hotline**

### **Kurzbeschreibung:**

Im praxisorientierten Workshop **AI342 Informationssicherheit 24/7: KI-basierte Compliance-Hotline** lernen Sie, wie Sie einen Echtzeit-Sprachassistenten für die Compliance-Hotline Ihres Unternehmens entwickeln können. Durch die Nutzung der OpenAI Realtime API und die Anbindung an Ihr internes Wissensmanagementsystem schaffen Sie eine Lösung, die rund um die Uhr verfügbar ist und den Anforderungen der Informationssicherheit gerecht wird.

Der Kurs beginnt mit einer Einführung in KI-basierte Compliance-Hotlines, wobei die Bedeutung und Vorteile solcher Systeme im Compliance-Bereich sowie deren Anwendungsfälle und Nutzen für die Informationssicherheit erläutert werden. Anschließend wird die Architektur eines Echtzeit-Sprachassistenten vorgestellt, einschließlich eines Überblicks über die OpenAI Realtime API und deren Einsatzmöglichkeiten sowie der Integration in bestehende Wissensmanagementsysteme.

Im weiteren Verlauf des Kurses konzentrieren wir uns auf die Implementierung der Sprachschnittstelle, einschließlich der Einrichtung und Konfiguration der OpenAI Realtime API für Sprachinteraktionen sowie der Verarbeitung von Spracheingaben und der Generierung von Sprachausgaben. Darüber hinaus wird die Anbindung an das Wissensmanagementsystem behandelt, um den Datenabruf und die Verarbeitung aus internen Wissensdatenbanken sicherzustellen und die Aktualität und Relevanz der bereitgestellten Informationen zu gewährleisten.

Ein besonderer Fokus liegt auf Sicherheits- und Datenschutzaspekten, wobei die Einhaltung von Compliance-Richtlinien und Datenschutzbestimmungen sowie die Implementierung von Sicherheitsmaßnahmen zum Schutz sensibler Daten thematisiert werden. Abschließend werden Methoden zum Testen und Optimieren des Sprachassistenten vorgestellt, einschließlich der Durchführung von Funktionstests, Fehlerbehebung und Anpassung des Systems basierend auf Nutzerfeedback. Der Kurs endet mit der Bereitstellung und Wartung des Sprachassistenten in der Unternehmensumgebung sowie der Planung regelmäßiger Aktualisierungen und Wartungsstrategien.

### **Zielgruppe:**

- Entwickler
- IT-Fachleute
- Compliance-Beauftragte

### **Voraussetzungen:**

Um den Inhalten und dem Lerntempo des Kurses **AI342 Informationssicherheit 24/7: KI-basierte Compliance-Hotline** gut folgen zu können, empfehlen wir folgende Vorkenntnisse:

- [AI020 AI & Data Science Practitioner](#) (alternativ Grundkenntnisse in Programmierung und Erfahrung mit IT-Systemen)
- [AI030 AI & Data Science Expert](#) (alternativ Grundkenntnisse in Empfehlungssystemen sowie Prompt Engineering)

- Grundkenntnisse im Bereich Datenschutz und Compliance sind von Vorteil

### Sonstiges:

**Dauer:** 3 Tage

**Preis:** 2150 Euro plus Mwst.

### Ziele:

Nach Abschluss der Schulung **AI342 Informationssicherheit 24/7: KI-basierte Compliance-Hotline** werden Sie in der Lage sein, die Grundlagen und Vorteile von KI-basierten Compliance-Hotlines zu verstehen, einen Echtzeit-Sprachassistenten mit OpenAI-Technologien zu implementieren, diesen in bestehende Wissensmanagementsysteme zu integrieren und dabei Sicherheits- und Datenschutzstandards einzuhalten. Sie werden somit befähigt, eine innovative und effektive Lösung für die 24/7-Informationssicherheit in Ihrem Unternehmen zu entwickeln und erfolgreich umzusetzen.

## Inhalte/Agenda:

- **◆ Modul 1: Einführung in KI-basierte Compliance-Hotlines**
  - ◆ Zweck und Zielsetzung: Erläuterung der Notwendigkeit einer 24/7 verfügbaren Compliance-Hotline und der Vorteile des Einsatzes von KI
  - ◆ Anwendungsbereiche: Diskussion relevanter Szenarien im Bereich der Informationssicherheit, in denen ein solcher Assistent Mehrwert bietet
- **◆ Modul 2: Architektur und Komponenten des Sprachagenten**
  - ◆ Echtzeit-Sprachverarbeitung: Implementierung der OpenAI Realtime API für natürliche Sprachinteraktionen
  - ◆ Knowledge Retrieval: Anbindung an das bestehende Knowledge-Management-System zur effizienten Informationsbeschaffung
  - ◆ Benutzerintentionen und Aktionen: Definition und Verarbeitung von User Intents und entsprechenden Assistant Skills
- **◆ Modul 3: Entwicklung der einzelnen Komponenten**
  - ◆ Spracherkennung und -synthese: Nutzung der OpenAI Realtime API für Echtzeit-Sprachinteraktionen
  - ◆ Integration mit dem Knowledge-Management-Tool: Verbindung des Sprachagenten mit internen Datenbanken oder Dokumentenmanagementsystemen
  - ◆ Sicherheits- und Datenschutzaspekte: Beachtung von Compliance-Richtlinien und Implementierung von Sicherheitsmaßnahmen
- **◆ Modul 4: Aufbau der Vektordatenbank für das Knowledge Retrieval**
  - ◆ Datenvorbereitung: Aufbereitung und Indexierung relevanter Dokumente und Informationen
  - ◆ Implementierung von Vektordatenbanken: Einsatz von Tools wie VectorDB zur effizienten Informationssuche
- **◆ Modul 5: Prompt Engineering für die Benutzerführung**
  - ◆ Erstellung effektiver Prompts: Gestaltung von Eingabeaufforderungen, die präzise und hilfreiche Antworten generieren
  - ◆ Optimierung der Benutzerinteraktion: Sicherstellung einer intuitiven und effektiven Kommunikation zwischen Nutzer und Assistent
- **◆ Modul 6: Erweiterungsmöglichkeiten und Anwendung auf die eigene Knowledgebase**
  - ◆ Anpassung an spezifische Anforderungen: Modifikation des Assistenten entsprechend der individuellen Bedürfnisse des Unternehmens
  - ◆ Skalierbarkeit und Wartung: Planung für zukünftige Erweiterungen und kontinuierliche Aktualisierung des Systems
- **◆ Modul 7: Best Practices und Fallstricke bei der Implementierung**
  - ◆ Häufige Herausforderungen: Identifizierung potenzieller Probleme und deren Lösungen
  - ◆ Erfolgsfaktoren: Strategien für eine erfolgreiche Implementierung und Akzeptanz des Systems
- **◆ Modul 8: Abschlussdiskussion und Übertragung des Gelernten**
  - ◆ Reflexion: Bewertung der erlernten Konzepte und deren Anwendung im eigenen Unternehmenskontext
  - ◆ Nächste Schritte: Planung weiterer Maßnahmen zur Implementierung des Sprachagenten