KI – Überblick

GRUNDLAGEN

Was ist KI – und was nicht?

Klassische Software:
Arbeitet nach festen Regeln (if/else). Die Ausgabe ist deterministisch und vorhersagbar – gleiche Eingabe führt immer zum gleichen Ergebnis.

KI/Machine Learning:
Lernt Muster aus Daten und trifft Vorhersagen oder Entscheidungen probabilistisch. Das System arbeitet mit Wahrscheinlichkeiten, nicht mit absoluter Gewissheit.

Generative KI:
Erzeugt neue Inhalte (Text, Bilder, Code) basierend auf Trainingsmustern und einem Prompt.

Prüfungsfalle: „KI versteht" – Nein! KI berechnet Wahrscheinlichkeiten und kann sehr überzeugend wirken, ohne tatsächlich zu verstehen.
Merksatz: KI klingt sicher – ist aber nicht automatisch richtig.

AP1-WISSEN

KI-Arten im Überblick

Machine Learning

Klassifikation (Spam/kein Spam) und Regression (Preisprognosen). Das System lernt aus Beispieldaten und wendet Muster auf neue Daten an.

Deep Learning

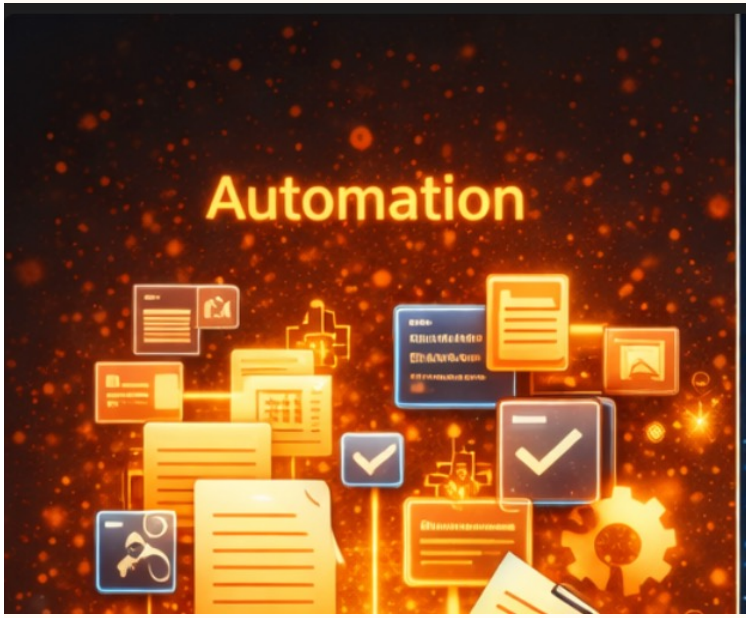
Viele neuronale Schichten ermöglichen komplexe Mustererkennung. Besonders stark bei Bild- und Sprachverarbeitung.

Generative Modelle

LLMs: Erzeugen Text, Code und Antworten. **Diffusion:** Generiert Bilder. Wichtig: Sie zitieren nicht automatisch Quellen!

Prüfungsfalle: „Generativ = Suchmaschine" ist falsch – generative KI erzeugt Inhalte, sie sucht sie nicht. Beispiel: Support-Chatbot (generativ) vs. Ticket-Priorisierung (klassisches ML).

Chancen im Betrieb



Automatisierung

Zusammenfassen von Dokumenten, Entwürfe erstellen, automatische Klassifikation und Übersetzungen – repetitive Aufgaben werden beschleunigt.

Unterstützung

Code-Vorschläge, automatische Dokumentation, Generierung von Testfällen und intelligente Wissensassistenz für Mitarbeitende.

Analyse

Mustererkennung in Logdateien, Anomalieerkennung und datenbasierte Forecasts zur besseren Entscheidungsfindung.

Wichtig: Output immer prüfen auf Fachlichkeit, Datenschutz, Rechte und Compliance. KI ist ei Praktikant mit Turbo – du bleibst verantwortlich.

⚠ RISIKEN

Die 5 klassischen KI-Risiken

Halluzination

KI erzeugt plausible, aber völlig falsche Aussagen oder erfindet nicht existierende Quellen. Die Ausgabe klingt überzeugend, ist aber faktisch inkorrekt.

Bias (Verzerrung)

Verzerrte oder diskriminierende Ergebnisse durch einseitige Trainingsdaten. Das Modell reproduziert und verstärkt bestehende Vorurteile.

Datenschutz

Eingaben können personenbezogene Daten, Betriebsgeheimnisse oder sensible Informationen enthalten, die nicht weitergegeben werden dürfen.

Urheberrecht

Generierte Inhalte können urheberrechtlich geschützte Werke berühren – sowohl bei Training als auch bei Output.

Sicherheit

Prompt-Injection-Angriffe, ungewollter Datenabfluss und fehlerhafte Automatisierung ohne menschliche Kontrolle.

Prüfungsfalle: „Wenn's professionell klingt, stimmt's" – gefährlich! **Mini-Regel:** Fakten mit zweiter Quelle prüfen, bevor du entscheidest.

Wichtige KI-Begriffe für die Prüfung

01

Modell

Die „gelernte Maschine" mit ihren Parametern – das Ergebnis des Trainingsprozesses.

02

Training

Der Prozess, bei dem das Modell aus großen Datenmengen lernt und Muster erkennt.

03

Inferenz

Das trainierte Modell erzeugt eine Antwort basierend auf einem Prompt – die eigentliche Nutzungsphase.

04

Prompt

Die Eingabe oder Anweisung, die dem Modell gegeben wird, um eine bestimmte Aufgabe zu erfüllen.

05

Kontextfenster

Die Menge an Text, die das Modell „gleichzeitig" berücksichtigen kann – begrenzt die Informationsmenge pro Anfrage.

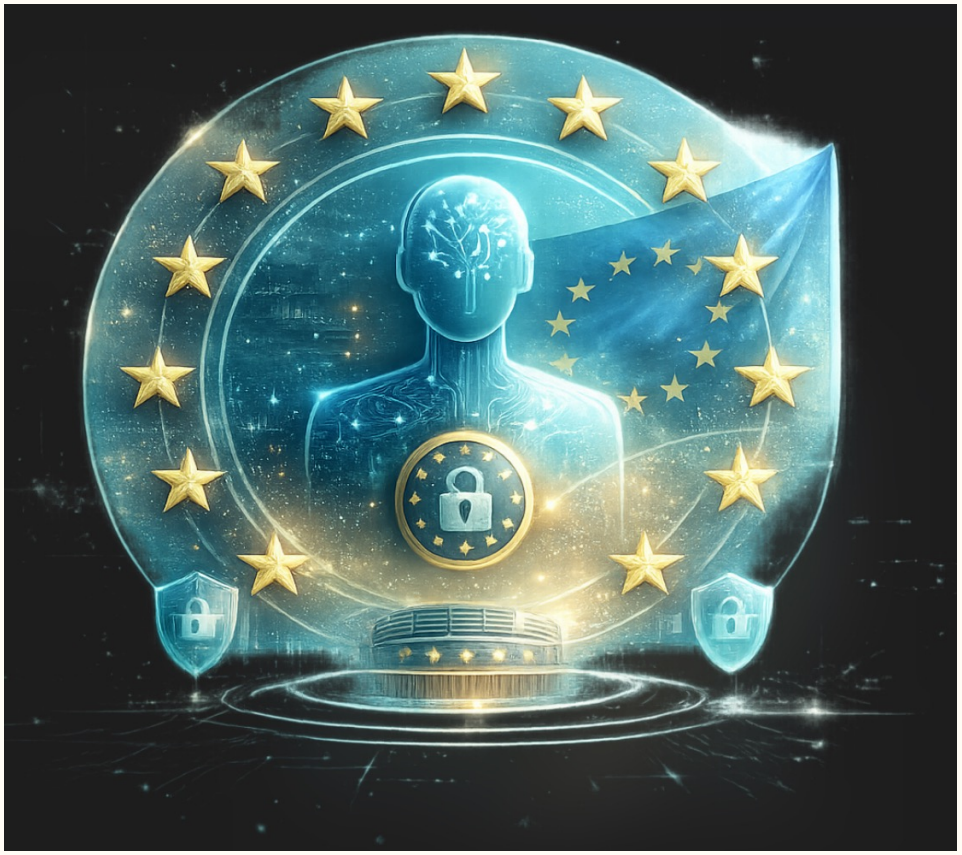
Prüfungsfalle

„KI merkt sich alles" – stimmt nicht! Meist funktioniert das Gedächtnis nur innerhalb des aktuellen Kontextes oder Systems.

Merksatz: Der Prompt steuert das Verhalten der KI, nicht die Wahrheit der Aussagen.

EU-REGULIERUNG

EU-KI-Verordnung (AI Act)



Idee & Rollen

Ziel: Sichere, transparente und menschenrechtskonforme KI in der Europäischen Union gewährleisten.

Geltungsbereich: Betrifft sowohl Anbieter/Hersteller von KI-Systemen als auch Betreiber/Nutzer („Deployer") – je nach Rolle ergeben sich unterschiedliche Pflichten.

Grundlogik: Risiko-basierte Regulierung – je höher das Risiko des KI-Einsatzes, desto strenger die Anforderungen und Pflichten.

Prüfungsfalle: „Gilt nur für große Tech-Firmen" – Nein! Auch kleinere Unternehmen, die KI einsetzen, können umfangreiche Pflichten haben. **Merksatz:** Wer KI einsetzt, braucht klare Regeln und Verantwortlichkeit.

EU-KI-VO: Die vier Risikoklassen

Verbotene KI

Unacceptable Risk: Unzulässige Praktiken wie Social Scoring oder manipulative KI-Systeme – diese dürfen nicht eingesetzt werden.

Hochrisiko-KI

High Risk: Strenge Anforderungen bei kritischen Anwendungen (z.B. Bewerber-Screening, Kreditvergabe, medizinische Diagnostik).

Begrenztes Risiko

Limited Risk: Transparenzpflichten – Nutzer müssen informiert werden, dass sie mit KI interagieren oder KI-generierte Inhalte vorliegen.

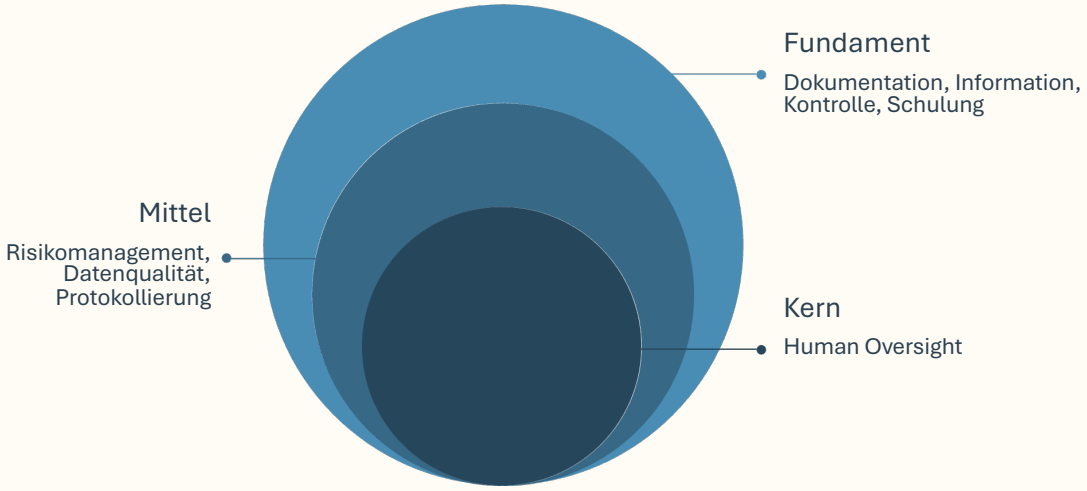
Minimales Risiko

Minimal Risk: Wenige bis keine speziellen Zusatzpflichten – z.B. einfache Spam-Filter oder Textvorschläge.

Prüfungsfalle: „Alles ist Hochrisiko" – Nein! Die Einordnung hängt stark vom Einsatzkontext ab. Beispiel: Bewerber-Screening kann hochriskant sein, eine Textzusammenfassung meist nicht.

PRAXIS

Was bedeutet die EU-KI-VO für Betriebe?



Grundpflichten im Alltag

- Dokumentieren: Welche KI-Systeme werden wo eingesetzt?
- Informieren: Mitarbeitende und Nutzer aufklären
- Kontrollieren: Regelmäßige Überprüfung der Ergebnisse
- Schulen: KI-Kompetenz im Team aufbauen

Hochrisiko-Systeme

Erfordern zusätzlich: Risiko- und Qualitätsmanagement, saubere Trainingsdaten, umfassendes Logging und Human Oversight (menschliche Aufsicht).

Prüfungsfalle: „Wir nutzen nur ein Tool, haben keine Verantwortung" – Falsch! Betreiberpflichten können trotzdem greifen. **Merksatz:** KI ohne Prozess = Haftungs- und Qualitätsfalle.

AI Literacy im Unternehmen

KI-Kompetenz bedeutet: Mitarbeitende verstehen Grenzen und Risiken von KI und können sie sinnvoll und sicher nutzen.

Datenschutz

Was darf in Prompts? Personenbezogene Daten und Geheimnisse schützen.

Bias & Halluzination

Verzerrungen erkennen und mit Vorsicht bei Fakten umgehen.

Sichere Prompts

Keine sensiblen Daten in öffentliche Tools eingeben.

Freigaben & Policies

Unternehmensinterne Richtlinien beachten und einhalten.

Prüfungsfalle: Einmalige Schulung reicht selten aus – besser sind kurze, regelmäßige Wiederholungen n praxisnahen Beispielen aus dem Arbeitsalltag. **Mini-Tipp:** „Was darf in Prompts rein?" als 1-Seiten-Rege bereitstellen.

PROMPTING

Die 5-Baustein-Formel für gute Prompts

Rolle

„Du bist..." (z.B. Ausbilder, Admin, Prüfer)

Ziel

„Erstelle..." (klar und messbar formuliert)

Kontext

Zielgruppe, Umfang, Rahmenbedingungen

Constraints

Stil, Länge, Regeln, No-Go's

Format

Tabelle, Liste, JSON, Checkliste

Prüfungsfalle: Vage Prompts führen zu vagen Antworten. Je präziser die Anweisung, desto besser das Ergebnis.

Merksatz: Gute Prompts sind wie technische Spezifikationen – detailliert, strukturiert und eindeutig.

Sechs Prompting-Techniken, die wirklich zählen

Prüfungsrelevant

Diese Techniken tauchen häufig in AP1-Aufgaben auf. Verstehe das Prinzip und wende es situativ an!

Prüfungsfalle: „Chain-of-thought erzwingt Wahrheit" – Nein! Besser: Begründung anfordern + Quellenwunsch äußern + Ergebnisse testen. **Mini-Template:** „Antwort + Begründung + Risiken + Checkliste".

- **Beispiele geben (Few-Shot)**
  Zeige der KI konkret: „So soll die Ausgabe aussehen." Beispiele verbessern Konsistenz und Format.
- **Schrittweise Aufgaben**
  Erst die Struktur, dann Details. Teile komplexe Anfragen in mehrere Prompts auf.
- **Prüfen lassen**
  „Markiere Unsicherheiten" oder „Nenne deine Annahmen" – so erkennst du Schwachstellen.
- **Varianten generieren**
  „Gib 3 Optionen mit Vor- und Nachteilen" – erhöht die Qualität durch Vergleich.
- **Rollenwechsel**
  „Antworte als Prüfer und nenne typische Fehler" – nutze verschiedene Perspektiven.
- **Sicherheitsgeländer**
  „Wenn Informationen fehlen: Liste Fragen, statt zu raten" – verhindert Halluzinationen.

QUALITÄT

KI-Ergebnisse sicher nutzen

4-Stufen-Kontrolle

01

Faktencheck

Überprüfe mit zweiter Quelle, interner Dokumentation oder Test in Sandbox-Umgebung.

02

Plausibilität

Prüfe Zahlen, Namen, Normen und Artikel auf logische Konsistenz.

03

Datenschutz

Keine Kundendaten, Passwörter oder Secrets in Prompts eingeben.

04

Freigabe

Menschliche Entscheidung bei wichtigen Themen (HR, Recht, Finanzen) ist Pflicht.

Prüfungsfalle: Automatisiert „durchreichen" ist die schnellste Art, Fehler zu skalieren und Verantwortung abzugeben.

Merksatz: KI ist ein Werkzeug – die Verantwortung bleibt immer beim Menschen.

Zusammenfassung: KI sicher und effektiv nutzen

1	**Verstehen** KI berechnet Wahrscheinlichkeiten, versteht nicht. Sie klingt überzeugend, kann aber falsch liegen.
2	**Chancen nutzen** Automatisierung, Unterstützung und Analyse beschleunigen Arbeitsprozesse erheblich.
3	**Risiken kennen** Halluzination, Bias, Datenschutz, Urheberrecht und Sicherheit immer im Blick behalten.
4	**Regeln beachten** EU-KI-VO bringt risiko-basierte Pflichten – auch für Betreiber von KI-Systemen.
5	**Kompetenzen aufbauen** AI Literacy im Team entwickeln durch Schulung, Beispiele und klare Richtlinien.
6	**Qualität sichern** Prüfen, testen, freigeben – keine KI-Ausgabe ungeprüft in Produktion geben.

PRÜFUNGSVORBEREITUNG

Mini-Quiz: Teste dein Wissen

1

Klassische Software vs. KI

Erkläre den Unterschied zwischen klassischer Software und KI anhand eines konkreten Beispiels aus der Praxis.

2

Risikomanagement

Nenne die 5 typischen KI-Risiken und beschreibe jeweils eine wirksame Gegenmaßnahme im betrieblichen Kontext.

3

EU-KI-VO Risikoklassen

Erkläre die vier Risikoklassen der EU-KI-Verordnung in eigenen Worten und gib für jede Klasse ein praktisches Beispiel.

4

Prompt-Engineering

Erstelle einen vollständigen Prompt (Rolle/Ziel/Kontext/Constraints/Format) für das Thema „AP1-Lernkarte Netzwerke".

Tipp: Bearbeite diese Fragen schriftlich und überprüfe deine Antworten anhand der Folieninhalte. Wiederholung festigt das Prüfungswissen!