

## Fachkompetenz IT-Systeme: EU AI Act

### Ausgangsszenario:

Im Jahr 2024 hat die EU Rechtsvorschriften im Umgang mit Künstlicher Intelligenz (KI) erlassen. Dieser EU AI Act (EU Artificial Intelligence Act) regelt den Umgang mit KI in der europäischen Union. Die wesentlichen Kapitel traten im Frühjahr 2025 in Kraft. Aus diesem Grund möchte die Firmenleitung der IT-Firma **ConSystem GmbH** die Mitarbeiter/-innen informieren. Das soll in Form eines Quiz geschehen, damit die Mitarbeiter/-innen sich intensiver mit der Thematik auseinandersetzen.

### Aufgabenstellung:

Als erfahrene/-r Auszubildende/-r erhalten Sie den Auftrag, das Quiz zu lösen und damit eine korrekte Musterlösung zu erstellen.

### Quiz zum EU AI Act

**Aufgabe 1:** Der **EU AI Act** definiert grundlegende Begriffe. Ordnen Sie folgende Begrifflichkeiten den Erklärungen korrekt zu:

KI-System	Anbieter	Deep Fake	Bereitsteller
Betreiber	Trainingsdaten	Eingabedaten	Risiko
Validierungsdaten	General Purpose AI (GPAI)		

Begrifflichkeit	Erklärung
Anbieter	Eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell für allgemeine Zwecke entwickelt oder ein KI-System oder ein KI-Modell für allgemeine Zwecke entwickeln lässt und es unter ihrem eigenen Namen oder ihrer eigenen Marke in Verkehr bringt oder in Betrieb nimmt, unabhängig davon, ob dies entgeltlich oder unentgeltlich geschieht.
Risiko	Die Kombination aus der Wahrscheinlichkeit des Eintritts eines Schadens und der Schwere dieses Schadens.
Betreiber	Das ist ein Anbieter, Produkthersteller, Verteiler, Bevollmächtigter, Importeur oder Händler.
KI-System	Ein maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie betrieben werden kann und nach seiner Einführung Anpassungsfähigkeit zeigt, und das für explizite oder implizite Ziele aus den Eingaben, die es erhält, ableitet, wie es Ausgaben wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen generieren kann, die physische oder virtuelle Umgebungen beeinflussen können.
Trainingsdaten	Daten, die zum Training eines KI-Systems durch Anpassung seiner lernfähigen Parameter verwendet werden.
Deep Fake	KI-generierte oder manipulierte Bild-, Audio- oder Videoinhalte, die existierenden Personen, Objekten, Orten, Einrichtungen oder Ereignissen ähneln und einer Person fälschlicherweise als authentisch oder wahrheitsgemäß erscheinen würden.
Bereitsteller	Eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System unter ihrer Aufsicht einsetzt, es sei denn, das KI-System wird im Rahmen einer persönlichen, nicht beruflichen Tätigkeit verwendet.
Eingabedaten	Daten, die einem KI-System zur Verfügung gestellt oder von diesem direkt erfasst werden und auf deren Grundlage das System eine Ausgabe erzeugt.
General Purpose AI (GPAI)	Das ist ein KI-System für allgemeine Zwecke, das auf einem KI-Modell basiert und für eine Vielzahl von Anwendungen eingesetzt werden kann, sowohl für den direkten Gebrauch als auch für die Integration in andere KI-Systeme.
Validierungsdaten	Daten, die zur Bewertung des trainierten KI-Systems und zur Abstimmung seiner nicht lernbaren Parameter und seines Lernprozesses verwendet werden, um unter anderem eine Unter- oder Überanpassung zu verhindern.

### Quiz zum EU AI Act (Fortsetzung)

**Aufgabe 2:** Der EU AI Act unterteilt KI-Systeme in verschiedene Kategorien (**verbotene KI-Systeme**, **Hochrisiko-KI-Systeme** und **nicht risikoreiche KI-Systeme**). Die folgenden Ausführungen sind aus diesen Kategorien. Bestimmen Sie, in welche Kategorie die jeweilige Ausführung einzuordnen ist.

Ausführungen	Verbotenes KI-System	Hochrisiko-KI-System	Nicht risikoreiches KI-System
Das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das eine Schwachstelle einer natürlichen Person oder einer bestimmten Personengruppe aufgrund ihres Alters, einer Behinderung oder einer besonderen sozialen oder wirtschaftlichen Situation ausnutzt, mit dem Ziel oder der Wirkung, das Verhalten dieser Person oder einer Person, die dieser Gruppe angehört, in einer Weise wesentlich zu beeinflussen, die dieser Person oder einer anderen Person einen erheblichen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit zufügen wird.	×		
KI-Systeme, die dazu dienen, den Zugang oder die Zulassung zu Einrichtungen der allgemeinen und beruflichen Bildung auf allen Ebenen zu bestimmen oder natürliche Personen zuzuweisen.		×	
Das Inverkehrbringen, die Inbetriebnahme zu diesem speziellen Zweck oder die Verwendung von KI-Systemen zur Ableitung von Emotionen einer natürlichen Person in den Bereichen Arbeitsplatz und Bildungseinrichtungen, es sei denn, die Verwendung des KI-Systems soll aus medizinischen oder sicherheitstechnischen Gründen eingeführt oder in Verkehr gebracht werden.	×		
Das KI-System ist dazu bestimmt, Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern zu erkennen, und ist nicht dazu bestimmt, die zuvor durchgeführte menschliche Bewertung ohne angemessene menschliche Überprüfung zu ersetzen oder zu beeinflussen.			×
KI-Systeme, die als Sicherheitskomponenten bei der Verwaltung und dem Betrieb kritischer digitaler Infrastrukturen, im Straßenverkehr oder bei der Versorgung mit Wasser, Gas, Wärme oder Strom eingesetzt werden sollen.		×	

**Aufgabe 3:** Welche der folgenden Aussagen sind korrekt?

- ☒ Anbieter von KI-Systemen mit hohem Risiko müssen ein Qualitätsmanagementsystem einrichten, das die Einhaltung des EU AI Acts gewährleistet.
- ☐ Der Dienstleistungserbringer muss nach dem Ende einer Inbetriebnahme eines Hochrisiko-KI-Systems keine Unterlagen für die zuständigen nationalen Behörden bereithalten.
- ☐ Der EU AI Act gilt auch für KI-Systeme oder KI-Modelle, einschließlich ihrer Ergebnisse, die speziell für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen werden.
- ☒ Die Nichteinhaltung Verbote von KI-Systemen nach dem EU AI Act wird mit einer Geldbuße von bis zu 35.000.000 EUR oder, wenn es sich um ein Unternehmen handelt, von bis zu 7 % seines gesamten weltweiten Jahresumsatzes im vorausgegangenen Geschäftsjahr belegt, je nachdem, welcher Betrag höher ist.



**Quiz zum EU AI Act (Fortsetzung)**

**Aufgabe 4:** Übersetzen Sie den folgenden **Artikel 4 des EU AI Acts** ins Deutsche:

“Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.”

Ihre Übersetzung:

Die Anbieter und Betreiber von KI-Systemen ergreifen Maßnahmen, um nach bestem Wissen und Gewissen sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ausreichende KI-Kompetenz verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Aus- und Weiterbildung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, berücksichtigt werden.

## Fachkompetenz IT-Systeme: KI-Anwendungen

### Ausgangsszenario:

KI-Software und KI-Anwendungen bestimmen inzwischen einen beachtlichen Teil des beruflichen Alltags. Neben der Verarbeitung von Sprache und Texten (Natural Language Processing NLP) oder der Analyse von großen Datenmengen (Big Data) kommen auch Einsätze von KI zur Automatisierung von Prozessen infrage. In diesem Zusammenhang erhält Ihre Firma **ConSystem GmbH** einen Auftrag zur Beratung eines mittelständischen Unternehmens.

### Aufgabenstellung:

Als erfahrene/-r Auszubildende/-r sollen Sie den Beratungsprozess unterstützen und für das nächste Kundengespräch Informationen bereitstellen.

### Informationen zu KI-Anwendungen

**Ausgangssituation:** Der Kunde produziert Werkstücke im Bereich der Fertigungstechnik. Die Aufträge des Kunden gehen per E-Mail ein, teilweise auch in anderen Sprachen als Deutsch. Die Aufträge werden dann gegebenenfalls übersetzt und die entsprechenden Pläne für die Herstellung der Werkstücke werden zentral ausgedruckt und in die Werkstatt gebracht. Nach der Herstellung warten die Werkstücke dann in einem zentralen Hochregal auf Abholung und Versendung an den Kunden. Nach der Versendung erhält die Buchhaltung eine Mitteilung – die Rechnung wird erstellt und an den Kunden gesendet.

#### Informationsbedarf 1:

Skizzieren Sie Möglichkeiten, wie KI-Anwendungen diese Prozesse optimieren könnten.

Ihre Skizzierung:

Die Aufträge per Mail bergen einige Probleme: Was passiert, wenn der zuständige Mitarbeiter krank ist und die Mails werden nicht weitergeleitet. Hier würde sich eine KI-gestützte Auftrags-erfassung anbieten, die dem Auftraggeber im Vorfeld auch Hilfe bei der Erstellung des Auftrages anbietet (Chatbot, KI-gestütztes Webinterface zur Auftragserfassung). Angegliedert könnte die automatische KI-gestützte Übersetzung von fremdsprachigen Texten sein. Die Mitarbeiter des Kunden hätten die Aufträge dann übersichtlich in einer Anwendung und könnten von dieser Anwendung weitere automatisierte Prozesse starten. Beispielsweise die automatisierte Suche und Bereitstellung der Herstellungspläne. In den Werkstätten müssten dazu Workstations installiert werden, die diese Pläne anzeigen (gegebenenfalls könnte in der Werkstatt auch gedruckt werden).

Nach Beendigung des Herstellungsprozesses könnten über diese Workstation auch der Versendungs- und parallel der Rechnungserstellungsprozess angestoßen werden.

Entsprechende KI-Systeme überwachen dabei immer auch den Einsatz der Maschinen und könnten auf Fehler sowie Wartungsintervalle reagieren.

**Informationen zu KI-Anwendungen (Fortsetzung)****Informationsbedarf 2:**

Der Kunde hat enorme Schwierigkeiten Fachkräfte zu finden und einzustellen. Er würde deshalb gerne eine KI-gestützte Headhunter-Software einsetzen lassen. Die Software wird zusammenfassend so beschrieben:

XXX ist ein automatisiertes Headhunting-System, das Bewerber und Unternehmen auf Basis von Unternehmenskultur, Persönlichkeit und Fähigkeiten zusammenbringt. XXX analysiert KI-basiert die Unternehmenswerte und sucht anschließend die passenden Bewerber. Ebenso analysiert XXX KI-basiert die Bewerbereigenschaften und schlägt Ihnen entsprechende Unternehmen vor.

Wie schätzen Sie den Einsatz einer solchen KI-Anwendung ein?

Ihre Einschätzung:

Der Wunsch des Kunden ist nachvollziehbar, aber beim Einsatz der Software ist Vorsicht geboten. Durch die KI-gestützte Analyse der Unternehmen und der Bewerber können beide Seiten in den Bereichen Sicherheit und Grundrechte beeinträchtigt werden. Nach dem EU AI Act müsste diese KI-Anwendung als Hochrisiko-KI-System angesehen werden. Der Anbieter/Betreiber des Systems müsste alle entsprechenden Auflagen (Risiko- und Qualitätsmanagementsystem, Dokumentationen etc.) erfüllen und beweisen, dass die Rechte nicht beeinträchtigt werden.

**Informationsbedarf 3:**

Die Sachbearbeiter des Kunden würden gerne Unterstützung bei der Erstellung von Formulierungen haben, beispielsweise bei Lieferantenanschriften, die nicht dem Standard entsprechen. Dazu möchten sie eine generative KI einsetzen. Deshalb soll ein Informationsblatt zu dieser Thematik entwickelt werden. Helfen Sie bei der Erstellung, indem Sie folgende Fragen beantworten:

**Frage 1:** Was genau ist ein Prompt?

Ihre Antwort:

Der Begriff Prompt bedeutet ursprünglich die Eingabeaufforderung eines Programms an den Nutzer. Mit den generativen KIs bekam der Begriff eine erweiterte Bedeutung und steht für die Anweisung(en), die ein Benutzer einer generativen KI in gesprochener oder geschriebener Form gibt. Das Ergebnis (die Antwort) der KI hängt stark von der Qualität des eingegebenen Prompts ab. Inzwischen gibt es auch eine eigene Fachrichtung dafür – das Prompt Engineering.