

Musterprüfung

Ausgabe 202603

Copyright © EXIN Holding B.V. 2026. All rights reserved.
EXIN® is a registered trademark.

No part of this publication may be reproduced, stored, utilized or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written permission from EXIN.

Inhalt

Einführung	4
Musterprüfung	5
Antwortschlüssel	22
Beurteilung	60

Einführung

Dies ist die EXIN Artificial Intelligence Compliance Professional (AICP.DE) Musterprüfung. Es gilt die Prüfungsordnung von EXIN.

Die Musterprüfung besteht aus 40 Multiple-Choice-Fragen. Zu jeder Multiple-Choice-Frage werden mehrere Antwortmöglichkeiten angeboten. Es gibt jeweils eine richtige Antwort.

Sie können maximal 40 Punkte erreichen. Jede richtige Antwort zählt 1 Punkt. Um die Prüfung zu bestehen, müssen Sie mindestens 26 Punkte erzielen.

Die Bearbeitungszeit beträgt 90 Minuten.

Sie dürfen für diese Prüfung den KI-VO Text verwenden.

Viel Erfolg!

Musterprüfung

1 / 40
Die KI-VO ist eine Rechtsvorschrift für die Europäische Union (EU). Artikel 1 KI-VO beschreibt ihre Ziele.

Was sind die **primären** Ziele der KI-VO?

A) Leitlinien, die sich ausschließlich auf Umweltschutz konzentrieren, keine spezifische Vorschriften für Hochrisiko-AI-Systeme, keine Verbote und Innovationsmaßnahmen nur für Großkonzerne
B) Harmonisierte Vorschriften für KI-Systeme in der EU, Verbote bestimmter KI-Praktiken, Anforderungen an Hochrisiko-KI-Systeme, Transparenzregeln, Marktüberwachung und Innovationsförderung
C) Verbote von KI-Praktiken, Vorschriften nur für KI-Systeme mit allgemeinem Verwendungszweck, Transparenzregeln, die nicht für Hochrisiko-KI-Systeme gelten, und Innovationsförderung, die auf nichteuropäische Einrichtungen beschränkt ist
D) Vorschriften für KI-Systeme, die auf Sicherheit und Gesundheit begrenzt sind, Verbote für alle KI-Praktiken, Transparenzvorschriften nur für Hochrisiko-KI-Systeme und Innovationsförderung, von der Start-up-Unternehmen ausgeschlossen sind

2 / 40
Wie definiert die KI-VO Verantwortlichkeit und Konformität (Compliance)?

A) Verantwortlichkeit legt den Schwerpunkt auf den Schutz der Privatsphäre der Nutzer und die Datensicherheit, während Konformität (Compliance) sich auf die Integration in die bestehende IT-Infrastruktur bezieht.
B) Verantwortlichkeit heißt, Entwickler und Akteure in der KI-Entwicklung zur Verantwortung zu ziehen, und Konformität (Compliance) bedeutet Einhaltung der rechtlichen Anforderungen.
C) Verantwortlichkeit soll sicherstellen, dass KI-Systeme gewinnbringend für die Entwickler sind, und Konformität (Compliance) heißt, die Forderungen und Präferenzen der Nutzer zu erfüllen.
D) Verantwortlichkeit bezieht sich darauf, dass KI-Nutzer für die richtige Verwendung des Systems verantwortlich sind, während Konformität (Compliance) bedeutet, dass die Branchenstandards für KI-Innovationen eingehalten werden müssen.

3 / 40
Die KI-VO gewährt natürlichen Personen die von KI-Systemen betroffen sind besondere Rechte, um Transparenz, Fairness und Verantwortlichkeit sicherzustellen.

Welches Recht gewährt die KI-VO natürlichen Personen explizit?

A) Das Recht, informiert zu werden, dass sie mit einem KI-System interagieren bzw. davon betroffen sind.
B) Das Recht, Zugriff auf den Quellcode des KI-Systems zu verlangen
C) Das Recht, die Verwendung von KI in jedem sie betreffenden Entscheidungsprozess zu untersagen
D) Das Recht, die Löschung personenbezogener Daten zu verlangen, die das KI-System verwendet

4 / 40
Anna, die als Compliance-Beauftragte für ein kleines bzw. mittleres Unternehmen (KMU) arbeitet, ist verantwortlich für die Überwachung der Implementierung eines neuen KI-Systems für automatisierte Kundenbetreuung. Das Unternehmen hat dieses System nicht selbst entwickelt, sondern von einem anderen Anbieter gekauft. Laut KI-VO ist dieses System als Hochrisiko-KI-System einzuordnen.

Anna soll sicherstellen, dass das Unternehmen bei der Inbetriebnahme und Überwachung dieses KI-Systems seine Pflichten als Nutzer einhält. Sie muss festlegen, welche Maßnahmen zu priorisieren sind und welche vermieden werden sollten.

Was sollte Anna angesichts der Pflichten von KI-Nutzern **nicht** in Erwägung ziehen?

A) Die Algorithmen des KI-Modells weiterentwickeln, um seine Entscheidungsfähigkeiten zu verbessern, ohne seinen Anbieter einzubinden
B) Detaillierte Aufzeichnungen der Leistung des KI-Systems führen und Konformität (Compliance) mit einschlägigen Berichtsanforderungen gewährleisten
C) Die Leistung des KI-Systems überwachen, um zu gewährleisten, dass es bestimmungsgemäß betrieben wird und die Sicherheitsstandards erfüllt
D) Schwerwiegende Vorfälle und Fehlfunktionen im Zusammenhang mit dem KI-System an die zuständigen Behörden melden wie gesetzlich vorgeschrieben

5 / 40
Ein KI-System zur Gesichtserkennung wird zu Sicherheitszwecken in öffentlichen Räumen verwendet. Eine Organisation ist besonders relevant für die Überwachung der Konformität (Compliance) dieses KI-Systems mit den Vorschriften zum Datenschutz und zur Privatsphäre wie der Datenschutz-Grundverordnung (DSGVO).

Welche Organisation ist das?

A) Der Europäische Verbraucherverband (BEUC)
B) Das Europäische Gremium für Künstliche Intelligenz (KI-Gremium)
C) Der Europäische Gerichtshof (EuGH)
D) Der Europäischer Datenschutzausschuss (EDPB)

6 / 40
Ein Unternehmen entwickelt ein KI-System für personalisiertes Marketing. Dieses System verwendet Algorithmen für maschinelles Lernen (ML), um Kunden maßgeschneiderte Werbung anzuzeigen. Bei einer Überprüfung der Konformität (Compliance) identifiziert das Team folgende Risiken:

- Es existiert keine Dokumentation, aus der klar hervorgeht, wie das KI-System Daten verarbeitet.
- Das Verfahren, mit dem das KI-System zu personalisierten Empfehlungen gelangt, wird nicht vollständig verstanden.
- Kunden beschweren sich über diese Aspekte.

Das Unternehmen muss die KI-VO einhalten. Dazu verwendet es die Norm ISO/IEC 42001 und das NIST AI Risk Management Framework (RMF).

Was sollte das Unternehmen laut dieser Norm und dem NIST-Rahmenwerk tun, um die Probleme zu lösen?

A) Eine Reihe von Nutzererlebnistests (UX Tests) durchführen, um Feedback zu Benutzerfreundlichkeit, Lernbarkeit und Kundenpräferenzen zu erhalten
B) Sich auf die Verbesserung der Vorhersagegenauigkeit des Systems konzentrieren, um seine Wirtschaftlichkeit, die Kundenzufriedenheit und das Kundenengagement zu verbessern
C) Ein Dokumentationsverfahren einführen, das Datenquellen, Verarbeitungsmethoden und die Entscheidungsfindung der Algorithmen detailliert aufzeichnet
D) Die Hardware des Systems upgraden, um seine Verarbeitungsgeschwindigkeit und Effizienz sowie die Kundenzufriedenheit zu verbessern

7 / 40
Ein Unternehmen entwickelt ein KI-System zur Überwachung von Patienten im Krankenhaus. Das System verwendet hochauflösende Kameras in den Krankenzimmern zur Echtzeit-Überwachung des Zustands der Patienten. Wenn das System einen Notfall erkennt, ruft es automatisch eine Pflegekraft an das Bett des Patienten.

Um die Leistung des KI-Systems zu verbessern, will das Unternehmen eine Datenbank mit Patientenvideos aufbauen – mit Anmerkungen von Sachverständigen an kritischen Stellen im Video, um mehr Trainingsdaten für das System zu erhalten.

Das Unternehmen erwägt, eine Datenschutzfolgenabschätzung (DPIA) durchzuführen. Das zuständige Team ist unsicher, ob eine DPIA überhaupt erfolgen sollte. Ist sie Pflicht, möchte das Team wissen, wann sie durchgeführt werden sollte: jetzt oder erst nach Inbetriebnahme des Update.

Das Unternehmen muss die KI-VO und die Datenschutz-Grundverordnung (DSGVO) einhalten.

Soll das Unternehmen jetzt eine DPIA durchführen?

A) Ja, weil eine DPIA bei KI-Projekten vorgeschrieben ist, die voraussichtlich ein hohes Risiko für die Rechte natürlicher Personen bergen.
B) Ja, weil eine DPIA für jedes Projekt erforderlich ist, das personenbezogene Daten erfasst, selbst wenn es ein Projekt mit geringem Risiko ist.
C) Nein, weil eine DPIA nicht erforderlich ist für die Verwendung von Daten für Trainingszwecke, Bildung oder wissenschaftliche Forschung.
D) Nein, weil eine DPIA nicht erforderlich ist, nachdem das KI-System vollständig entwickelt, getestet und in Betrieb genommen wurde.

8 / 40
Ein Unternehmen entwickelt ein KI-System zur Echtzeit-Gesichtserkennung. Eine private Sicherheitsfirma setzt dieses KI-System zur Überwachung eines öffentlichen Einkaufszentrums ein. Das System scannt alle Besucher, vergleicht ihre Gesichter mit Datenbanken früherer Straftäter und politischer Aktivisten und markiert Besucher, die in einer dieser Datenbanken geführt werden. Markierte Besucher werden während ihres gesamten Aufenthalts heimlich überwacht, um zu beurteilen, ob sie sich nach Einschätzung der Sicherheitsfirma verdächtig verhalten.

In welche Kategorie sollte die Verwendung dieses KI-Systems laut KI-VO eingestuft werden?

A) Unannehmbares Risiko
B) Hochriskant
C) Begrenztes Risiko
D) Minimales oder kein Risiko

9 / 40
Ein Reisebüro verwendet ein KI-System für die Entwicklung dynamischer, gezielter Marketingkampagnen für seine Pauschalreisen. Diese Kampagnen beinhalten die Echtzeit-Platzierung von Werbung auf sozialen Medien basierend auf dem Browserverlauf der betreffenden Person. Das Reisebüro verwendet KI, um Schlussfolgerungen über den emotionalen Zustand der Nutzer zu ziehen und dann individuell angepasste Reiseziele und Aktivitäten vorzuschlagen.

Das Reisebüro muss die KI-VO einhalten.

Welches Risiko muss das Reisebüro adressieren?

A) Das Risiko möglicher Verzerrungen (Bias). Das Unternehmen sollte die Trainingsdaten regelmäßig aktualisieren, um zu vermeiden, dass uninteressante Reiseziele vorgeschlagen oder falsche emotionale Zustände abgeleitet werden.
B) Das Risiko unwirksamer Werbemaßnahmen. Das Unternehmen sollte sich darauf konzentrieren, den Algorithmus zu aktualisieren, weil die KI-VO personalisierte Werbung nicht abdeckt.
C) Das Risiko fehlender Transparenz. Das Unternehmen sollte Offenheit in Bezug auf die KI gewährleisten, Voreingenommenheit (Bias) in den Vorschlägen reduzieren und überprüfen, ob die Werbeaktivitäten ethisch sind.
D) Das Risiko des Missbrauchs personenbezogener Daten. Das Unternehmen sollte keine KI-gestützte Personalisierung mehr verwenden, weil die KI-VO die Verwendung personenbezogener Daten für gezielte Werbung untersagt.

10 / 40
Ein Unternehmen entwickelt ein KI-Modell, das in verschiedenen Branchen verwendet werden kann, unter anderem im Gesundheits- und Finanzsektor. Wegen seiner breiten Anwendung birgt das KI-Modell mögliche Risiken für die öffentliche Gesundheit.

Was hat das Unternehmen entwickelt und welche Praktiken sollte es laut KI-VO umsetzen?

A) Das Unternehmen hat ein KI-Modell mit allgemeinem Verwendungszweck mit systemischen Risiken entwickelt. Es sollte zusätzliche Tests durchführen, um die Risiken zu mindern.
B) Das Unternehmen hat ein Hochrisiko-KI-System entwickelt. Es sollte alle Anforderungen an Hochrisiko-KI-Systeme umsetzen, die in der KI-VO vorgeschrieben sind.
C) Das Unternehmen hat ein eng gefasstes KI-Modell entwickelt. Um Risiken vorzubeugen, sollte es sicherstellen, dass das Modell nur innerhalb vordefinierter Parameter betrieben wird.
D) Das Unternehmen hat ein experimentelles KI-Modell entwickelt. Es sollte sich auf Forschung und Entwicklung konzentrieren, ohne sofortiges Risikomanagement zu betreiben.

11 / 40
Eine Organisation entwickelt ein Hochrisiko-KI-System. In den Tests identifiziert das Entwicklungsteam verschiedene Risiken, einschließlich Unstimmigkeiten in der Vollständigkeit der Daten und veraltete Datensätze. Diese Risiken könnten die Leistung des Modells beeinträchtigen.

Die Organisation muss die KI-VO einhalten. Sie verwendet dazu das Rahmenwerk CEN/CLC/TR 18115.

Was sollte die Organisation laut diesem Rahmenwerk tun, um diese Risiken zu adressieren?

A) Eine Datenschutzfolgenabschätzung (DPIA) durchführen, um die Fairness der KI-Entscheidungsfindung zu adressieren
B) Alle Trainings- und Testdatensätze auf der Grundlage von Protokollen verschlüsseln, um unbefugten Zugriff auf personenbezogene Daten zu verhindern
C) Allgemeine Risikokontrollen einführen, um die genannten Betriebs- und Reputationsrisiken zu verringern
D) Die Datenqualität durch Anwendung strukturierter Qualitätskennzahlen und statistischer Bewertungsmethoden verbessern

12 / 40
Im Zusammenhang mit KI-Systemen beschreibt die KI-VO verschiedene Rollen.

Wie wird die Rolle "Einführer eines KI-Systems" definiert?

A) Eine natürliche oder juristische Person, die ein KI-System konzipiert, entwickelt und unter ihrem eigenen Namen oder ihrer Handelsmarkte in Verkehr bringt.
B) Eine natürliche oder juristische Person, die ein KI-System in Verkehr bringt, aber nicht für seine ursprüngliche Entwicklung verantwortlich ist.
C) Eine natürliche oder juristische Person, die ein KI-System in ihrem Betrieb verwendet und die lokale Konformität (Compliance) mit den Nutzerpflichten sicherstellt.
D) Eine Aufsichtsbehörde, deren Aufgabe es ist zu überwachen, ob das KI-System in Übereinstimmung mit den Bestimmungen der KI-VO eingeführt wird.

13 / 40
Ein Unternehmen entwickelt ein KI-System zur Betrugserkennung in Finanztransaktionen. Dieses System analysiert Transaktionsmuster, um verdächtige Aktivitäten zu erkennen und Betrugsversuchen vorzubeugen. Angesichts der Möglichkeit von Fehlalarmen, die sich auf rechtmäßige Transaktionen auswirken können, und der Tatsache, dass sich die Betrugstaktiken weiterentwickeln, weiß das Unternehmen, dass wirksame Schutzvorkehrungen erforderlich sind.

Das Unternehmen muss die KI-VO einhalten. Um Problemen durch Fehlalarme vorzubeugen, nutzt es die Norm ISO/IEC 23894.

Was sollte das Unternehmen laut dieser Norm tun, um solchen Probleme vorzubeugen?

A) Risikomanagement zum integralen Bestandteil aller Aktivitäten machen, um umfassende Aufsicht und proaktive Risikominderung sicherzustellen
B) Die Datenschutzmaßnahmen verbessern, um sensible Informationen zu schützen und die Bestimmungen zum Schutz der Privatsphäre einzuhalten
C) Sich auf die Verbesserung der Modellgenauigkeit konzentrieren, um zuverlässige Leistung sicherzustellen und Fehlalarme zu minimieren
D) Cybersicherheitsmaßnahmen umsetzen, um das System vor Bedrohungen von außen und unbefugtem Zugriff zu schützen

14 / 40
Ein Fertigungsunternehmen verwendet KI-gestützte Robotertechnologie zur Qualitätskontrolle an seinen Montagebändern. Das Ermittlungsteam erfährt von einem anonymen Hinweisgeber, dass das KI-System in letzter Zeit eine ungewöhnlich niedrige Anzahl fehlerhafter Produkte ausweist. Grund für diese Untererfassung ist ein Software-Update des KI-Systems. Eine manuelle Prüfung zeigt, dass die Produkte fehlerhaft und unsicher sind.

Im Bericht heißt es, dass der neue Fehlererkennungsalgorithmus einen kritischen Fehler erzeugt, der zu falsch-negativen Ergebnissen führt. Dem Hinweisgeber zufolge war den Führungskräften dieses Problem bekannt, doch wurde nichts dagegen unternommen, um der Reputation des Unternehmens nicht zu schaden.

Was sollten die nächsten Schritte sein?

A) - Den internen Algorithmus anpassen, um das Problem zu beseitigen
- Die zuständige Behörde unterrichten, wenn das Problem nach 30 Tagen immer noch auftritt
B) - Das Problem intern untersuchen und mit einer Lösung beginnen
- Die zuständige Behörde unverzüglich über den Vorfall unterrichten
C) - Die Gründe ermitteln, warum der Hinweisgeber das Problem gemeldet hat
- Die zuständige Behörde unterrichten, wenn Verbraucher sich zu beschweren beginnen
D) - Das KI-Systems stilllegen und zu einer älteren Methode übergehen
- Eine Unterrichtung der zuständigen Behörde ist dann nicht mehr erforderlich.

15 / 40
MedTech Diagnostics verwendet ein Hochrisiko-KI-System zur Diagnose von Krankheiten anhand von Röntgenbildern. Folgende Maßnahmen wurden ergriffen:

- Das Unternehmen hat ein externes Audit bestanden, um sicherzustellen, dass das KI-System die Standards der KI-VO erfüllt.
- Ein robustes Rahmenwerk für das Risikomanagement identifiziert und mindert mögliche Probleme, und es existieren Notfallpläne.
- Detaillierte Aufzeichnungen zum Betrieb des KI-Systems werden sicher aufbewahrt, um für Verantwortlichkeitsfragen und Audits zur Verfügung zu stehen.
- Nutzer erhalten eine klare Dokumentation und Schulungen, in denen die Entscheidungsfindung und Einschränkungen der KI erklärt werden.
- Alle AI-generierten Diagnosen werden vor der finalen Festlegung von medizinischen Fachkräften überprüft, um ein menschliches Urteil zu integrieren.

Was sollte das Unternehmen sonst noch tun?

A) Robuste Daten-Governance-Verfahren hinzunehmen, um die Zuverlässigkeit und Fairness des KI-Systems beizubehalten
B) Aus Effizienzgründen sicherstellen, dass das KI-System autonom ohne menschliches Eingreifen läuft
C) Ein System implementieren, das menschliche Entscheidungen automatisch außer Kraft setzt, um den Diagnoseprozess zu beschleunigen
D) Eine Funktion aufnehmen, die Patienten ermöglicht, ihre Krankenakten auf der Grundlage von KI-Vorschlägen selbst anzupassen

16 / 40
Eine Versicherung implementiert eines neues KI-gestütztes Credit-Scoring-System mit Zugriff auf interne und öffentliche Datenbanken. Folgende Risiken werden identifiziert:

- **Fehlen angemessener Trainingsdaten.**Ein schlecht trainiertes Modell erschwert die genaue Feststellung fairer Kredit-Scores für natürliche Personen.
- **Integration mit anderen Anwendungen**. Das KI-gestützte System lässt sich nur schwer in die eher komplexe und an manchen Stellen veraltete Anwendungsumgebung integrieren.
- **Nichteinhaltung der DSGVO**. Laut Datenschutz-Grundverordnung (DSGVO) gelten für die autonome Verarbeitung personenbezogener Daten in automatisierten Systemen besondere Anforderungen.
- **Transparenz und Qualität des Modells**. Die Mitarbeitenden und Kunden müssen jeweils in der Lage sein, die Ergebnisse und Entscheidungen des KI-Modells zu verstehen.

Die Versicherung muss die KI-VO einhalten.

Welches Risiko spielt für die Konformität (Compliance) mit der KI-VO **keine** wichtige Rolle?

A) Fehlen angemessener Trainingsdaten
B) Integration mit anderen Anwendungen
C) Nichteinhaltung der DSGVO
D) Transparenz und Qualität des Modells

17 / 40
Eine Regierungsbehörde schlägt ein KI-System vor, das bei der Vorhersage von Kriminalitäts-Hotspots im Innenstadtbereich einer größeren Stadt helfen soll. Das System wird zur automatisierte Überwachung eingesetzt. Es ist so programmiert, dass es automatisch Personen identifiziert, die sich verdächtig verhalten, und diese dann der örtlichen Polizei meldet. Das ist eine große Chance für die Verbrechensverhütung, ein erhöhtes Sicherheitsgefühl und eine gerechte Strafverfolgung nach einem Verbrechen.

Können bei der Implementierung dieses KI-Systems Risiken auftreten?

A) Ja, weil ein KI-System, das für automatisierte Entscheidungen verwendet wird, stets das Risiko von Verzerrungen (Bias) birgt. Das kann zu einer unfairen Benachteiligung natürlicher Personen führen.
B) Ja, weil die KI-VO bei Überwachungssystemen so viele Risiken für die Privatsphäre sieht, dass sie deren Einsatz im öffentlichen Raum ganz verbietet.
C) Nein, weil KI-Systeme in der Verbrechensverfolgung und -verhütung keine besonderen Risiken bergen, da sie zur Verbesserung der öffentlichen Sicherheit eingesetzt werden.
D) Nein, weil KI-Systeme im öffentlichen Raum die Effizienz steigern und keine Risiken bergen, da die Entscheidungen objektiv sind und menschliches Versagen ausschließen.

18 / 40
Eine Organisation entwickelt ein KI-System für Personaleinstellungszwecke. Bei internen Tests identifizierte das Team ein Risiko: Das System bevorzugte manchmal unabsichtlich Kandidaten mit bestimmten Hintergründen, was zu diskriminierenden Ausgaben führen könnte. Das Team ist jetzt unsicher, wie es auf diese Bedenken reagieren soll.

Die Organisation muss die KI-VO einhalten. Zur Risikominderung verwendet sie die Norm ISO/IEC TR 24368.

Was sollte die Organisation laut dieser Norm tun, um dieses Risiko zu mindern?

A) Den Algorithmus anpassen, so dass demografische Quoten auf der Grundlage von Beschäftigungsstatistiken priorisiert werden
B) Einen Zero-Data-Ansatz einführen, indem sie alle demografischen Daten aus dem Trainingsdatensatz entfernt
C) Cybersicherheitsmaßnahmen anwenden, um Kandidatendaten zu schützen und die Systemintegrität zu verbessern
D) Einen Prozess zur Einbindung von Interessenträgern umsetzen, um mögliche Verzerrungen (Bias) zu erkennen und zu mindern

19 / 40
Eine Organisation entwickelt ein KI-System für die Kreditbewilligung. Bei internen Tests stellt das Compliance-Team ein Risiko fest: Die Entscheidungsfindung des Systems ist nicht transparent, und die Dokumentation für die Risikobewertung ist ebenfalls begrenzt.

Die Organisation muss die KI-VO einhalten. Sie verwendet dazu die Norm ISO/IEC 42001 und das NIST AI Risk Management Framework (RMF) .

Wie sollte das Unternehmen laut dieser Norm und dem NIST-Rahmenwerk mit diesem Risiko umgehen?

A) Eine Bewertung der Sicherheitskonformität (Compliance) auf der Grundlage empfohlener Cybersicherheitsleitlinien durchführen
B) Das KI-System unverzüglich stilllegen und zu einem manuellen Kreditbewilligungsverfahren übergehen
C) Einen Maßnahmenplan mit Transparenzkennzahlen festlegen und die Entscheidungslogik zu Aufsichtszwecken aufzeichnen
D) Das System neu aufbauen und dabei synthetische Daten verwenden, um möglichst viele Quellen von Verzerrungen (Bias) auszuschalten

20 / 40
Ein führender Automobilhersteller hat ein hochautomatisiertes Fahrzeug (Stufe 4) entwickelt, das zur Verkehrssicherheit mit KI-gestützter Objekterkennungstechnologie ausgestattet ist. Beim Testen werden folgende Risiken erkannt:

- Bei schlechten Lichtverhältnissen kann das System Bodenschwellen nur eingeschränkt erkennen.
- Das Modell könnte schwer verkäuflich sein, weil es die Abmessungen anderer Fahrzeuge nicht kennt.
- Die Entwickler wissen nicht genau, wie sie die Entscheidungsfindung des Modells erklären sollen.
- In der Entwicklungsphase des KI-Systems wurden nicht alle Interessenträger um ihren Input gebeten.

Was muss adressiert werden, wenn man **ausschließlich** die Konformität (Compliance) mit der KI-VO betrachtet?

A) Das Risiko unzureichender Tests unter Realbedingungen
B) Das Risiko fehlender Transparenz in der KI-Entscheidungsfindung
C) Das Risiko begrenzter Skalierbarkeit des KI-Systems für andere Fahrzeugmodelle
D) Das Risiko der begrenzten Einbindung von Interessenträgern während der KI-Entwicklung

21 / 40
Ein Logistikunternehmen entwickelt ein KI-System, das Lieferwege optimieren und den Kraftstoffverbrauch senken soll. Das Unternehmen zieht zwei Alternativen in Betracht:

- Ein Closed-Source-KI-Modell eines Anbieters, der eine schnellere Installation und verifizierte Zertifizierung der Konformität (Compliance) garantiert.
- Ein Open-Source-KI-Modell (quelloffenes KI-Modell), das ein hohes Maß an individueller Anpassung und Transparenz ermöglicht.

Das Unternehmen muss die KI-VO einhalten, möchte aber auch ein Gleichgewicht zwischen Innovationen und Kosten herstellen.

Welches Modell passt **am besten** für dieses Unternehmen?

A) Ein Closed-Source-KI-Modell, weil es von Haus aus sicherer ist und bei den Behörden mehr Vertrauen genießt. Nichtkonformität wird dadurch weniger wahrscheinlich.
B) Ein Closed-Source-KI-Modell, weil es vorzertifizierte Konformität (Compliance) bietet. Das Unternehmen ist dann weniger damit belastet, die Konformität mit der KI-VO zu beweisen.
C) Ein Open-Source-KI-Modell, weil es vollkommene Transparenz gewährleistet. Das hilft, die Anforderungen zur Dokumentation und Prüfbarkeit in Audits zu erfüllen.
D) Ein Open-Source-KI-Modell, weil es von der Konformität (Compliance) mit der KI-VO ausgenommen ist. Das liegt daran, dass der Quellcode öffentlich zugänglich ist.

22 / 40
Die KI-VO legt Ethikgrundsätze für die KI-Entwicklung fest.

Was gehört **nicht** zu diesen Grundsätzen?

A) Erklärbarkeit
B) Fairness
C) Schadensverhütung
D) Achtung der KI-Autonomie

23 / 40
Ein Start-up-Unternehmen entwickelt ein KI-System zur Unterstützung von personalisiertem Lernen in Schulen mit maßgeschneiderten Lehrplänen, die an die Bedürfnisse der einzelnen Schüler angepasst sind. Das System erfasst Daten zur Leistung und zum Lernverhalten der Schüler.

Was sollte das Start-up-Unternehmen der KI-VO zufolge berücksichtigen, um Innovationen und Regulierung in Einklang zu bringen?

A) Vermeiden, das System als hochriskant zu kennzeichnen, um zusätzliche regulatorische Belastungen zu umgehen und die Innovation zu optimieren
B) Sicherstellen, dass das KI-System eine Konformitätsbewertung durchläuft und die Bestimmungen für Hochrisiko-KI-Systeme erfüllt
C) Robuste Datenschutzfunktionen implementieren, aber Benutzerbenachrichtigungen entfernen, um Verzögerungen bei der Inbetriebnahme zu vermeiden
D) Das System ausschließlich bei Privatschulen in Verkehr bringen, um die Auswirkungen der Konformitätsanforderungen an Hochrisiko-KI-Systeme zu begrenzen

24 / 40
Das Finanzinstitut Fintegra implementiert ein KI-System zur Betrugserkennung in Transaktionen. Für seine Analysen benötigt das System Zugriff auf Transaktionsinformationen von Kunden und demografische Daten. Fintegra muss die Datenminimierungsanforderung der KI-VO einhalten.

Wie kann Fintegra die Anforderung, die Datenerfassung zu minimieren, **am besten** erfüllen?

A) Alle Transaktionsdaten anonymisieren und sämtliche Daten entfernen, die eine natürliche Person identifizieren, um diese Anforderung zu erfüllen, selbst wenn diese Daten unerlässlich für die Betrugserkennung sind
B) Alle personenbezogenen Details erheben, einschließlich des vollständigen Namens und der genauen Adresse, um eine genaue Analyse und Verbesserungen im Laufe der Zeit sicherzustellen, und diese Daten so lange wie nötig sicher speichern
C) Die Datenerfassung auf Transaktionsdaten beschränken, die für die Betrugserkennung relevant sind, und die Verarbeitung personenbezogener Details wie vollständige Namen oder genaue Adressen von Kunden vermeiden
D) Die erfassten Daten nur mit anerkannten Anbietern teilen, die die KI-VO einhalten. Das minimiert die interne Verarbeitung von personenbezogenen Details wie vollständige Namen von Kunden.

25 / 40
EduTech implementiert eine adaptive Lernplattform, die KI verwendet, um Lernpfade für Schüler zu personalisieren. Die Plattform passt den Schwierigkeitsgrad von Aufgaben an die individuelle Leistung an.

Welches Risiko sollte EduTech mindern, um eine ethische Verwendung dieses KI-Systems sicherzustellen?

A) Das Risiko von Voreingenommenheit (Bias) und Diskriminierung, weil dies zu unfairen Vor- bzw. Nachteilen für bestimmte Schüler führen würde. Diese Risiko kann EduTech mindern, indem es die Datensätze und Algorithmen des KI-Systems regelmäßig überprüft und aktualisiert.
B) Das Risiko einer übermäßigen Abhängigkeit von der Technologie, die dazu führen könnte, dass Schüler die Fähigkeit zu kritischem Denken nicht entwickeln. Dieses Risiko kann EduTech durch vertrauliche Behandlung des Entscheidungsprozesses des KI-Systems mindern. Das regt Schüler dazu an, mehr zu denken.
C) Das Risiko von Verletzungen der Privatsphäre, weil sensible Schülerdaten einschließlich ihrer Leistungen missbraucht oder offengelegt werden könnten. EduTech kann dieses Risiko mindern, indem es sich stärker auf die Verbesserung der technischen Leistung des KI-Systems konzentriert.
D) Das Risiko von Transparenzproblemen, weil Schüler und Lehrkräfte unter Umständen nicht verstehen, wie Entscheidungen getroffen werden. EduTech kann dieses Risiko mindern, indem es sicherstellt, dass das KI-System ohne menschliche Aufsicht betrieben wird. Das sorgt für Fairness.

26 / 40
Eine Krankenhausabteilung ist auf die Diagnose und Behandlung von Krankheiten spezialisiert. Sie entwickelt ein KI-Diagnosesystem, das bei seltenen Erkrankungen zur Diagnoseassistenz eingesetzt werden soll. Das System analysiert Patientendaten, Vorerkrankungen und Bilddaten.

Das System wurde in den USA erfolgreich eingeführt. Einige medizinische Spezialisten in der Europäischen Union (EU) möchten das System einführen, verstehen jedoch nicht genau, wie es funktioniert. Sie verfügen auch nicht über besondere Fachkenntnisse und Erfahrungen in der Überwachung von KI oder im Erkennen von Störungen oder Fehldiagnosen.

Welches Risiko ist mit der Einführung dieses KI-Systems **nicht** verbunden?

A) Das Risiko fehlender wirksamer menschlicher Aufsicht
B) Das Risiko von Fehldiagnosen aufgrund von Automatisierungsbias
C) Das Risiko von Misstrauen wegen mangelnder Transparenz
D) Das Risiko eines unbefugten Zugriffs auf Patientenakten

27 / 40
Ein Unternehmen stellt ein KI-System für Smart-Home- Assistenten her. Bei den Tests stellt das Team fest, dass Spracherkennungsfehler wie Verwechslungen ähnlich klingender Wörter zu unbeabsichtigten Handlungen führen. Beispielsweise werden die falschen Hausgeräte eingeschaltet. Diese Fehler können die Privatsphäre verletzen, z.B. Gespräche ohne Einwilligung aufzeichnen oder Benutzer verwechseln, so dass unter Umständen sensible Informationen mit unbefugten Parteien geteilt werden.

Das Unternehmen muss die KI-VO einhalten. Es verwendet dazu das Rahmenwerk CEN/CLC/TR 18115.

Was sollte der KI-Anbieter laut diesem Rahmenwerk tun, um das Problem zu adressieren?

A) Einen Plan zur Einbindung von Interessenträgern erstellen, um unterschiedliche Sichtweisen einzuholen, wie das KI-System funktioniert
B) Eine Ethikfolgenabschätzung durchführen, um die Risiken für die Privatsphäre bei Smart-Home-Assistenten zu verstehen
C) Durch systematische Validierung und Fehlerprüfmethoden die Qualität der Trainingsdaten verbessern
D) Die Datensicherheit durch Verschlüsselung erhöhen, um Sprachdaten zu schützen und Verletzungen des Schutzes personenbezogener Daten zu verhindern

28 / 40
Bei einem Technologieunternehmen wurde festgestellt, dass es ein KI-System zur biometrischen Echtzeit-Fernidentifizierung verwendet. Die KI-VO verbietet das ausdrücklich.

Welche Sanktion ist für diesen Verstoß angemessen?

A) Eine formelle Verwarnung ohne finanzielle Maßnahme
B) Eine Geldbuße von bis zu 7,5 Mio. € bzw. 1% des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres
C) Eine Geldbuße von bis zu 15 Mio. € bzw. 3% des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres
D) Eine Geldbuße von bis zu 35 Mio. € bzw. 7% des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres

29 / 40
Die KI-VO betont insbesondere, wie wichtig zwei Aspekte von KI-Systemen sind: Transparenz und Rückverfolgbarkeit.

Warum sind Transparenz und Rückverfolgbarkeit wichtig?

A) Weil sie eine entscheidende Rolle für die Verantwortlichkeit und die Förderung von Vertrauen in KI-Systeme spielen
B) Weil sie verpflichtende Anforderungen an alle Produkte sind, einschließlich KI-Systeme
C) Weil sie besonders wesentlich sind für die Zuverlässigkeit und Automatisierung von KI-Systemen
D) Weil sie jeweils Bestandteil der europäischen, chinesischen und amerikanischen Rechtsvorschriften sind

30 / 40
Ein Einzelhändler verwendet ein KI-System, das auf der Grundlage von Nutzerpräferenzen und dem verwendeten Gerät automatisch die Darstellung von Elementen auf der Website ändert. Das System empfiehlt Produkte und verbessert das Benutzererlebnis unter Verwendung der Klickhistorie und der auf einer Seite verbrachten Zeit.

In welche Kategorie sollte die Verwendung dieses KI-Systems der KI-VO zufolge eingestuft werden?

A) Unannehmbares Risiko
B) Hochriskant
C) Begrenztes Risiko
D) Minimales oder kein Risiko

31 / 40
Ein Unternehmen entwickelt ein KI-System für automatisierte Entscheidungen im Personaleinstellungsprozess. Das KI-System wird Lebensläufe sichten, Kandidaten in eine Rangfolge bringen und Empfehlungen für Vorstellungsgespräche geben.

Das Unternehmen macht sich Sorgen, dass dieses KI-System Verzerrungen (Bias) enthalten könnte, die den Einstellungsprozess beeinträchtigen könnten.

Wie kann das Unternehmen Verzerrungen im KI-System **am besten** mindern?

A) Es kann dem KI-System erlauben, ohne menschliches Eingreifen zu lernen und sich anzupassen.
B) Es kann den Bias in den Trainingsdaten ignorieren und sich auf die Leistung des KI-Systems konzentrieren.
C) Es kann für die Erstellung und Überwachung des KI-Systems ein vielfältiges Entwicklungsteam einsetzen.
D) Es kann beim Trainieren des KI-Systems nur eine einzige Datenquelle verwenden, um Kohärenz zu gewährleisten.

32 / 40
Feline Finesse ist ein Webshop, der Katzenaccessoires und -kissen verkauft, einschließlich personalisierter Katzenplüschtiere basierend auf Bildern der Kunden. Der Webshop verwendet ein KI-System, das folgende Funktionen bietet:

- Es ändert Preise dynamisch in Abhängigkeit von Verbraucheraktivitäten.
- Es ordnet Suchergebnisse in einer Rangfolge an, die auf Kundenpräferenzen beruht.
- Es gibt persönliche Empfehlungen für andere Produkte, von denen es meint, dass sie dem Kunden gefallen.

Derzeit macht der Webshop Kunden darauf aufmerksam, was das KI-System macht, und zeigt sehr transparent, wie der Algorithmus funktioniert. Die CEO hinterfragt diese Praktik jedoch und will wissen, welcher Transparenzgrad erforderlich ist und wie er sich auf den Umsatz auswirkt.

Was sollte die CEO zum Thema Transparenz im Sinne der KI-VO wissen?

A) Transparenz kann Verbrauchern beweisen, dass das System objektiv ist. Die KI-VO räumt Verbrauchern das Recht ein zu verstehen, wie ihre Daten verwendet werden, und dieses Verständnis ist vertrauensfördernd.
B) Transparenz kann die Grenzen oder Einschränkungen des KI-Systems aufzeigen. Die Verbraucher könnten das Vertrauen in das Unternehmen verlieren, wenn sie das verstehen. Dies wiederum würde der Reputation des Unternehmens schaden.
C) Transparenz ist im E-Commerce nicht vorgeschrieben. Die bequeme Personalisierung ist hilfreich für die Verbraucher. Sie müssen weder wissen noch verstehen, wie das KI-System funktioniert.
D) Transparenz beschränkt sich darauf, den Quellcode des KI-Systems zur Verfügung zu stellen. Das Vertrauen der Verbraucher in das System könnte schwinden, wenn sie verstehen, wie der Algorithmus genau funktioniert.

33 / 40
In einem Personaleinstellungsprozess wird ein Hochrisiko-KI-System verwendet, das automatisch Kandidaten anhand ihrer Qualifikation herausfiltert. Der Betreiber des Systems hat jedoch keinen Mechanismus für menschliches Eingreifen oder menschliche Aufsicht implementiert für Fälle, in denen fragwürdige Entscheidungen getroffen werden.

Ist der KI-VO zufolge bei diesem System menschliche Aufsicht erforderlich?

A) Ja, weil menschliche Aufsicht erforderlich ist, um in Entscheidungsprozesse eingreifen zu können.
B) Ja, weil menschliche Aufsicht die Konformität (Compliance) mit Fairness- und Transparenzpflichten sicherstellt.
C) Nein, weil automatisierte Systeme so konzipiert sind, dass sie ohne menschliches Eingreifen funktionieren.
D) Nein, weil Personaleinstellungsprozesse keine kritischen Sicherheitsrisiken für natürliche Personen beinhalten.

34 / 40
Ein Unternehmen bereitet die Einführung eines KI-Modells mit allgemeinem Verwendungszweck vor. Das Modell kann angepasst werden, um Aufgaben wie Kundenservice-Automatisierung, Inhaltserstellung und Datenanalyse zu erfüllen. Das Unternehmen hat seinen Sitz außerhalb der Europäischen Union (EU), will das Modell aber in mehreren EU-Mitgliedstaaten in Verkehr bringen.

Welche Voraussetzung muss laut KI-VO **nicht** erfüllt sein, bevor das KI-Modell mit allgemeinem Verwendungszweck in der EU in Verkehr gebracht werden kann?

A) Benennung eines in der EU niedergelassenen Bevollmächtigten, der Aufgaben im Bereich Konformität (Compliance) übernimmt
B) Einhaltung des EU-Urheberrechts, um das Modell mit urheberrechtlich geschützten Daten zu trainieren
C) Durchführung eines gründlichen Audits, um die vollständige Konformität (Compliance) mit allen EU-Gesetzen und -Verordnungen zu verifizieren
D) Veröffentlichung einer detaillierten Zusammenfassung der Inhalte, die verwendet werden, um das Modell mit allgemeinem Verwendungszweck zu trainieren

35 / 40
Ein Unternehmen betreibt ein KI-System für vorausschauende Wartung (Predictive Maintenance) von Industrieanlagen. Nachdem das System einige Monate in Betrieb ist, generiert es eine sehr hohe Anzahl von Fehlalarmen, was die Arbeitsabläufe stört. Eine Untersuchung führt zu folgenden Feststellungen:

- Die Organisation hat die dynamischen Veränderungen in der Produktionsumgebung nicht berücksichtigt.
- Die Organisation hat kein formelles Verfahren für die Neubewertung von Risiken nach der Inbetriebnahme.

Die Organisation muss die Anforderungen der KI-VO erfüllen. Zur Lösung dieser Probleme verwendet sie die Norm ISO/IEC 23894.

Was sollte die Organisation laut dieser Norm tun, um diese Probleme zu adressieren?

A) Einen menschenzentrierten Design-Workshop abhalten, um die Benutzerfreundlichkeit des Systems zu verbessern
B) Einen Risikomanagementprozess mit laufender Bewertung und Überwachung konzipieren
C) Ein Audit im Bereich Cybersicherheit durchführen, um mögliche Sicherheitslücken zu identifizieren und zu adressieren
D) Das KI-System durch ein einfacheres, regelbasiertes Modell ersetzen, das leichter zu kontrollieren ist

36 / 40
Ein Flottenmanagement-Unternehmen verwendet ein KI-System, um das Verhalten der Fahrer zu verfolgen und Wartungsanforderungen vorherzusagen. Das System erfasst und verarbeitet umfangreiche Datenmengen wie GPS-Standorte, Fahrmuster und Leistungskennzahlen der Fahrzeuge. Bei einem Audit wurde vor kurzem festgestellt, dass das Unternehmen nicht genügend Datenschutzverfahren eingeführt hat.

Laut KI-VO sind Datenmanagement und Schutz der Privatsphäre für dieses Unternehmen unerlässlich.

Warum sind diese Aspekte so wichtig?

A) Weil das Unternehmen dadurch Geschäftsziele und operative Effizienz priorisieren kann
B) Weil dies das Vertrauen der Nutzer verbessert, personenbezogene Daten schützt und unbefugtem Zugriff vorbeugt
C) Weil das verpflichtend vorgeschrieben ist und die Einhaltung der KI-VO rechtliche Probleme und mögliche Geldbußen vermeidet
D) Weil dadurch die Datenerfassungsverfahren gestrafft werden, da die Einwilligung der Nutzer nicht mehr erforderlich ist

37 / 40
Welche Verwendung eines KI-Systems passt zur Einordnung als System mit begrenztem Risiko im Sinne der KI-VO?

A) Ein Chatbot, der Kunden bei allgemeinen Anfragen behilflich sein soll und so programmiert ist, dass offengelegt wird, dass es sich hier um KI handelt
B) Ein Gesichtserkennungssystem, das zur Echtzeit-Identifizierung von Kunden in öffentlichen Räumen wie Einkaufszentren verwendet wird
C) Ein medizinisches Diagnose-Tool, das Ärzten dabei hilft, auf der Grundlage von Patientendaten Behandlungsempfehlungen zu geben
D) Ein KI-System, das ein autonomes Fahrzeug betreibt, welches ohne menschliche Aufsicht auf öffentlichen Straßen fährt

38 / 40
Ein Unternehmen entwickelt ein KI-System für den Bildungsbereich. Das KI-System wird festlegen, ob ein Schüler Zugang zu Materialien erhält, in eine Schule aufgenommen bzw. einer Klasse zugewiesen wird. Bereitgestellt wird das KI-System über Cloud-Dienste.

In welche Kategorie sollte die Verwendung dieses KI-Systems laut KI-VO eingestuft werden?

A) Unannehmbares Risiko
B) Hochriskant
C) Begrenztes Risiko
D) Minimales oder kein Risiko

39 / 40
Ein Unternehmen hat ein KI-System für automatisierte Personaleinstellung entwickelt. In den Tests gelangt das Team zu folgenden Feststellungen:

- Das System gibt Kandidaten mit bestimmten ethnischen Hintergründen durchwegs niedrigere Wertungen, weil die Trainingsdaten demografische Verzerrungen (Bias) enthalten.
- Derzeit existiert weder ein internes Überprüfungsverfahren noch ein Mechanismus, um das Feedback relevanter Parteien einzuholen, die auf das Risiko dieses konkreten Bias hätten hinweisen können.

Das Unternehmen muss die KI-VO einhalten. Um diese Probleme zu lösen, verwendet es die Norm ISO/IEC TR 24368.

Was sollte das Unternehmen laut dieser Norm tun, um diese Probleme zu lösen?

A) Einen synthetischen Datensatz erstellen, um die demografischen Ungleichgewichte zu adressieren und die Fairness zu verbessern
B) Transparenz umsetzen, um die Erklärbarkeit und Verantwortlichkeit des Systems zu erhöhen
C) Die Datenverschlüsselungspraktiken stärken und Zugriffskontrollen verwenden, um Verstöße zu verhindern
D) Ein Ethikrahmenwerk mit Input von Interessenträger verwenden, um die Menschenrechtsthemen zu bewerten

40 / 40
Ein KI-Start-up-Unternehmen entwickelt ein KI-Modell mit allgemeinem Verwendungszweck, das mit öffentlich verfügbaren Online-Inhalten trainiert wird, einschließlich Presseartikeln, Forschungsberichten und Social-Media-Beiträgen. Nach der Einführung erhält das Unternehmen ein Anwaltsschreiben von einer Autorengruppe, in dem ihm vorgeworfen wird, das geistige Eigentum der Gruppe ohne entsprechende Genehmigung verwendet zu haben, um das Modell zu trainieren.

Was sollte getan werden, um die geistigen Eigentumsrechte in diesem Fall zu schützen?

A) Das Unternehmen sollte argumentieren, dass das KI-Modell mit allgemeinem Verwendungszweck als quelloffen einzustufen ist und daher von den Verpflichtungen zur Einhaltung des Urheberrechts befreit ist.
B) Das Unternehmen sollte sich auf angemessene Verwendung (Fair Use) im Sinne der KI-VO berufen, da die Inhalte öffentlich verfügbar waren, und sollte den Datensatz weiterhin verwenden.
C) Das Unternehmen sollte die KI-generierten Ergebnisse löschen, die Ähnlichkeiten mit den strittigen Werken aufweisen, um Ansprüche wegen Urheberrechtsverletzung zu vermeiden.
D) Das Unternehmen sollte Einzelheiten zum Trainingsdatensatz des KI-Modells mit allgemeinem Verwendungszweck einschließlich der Herkunft dokumentieren und teilen, um Konformität (Compliance) sicherzustellen.

Antwortschlüssel

1 / 40
Die KI-VO ist eine Rechtsvorschrift für die Europäische Union (EU). Artikel 1 KI-VO beschreibt ihre Ziele.

Was sind die **primären** Ziele der KI-VO?

A) Leitlinien, die sich ausschließlich auf Umweltschutz konzentrieren, keine spezifische Vorschriften für Hochrisiko-AI-Systeme, keine Verbote und Innovationsmaßnahmen nur für Großkonzerne
B) Harmonisierte Vorschriften für KI-Systeme in der EU, Verbote bestimmter KI-Praktiken, Anforderungen an Hochrisiko-KI-Systeme, Transparenzregeln, Marktüberwachung und Innovationsförderung
C) Verbote von KI-Praktiken, Vorschriften nur für KI-Systeme mit allgemeinem Verwendungszweck, Transparenzregeln, die nicht für Hochrisiko-KI-Systeme gelten, und Innovationsförderung, die auf nichteuropäische Einrichtungen beschränkt ist
D) Vorschriften für KI-Systeme, die auf Sicherheit und Gesundheit begrenzt sind, Verbote für alle KI-Praktiken, Transparenzvorschriften nur für Hochrisiko-KI-Systeme und Innovationsförderung, von der Start-up-Unternehmen ausgeschlossen sind

A) Falsch. Diese Option konzentriert sich nur auf Umweltschutz, und ignoriert die spezifische Vorschriften für Hochrisiko-KI-Systeme, die Verbote, und die Innovationsmaßnahmen nur für Großkonzerne. Das entspricht nicht dem umfassenden Ansatz der KI-VO.
B) Richtig. Diese Option beschreibt die Hauptpunkte der KI-VO zutreffend, einschließlich harmonisierter Vorschriften für KI-Systeme, Verbote bestimmter KI-Praktiken, besonderer Anforderungen an Hochrisiko-KI-Systeme, Transparenzvorschriften, Marktüberwachung und Innovationsförderung mit besonderem Augenmerk auf kleinen und mittleren Unternehmen (KMU). (Literatur: A, Kapitel 3.1, 3.2; KI-VO Artikel 1)
C) Falsch. Diese Option erweckt den Eindruck, als würde die KI-VO nur für KI-Systeme mit allgemeinem Verwendungszweck gelten und Hochrisiko-KI-Systeme von den Transparenzvorschriften befreien, zugleich aber die Innovationsförderung auf nichteuropäische Einrichtungen beschränken. Das unterstützen die Ziele der KI-VO nicht.
D) Falsch. Die Ziele der KI-VO gehen über Sicherheit und Gesundheit hinaus. In dieser Option wird fälschlicherweise behauptet, dass die Regeln auf Sicherheit und Gesundheit beschränkt und Start-up-Unternehmen von der Innovationsförderung ausgeschlossen seien. Außerdem heißt es, alle KI-Praktiken seien verboten. Das entspricht nicht den Bestimmungen der KI-VO.

2 / 40
Wie definiert die KI-VO Verantwortlichkeit und Konformität (Compliance)?

A) Verantwortlichkeit legt den Schwerpunkt auf den Schutz der Privatsphäre der Nutzer und die Datensicherheit, während Konformität (Compliance) sich auf die Integration in die bestehende IT-Infrastruktur bezieht.
B) Verantwortlichkeit heißt, Entwickler und Akteure in der KI-Entwicklung zur Verantwortung zu ziehen, und Konformität (Compliance) bedeutet Einhaltung der rechtlichen Anforderungen.
C) Verantwortlichkeit soll sicherstellen, dass KI-Systeme gewinnbringend für die Entwickler sind, und Konformität (Compliance) heißt, die Forderungen und Präferenzen der Nutzer zu erfüllen.
D) Verantwortlichkeit bezieht sich darauf, dass KI-Nutzer für die richtige Verwendung des Systems verantwortlich sind, während Konformität (Compliance) bedeutet, dass die Branchenstandards für KI-Innovationen eingehalten werden müssen.

A) Falsch. Die Privatsphäre der Nutzer und Datensicherheit sind zwar wichtig, doch sind Verantwortlichkeit und Konformität (Compliance) breiter gefasste Begriffe, deren Fokus auf der Verantwortung für und der Einhaltung der rechtlichen und regulatorischen Anforderungen liegt, nicht allein auf dem Schutz der Privatsphäre oder Integrationsbelangen. Konformität (Compliance) bezieht sich auf die Einhaltung rechtlicher und ethischer Vorschriften, nicht auf IT-Integration.
B) Richtig. Verantwortlichkeit bedeutet, dass Entwickler und Akteure von KI-Systemen für ihre Handlungen und Ergebnisse zur Verantwortung gezogen werden können. Konformität (Compliance) bezieht sich auf die Einhaltung der in der KI-VO beschriebenen rechtlichen und regulatorischen Anforderungen, die sicherstellen sollen, dass KI-Systeme sicher, transparent und fair sind. (Literatur: A, Kapitel 3.10)
C) Falsch. Verantwortlichkeit hat nichts mit Profitabilität oder Nutzerpräferenzen zu tun, und Konformität (Compliance) bedeutet nicht, die Forderungen der Nutzer zu erfüllen. Vielmehr liegt der Fokus dieser Begriffe auf Verantwortung und Einhaltung der rechtlichen Standards für KI-Systeme.
D) Falsch. Verantwortlichkeit bedeutet, Entwickler und Akteure für die Handlungen der KI-Systeme zur Verantwortung zu ziehen; es geht nicht um Schuldzuweisungen. Bei der Konformität (Compliance) geht es eher darum, spezifische rechtliche und regulatorische Standards zu erfüllen, nicht um allgemeine Branchenstandards.

3 / 40
Die KI-VO gewährt natürlichen Personen die von KI-Systemen betroffen sind besondere Rechte, um Transparenz, Fairness und Verantwortlichkeit sicherzustellen.

Welches Recht gewährt die KI-VO natürlichen Personen explizit?

A) Das Recht, informiert zu werden, dass sie mit einem KI-System interagieren bzw. davon betroffen sind.
B) Das Recht, Zugriff auf den Quellcode des KI-Systems zu verlangen
C) Das Recht, die Verwendung von KI in jedem sie betreffenden Entscheidungsprozess zu untersagen
D) Das Recht, die Löschung personenbezogener Daten zu verlangen, die das KI-System verwendet

A) Richtig. Natürliche Personen müssen informiert werden, dass sie mit einem KI-System interagieren, es sei denn, dies ist aus Sicht einer angemessen informierten Person offensichtlich. Das sorgt für Transparenz und hilft natürlichen Personen zu verstehen, wann KI Entscheidungen beeinflusst, die sie möglicherweise betreffen. (Literatur: A, Kapitel 3.6; KI-VO Artikel 50)
B) Falsch. Die KI-VO gewährt natürlichen Personen nicht das Recht auf Zugriff auf den Quellcode eines KI-Systems. Die Transparenzpflichten konzentrieren sich auf Erläuterungen und Diskussionen, nicht auf vollen Zugriff auf urheberrechtlich geschützten Code.
C) Falsch. Die KI-VO gewährt natürlichen Personen nicht das Recht, die Verwendung von KI-Systemen in der Entscheidungsfindung zu untersagen, sorgt jedoch für Überwachung und Transparenz.
D) Falsch. Während die Datenschutzgesetze natürlichen Personen bestimmte Rechte bezüglich ihrer Daten einräumen, gewährt die KI-VO kein pauschales Recht, die Löschung aller von einem KI-System verwendeten Daten zu verlangen.

4 / 40
Anna, die als Compliance-Beauftragte für ein kleines bzw. mittleres Unternehmen (KMU) arbeitet, ist verantwortlich für die Überwachung der Implementierung eines neuen KI-Systems für automatisierte Kundenbetreuung. Das Unternehmen hat dieses System nicht selbst entwickelt, sondern von einem anderen Anbieter gekauft. Laut KI-VO ist dieses System als Hochrisiko-KI-System einzuordnen.

Anna soll sicherstellen, dass das Unternehmen bei der Inbetriebnahme und Überwachung dieses KI-Systems seine Pflichten als Nutzer einhält. Sie muss festlegen, welche Maßnahmen zu priorisieren sind und welche vermieden werden sollten.

Was sollte Anna angesichts der Pflichten von KI-Nutzern **nicht** in Erwägung ziehen?

A) Die Algorithmen des KI-Modells weiterentwickeln, um seine Entscheidungsfähigkeiten zu verbessern, ohne seinen Anbieter einzubinden
B) Detaillierte Aufzeichnungen der Leistung des KI-Systems führen und Konformität (Compliance) mit einschlägigen Berichtsanforderungen gewährleisten
C) Die Leistung des KI-Systems überwachen, um zu gewährleisten, dass es bestimmungsgemäß betrieben wird und die Sicherheitsstandards erfüllt
D) Schwerwiegende Vorfälle und Fehlfunktionen im Zusammenhang mit dem KI-System an die zuständigen Behörden melden wie gesetzlich vorgeschrieben

A) Richtig. Anna sollte nicht versuchen, die Algorithmen des KI-Systems unabhängig weiterzuentwickeln oder seine Entscheidungsfähigkeiten ohne Mitwirkung des Anbieters anzupassen. Das übersteigt den Umfang der Nutzerpflichten und könnte zur Verletzung der Konformität (Compliance) oder unbeabsichtigten Folgen führen. Änderungen der internen Struktur des Systems liegen nicht in der Verantwortung der Nutzer. (Literatur: A, Kapitel 1.1)
B) Falsch. Die rechtlichen Anforderungen der KI-VO an Nutzer von Hochrisiko-KI-Systemen beinhalten das Führen von Aufzeichnungen und die Gewährleistung der Transparenz. Das unterstützt die Verantwortlichkeit und die Einhaltung der Rechtvorschriften.
C) Falsch. Leistungsüberwachung ist laut KI-VO eine wesentliche Pflicht der Nutzer. Das soll gewährleisten, dass das KI-System bestimmungsgemäß betrieben wird und keine Sicherheitsrisiken birgt.
D) Falsch. Laut KI-VO ist die Meldung von Fehlfunktionen oder schwerwiegenden Vorfällen eine wesentliche Anforderung an Nutzer von Hochrisiko-KI-Systemen, um die Konformität (Compliance) beizubehalten und mögliche Risiken umgehend zu adressieren.

5 / 40
Ein KI-System zur Gesichtserkennung wird zu Sicherheitszwecken in öffentlichen Räumen verwendet. Eine Organisation ist besonders relevant für die Überwachung der Konformität (Compliance) dieses KI-Systems mit den Vorschriften zum Datenschutz und zur Privatsphäre wie der Datenschutz-Grundverordnung (DSGVO).

Welche Organisation ist das?

A) Der Europäische Verbraucherverband (BEUC)
B) Das Europäische Gremium für Künstliche Intelligenz (KI-Gremium)
C) Der Europäische Gerichtshof (EuGH)
D) Der Europäischer Datenschutzausschuss (EDPB)

A) Falsch. Der BEUC konzentriert sich auf Verbraucherrechte, die mit Biometrie- und Datenschutz für KI-bezogene Vorschriften im Zusammenhang stehen.
B) Falsch. Das KI-Gremium überwacht die Konformität (Compliance) mit der KI-VO und konzentriert sich auf KI-spezifische Regulierungsvorschriften. Diese Frage betrifft jedoch den Datenschutz und die Privatsphäre, die unter die DSGVO fallen.
C) Falsch. Der EuGH ist für rechtliche Angelegenheiten zuständig, nicht für KI-Regulierungsvorschriften oder biometrische Daten.
D) Richtig. Der EDPB ist für die einheitliche Anwendung der DSGVO in allen Mitgliedstaaten der Europäischen Union (EU) zuständig. Zusammen mit nationalen Datenschutzbehörden arbeitet er an Themen wie der Verwendung biometrischer Daten in KI-Sicherheitssystemen. (Literatur: A, Kapitel 3.9, 3.10, 4.5)

6 / 40
Ein Unternehmen entwickelt ein KI-System für personalisiertes Marketing. Dieses System verwendet Algorithmen für maschinelles Lernen (ML), um Kunden maßgeschneiderte Werbung anzuzeigen. Bei einer Überprüfung der Konformität (Compliance) identifiziert das Team folgende Risiken:

- Es existiert keine Dokumentation, aus der klar hervorgeht, wie das KI-System Daten verarbeitet.
- Das Verfahren, mit dem das KI-System zu personalisierten Empfehlungen gelangt, wird nicht vollständig verstanden.
- Kunden beschweren sich über diese Aspekte.

Das Unternehmen muss die KI-VO einhalten. Dazu verwendet es die Norm ISO/IEC 42001 und das NIST AI Risk Management Framework (RMF).

Was sollte das Unternehmen laut dieser Norm und dem NIST-Rahmenwerk tun, um die Probleme zu lösen?

A) Eine Reihe von Nutzererlebnistests (UX Tests) durchführen, um Feedback zu Benutzerfreundlichkeit, Lernbarkeit und Kundenpräferenzen zu erhalten
B) Sich auf die Verbesserung der Vorhersagegenauigkeit des Systems konzentrieren, um seine Wirtschaftlichkeit, die Kundenzufriedenheit und das Kundenengagement zu verbessern
C) Ein Dokumentationsverfahren einführen, das Datenquellen, Verarbeitungsmethoden und die Entscheidungsfindung der Algorithmen detailliert aufzeichnet
D) Die Hardware des Systems upgraden, um seine Verarbeitungsgeschwindigkeit und Effizienz sowie die Kundenzufriedenheit zu verbessern

A) Falsch. Nutzererlebnistests liefern wertvolle Erkenntnisse zur Wirksamkeit des Systems, lösen aber nicht das zugrundeliegende Probleme fehlender Dokumentation und Transparenz von Daten und Entscheidungsprozessen.
B) Falsch. Eine Verbesserung der Vorhersagegenauigkeit kann zwar die Kundenzufriedenheit verbessern, beseitigt jedoch nicht das zentrale Problem mit der Dokumentation und Transparenz in der Datenverarbeitung und Entscheidungsfindung.
C) Richtig. Die Umsetzung eines umfassenden Dokumentationsverfahrens entspricht der Norm ISO/IEC 42001, die Transparenz und Dokumentation über den gesamten KI-Lebenszyklus hinweg betont. Das NIST AI Risk Management Framework unterstützt dies ebenfalls, indem es detaillierte Aufzeichnungen von Daten und Entscheidungen fördert, um Verantwortlichkeit und Rückverfolgbarkeit sicherzustellen. (Literatur: B, Kapitel 2.3)
D) Falsch. Ein Hardware-Upgrade kann die Verarbeitungsgeschwindigkeit verbessern, löst aber nicht die Probleme mit der Transparenz oder Dokumentation, die für Konformität (Compliance) mit der KI-VO erforderlich sind.

7 / 40
Ein Unternehmen entwickelt ein KI-System zur Überwachung von Patienten im Krankenhaus. Das System verwendet hochauflösende Kameras in den Krankenzimmern zur Echtzeit-Überwachung des Zustands der Patienten. Wenn das System einen Notfall erkennt, ruft es automatisch eine Pflegekraft an das Bett des Patienten.

Um die Leistung des KI-Systems zu verbessern, will das Unternehmen eine Datenbank mit Patientenvideos aufbauen – mit Anmerkungen von Sachverständigen an kritischen Stellen im Video, um mehr Trainingsdaten für das System zu erhalten.

Das Unternehmen erwägt, eine Datenschutzfolgenabschätzung (DPIA) durchzuführen. Das zuständige Team ist unsicher, ob eine DPIA überhaupt erfolgen sollte. Ist sie Pflicht, möchte das Team wissen, wann sie durchgeführt werden sollte: jetzt oder erst nach Inbetriebnahme des Update.

Das Unternehmen muss die KI-VO und die Datenschutz-Grundverordnung (DSGVO) einhalten.

Soll das Unternehmen jetzt eine DPIA durchführen?

A) Ja, weil eine DPIA bei KI-Projekten vorgeschrieben ist, die voraussichtlich ein hohes Risiko für die Rechte natürlicher Personen bergen.
B) Ja, weil eine DPIA für jedes Projekt erforderlich ist, das personenbezogene Daten erfasst, selbst wenn es ein Projekt mit geringem Risiko ist.
C) Nein, weil eine DPIA nicht erforderlich ist für die Verwendung von Daten für Trainingszwecke, Bildung oder wissenschaftliche Forschung.
D) Nein, weil eine DPIA nicht erforderlich ist, nachdem das KI-System vollständig entwickelt, getestet und in Betrieb genommen wurde.

A) Richtig. Diese Option entspricht den Anforderungen der DSGVO. Eine DPIA ist erforderlich, wenn die Verarbeitung voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt, insbesondere bei Verwendung neuer Technologien wie KI-Systemen, die (besonders) sensible Daten wie Patientenvideos verarbeiten. Sie fallen in die Kategorie Gesundheitsdaten, für die zusätzliche Schutzmaßnahmen erforderlich sind. (Literatur: A, Kapitel 4.5)
B) Falsch. Eine DPIA ist zwar wichtig, aber nicht automatisch erforderlich für alle Projekte, die personenbezogene Daten erfassen. Die DSGVO verlangt eine DPIA insbesondere, wenn die Datenverarbeitung voraussichtlich zu hohen Risiken für die Rechte und Freiheiten natürlicher Personen führt, nicht einfach nur wegen der Erfassung personenbezogener Daten wie biometrischen Daten, Gesundheitsdaten oder großflächiger Überwachung.
C) Falsch. Der Zweck der Datennutzung (z.B. Training oder Forschung) befreit ein Projekt nicht von der Anforderung, eine DPIA durchzuführen. Die DSGVO gilt weiterhin, insbesondere wenn die Verarbeitung zu hohen Risiken für natürliche Personen führen könnte, speziell wenn es um sensible Daten wie Patientenvideos geht.
D) Falsch. Eine DPIA sollte vor Beginn der Verarbeitung durchgeführt werden, insbesondere während der Planungs- und Entwicklungsphasen eines Projekts. Ziel ist die proaktive Identifizierung und Minderung von Risiken. Wird bis nach der Inbetriebnahme gewartet, könnte dies zur Nichtkonformität (Non-Compliance) mit der DSGVO führen.

8 / 40
Ein Unternehmen entwickelt ein KI-System zur Echtzeit-Gesichtserkennung. Eine private Sicherheitsfirma setzt dieses KI-System zur Überwachung eines öffentlichen Einkaufszentrums ein. Das System scannt alle Besucher, vergleicht ihre Gesichter mit Datenbanken früherer Straftäter und politischer Aktivisten und markiert Besucher, die in einer dieser Datenbanken geführt werden. Markierte Besucher werden während ihres gesamten Aufenthalts heimlich überwacht, um zu beurteilen, ob sie sich nach Einschätzung der Sicherheitsfirma verdächtig verhalten.

In welche Kategorie sollte die Verwendung dieses KI-Systems laut KI-VO eingestuft werden?

A) Unannehmbares Risiko
B) Hochriskant
C) Begrenztes Risiko
D) Minimales oder kein Risiko

A) Richtig. Artikel 5 KI-VO verbietet biometrische Echtzeit-Identifizierung in der Öffentlichkeit von Personen auf der Grundlage politischer Aktivitäten. Die Verordnung untersagt die Verwendung von KI-Systemen für nicht zielgerichtete Überwachung und soziale Bewertung, die gegen Grundrechte verstoßen. (Literatur: A, Kapitel 3.3, 3.4; KI-VO Artikel 5 Abs. 1 Buchst. d)
B) Falsch. Das System ist nicht einfach nur hochriskant, sondern verboten, weil es politische Aktivitäten nutzt, um natürliche Personen zu beobachten, und ihre Zustimmung dazu nicht einholt. Das ist eine verbotene Verwendung eines KI-Systems.
C) Falsch. Systeme mit begrenztem Risiko sind Chatbots oder Emotionserkennungswerkzeuge mit Transparenzpflichten. In diesem Fall geht es um biometrische Überwachung mit schwerwiegenden Auswirkungen auf die Rechte natürlicher Personen. Daher fällt das System nicht in diese Kategorie.
D) Falsch. Ein minimales Risiko geht von Systemen mit geringen Auswirkungen wie Spamfiltern aus. Gesichtserkennung zu Beobachtungszwecken übersteigt dieses Risikoniveau und ist ausdrücklich verboten.

9 / 40
Ein Reisebüro verwendet ein KI-System für die Entwicklung dynamischer, gezielter Marketingkampagnen für seine Pauschalreisen. Diese Kampagnen beinhalten die Echtzeit-Platzierung von Werbung auf sozialen Medien basierend auf dem Browserverlauf der betreffenden Person. Das Reisebüro verwendet KI, um Schlussfolgerungen über den emotionalen Zustand der Nutzer zu ziehen und dann individuell angepasste Reiseziele und Aktivitäten vorzuschlagen.

Das Reisebüro muss die KI-VO einhalten.

Welches Risiko muss das Reisebüro adressieren?

A) Das Risiko möglicher Verzerrungen (Bias). Das Unternehmen sollte die Trainingsdaten regelmäßig aktualisieren, um zu vermeiden, dass uninteressante Reiseziele vorgeschlagen oder falsche emotionale Zustände abgeleitet werden.
B) Das Risiko unwirksamer Werbemaßnahmen. Das Unternehmen sollte sich darauf konzentrieren, den Algorithmus zu aktualisieren, weil die KI-VO personalisierte Werbung nicht abdeckt.
C) Das Risiko fehlender Transparenz. Das Unternehmen sollte Offenheit in Bezug auf die KI gewährleisten, Voreingenommenheit (Bias) in den Vorschlägen reduzieren und überprüfen, ob die Werbeaktivitäten ethisch sind.
D) Das Risiko des Missbrauchs personenbezogener Daten. Das Unternehmen sollte keine KI-gestützte Personalisierung mehr verwenden, weil die KI-VO die Verwendung personenbezogener Daten für gezielte Werbung untersagt.

A) Falsch. Hier sind Verzerrungen gemeint, die bestimmte Kundengruppen benachteiligen. Ein uninteressantes Reiseziel hat wohl kaum größere Auswirkungen auf die Kunden.
B) Falsch. Die KI-VO räumt Hochrisiko-KI-Anwendungen zwar oberste Priorität ein, doch gelten ihre Bestimmungen auch für kommerzielle Sektoren wie Werbung und Tourismus, insbesondere wenn es um Kundenprofiling und Entscheidungsfindung geht.
C) Richtig. Das deckt die wesentlichen Pflichten im Sinne der KI-VO ab. Reisebüros müssen für Transparenz sorgen, indem sie Verbraucher über die KI-Einbindung informieren, Voreingenommenheit verhindern und gewährleisten, dass ihre Werbemaßnahmen Ethikgrundsätze einhalten. (Literatur: A, Kapitel 7.8, 7.9)
D) Falsch. Die KI-VO verbietet maßgeschneiderte Werbung oder KI-gestützte Personalisierung nicht ausdrücklich. Vielmehr bietet sie Leitlinien für moralisches Verhalten, die Offenheit, Gerechtigkeit und Datensicherheit fordern, um sicherzustellen, dass solche Methoden im Einklang mit den Werten der Europäischen Union (EU) sind.

10 / 40
Ein Unternehmen entwickelt ein KI-Modell, das in verschiedenen Branchen verwendet werden kann, unter anderem im Gesundheits- und Finanzsektor. Wegen seiner breiten Anwendung birgt das KI-Modell mögliche Risiken für die öffentliche Gesundheit.

Was hat das Unternehmen entwickelt und welche Praktiken sollte es laut KI-VO umsetzen?

A) Das Unternehmen hat ein KI-Modell mit allgemeinem Verwendungszweck mit systemischen Risiken entwickelt. Es sollte zusätzliche Tests durchführen, um die Risiken zu mindern.
B) Das Unternehmen hat ein Hochrisiko-KI-System entwickelt. Es sollte alle Anforderungen an Hochrisiko-KI-Systeme umsetzen, die in der KI-VO vorgeschrieben sind.
C) Das Unternehmen hat ein eng gefasstes KI-Modell entwickelt. Um Risiken vorzubeugen, sollte es sicherstellen, dass das Modell nur innerhalb vordefinierter Parameter betrieben wird.
D) Das Unternehmen hat ein experimentelles KI-Modell entwickelt. Es sollte sich auf Forschung und Entwicklung konzentrieren, ohne sofortiges Risikomanagement zu betreiben.

A) Richtig. Das Unternehmen hat ein KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko entwickelt. Es sollte eine zusätzliche Modellbewertung durchführen – mit standardisierten Protokollen und Instrumenten, die dem Stand der Technik entsprechen. Dazu gehören auch die Durchführung und Dokumentation von Sicherheitstests (Literatur: A, Kapitel 3.7; KI-VO Artikel 3, Artikel 55)
B) Falsch. Das KI-Modell birgt zwar mögliche Risiken, ist jedoch als KI-Modell mit allgemeinem Verwendungszweck einzustufen, nicht speziell als Hochrisiko-KI-System.
C) Falsch. Ein eng gefasstes KI-Modell ist auf spezifische Aufgaben begrenzt und birgt nicht die systemischen Risiken, die mit KI-Modellen mit allgemeinem Verwendungszweck verbunden sind.
D) Falsch. Selbst experimentelle KI-Modelle müssen die Risikomanagementpraktiken einhalten, wenn sie mögliche systemische Risiken bergen.

11 / 40
Eine Organisation entwickelt ein Hochrisiko-KI-System. In den Tests identifiziert das Entwicklungsteam verschiedene Risiken, einschließlich Unstimmigkeiten in der Vollständigkeit der Daten und veraltete Datensätze. Diese Risiken könnten die Leistung des Modells beeinträchtigen.

Die Organisation muss die KI-VO einhalten. Sie verwendet dazu das Rahmenwerk CEN/CLC/TR 18115.

Was sollte die Organisation laut diesem Rahmenwerk tun, um diese Risiken zu adressieren?

A) Eine Datenschutzfolgenabschätzung (DPIA) durchführen, um die Fairness der KI-Entscheidungsfindung zu adressieren
B) Alle Trainings- und Testdatensätze auf der Grundlage von Protokollen verschlüsseln, um unbefugten Zugriff auf personenbezogene Daten zu verhindern
C) Allgemeine Risikokontrollen einführen, um die genannten Betriebs- und Reputationsrisiken zu verringern
D) Die Datenqualität durch Anwendung strukturierter Qualitätskennzahlen und statistischer Bewertungsmethoden verbessern

A) Falsch. Eine Datenschutzfolgenabschätzung (DPIA) ist sinnvoll zur Bewertung der Risiken für die Rechte und Freiheiten natürlicher Personen. Sie eignet sich jedoch nicht für den unmittelbaren Umgang mit Problemen wegen veralteter oder unvollständiger Daten. Zur Verbesserungen der Datenqualität sind technische Maßnahmen erforderlich, keine rechtliche Bewertung.
B) Falsch. Verschlüsselung ist zwar wichtig für die Datensicherheit, hilft aber nicht bei Problemen mit der Datenqualität wie mangelnde Vollständigkeit oder Aktualität. Artikel 10 KI-VO betont nicht nur den Datenschutz, sondern schreibt auch vor, dass die für KI-Training und -Tests verwendeten Daten relevant, repräsentativ und von hoher Qualität sein sollen.
C) Falsch. Risikomanagement ist zwar sehr wichtig im KI-Bereich, bietet aber nicht das Rahmenwerk für die Datenqualität, das zur Lösung der identifizierten Probleme erforderlich ist. Die Vollständigkeit und Aktualität der Daten kann über eine Verbesserung der Datenqualität gesteuert werden, nicht über allgemeine KI-Risikostandards.
D) Richtig. CEN/CLC/TR 18115 enthält Leitlinien für die Bewertung und Verbesserung der Datenqualität entlang des Lebenszyklus von KI-Systemen. Das Rahmenwerk legt besonderes Gewicht auf die Verwendung von Kennzahlen für Merkmale wie Vollständigkeit und Aktualität, insbesondere während der Datenaufbereitung, um die Einhaltung von Artikel 10 KI-VO sicherzustellen . (Literatur: B, Kapitel 1; KI-VO Artikel 10)

12 / 40
Im Zusammenhang mit KI-Systemen beschreibt die KI-VO verschiedene Rollen.

Wie wird die Rolle "Einführer eines KI-Systems" definiert?

A) Eine natürliche oder juristische Person, die ein KI-System konzipiert, entwickelt und unter ihrem eigenen Namen oder ihrer Handelsmarkte in Verkehr bringt.
B) Eine natürliche oder juristische Person, die ein KI-System in Verkehr bringt, aber nicht für seine ursprüngliche Entwicklung verantwortlich ist.
C) Eine natürliche oder juristische Person, die ein KI-System in ihrem Betrieb verwendet und die lokale Konformität (Compliance) mit den Nutzerpflichten sicherstellt.
D) Eine Aufsichtsbehörde, deren Aufgabe es ist zu überwachen, ob das KI-System in Übereinstimmung mit den Bestimmungen der KI-VO eingeführt wird.

A) Falsch. Hier wird die Rolle des "Anbieters" beschrieben, der für die Entwicklung und das Inverkehrbringen des KI-Systems verantwortlich ist, nicht für seine Einführung.
B) Richtig. Das ist die Definition des "Einführers", in der Regel wenn das System außerhalb der Europäischen Union (EU) entwickelt wurde. Einführer sind dafür verantwortlich sicherzustellen, dass das System den regulatorischen Anforderungen der EU entspricht. Beim Nachweis der Konformität (Compliance) arbeiten sie mit Anbietern zusammen. (Literatur: A, Kapitel 3.1)
C) Falsch. Hier wird die Rolle des "Nutzers" beschrieben, der das KI-System betreibt und überwacht, nicht der Einführer.
D) Falsch. Aufsichtsbehörden sind keine Einführer. Sie sind dafür verantwortlich, die Konformität (Compliance) durchzusetzen, jedoch nicht aktiv daran beteiligt, Systeme in Verkehr zu bringen.

13 / 40
Ein Unternehmen entwickelt ein KI-System zur Betrugserkennung in Finanztransaktionen. Dieses System analysiert Transaktionsmuster, um verdächtige Aktivitäten zu erkennen und Betrugsversuchen vorzubeugen. Angesichts der Möglichkeit von Fehlalarmen, die sich auf rechtmäßige Transaktionen auswirken können, und der Tatsache, dass sich die Betrugstaktiken weiterentwickeln, weiß das Unternehmen, dass wirksame Schutzvorkehrungen erforderlich sind.

Das Unternehmen muss die KI-VO einhalten. Um Problemen durch Fehlalarme vorzubeugen, nutzt es die Norm ISO/IEC 23894.

Was sollte das Unternehmen laut dieser Norm tun, um solchen Probleme vorzubeugen?

A) Risikomanagement zum integralen Bestandteil aller Aktivitäten machen, um umfassende Aufsicht und proaktive Risikominderung sicherzustellen
B) Die Datenschutzmaßnahmen verbessern, um sensible Informationen zu schützen und die Bestimmungen zum Schutz der Privatsphäre einzuhalten
C) Sich auf die Verbesserung der Modellgenauigkeit konzentrieren, um zuverlässige Leistung sicherzustellen und Fehlalarme zu minimieren
D) Cybersicherheitsmaßnahmen umsetzen, um das System vor Bedrohungen von außen und unbefugtem Zugriff zu schützen

A) Richtig. Dieser Ansatz macht Risikomanagement zum integralen Bestandteil aller Aktivitäten der Organisation, passt Rahmenwerke maßgeschneidert an den spezifischen Kontext an und bezieht Interessenträger ein, um KI-bezogene Risiken wirksam zu erkennen und zu mindern. Dies entspricht der Norm ISO/IEC 23894 und hilft am besten, um Konformität (Compliance) herzustellen. (Literatur: B, Kapitel 3.2)
B) Falsch. Das Unternehmen muss sich um wichtige Datenschutzbelange kümmern. Dies führt jedoch nicht zwangsläufig zur Integration der umfassenden Risikomanagementpraktiken, die für KI erforderlich und in der Norm ISO/IEC 23894 beschrieben sind. Letzteres wäre die Voraussetzung für Konformität (Compliance).
C) Falsch. Konzentriert sich das Unternehmen auf die Verbesserung der Modellgenauigkeit, um zuverlässige Leistung sicherzustellen und Fehlalarme zu minimieren, verbessert es die Wirksamkeit des Modells, adressiert aber nicht breiter gefasste Aspekte des Risikomanagements wie Identifizierung, Bewertung und Minderung möglicher KI-bezogener Risiken. ISO/IEC 23894 legt besonderes Gewicht auf einen umfassenden Risikomanagementansatz.
D) Falsch. Mit der Umsetzung von Cybersicherheitsmaßnahmen zum Schutz des Systems vor Bedrohungen von außen und unbefugten Zugriff adressiert das Unternehmen ein wesentliches Element der Systemsicherheit. Das deckt jedoch nicht den vollen Umfang der für KI erforderlichen Risikomanagementpraktiken ab, die in der Norm ISO/IEC 23894 spezifiziert sind.

14 / 40
Ein Fertigungsunternehmen verwendet KI-gestützte Robotertechnologie zur Qualitätskontrolle an seinen Montagebändern. Das Ermittlungsteam erfährt von einem anonymen Hinweisgeber, dass das KI-System in letzter Zeit eine ungewöhnlich niedrige Anzahl fehlerhafter Produkte ausweist. Grund für diese Untererfassung ist ein Software-Update des KI-Systems. Eine manuelle Prüfung zeigt, dass die Produkte fehlerhaft und unsicher sind.

Im Bericht heißt es, dass der neue Fehlererkennungsalgorithmus einen kritischen Fehler erzeugt, der zu falsch-negativen Ergebnissen führt. Dem Hinweisgeber zufolge war den Führungskräften dieses Problem bekannt, doch wurde nichts dagegen unternommen, um der Reputation des Unternehmens nicht zu schaden.

Was sollten die nächsten Schritte sein?

A) - Den internen Algorithmus anpassen, um das Problem zu beseitigen
- Die zuständige Behörde unterrichten, wenn das Problem nach 30 Tagen immer noch auftritt

B) - Das Problem intern untersuchen und mit einer Lösung beginnen
- Die zuständige Behörde unverzüglich über den Vorfall unterrichten

C) - Die Gründe ermitteln, warum der Hinweisgeber das Problem gemeldet hat
- Die zuständige Behörde unterrichten, wenn Verbraucher sich zu beschweren beginnen

D) - Das KI-Systems stilllegen und zu einer älteren Methode übergehen
- Eine Unterrichtung der zuständigen Behörde ist dann nicht mehr erforderlich.

A) Falsch. Wird an dem Problem gearbeitet, ohne eine Behörde davon zu unterrichten, umgeht das Unternehmen die rechtliche Anforderung, schwerwiegende Vorfälle zu melden. Dies könnte Sanktionen und Misstrauen gegenüber dem Umgang des Unternehmens mit KI-Systemen zur Folge haben.

B) Richtig. Eine Untersuchung gewährleistet, dass die zugrundeliegende Problemursache erkannt und angegangen wird. Die Unterrichtung der zuständigen Behörde sorgt für die Einhaltung der Vorschriften. (Literatur: A, Kapitel 7.4, 3.10; KI-VO Artikel 73)

C) Falsch. Eine Untersuchung der Motive des Hinweisgebers ist ein Verstoß gegen den Grundsatz, Hinweisgeber zu schützen, und schreckt von ethischen Meldungen ab. Dieser Ansatz priorisiert die Steuerung der Reputation gegenüber rechtlichen und ethischen Pflichten und verletzt daher die Anforderungen der KI-VO und die Integrität der Organisation.

D) Falsch. Die Stilllegung des KI-Systems könnte zwar das Problem lösen, erfüllt jedoch nicht die Meldekriterien der KI-VO. Diese Option ist unannehmbar, weil es sich um einen schwerwiegenden Vorfall handelt, der sich auf die Produktsicherheit auswirkt. Ein solcher Vorfall muss gemeldet und angegangen werden.

15 / 40
MedTech Diagnostics verwendet ein Hochrisiko-KI-System zur Diagnose von Krankheiten anhand von Röntgenbildern. Folgende Maßnahmen wurden ergriffen:

- Das Unternehmen hat ein externes Audit bestanden, um sicherzustellen, dass das KI-System die Standards der KI-VO erfüllt.
- Ein robustes Rahmenwerk für das Risikomanagement identifiziert und mindert mögliche Probleme, und es existieren Notfallpläne.
- Detaillierte Aufzeichnungen zum Betrieb des KI-Systems werden sicher aufbewahrt, um für Verantwortlichkeitsfragen und Audits zur Verfügung zu stehen.
- Nutzer erhalten eine klare Dokumentation und Schulungen, in denen die Entscheidungsfindung und Einschränkungen der KI erklärt werden.
- Alle AI-generierten Diagnosen werden vor der finalen Festlegung von medizinischen Fachkräften überprüft, um ein menschliches Urteil zu integrieren.

Was sollte das Unternehmen sonst noch tun?

A) Robuste Daten-Governance-Verfahren hinzunehmen, um die Zuverlässigkeit und Fairness des KI-Systems beizubehalten
B) Aus Effizienzgründen sicherstellen, dass das KI-System autonom ohne menschliches Eingreifen läuft
C) Ein System implementieren, das menschliche Entscheidungen automatisch außer Kraft setzt, um den Diagnoseprozess zu beschleunigen
D) Eine Funktion aufnehmen, die Patienten ermöglicht, ihre Krankenakten auf der Grundlage von KI-Vorschlägen selbst anzupassen

A) Richtig. Robuste Daten und Daten-Governance decken die Qualität, die Minderung von Verzerrungen (Bias) und die Rückverfolgbarkeit von Trainings- und Betriebsdaten ab. Dadurch werden die Zuverlässigkeit und Fairness des Systems sichergestellt. (Literatur: A, Kapitel 3.3; KI-VO Artikel 15)
B) Falsch. In der medizinischen Diagnose erlaubt die KI-VO keine vollständige Automatisierung. Bei Hochrisiko-KI-Systemen im Gesundheitsbereich ist menschliche Aufsicht vorgeschrieben, um Sicherheit und Genauigkeit zu gewährleisten. Vollständige Autonomie ist daher unangemessen. Menschliche Überprüfung ist essenziell für Patientensicherheit und Konformität (Compliance) mit den regulatorischen Vorgaben.
C) Falsch. In Hochrisiko-KI-Systemen wie medizinische Diagnose kann ein automatisches Außerkraftsetzen menschlicher Entscheidungen die Patientensicherheit gefährden und die wesentliche Rolle der menschlichen Aufsicht unterminieren.
D) Falsch. Würde Patienten erlaubt, Krankenakten auf der Grundlage von KI-Vorschlägen zu ändern, könnte dies zu Ungenauigkeiten führen. Dies entspräche nicht den üblichen medizinischen Praktiken, die fachliche Aufsicht vorschreiben, und würde zu Rechtsrisiken führen.

16 / 40
Eine Versicherung implementiert eines neues KI-gestütztes Credit-Scoring-System mit Zugriff auf interne und öffentliche Datenbanken. Folgende Risiken werden identifiziert:

- **Fehlen angemessener Trainingsdaten.**Ein schlecht trainiertes Modell erschwert die genaue Feststellung fairer Kredit-Scores für natürliche Personen.
- **Integration mit anderen Anwendungen**. Das KI-gestützte System lässt sich nur schwer in die eher komplexe und an manchen Stellen veraltete Anwendungsumgebung integrieren.
- **Nichteinhaltung der DSGVO**. Laut Datenschutz-Grundverordnung (DSGVO) gelten für die autonome Verarbeitung personenbezogener Daten in automatisierten Systemen besondere Anforderungen.
- **Transparenz und Qualität des Modells**. Die Mitarbeitenden und Kunden müssen jeweils in der Lage sein, die Ergebnisse und Entscheidungen des KI-Modells zu verstehen.

Die Versicherung muss die KI-VO einhalten.

Welches Risiko spielt für die Konformität (Compliance) mit der KI-VO **keine** wichtige Rolle?

A) Fehlen angemessener Trainingsdaten
B) Integration mit anderen Anwendungen
C) Nichteinhaltung der DSGVO
D) Transparenz und Qualität des Modells

A) Falsch. KI-Systeme müssen hochwertige, nicht verzerrte Daten verwenden, um Diskriminierung oder unfairen Entscheidungen vorzubeugen. Schlechte Trainingsdaten können zu Verzerrungen (Bias) oder ungenauen Kredit-Scores führen und somit gegen die Anforderungen der KI-VO verstoßen.
B) Richtig. Eine nicht gut funktionierende Integration mit anderen Anwendungen birgt sicherlich Risiken, aber keine, die in der KI-VO definiert sind. (Literatur: A, Kapitel 7.2, 7.3)
C) Falsch. Die DSGVO legt besondere Einschränkungen für Systeme fest, die personenbezogene Daten autonom verarbeiten. Das ist jedoch nicht die größte Herausforderung, die hier angegangen werden muss. Die KI-VO ist an die DSGVO angeglichen, insbesondere hinsichtlich der Verarbeitung personenbezogener Daten, der Rechtsgrundlage für KI-Entscheidungen und der Rechte natürlicher Personen (z.B. Recht auf Erläuterung und Einspruch).
D) Falsch. Datenqualität und Genauigkeit des KI-Modells sind die wichtigsten Herausforderungen, die bei dieser Art von Anwendungsprojekten angegangen werden müssen. Wichtig ist auch, dass die Ausgaben des KI-Modells verständlich und erklärbar sind. Die KI-VO schreibt Erklärbarkeit und Transparenz vor, insbesondere bei Hochrisiko-KI-Systemen wie Credit-Scoring-Modellen, bei denen KI-Entscheidungen den Zugang zu Finanzmitteln beeinflussen.

17 / 40
Eine Regierungsbehörde schlägt ein KI-System vor, das bei der Vorhersage von Kriminalitäts-Hotspots im Innenstadtbereich einer größeren Stadt helfen soll. Das System wird zur automatisierte Überwachung eingesetzt. Es ist so programmiert, dass es automatisch Personen identifiziert, die sich verdächtig verhalten, und diese dann der örtlichen Polizei meldet. Das ist eine große Chance für die Verbrechensverhütung, ein erhöhtes Sicherheitsgefühl und eine gerechte Strafverfolgung nach einem Verbrechen.

Können bei der Implementierung dieses KI-Systems Risiken auftreten?

A) Ja, weil ein KI-System, das für automatisierte Entscheidungen verwendet wird, stets das Risiko von Verzerrungen (Bias) birgt. Das kann zu einer unfairen Benachteiligung natürlicher Personen führen.
B) Ja, weil die KI-VO bei Überwachungssystemen so viele Risiken für die Privatsphäre sieht, dass sie deren Einsatz im öffentlichen Raum ganz verbietet.
C) Nein, weil KI-Systeme in der Verbrechensverfolgung und -verhütung keine besonderen Risiken bergen, da sie zur Verbesserung der öffentlichen Sicherheit eingesetzt werden.
D) Nein, weil KI-Systeme im öffentlichen Raum die Effizienz steigern und keine Risiken bergen, da die Entscheidungen objektiv sind und menschliches Versagen ausschließen.

A) Richtig. Die KI-VO nennt dies ausdrücklich als größte Sorge. In sensiblen Bereichen wie Verbrechensverfolgung können möglicherweise verzerrte Daten oder fehlerhafte Algorithmen in KI-Systemen zu diskriminierenden Ergebnissen führen. Bei KI-Systemen in Hochrisiko-Anwendungen fordert die KI-VO Offenheit, Risikobewertungen und Maßnahmen zur Minderung von Verzerrungen. (Literatur: A, Kapitel 8.1, 8.2, 8.3)
B) Falsch. Ziel der KI-VO ist es, eine sichere, offene und faire Verwendung (Fair Use) von KI zu kontrollieren und zu gewährleisten, nicht ihre Verwendung in öffentlichen Räumen zu unterbinden. Sie setzt zwar Schutzmaßnahmen zum Umgang mit Gefahren durch, fördert aber auch die Kreativität.
C) Falsch. Die Verbesserung der öffentlichen Sicherheit ist ein hehres Ziel, entbindet jedoch nicht von der Pflicht, Risiken für die Privatsphäre und die Benachteiligung natürlicher Personen, die sich in der Öffentlichkeit nicht unangemessen verhalten, zu mindern.
D) Falsch. KI-Ausgaben hängen von den angewendeten Trainingsdaten und Algorithmen ab. Bias in Trainingsdaten schlägt sich daher in den Entscheidungen des Systems nieder. Sie sind nicht unbedingt objektiver als menschliche Urteile. Außerdem räumt die KI-VO natürlichen Personen das Recht ein zu verlangen, dass Entscheidungen zu ihnen menschlicher Aufsicht unterliegen.

18 / 40
Eine Organisation entwickelt ein KI-System für Personaleinstellungszwecke. Bei internen Tests identifizierte das Team ein Risiko: Das System bevorzugte manchmal unabsichtlich Kandidaten mit bestimmten Hintergründen, was zu diskriminierenden Ausgaben führen könnte. Das Team ist jetzt unsicher, wie es auf diese Bedenken reagieren soll.

Die Organisation muss die KI-VO einhalten. Zur Risikominderung verwendet sie die Norm ISO/IEC TR 24368.

Was sollte die Organisation laut dieser Norm tun, um dieses Risiko zu mindern?

A) Den Algorithmus anpassen, so dass demografische Quoten auf der Grundlage von Beschäftigungsstatistiken priorisiert werden
B) Einen Zero-Data-Ansatz einführen, indem sie alle demografischen Daten aus dem Trainingsdatensatz entfernt
C) Cybersicherheitsmaßnahmen anwenden, um Kandidatendaten zu schützen und die Systemintegrität zu verbessern
D) Einen Prozess zur Einbindung von Interessenträgern umsetzen, um mögliche Verzerrungen (Bias) zu erkennen und zu mindern

A) Falsch. Es mag zwar ethisch erscheinen, eine ausgewogene Repräsentation herzustellen, doch strenge Quoten ohne Kontext könnten neue Voreingenommenheiten (Bias) einführen. ISO/IEC TR 24368 legt den Schwerpunkt eher auf Fairness und Einbindung von Interessenträgern als auf willkürliche demografische Ziele.
B) Falsch. Werden demografische Daten einfach entfernt, verhindert das Diskriminierung nicht und kann sogar bestehende Voreingenommenheit (Bias) verdecken. ISO/IEC TR 24368 fördert transparente Methoden und Minderung von Bias, nicht unüberlegtes Entfernen von Daten.
C) Falsch. Cybersicherheit ist zwar wichtig, deckt jedoch ethische Probleme wie Voreingenommenheit (Bias) oder Fairness nicht ab. Für ethische Bedenken sind Ansätze erforderlich, die mit ISO/IEC TR 24368 im Einklang stehen.
D) Richtig. ISO/IEC TR 24368 fördert die Einbindung von Interessenträgern bei der Identifizierung ethischer Risiken wie Voreingenommenheit (Bias) und der Entwicklung inklusiver, fairer KI-Systeme. Das unterstützt die Ziele der KI-VO in Bezug auf Fairness und Nichtdiskriminierung. (Literatur: B, Kapitel 4)

19 / 40
Eine Organisation entwickelt ein KI-System für die Kreditbewilligung. Bei internen Tests stellt das Compliance-Team ein Risiko fest: Die Entscheidungsfindung des Systems ist nicht transparent, und die Dokumentation für die Risikobewertung ist ebenfalls begrenzt.

Die Organisation muss die KI-VO einhalten. Sie verwendet dazu die Norm ISO/IEC 42001 und das NIST AI Risk Management Framework (RMF) .

Wie sollte das Unternehmen laut dieser Norm und dem NIST-Rahmenwerk mit diesem Risiko umgehen?

A) Eine Bewertung der Sicherheitskonformität (Compliance) auf der Grundlage empfohlener Cybersicherheitsleitlinien durchführen
B) Das KI-System unverzüglich stilllegen und zu einem manuellen Kreditbewilligungsverfahren übergehen
C) Einen Maßnahmenplan mit Transparenzkennzahlen festlegen und die Entscheidungslogik zu Aufsichtszwecken aufzeichnen
D) Das System neu aufbauen und dabei synthetische Daten verwenden, um möglichst viele Quellen von Verzerrungen (Bias) auszuschalten

A) Falsch. Die Einhaltung von Sicherheitsleitlinien adressiert nicht explizit die Transparenz oder die Risikodokumentation. Daher ist sie für das festgestellte Problem nicht unmittelbar relevant.
B) Falsch. Eine Stilllegung des Systems ist nicht erforderlich, weil es lediglich interne Tests durchläuft. Ein Wechsel zu manuellen Kreditbewilligungen würde das Problem vermeiden, doch wären dann auch die gesamten Investitionen verloren. Das Risiko kann durch strukturierte Governance gemanagt werden.
C) Richtig. ISO/IEC 42001 legt den Fokus auf transparente und erklärbare Entscheidungen sowie sorgfältige Dokumentation entlang des gesamten KI-Lebenszyklus. Das NIST AI RMF unterstützt die Definition von Kennzahlen in der Funktion "Messen" und fördert die Rückverfolgbarkeit. In der Summe adressieren diese Ansätze unmittelbar die im Szenario beschriebenen Probleme. (Literatur: B, Kapitel 2.2, 2.5)
D) Falsch. Die reine Verwendung synthetischer Daten stellt nicht sicher, dass Bias gemindert wird, und trägt nicht dazu bei, die wesentlichen Anforderungen zu Transparenz und Risikodokumentation zu erfüllen.

20 / 40
Ein führender Automobilhersteller hat ein hochautomatisiertes Fahrzeug (Stufe 4) entwickelt, das zur Verkehrssicherheit mit KI-gestützter Objekterkennungstechnologie ausgestattet ist. Beim Testen werden folgende Risiken erkannt:

- Bei schlechten Lichtverhältnissen kann das System Bodenschwellen nur eingeschränkt erkennen.
- Das Modell könnte schwer verkäuflich sein, weil es die Abmessungen anderer Fahrzeuge nicht kennt.
- Die Entwickler wissen nicht genau, wie sie die Entscheidungsfindung des Modells erklären sollen.
- In der Entwicklungsphase des KI-Systems wurden nicht alle Interessenträger um ihren Input gebeten.

Was muss adressiert werden, wenn man **ausschließlich** die Konformität (Compliance) mit der KI-VO betrachtet?

A) Das Risiko unzureichender Tests unter Realbedingungen
B) Das Risiko fehlender Transparenz in der KI-Entscheidungsfindung
C) Das Risiko begrenzter Skalierbarkeit des KI-Systems für andere Fahrzeugmodelle
D) Das Risiko der begrenzten Einbindung von Interessenträgern während der KI-Entwicklung

A) Falsch. Die KI-VO legt den Schwerpunkt eher darauf, identifizierte Risiken zu mindern und Transparenz und Grundrechte sicherzustellen, als auf den Umgang mit unzureichenden Tests unter Realbedingungen.
B) Richtig. Artikel 11 KI-VO unterstreicht die Transparenz von KI-Systemen bei der Identifizierung und Beseitigung möglicher Risiken. Das ist das Hauptproblem in diesem Szenario. (Literatur: A, Kapitel 7.10)
C) Falsch. Skalierbarkeit ist zwar aus kommerzieller Sicht entscheidend, adressiert aber nicht unmittelbar die Anforderungen der KI-VO an Risikominderung und Transparenz.
D) Falsch. Die Einbindung von Interessenträgern ist zwar wichtig, steht aber nicht im Fokus der KI-VO.

21 / 40
Ein Logistikunternehmen entwickelt ein KI-System, das Lieferwege optimieren und den Kraftstoffverbrauch senken soll. Das Unternehmen zieht zwei Alternativen in Betracht:

- Ein Closed-Source-KI-Modell eines Anbieters, der eine schnellere Installation und verifizierte Zertifizierung der Konformität (Compliance) garantiert.
- Ein Open-Source-KI-Modell (quelloffenes KI-Modell), das ein hohes Maß an individueller Anpassung und Transparenz ermöglicht.

Das Unternehmen muss die KI-VO einhalten, möchte aber auch ein Gleichgewicht zwischen Innovationen und Kosten herstellen.

Welches Modell passt **am besten** für dieses Unternehmen?

A) Ein Closed-Source-KI-Modell, weil es von Haus aus sicherer ist und bei den Behörden mehr Vertrauen genießt. Nichtkonformität wird dadurch weniger wahrscheinlich.
B) Ein Closed-Source-KI-Modell, weil es vorzertifizierte Konformität (Compliance) bietet. Das Unternehmen ist dann weniger damit belastet, die Konformität mit der KI-VO zu beweisen.
C) Ein Open-Source-KI-Modell, weil es vollkommene Transparenz gewährleistet. Das hilft, die Anforderungen zur Dokumentation und Prüfbarkeit in Audits zu erfüllen.
D) Ein Open-Source-KI-Modell, weil es von der Konformität (Compliance) mit der KI-VO ausgenommen ist. Das liegt daran, dass der Quellcode öffentlich zugänglich ist.

A) Falsch. Closed-Source-Ansätze bieten nicht von Haus aus mehr Konformität oder Sicherheit.
B) Falsch. Closed-Source-Modelle können zwar Konformitätszertifizierungen beinhalten, doch fehlt hier unter Umständen die Flexibilität und Offenheit, die für eine Anpassung an die Bedürfnisse des Unternehmens oder sich ändernde rechtliche Anforderungen erforderlich sind.
C) Richtig. Die vollständige Transparenz, die Open-Source-Modelle bieten, entspricht den Kriterien der KI-VO für Prüfbarkeit in Audits, Rückverfolgbarkeit und Risikokontrolle. Diese Vorteile führen dazu, dass das Logistikunternehmen Konformität (Compliance) leichter nachweisen kann. (Literatur: A, Kapitel 6)
D) Falsch. Die KI-VO entbindet Open-Source-Modelle nicht von Konformitätsanforderungen.

22 / 40
Die KI-VO legt Ethikgrundsätze für die KI-Entwicklung fest.

Was gehört **nicht** zu diesen Grundsätzen?

A) Erklärbarkeit
B) Fairness
C) Schadensverhütung
D) Achtung der KI-Autonomie

A) Falsch. Das ist ein Grundsatz in der KI-VO. Sie schreibt vor, dass KI-Systeme transparent und verständlich sein müssen, damit sichergestellt ist, dass Nutzer und Interessenträger verstehen können, wie Entscheidungen getroffen werden und welche Argumentation dahintersteht.
B) Falsch. Das ist ein Grundsatz in der KI-VO. Sie schreibt vor, dass KI-Systeme so entwickelt und eingesetzt werden sollen, dass sie ohne Bias und Diskriminierung betrieben werden, damit gleiche und gerechte Ergebnisse für alle natürlichen Personen sichergestellt sind.
C) Falsch. Das ist ein Grundsatz in der KI-VO. Sie unterstreicht, wie wichtig es ist, KI-Systeme so zu konzipieren, dass die Risiken minimiert und Schäden verhütet werden. Das gewährleistet Betriebs- und Informationssicherheit für Nutzer und von KI-Technologie betroffene Personen.
D) Richtig. Der richtige Grundsatz ist die Achtung der menschlichen Autonomie. Die KI-VO legt den Fokus primär auf Grundsätze wie Fairness, Schadensverhütung und Erklärbarkeit, die sicherstellen sollen, dass KI-Systeme verantwortungsvoll, transparent und ohne Voreingenommenheit (Bias) entwickelt und verwendet werden. (Literatur: A, Kapitel 9.1)

23 / 40
Ein Start-up-Unternehmen entwickelt ein KI-System zur Unterstützung von personalisiertem Lernen in Schulen mit maßgeschneiderten Lehrplänen, die an die Bedürfnisse der einzelnen Schüler angepasst sind. Das System erfasst Daten zur Leistung und zum Lernverhalten der Schüler.

Was sollte das Start-up-Unternehmen der KI-VO zufolge berücksichtigen, um Innovationen und Regulierung in Einklang zu bringen?

A) Vermeiden, das System als hochriskant zu kennzeichnen, um zusätzliche regulatorische Belastungen zu umgehen und die Innovation zu optimieren
B) Sicherstellen, dass das KI-System eine Konformitätsbewertung durchläuft und die Bestimmungen für Hochrisiko-KI-Systeme erfüllt
C) Robuste Datenschutzfunktionen implementieren, aber Benutzerbenachrichtigungen entfernen, um Verzögerungen bei der Inbetriebnahme zu vermeiden
D) Das System ausschließlich bei Privatschulen in Verkehr bringen, um die Auswirkungen der Konformitätsanforderungen an Hochrisiko-KI-Systeme zu begrenzen

A) Falsch. Eine falsche Kennzeichnung des Systems, um Vorschriften zu umgehen, ist unethisch und kann schwerwiegende rechtliche Konsequenzen haben.
B) Richtig. Die Durchführung einer Konformitätsbewertung und die Sicherstellung der Transparenz sind entscheidend für die Konformität (Compliance) mit den Anforderungen an Hochrisiko-KI-Systeme. (Literatur: A, Kapitel 7.6; KI-VO Artikel 6, Anhang III)
C) Falsch. Benutzerbenachrichtigungen sind unerlässlich für die Transparenz und die Konformität (Compliance) mit den Datenschutzbestimmungen.
D) Falsch. Die Konformität (Compliance) ist bei Privatschulen nicht unbedingt lockerer, und die Bestimmungen müssen eingehalten werden, ganz gleich in welchem Markt das System in Verkehr gebracht wird.

24 / 40
Das Finanzinstitut Fintegra implementiert ein KI-System zur Betrugserkennung in Transaktionen. Für seine Analysen benötigt das System Zugriff auf Transaktionsinformationen von Kunden und demografische Daten. Fintegra muss die Datenminimierungsanforderung der KI-VO einhalten.

Wie kann Fintegra die Anforderung, die Datenerfassung zu minimieren, **am besten** erfüllen?

A) Alle Transaktionsdaten anonymisieren und sämtliche Daten entfernen, die eine natürliche Person identifizieren, um diese Anforderung zu erfüllen, selbst wenn diese Daten unerlässlich für die Betrugserkennung sind

B) Alle personenbezogenen Details erheben, einschließlich des vollständigen Namens und der genauen Adresse, um eine genaue Analyse und Verbesserungen im Laufe der Zeit sicherzustellen, und diese Daten so lange wie nötig sicher speichern

C) Die Datenerfassung auf Transaktionsdaten beschränken, die für die Betrugserkennung relevant sind, und die Verarbeitung personenbezogener Details wie vollständige Namen oder genaue Adressen von Kunden vermeiden

D) Die erfassten Daten nur mit anerkannten Anbietern teilen, die die KI-VO einhalten. Das minimiert die interne Verarbeitung von personenbezogenen Details wie vollständige Namen von Kunden.

A) Falsch. Anonymisierung ist zwar wichtig, aber die Entfernung kritischer Daten, die für die Betrugserkennung benötigt werden, beeinträchtigt die Wirksamkeit des KI-Systems und wird vom Grundsatz der Datenminimierung in der KI-VO nicht verlangt.

B) Falsch. Die Erfassung und Speicherung aller verfügbaren Daten verletzt den Grundsatz der Datenminimierung – selbst wenn dies sicher erfolgt – und erhöht das Risiko der Nichtkonformität mit der KI-VO.

C) Richtig. Der Grundsatz der Datenminimierung in der KI-VO schreibt vor, dass Organisationen nur Daten erfassen und verarbeiten dürfen, die für den besonderen Zweck des KI-Systems unbedingt erforderlich sind. Das Unternehmen erfüllt diese Anforderung, wenn es sich auf Transaktionsdaten konzentriert, die für die Betrugserkennung relevant sind, und unnötige personenbezogene Details vermeidet. (Literatur: A, Kapitel 4.1)

D) Falsch. Das ist keine gute Option, denn gemeinsame Datennutzung mit externen Anbietern könnte gegen Datenschutzbestimmungen verstoßen. Selbst wenn Fintegra und der Anbieter jeweils die KI-VO einhalten, entspricht dies auch nicht dem Grundsatz der Minimierung der Datennutzung.

25 / 40
EduTech implementiert eine adaptive Lernplattform, die KI verwendet, um Lernpfade für Schüler zu personalisieren. Die Plattform passt den Schwierigkeitsgrad von Aufgaben an die individuelle Leistung an.

Welches Risiko sollte EduTech mindern, um eine ethische Verwendung dieses KI-Systems sicherzustellen?

A) Das Risiko von Voreingenommenheit (Bias) und Diskriminierung, weil dies zu unfairen Vor- bzw. Nachteilen für bestimmte Schüler führen würde. Diese Risiko kann EduTech mindern, indem es die Datensätze und Algorithmen des KI-Systems regelmäßig überprüft und aktualisiert.
B) Das Risiko einer übermäßigen Abhängigkeit von der Technologie, die dazu führen könnte, dass Schüler die Fähigkeit zu kritischem Denken nicht entwickeln. Dieses Risiko kann EduTech durch vertrauliche Behandlung des Entscheidungsprozesses des KI-Systems mindern. Das regt Schüler dazu an, mehr zu denken.
C) Das Risiko von Verletzungen der Privatsphäre, weil sensible Schülerdaten einschließlich ihrer Leistungen missbraucht oder offengelegt werden könnten. EduTech kann dieses Risiko mindern, indem es sich stärker auf die Verbesserung der technischen Leistung des KI-Systems konzentriert.
D) Das Risiko von Transparenzproblemen, weil Schüler und Lehrkräfte unter Umständen nicht verstehen, wie Entscheidungen getroffen werden. EduTech kann dieses Risiko mindern, indem es sicherstellt, dass das KI-System ohne menschliche Aufsicht betrieben wird. Das sorgt für Fairness.

A) Richtig. Voreingenommenheit und Diskriminierung sind große Risikos im Bildungsbereich. Die regelmäßige Überprüfung und Aktualisierung von Datensätzen und Algorithmen trägt zur Minderung dieses Risikos bei. (Literatur: A, Kapitel 7.6)
B) Falsch. Transparenz ist entscheidend für ethische KI-Verwendung. Die Förderung kritischen Denkens ist in der Bildung wichtig, hat aber nichts mit der Transparenz von KI-Systemen zu tun.
C) Falsch. Die technische Leistung adressiert für sich genommen keine ethischen Bedenken und verringert auch nicht das Risiko von Verstößen gegen den Schutz der Privatsphäre.
D) Falsch. Entscheidungen ohne menschliches Eingreifen können zwar die Fairness erhöhen, doch fehlende menschliche Aufsicht erhöht das Risiko von Voreingenommenheit und Diskriminierung. Menschliche Aufsicht ist eine wesentliche Voraussetzung für die ethische Verwendung von KI.

26 / 40
Eine Krankenhausabteilung ist auf die Diagnose und Behandlung von Krankheiten spezialisiert. Sie entwickelt ein KI-Diagnosesystem, das bei seltenen Erkrankungen zur Diagnoseassistenz eingesetzt werden soll. Das System analysiert Patientendaten, Vorerkrankungen und Bilddaten.

Das System wurde in den USA erfolgreich eingeführt. Einige medizinische Spezialisten in der Europäischen Union (EU) möchten das System einführen, verstehen jedoch nicht genau, wie es funktioniert. Sie verfügen auch nicht über besondere Fachkenntnisse und Erfahrungen in der Überwachung von KI oder im Erkennen von Störungen oder Fehldiagnosen.

Welches Risiko ist mit der Einführung dieses KI-Systems **nicht** verbunden?

A) Das Risiko fehlender wirksamer menschlicher Aufsicht
B) Das Risiko von Fehldiagnosen aufgrund von Automatisierungsbias
C) Das Risiko von Misstrauen wegen mangelnder Transparenz
D) Das Risiko eines unbefugten Zugriffs auf Patientenakten

A) Falsch. Fehlendes Fachwissen kann dazu führen, dass das Team, das das System verwendet, nicht in der Lage ist, die KI zu überwachen und Störungen oder ungenaue Ausgaben zu erkennen.
B) Falsch. Fehlendes Fachwissen, wie die Ausgaben des Systems richtig zu interpretieren sind, kann zu Bias und Fehldiagnosen führen.
C) Falsch. Die medizinische Spezialisten verstehen nicht, wie das KI-System funktioniert. Das kann zu Misstrauen wegen mangelnder Transparenz führen.
D) Richtig. Datenschutz und unbefugter Zugriff sind zwar wichtige Belange, doch werden sie in diesem Szenario nicht besonders hervorgehoben als Risiken im Zuge der operativen Einführung und des Verständnis dieses KI-Diagnosesystems. (Literatur: A, Kapitel 7.7)

27 / 40
Ein Unternehmen stellt ein KI-System für Smart-Home- Assistenten her. Bei den Tests stellt das Team fest, dass Spracherkennungsfehler wie Verwechslungen ähnlich klingender Wörter zu unbeabsichtigten Handlungen führen. Beispielsweise werden die falschen Hausgeräte eingeschaltet. Diese Fehler können die Privatsphäre verletzen, z.B. Gespräche ohne Einwilligung aufzeichnen oder Benutzer verwechseln, so dass unter Umständen sensible Informationen mit unbefugten Parteien geteilt werden.

Das Unternehmen muss die KI-VO einhalten. Es verwendet dazu das Rahmenwerk CEN/CLC/TR 18115.

Was sollte der KI-Anbieter laut diesem Rahmenwerk tun, um das Problem zu adressieren?

A) Einen Plan zur Einbindung von Interessenträgern erstellen, um unterschiedliche Sichtweisen einzuholen, wie das KI-System funktioniert
B) Eine Ethikfolgenabschätzung durchführen, um die Risiken für die Privatsphäre bei Smart-Home-Assistenten zu verstehen
C) Durch systematische Validierung und Fehlerprüfmethoden die Qualität der Trainingsdaten verbessern
D) Die Datensicherheit durch Verschlüsselung erhöhen, um Sprachdaten zu schützen und Verletzungen des Schutzes personenbezogener Daten zu verhindern

A) Falsch. Die Einbindung von Interessenträgern ist sinnvoll für das Verständnis weitreichenderer Auswirkungen, adressiert aber nicht die technisch unmittelbar erforderliche Verbesserung der Datenqualität.
B) Falsch. Ethikfolgenabschätzungen sind zwar wichtig, lösen aber nicht das Problem schlechter Datenqualität, das diese Fehlinterpretationen verursacht.
C) Richtig. Die Verbesserung der Datenqualität durch systemische Validierung und Fehlerprüfmethoden entspricht dem Rahmenwerk CEN/CLC TR 18115 und sorgt für die nötige Genauigkeit und Vollständigkeit der Daten, um eine sichere und wirksame KI-Systemleistung sicherzustellen. (Literatur: B, Kapitel 1)
D) Falsch. Datensicherheit ist zwar wichtig, doch löst Verschlüsselung nicht das Datenqualitätsproblem, das in diesem Szenario im Mittelpunkt steht.

28 / 40
Bei einem Technologieunternehmen wurde festgestellt, dass es ein KI-System zur biometrischen Echtzeit-Fernidentifizierung verwendet. Die KI-VO verbietet das ausdrücklich.

Welche Sanktion ist für diesen Verstoß angemessen?

A) Eine formelle Verwarnung ohne finanzielle Maßnahme
B) Eine Geldbuße von bis zu 7,5 Mio. € bzw. 1% des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres
C) Eine Geldbuße von bis zu 15 Mio. € bzw. 3% des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres
D) Eine Geldbuße von bis zu 35 Mio. € bzw. 7% des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres

A) Falsch. Eine formelle Verwarnung ohne finanzielle Maßnahme ist bei einer schwerwiegenden Verletzung der KI-Vorschriften nicht angemessen.
B) Falsch. Diese Geldbuße ist zu niedrig für einen Verstoß eines Unternehmen mit verbotenen Handlungen.
C) Falsch. Das ist zwar eine beträchtliche Geldbuße, doch passt sie nicht zur Schwere des betreffenden Verstoßes.
D) Richtig. Diese Sanktion entspricht der maximal möglichen Geldbuße für die schwersten Verstöße gegen die KI-Vorschriften. (Literatur: A, Kapitel 3.11; KI-VO Artikel 52 und Artikel 99)

29 / 40
Die KI-VO betont insbesondere, wie wichtig zwei Aspekte von KI-Systemen sind: Transparenz und Rückverfolgbarkeit.

Warum sind Transparenz und Rückverfolgbarkeit wichtig?

A) Weil sie eine entscheidende Rolle für die Verantwortlichkeit und die Förderung von Vertrauen in KI-Systeme spielen
B) Weil sie verpflichtende Anforderungen an alle Produkte sind, einschließlich KI-Systeme
C) Weil sie besonders wesentlich sind für die Zuverlässigkeit und Automatisierung von KI-Systemen
D) Weil sie jeweils Bestandteil der europäischen, chinesischen und amerikanischen Rechtsvorschriften sind

A) Richtig. Detaillierte Informationen zu den verwendeten Daten helfen, die Entscheidungen und Handlungen eines KI-Systems zu verstehen. Rückverfolgbarkeit gewährleistet, dass die Entscheidungsprozesse, die Datensätze und der Systembetrieb von KI überprüft und Audits unterzogen werden kann. Das ist entscheidend für die Identifizierung von Bias, Fehlern und Verantwortlichkeitsproblemen. Transparenz und Rückverfolgbarkeit sind wichtig für die Verantwortlichkeit und das Vertrauen der Nutzer in KI-Systeme. (Literatur: A, Kapitel 3.1)
B) Falsch. Transparenz und Rückverfolgbarkeit sind zwar wichtig für KI-Systeme, aber nicht für alle Produkte verpflichtend vorgeschrieben.
C) Falsch. Transparenz und Rückverfolgbarkeit sind wichtig für die Verantwortlichkeit und das Vertrauen (nicht die Zuverlässigkeit) der Bürger in der Europäischen Union (EU) und der Nutzer von KI-Systemen und -Technologien. Zuverlässigkeit und Automatisierung beziehen sich eher auf die Leistung und Robustheit von KI-Systemen, nicht unbedingt auf diese beiden Grundsätze.
D) Falsch. Kohärenz und Homogenität zwischen den drei großen KI-Rechtsvorschriften der Welt ist kein Aspekt, der von der Europäischen Union (EU) berücksichtigt wird. Die KI-VO ist eine europäische Verordnung. China und die Vereinigten Staaten haben andere Schwerpunkte und rechtliche Rahmenbedingungen.

30 / 40
Ein Einzelhändler verwendet ein KI-System, das auf der Grundlage von Nutzerpräferenzen und dem verwendeten Gerät automatisch die Darstellung von Elementen auf der Website ändert. Das System empfiehlt Produkte und verbessert das Benutzererlebnis unter Verwendung der Klickhistorie und der auf einer Seite verbrachten Zeit.

In welche Kategorie sollte die Verwendung dieses KI-Systems der KI-VO zufolge eingestuft werden?

A) Unannehmbares Risiko
B) Hochriskant
C) Begrenztes Risiko
D) Minimales oder kein Risiko

A) Falsch. Das System entspricht nicht den Standards für unannehmbares Risiko, die sich auf KI-Systeme beziehen, die Menschenwürde, Sicherheit oder Grundrechte gefährden. Die Beeinflussung von Kaufentscheidungen in einer Einzelhandelsumgebung ist nicht von Haus aus schädlich.
B) Falsch. KI-Systeme in Bereichen wie Gesundheit, Bankwesen oder Beschäftigung, bei denen wesentliche Bedenken zu Rechten und Sicherheit wahrscheinlich sind, werden als hochriskant eingestuft. Die Art und Weise, wie diese Technologie nicht sensible Daten zur Verbesserung von Darstellungen auf einer Website verwendet, erfüllt nicht die Kriterien für Hochrisiko-KI-Systeme.
C) Falsch. Obwohl das System Verbraucherentscheidungen beeinflusst, fällt es angesichts seiner moderaten Auswirkungen und der Verwendung nicht sensibler Daten eher in die Kategorie "Minimales oder kein Risiko".
D) Richtig. Das System verwendet nicht sensible Daten, wird in einem Umfeld betrieben, in dem es nicht um hohe Einsätze geht, und beeinflusst lediglich das Einkaufserlebnis der Nutzer. Daher kann es in die Kategorie "Minimales oder kein Risiko" eingestuft werden. (Literatur: A, Kapitel 3.3, 3.4)

31 / 40
Ein Unternehmen entwickelt ein KI-System für automatisierte Entscheidungen im Personaleinstellungsprozess. Das KI-System wird Lebensläufe sichten, Kandidaten in eine Rangfolge bringen und Empfehlungen für Vorstellungsgespräche geben.

Das Unternehmen macht sich Sorgen, dass dieses KI-System Verzerrungen (Bias) enthalten könnte, die den Einstellungsprozess beeinträchtigen könnten.

Wie kann das Unternehmen Verzerrungen im KI-System **am besten** mindern?

A) Es kann dem KI-System erlauben, ohne menschliches Eingreifen zu lernen und sich anzupassen.
B) Es kann den Bias in den Trainingsdaten ignorieren und sich auf die Leistung des KI-Systems konzentrieren.
C) Es kann für die Erstellung und Überwachung des KI-Systems ein vielfältiges Entwicklungsteam einsetzen.
D) Es kann beim Trainieren des KI-Systems nur eine einzige Datenquelle verwenden, um Kohärenz zu gewährleisten.

A) Falsch. Erlaubt das Unternehmen dem KI-System, ohne menschliches Eingreifen zu lernen, kann dies zu unbeabsichtigtem Bias und mangelnder Verantwortlichkeit führen. (KI-VO Leitlinie 65)
B) Falsch. Ignoriert das Unternehmen Bias, kann dies zu diskriminierenden Ergebnissen führen und der Konformität (Compliance) mit Ethikleitlinien entgegenstehen. Das System muss lernen, Bias zu erkennen und entsprechende Anpassungen vorzunehmen. (KI-VO Leitlinie 72)
C) Richtig. Ein vielfältiges Team kann dazu beitragen, Bias zu identifizieren und zu mindern, um sicherzustellen, dass das KI-System fair und inklusiv ist. (Literatur: A, Kapitel 4.5; KI-VO Leitlinie 81)
D) Falsch. Die Verwendung einer einzigen Datenquelle kann die Verallgemeinerungsfähigkeit des KI-Systems einschränken und Verzerrungen einführen. (KI-VO Leitlinie 73)

32 / 40
Feline Finesse ist ein Webshop, der Katzenaccessoires und -kissen verkauft, einschließlich personalisierter Katzenplüschtiere basierend auf Bildern der Kunden. Der Webshop verwendet ein KI-System, das folgende Funktionen bietet:

- Es ändert Preise dynamisch in Abhängigkeit von Verbraucheraktivitäten.
- Es ordnet Suchergebnisse in einer Rangfolge an, die auf Kundenpräferenzen beruht.
- Es gibt persönliche Empfehlungen für andere Produkte, von denen es meint, dass sie dem Kunden gefallen.

Derzeit macht der Webshop Kunden darauf aufmerksam, was das KI-System macht, und zeigt sehr transparent, wie der Algorithmus funktioniert. Die CEO hinterfragt diese Praktik jedoch und will wissen, welcher Transparenzgrad erforderlich ist und wie er sich auf den Umsatz auswirkt.

Was sollte die CEO zum Thema Transparenz im Sinne der KI-VO wissen?

A) Transparenz kann Verbrauchern beweisen, dass das System objektiv ist. Die KI-VO räumt Verbrauchern das Recht ein zu verstehen, wie ihre Daten verwendet werden, und dieses Verständnis ist vertrauensfördernd.
B) Transparenz kann die Grenzen oder Einschränkungen des KI-Systems aufzeigen. Die Verbraucher könnten das Vertrauen in das Unternehmen verlieren, wenn sie das verstehen. Dies wiederum würde der Reputation des Unternehmens schaden.
C) Transparenz ist im E-Commerce nicht vorgeschrieben. Die bequeme Personalisierung ist hilfreich für die Verbraucher. Sie müssen weder wissen noch verstehen, wie das KI-System funktioniert.
D) Transparenz beschränkt sich darauf, den Quellcode des KI-Systems zur Verfügung zu stellen. Das Vertrauen der Verbraucher in das System könnte schwinden, wenn sie verstehen, wie der Algorithmus genau funktioniert.

A) Richtig. Transparenz ist ein wesentliches Element der KI-VO und beeinflusst das Vertrauen der Öffentlichkeit maßgeblich. (Literatur: A, Kapitel 3.6)
B) Falsch. Die Offenlegung von Einschränkungen ist zwar Teil der Transparenz, soll das Vertrauen jedoch nicht mindern. Vielmehr soll dadurch Vertrauen aufgebaut werden, indem Verantwortlichkeit und realistische Erwartungen gewährleistet sind.
C) Falsch. Bequemlichkeit ist für die meisten Verbraucher zwar angenehm, doch ist Transparenz in der KI-VO rechtlich vorgeschrieben. Ethische KI-Methoden werden den Verbrauchern zunehmend bewusst, und sie machen sich deswegen Sorgen. Transparenz fördert daher das Vertrauen in das System.
D) Falsch. Transparenz ist nicht auf die Veröffentlichung des Quellcodes beschränkt. Sie beinhaltet auch eine klare Beschreibung der Richtlinien für den Betrieb des KI-Systems, der Datennutzung und der Entscheidungsfindung. Davon hängt ab, ob Vertrauen aufgebaut und Verantwortung gewährleistet wird.

33 / 40
In einem Personaleinstellungsprozess wird ein Hochrisiko-KI-System verwendet, das automatisch Kandidaten anhand ihrer Qualifikation herausfiltert. Der Betreiber des Systems hat jedoch keinen Mechanismus für menschliches Eingreifen oder menschliche Aufsicht implementiert für Fälle, in denen fragwürdige Entscheidungen getroffen werden.

Ist der KI-VO zufolge bei diesem System menschliche Aufsicht erforderlich?

A) Ja, weil menschliche Aufsicht erforderlich ist, um in Entscheidungsprozesse eingreifen zu können.
B) Ja, weil menschliche Aufsicht die Konformität (Compliance) mit Fairness- und Transparenzpflichten sicherstellt.
C) Nein, weil automatisierte Systeme so konzipiert sind, dass sie ohne menschliches Eingreifen funktionieren.
D) Nein, weil Personaleinstellungsprozesse keine kritischen Sicherheitsrisiken für natürliche Personen beinhalten.

A) Richtig. Die KI-VO betont, wie wichtig menschliche Aufsicht bei Hochrisiko-KI-Systemen ist. Dadurch soll sichergestellt werden, dass es einen Mechanismus für menschliches Eingriffen gibt, insbesondere in Szenarien, in denen Entscheidungen fragwürdig sein oder wesentliche Auswirkungen auf natürliche Personen haben könnten. (Literatur: A, Kapitel 10.2.3)
B) Falsch. Fairness und Transparenz sind zwar wichtige Aspekte der KI-VO, doch ist menschliche Aufsicht nur bei Systemen mit begrenztem oder hohem Risiko erforderlich.
C) Falsch. Die KI-VO betont, wie wichtig menschliche Aufsicht bei Hochrisiko-KI-Systemen ist. Dadurch soll sichergestellt werden, dass es einen Mechanismus für menschliche Eingriffe gibt, insbesondere in Szenarien, in denen Entscheidungen fragwürdig sein oder wesentliche Auswirkungen auf natürliche Personen haben könnten.
D) Falsch. Personaleinstellung ist zwar nicht mit Sicherheitsrisiken verbunden, doch die KI-VO berücksichtigt die ethischen und gesellschaftlichen Auswirkungen von KI-Systemen. Menschliche Aufsicht ist erforderlich, um Bedenken hinsichtlich Fairness und Transparenz zu adressieren. Das sind kritische Aspekte im Personaleinstellungsprozess.

34 / 40
Ein Unternehmen bereitet die Einführung eines KI-Modells mit allgemeinem Verwendungszweck vor. Das Modell kann angepasst werden, um Aufgaben wie Kundenservice-Automatisierung, Inhaltserstellung und Datenanalyse zu erfüllen. Das Unternehmen hat seinen Sitz außerhalb der Europäischen Union (EU), will das Modell aber in mehreren EU-Mitgliedstaaten in Verkehr bringen.

Welche Voraussetzung muss laut KI-VO **nicht** erfüllt sein, bevor das KI-Modell mit allgemeinem Verwendungszweck in der EU in Verkehr gebracht werden kann?

A) Benennung eines in der EU niedergelassenen Bevollmächtigten, der Aufgaben im Bereich Konformität (Compliance) übernimmt
B) Einhaltung des EU-Urheberrechts, um das Modell mit urheberrechtlich geschützten Daten zu trainieren
C) Durchführung eines gründlichen Audits, um die vollständige Konformität (Compliance) mit allen EU-Gesetzen und -Verordnungen zu verifizieren
D) Veröffentlichung einer detaillierten Zusammenfassung der Inhalte, die verwendet werden, um das Modell mit allgemeinem Verwendungszweck zu trainieren

A) Falsch. Alle Anbieter, die in Drittländern niedergelassen sind, müssen einen in der EU niedergelassenen Bevollmächtigten benennen, der Aufgaben im Bereich Konformität (Compliance) übernimmt. (KI-VO Artikel 54)
B) Falsch. Auch wenn bei KI-Modellen mit allgemeinem Verwendungszweck keine vollständige Konformitätsbewertung erforderlich ist, müssen sie dennoch die Vorschriften des EU-Urheberrechts erfüllen. Dadurch soll sichergestellt werden, dass beim Training verwendete geschützte Inhalte die rechtlichen Anforderungen einhalten. (KI-VO Artikel 53 Abs. 1 Buchst. c)
C) Richtig. Eine vollständige Konformitätsbewertung ist nur bei Hochrisiko-KI-Systemen erforderlich. KI-Modelle mit allgemeinem Verwendungszweck fallen nicht in diese Kategorie. Daher muss das Unternehmen keine vollständige Konformitätsbewertung durchführen. (Literatur: A, Kapitel 3)
D) Falsch. Laut KI-VO muss eine Zusammenfassung der für das Training des KI-Modells verwendeten Daten veröffentlicht werden. (KI-VO Artikel 53)

35 / 40
Ein Unternehmen betreibt ein KI-System für vorausschauende Wartung (Predictive Maintenance) von Industrieanlagen. Nachdem das System einige Monate in Betrieb ist, generiert es eine sehr hohe Anzahl von Fehlalarmen, was die Arbeitsabläufe stört. Eine Untersuchung führt zu folgenden Feststellungen:

- Die Organisation hat die dynamischen Veränderungen in der Produktionsumgebung nicht berücksichtigt.
- Die Organisation hat kein formelles Verfahren für die Neubewertung von Risiken nach der Inbetriebnahme.

Die Organisation muss die Anforderungen der KI-VO erfüllen. Zur Lösung dieser Probleme verwendet sie die Norm ISO/IEC 23894.

Was sollte die Organisation laut dieser Norm tun, um diese Probleme zu adressieren?

A) Einen menschenzentrierten Design-Workshop abhalten, um die Benutzerfreundlichkeit des Systems zu verbessern
B) Einen Risikomanagementprozess mit laufender Bewertung und Überwachung konzipieren
C) Ein Audit im Bereich Cybersicherheit durchführen, um mögliche Sicherheitslücken zu identifizieren und zu adressieren
D) Das KI-System durch ein einfacheres, regelbasiertes Modell ersetzen, das leichter zu kontrollieren ist

A) Falsch. Eine menschenzentriertes Design verbessert zwar die Benutzerfreundlichkeit, geht jedoch nicht die Problemursache an: fehlendes dynamisches und anpassungsfähiges Risikomanagement für in Betrieb genommene KI-Systeme.
B) Richtig. ISO/IEC 23894 unterstreicht, wie wichtig es ist, dynamisches, kontinuierliches Risikomanagement entlang des gesamten KI-Lebenszyklus zu integrieren, auch nach der Inbetriebnahme. Eine Neubewertung hätte das System anpassen können, bevor die hohe Anzahl von Fehlalarmen generiert wurde. (Literatur: B, Kapitel 3.2, 3.4)
C) Falsch. Die Cybersicherheit ist wohl kaum die Ursache für die Fehlalarme. Diese Lösung berücksichtigt weder das Risikomanagement entlang des gesamten Lebenszyklus noch die Notwendigkeit einer kontinuierlichen Neubewertung des KI-Systems.
D) Falsch. Wird das System ersetzt, wird nicht berücksichtigt, dass ISO/IEC 23894 den Fokus auf die iterative Behandlung und Neubewertung von Risiken legt, nicht auf die Stilllegung der Technologie.

36 / 40
Ein Flottenmanagement-Unternehmen verwendet ein KI-System, um das Verhalten der Fahrer zu verfolgen und Wartungsanforderungen vorherzusagen. Das System erfasst und verarbeitet umfangreiche Datenmengen wie GPS-Standorte, Fahrmuster und Leistungskennzahlen der Fahrzeuge. Bei einem Audit wurde vor kurzem festgestellt, dass das Unternehmen nicht genügend Datenschutzverfahren eingeführt hat.

Laut KI-VO sind Datenmanagement und Schutz der Privatsphäre für dieses Unternehmen unerlässlich.

Warum sind diese Aspekte so wichtig?

A) Weil das Unternehmen dadurch Geschäftsziele und operative Effizienz priorisieren kann
B) Weil dies das Vertrauen der Nutzer verbessert, personenbezogene Daten schützt und unbefugtem Zugriff vorbeugt
C) Weil das verpflichtend vorgeschrieben ist und die Einhaltung der KI-VO rechtliche Probleme und mögliche Geldbußen vermeidet
D) Weil dadurch die Datenerfassungsverfahren gestrafft werden, da die Einwilligung der Nutzer nicht mehr erforderlich ist

A) Falsch. Die Umsetzung von Datenmanagement und der Schutz der Privatsphäre sollen das Unternehmen nicht dabei unterstützen, Effizienz gegenüber Konformität (Compliance) zu priorisieren.
B) Richtig. Die KI-VO betont den Schutz der Privatsphäre natürlicher Personen und ethisches Datenmanagement, was einen genauen und fairen Betrieb von KI-Systemen unterstützt. (Literatur: A, Kapitel 4.3, 4.4, 4.6)
C) Falsch. Konformität (Compliance) ist zwar wichtig, doch legt die KI-VO den Schwerpunkt auf den Schutz der Rechte natürlicher Personen und die Einhaltung von Ethiknormen.
D) Falsch. Die KI-VO und andere relevante Datenschutzverordnungen verlangen die Einwilligung der Nutzer und Datenschutz. Diese Anforderungen zu umgehen ist rechtswidrig und unethisch.

37 / 40
Welche Verwendung eines KI-Systems passt zur Einordnung als System mit begrenztem Risiko im Sinne der KI-VO?

A) Ein Chatbot, der Kunden bei allgemeinen Anfragen behilflich sein soll und so programmiert ist, dass offengelegt wird, dass es sich hier um KI handelt
B) Ein Gesichtserkennungssystem, das zur Echtzeit-Identifizierung von Kunden in öffentlichen Räumen wie Einkaufszentren verwendet wird
C) Ein medizinisches Diagnose-Tool, das Ärzten dabei hilft, auf der Grundlage von Patientendaten Behandlungsempfehlungen zu geben
D) Ein KI-System, das ein autonomes Fahrzeug betreibt, welches ohne menschliche Aufsicht auf öffentlichen Straßen fährt

A) Richtig. Die KI-VO klassifiziert KI-Systeme, die mit Nutzern interagieren, aber Rechte, Sicherheit oder rechtliche Pflichten nicht wesentlich beeinflussen können, als Systeme mit begrenztem Risiko. Diese Systeme müssen Transparenzpflichten erfüllen – beispielsweise Nutzer davon in Kenntnis setzen, dass sie mit einem KI-System interagieren. (Literatur: A, Kapitel 3.3)
B) Falsch. Je nachdem, welche Entscheidungen nach der Identifizierung getroffen werden, fällt dieses System wegen seiner Auswirkungen auf die Privatsphäre und der Überwachung entweder in die Kategorie "hochriskant" oder könnte sogar verboten sein.
C) Falsch. Dieses Tool gehört in die Kategorie der Hochrisiko-KI-Anwendungen, weil das KI-System Gesundheits- und Sicherheitsdaten verarbeitet.
D) Falsch. Aufgrund von Sicherheitsbedenken und der Auswirkungen möglicher Unfälle werden autonome Fahrzeuge als hochriskant eingestuft.

38 / 40
Ein Unternehmen entwickelt ein KI-System für den Bildungsbereich. Das KI-System wird festlegen, ob ein Schüler Zugang zu Materialien erhält, in eine Schule aufgenommen bzw. einer Klasse zugewiesen wird. Bereitgestellt wird das KI-System über Cloud-Dienste.

In welche Kategorie sollte die Verwendung dieses KI-Systems laut KI-VO eingestuft werden?

A) Unannehmbares Risiko
B) Hochriskant
C) Begrenztes Risiko
D) Minimales oder kein Risiko

A) Falsch. KI-Systeme, die große Auswirkungen auf natürliche Personen haben können, z.B. deren Zugang zu Bildung bestimmen können, werden in der KI-VO nicht als verboten, sondern als hochriskant eingestuft, weil ihr Einsatz strengen Anforderungen unterliegt, aber nicht direkt untersagt ist.
B) Richtig. KI-Systeme, die bestimmungsgemäß zur Feststellung des Zugangs zur Bildung verwendet werden sollen, sind als Hochrisiko-KI-Systeme einzustufen, weil sie große Auswirkungen auf natürliche Personen haben. Die KI beeinflusst unmittelbar, ob Schüler Zugang zu Bildungsressourcen erhalten oder aufgenommen werden. Das wirkt sich auf ihre Grundrechte aus. (Literatur: A, Kapitel 3.3, 3.4; KI-VO Artikel 6 (Anhang III))
C) Falsch. Zu KI-Systemen mit begrenztem Risiko gehören KI-gestützte Chatbots, Empfehlungssysteme oder KI-Assistenten, die keine kritischen Entscheidungen über die Rechte oder Chancen natürlicher Personen treffen oder natürliche Personen vom Zugang zu Bildung ausschließen können. Bei dem System in diesem Szenario ist von einem hohen Risiko auszugehen.
D) Falsch. Eine Einstufung als System mit geringem Risiko spiegelt die möglichen Risiken, die mit dieser Art von KI-System verbunden sind, nicht zutreffend wider. Das System in diesem Szenario kann natürliche Personen vom Zugang zur Bildung ausschließen, was für die Betroffenen schwerwiegende Konsequenzen hätte.

39 / 40
Ein Unternehmen hat ein KI-System für automatisierte Personaleinstellung entwickelt. In den Tests gelangt das Team zu folgenden Feststellungen:

- Das System gibt Kandidaten mit bestimmten ethnischen Hintergründen durchwegs niedrigere Wertungen, weil die Trainingsdaten demografische Verzerrungen (Bias) enthalten.
- Derzeit existiert weder ein internes Überprüfungsverfahren noch ein Mechanismus, um das Feedback relevanter Parteien einzuholen, die auf das Risiko dieses konkreten Bias hätten hinweisen können.

Das Unternehmen muss die KI-VO einhalten. Um diese Probleme zu lösen, verwendet es die Norm ISO/IEC TR 24368.

Was sollte das Unternehmen laut dieser Norm tun, um diese Probleme zu lösen?

A) Einen synthetischen Datensatz erstellen, um die demografischen Ungleichgewichte zu adressieren und die Fairness zu verbessern
B) Transparenz umsetzen, um die Erklärbarkeit und Verantwortlichkeit des Systems zu erhöhen
C) Die Datenverschlüsselungspraktiken stärken und Zugriffskontrollen verwenden, um Verstöße zu verhindern
D) Ein Ethikrahmenwerk mit Input von Interessenträger verwenden, um die Menschenrechtsthemen zu bewerten

A) Falsch. Für sich genommen mindert die Verwendung synthetischer Daten Verzerrungen nicht und adressiert auch nicht die wesentlichen Anforderungen in Bezug auf ethische KI-Entwicklung. Darüber hinaus ist sie nicht Bestandteil der genannten Norm ISO/IEC TR 24368.
B) Falsch. Transparenz adressiert nicht unmittelbar die Fairness, ethische Überprüfungsprozesse oder die Einbindung von Interessenträgern in der verlangten Form. Die relevante Lösung für diese Probleme ist die Umsetzung eines Ethikprüfungsverfahrens.
C) Falsch. Datenverschlüsselung und Zugriffskontrollen sind zwar entscheidend für die Gewährleistung von Informationssicherheit, für das vorliegende Problem jedoch nicht relevant. Ein angemessenerer Fokus wäre die Umsetzung eines Ethikprüfungsverfahrens.
D) Richtig. ISO/IEC TR 24368 unterstreicht, wie wichtig Ethikrahmenwerke, Menschenrechtspraktiken, die Einbindung von Interessenträgern und Fairness in der KI-Entwicklung sind. Die Einrichtung eines Ethikprüfungsverfahrens hilft, Diskriminierung zu erkennen und zu mindern, und ist im Einklang mit den wesentlichen Grundsätzen der Norm. (Literatur: B, Kapitel 4.2, 4.3)

40 / 40
Ein KI-Start-up-Unternehmen entwickelt ein KI-Modell mit allgemeinem Verwendungszweck, das mit öffentlich verfügbaren Online-Inhalten trainiert wird, einschließlich Presseartikeln, Forschungsberichten und Social-Media-Beiträgen. Nach der Einführung erhält das Unternehmen ein Anwaltsschreiben von einer Autorengruppe, in dem ihm vorgeworfen wird, das geistige Eigentum der Gruppe ohne entsprechende Genehmigung verwendet zu haben, um das Modell zu trainieren.

Was sollte getan werden, um die geistigen Eigentumsrechte in diesem Fall zu schützen?

A) Das Unternehmen sollte argumentieren, dass das KI-Modell mit allgemeinem Verwendungszweck als quelloffen einzustufen ist und daher von den Verpflichtungen zur Einhaltung des Urheberrechts befreit ist.
B) Das Unternehmen sollte sich auf angemessene Verwendung (Fair Use) im Sinne der KI-VO berufen, da die Inhalte öffentlich verfügbar waren, und sollte den Datensatz weiterhin verwenden.
C) Das Unternehmen sollte die KI-generierten Ergebnisse löschen, die Ähnlichkeiten mit den strittigen Werken aufweisen, um Ansprüche wegen Urheberrechtsverletzung zu vermeiden.
D) Das Unternehmen sollte Einzelheiten zum Trainingsdatensatz des KI-Modells mit allgemeinem Verwendungszweck einschließlich der Herkunft dokumentieren und teilen, um Konformität (Compliance) sicherzustellen.

A) Falsch. Quelloffene KI-Modelle sind nicht automatisch von der Einhaltung von Urheberrechten befreit, wenn sie systemische Risiken bergen oder monetarisiert werden.
B) Falsch. Die KI-VO erlaubt keine Fair-Use-Ausnahmen. Öffentlich verfügbare Inhalte könnten immer noch urheberrechtlich geschützt sein.
C) Falsch. Die KI-VO schreibt nicht vor, dass KI-generierte Inhalte gelöscht werden müssen, nur weil Ähnlichkeiten zu urheberrechtlich geschützten Werken bestehen.
D) Richtig. Gemäß Artikel 53 KI-VO müssen Anbieter das Trainingsverfahren dokumentieren und dabei auch detaillierte Informationen zur Herkunft und den Merkmalen der Daten liefern. (Literatur: A, Kapitel 3)

Beurteilung

Die richtigen Antworten auf die Fragen in dieser Musterprüfung finden Sie in nachstehender Tabelle.

Frage	Antwort	Frage	Antwort
1	B	**21**	C
2	B	**22**	D
3	A	**23**	B
4	A	**24**	C
5	D	**25**	A
6	C	**26**	D
7	A	**27**	C
8	A	**28**	D
9	C	**29**	A
10	A	**30**	D
11	D	**31**	C
12	B	**32**	A
13	A	**33**	A
14	B	**34**	C
15	A	**35**	B
16	B	**36**	B
17	A	**37**	A
18	D	**38**	B
19	C	**39**	D
20	B	**40**	D

Certified for what's next

Kontakt EXIN

www.exin.com