ADVISORI

AI Act in the Making

DAS EU KI GESETZ UND DIE ARBEIT DER FACHGRUPPE ARTIFICIAL INTELLIGENCE

ISACA Germany Chapter EXPERTS TOGETHER

21. März 2024

Über uns

Über uns

Nora Haberkorn

M.Sc. Risikomanagement

Advisori FTC GmbH, Audit & Compliance
Consultant für IT-Audits, IT-Compliance
reg. GAP-Analysen und Softwareeinführungen

Eric Vogel

M.Sc. Physik

Advisori FTC GmbH, Data Driven Products & KI
Consultant für Datengetriebene
Produktentwicklung und KI

Die Fachgruppe Artificial Intelligence

Status

- Januar 2024 gegründet
- 4 Mitglieder (ab Mai laden wir Interessenten ein)

Aktueller Fokus

- Evaluierungsphase der rechtlichen Rahmenbedingungen und Planung der Ausrichtung der Fachgruppe

Fachgruppenseite

https://www.isaca.de/ueber-uns/fachgruppen-1/fachgruppe-artificial-intelligence.html

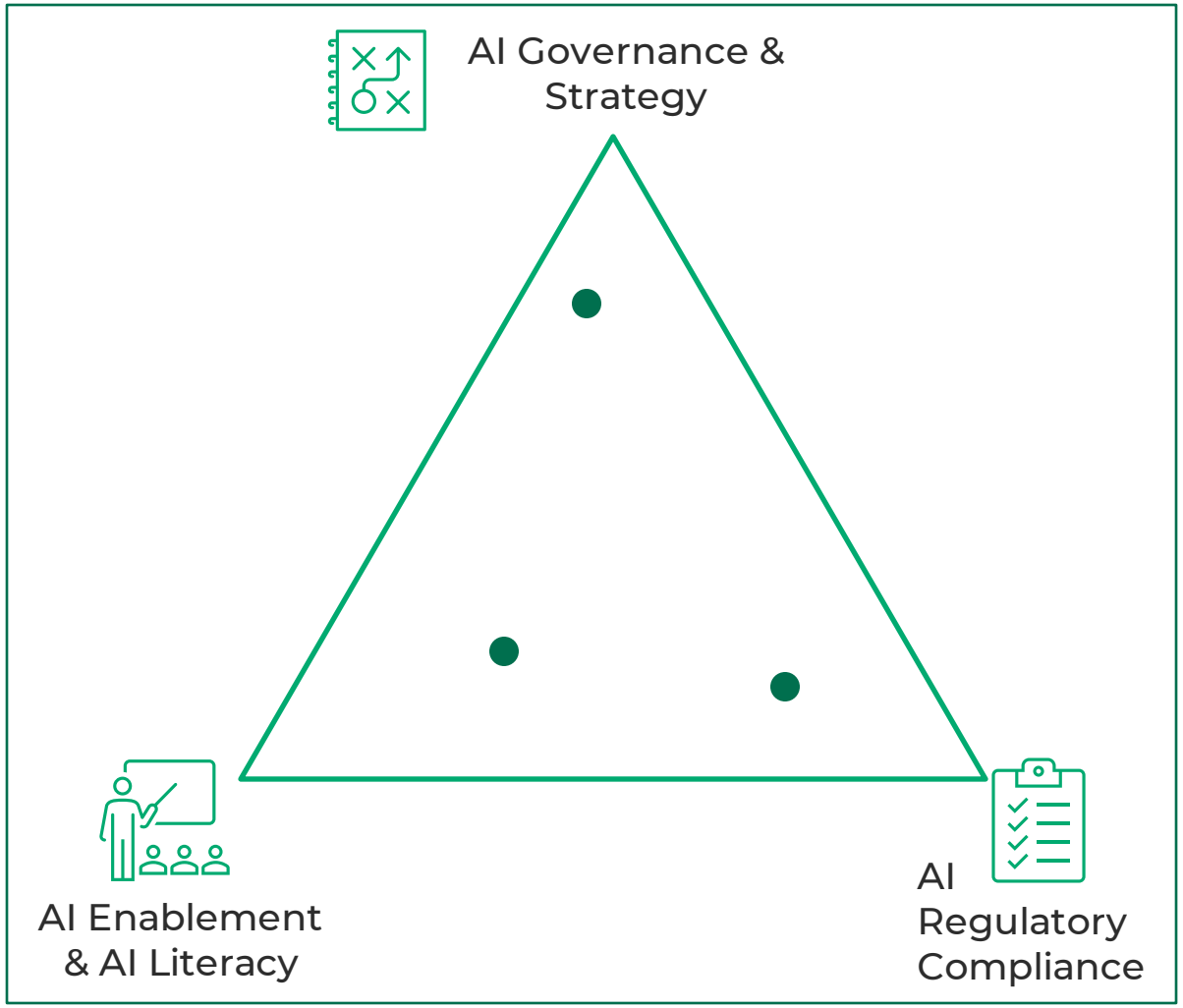
Die Fachgruppe Artificial Intelligence

Vermittelt zwischen

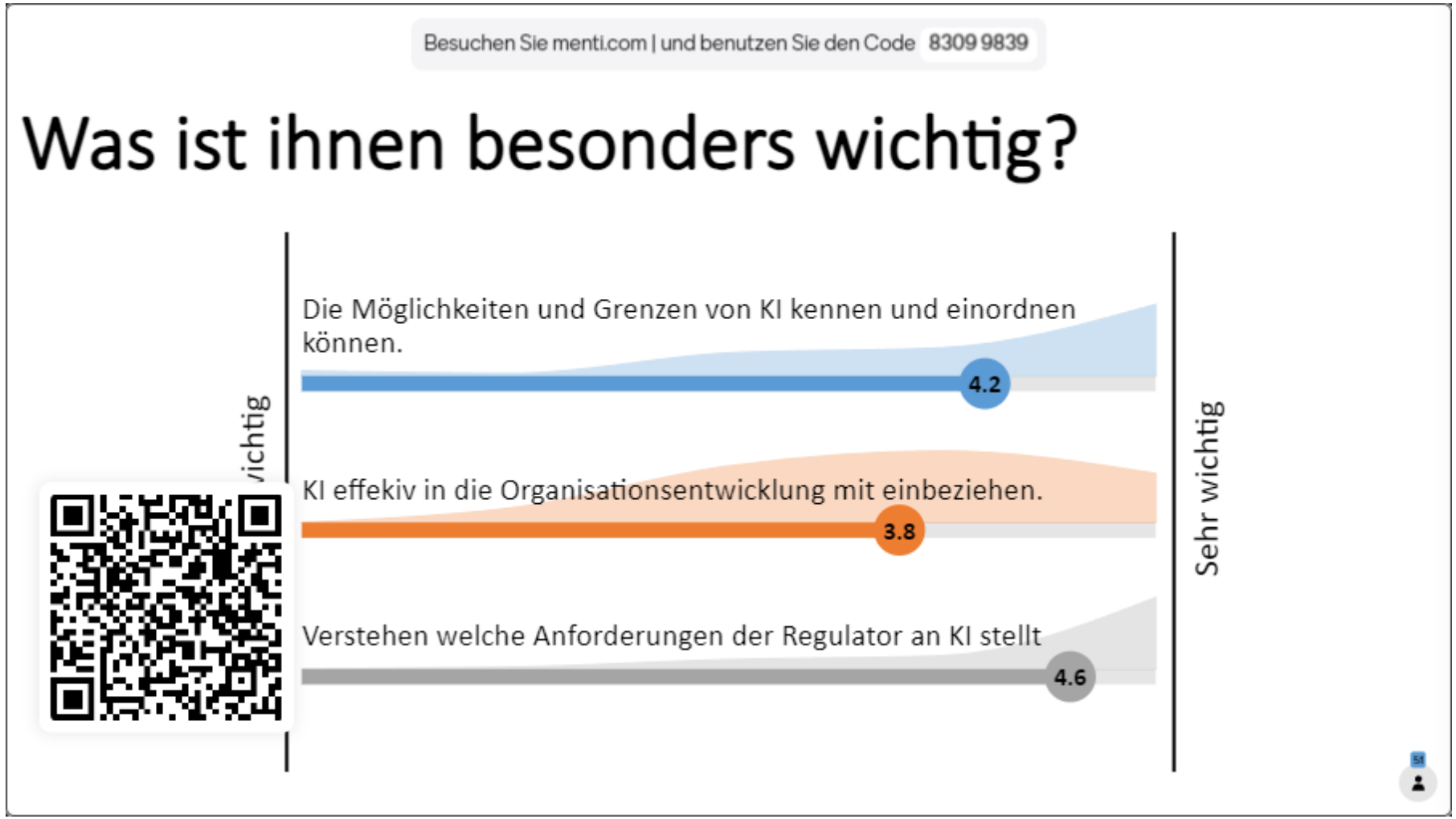
- Den Bereichen Technik, Governance und Compliance von KI Systemen

Fokussiert sich auf

- Fach- und Führungskräfte befähigen KI zu nutzen und zu bewerten (AI Enablement & Literacy
- Bewertung und Einordnung regulatorischer Vorgaben
- Integration von KI in die Organisations-Governance und Strategie



Wo stehen sie



AI Act in the Making

Was macht KI eigentlich besonders?

KI erlaubt mehr Autonomie + Komplexität

Daten → Frage + KI → Handlung

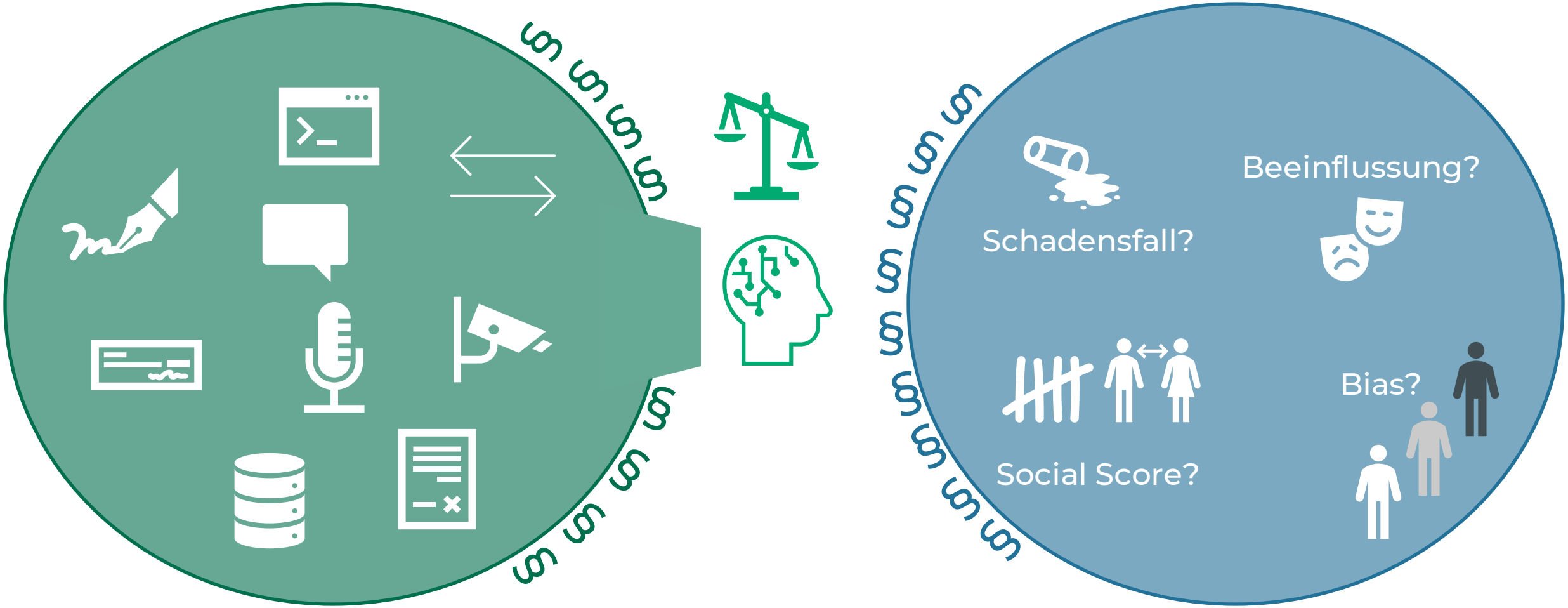
ISACA Germany Chapter EXPERTS TOGETHER

KI erlaubt mehr Autonomie + Komplexität

Daten → Frage + KI → Handlung

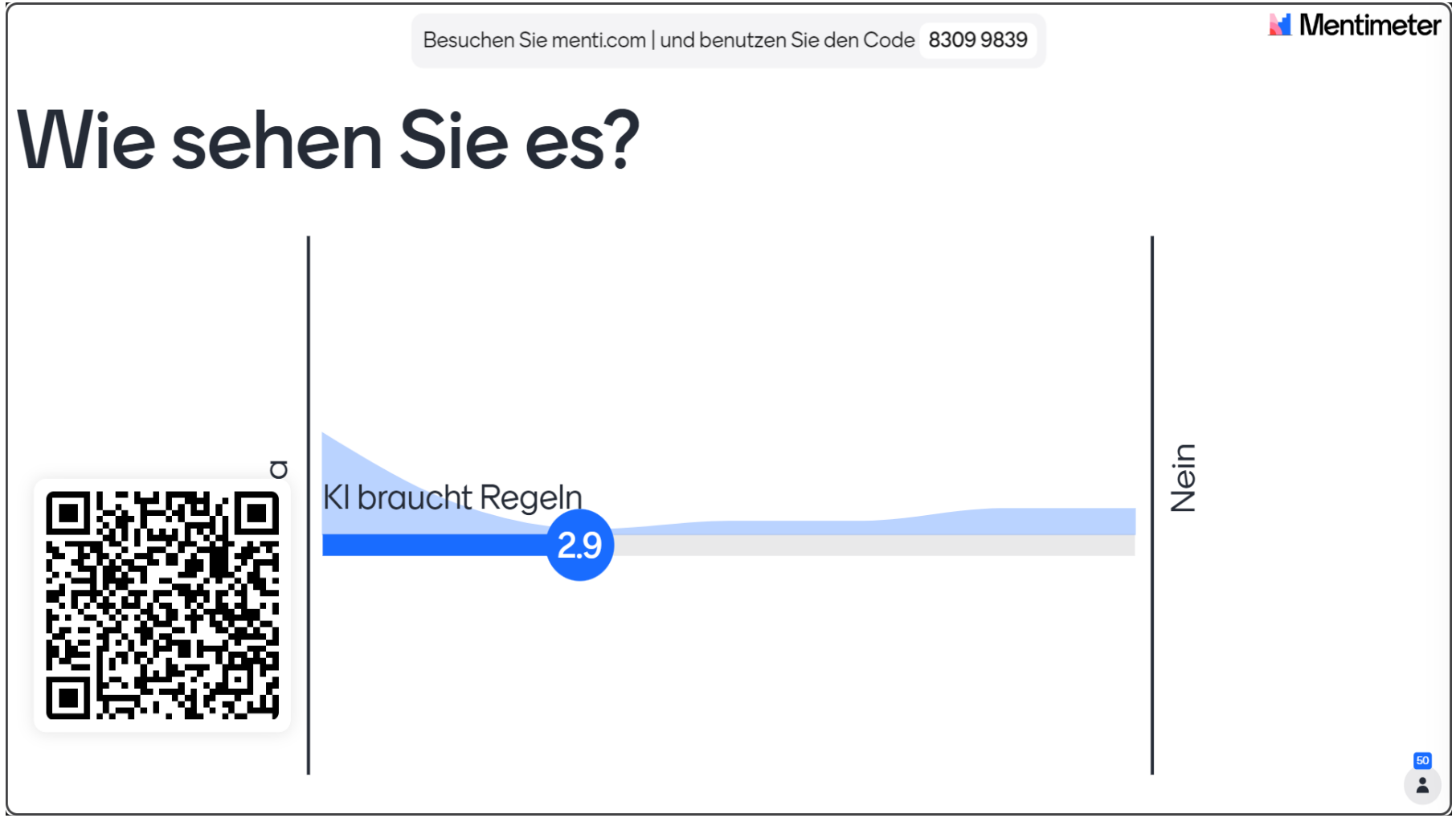
ISACA Germany Chapter EXPERTS TOGETHER

KI braucht Regeln



ISACA Germany Chapter EXPERTS TOGETHER

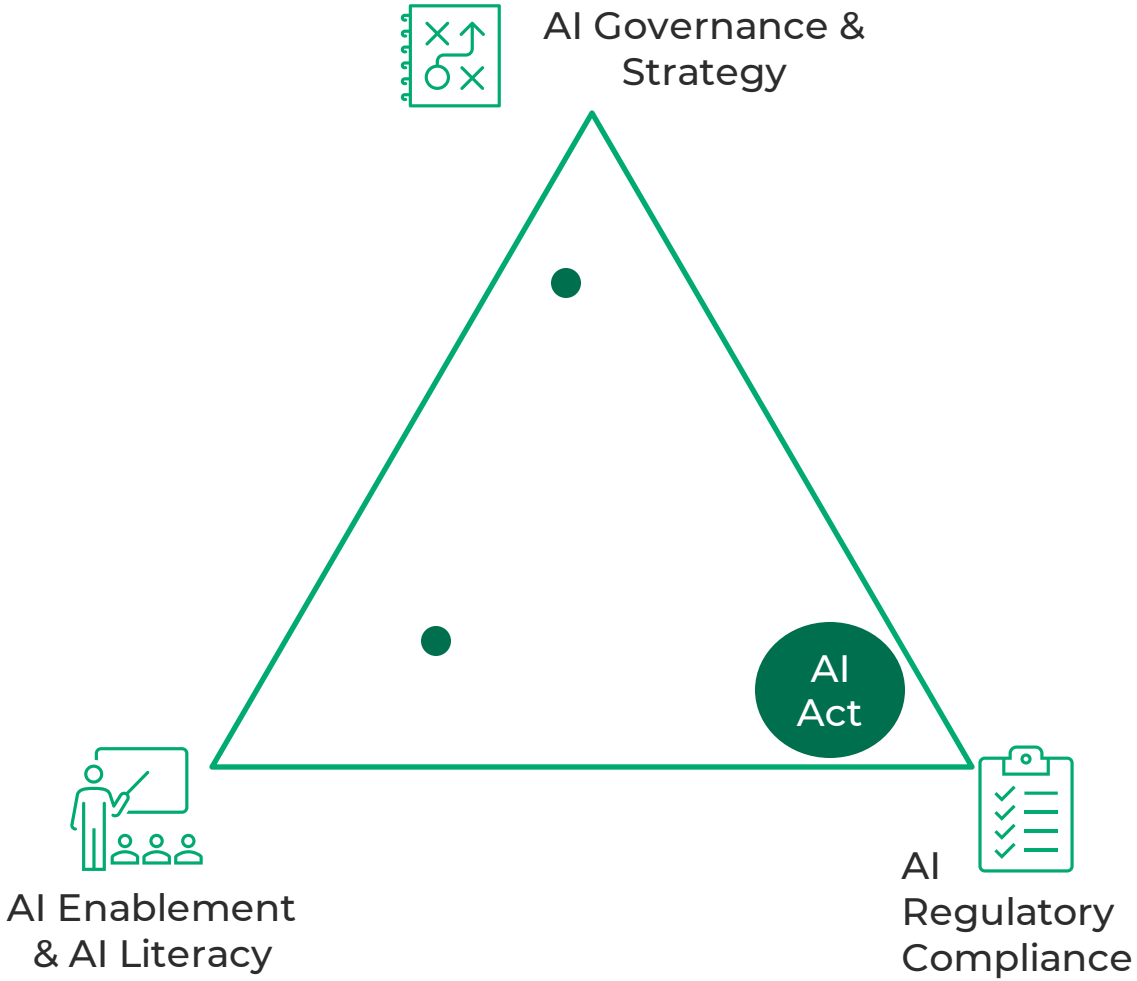
Wo stehen sie



ISACA Germany Chapter

Der AI Act in 60 Sekunden

Die Fachgruppe Artificial Intelligence



ISACA Germany Chapter EXPERTS TOGETHER

AI Act in the Making

Der AI Act in 60 Sekunden

Verbote: Von schädlichen KI-Praktiken.

Risikostufen: Klassifizierung von KI-Systemen basierend auf Risiko.

Harmonisierte Regeln: Für Markteintritt und Betrieb.

Transparenz und Verantwortlichkeit: Für KI-Anbieter und Nutzer.

Unterstützt Innovation: Durch regulatorische Experimentierräume.

Strenge Strafen: Bei Nichteinhaltung.

Timeline AI Act: Bald ist es so weit...

April 2021

EU Kommission schlägt KI Gesetz vor

Juni 2021

Erste Lesung im Parlament

November 2022

chatGPT ist verfügbar

Dezember 2023

Finale Version des Entwurfs wird angenommen

Februar 2024

Das AI-Office startet

März 2024

EU-Parlament nimmt KI-Verordnungs-Entwurf an

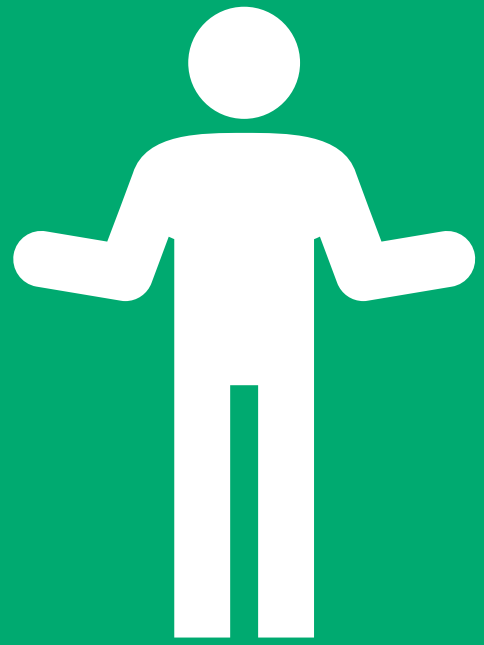
Der AI Act in mehr als 60 Sekunden

Der AI Act im Detail

- Risikokategorien & Hochrisikosysteme
- General Purpose AI Systeme
- Auflagen und Transparenzregeln
- Strafen und Support
- Woran wir arbeiten

ISACA Germany Chapter EXPERTS TOGETHER

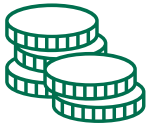
Wen betrifft es?



Wer ist vom AI Act betroffen

- Anbieter, Importeure, Vertreiber und Nicht-EU-Vertreter von KI-Systemen

kommerzielle Nutzer



Ja

- KMU, Start-ups
- Anbieter von allgemeiner KI, Open-Source-KI
- Wissenschaftliche Einrichtungen

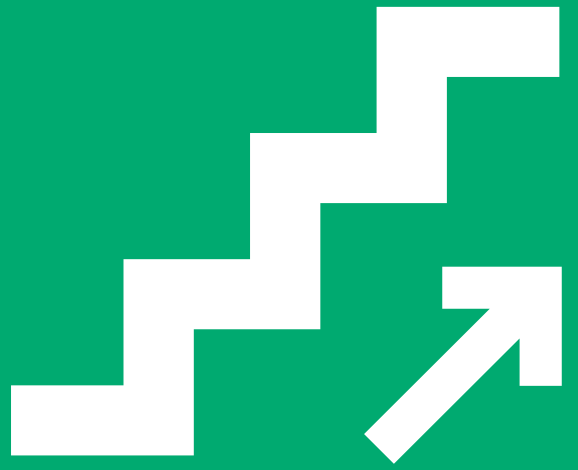
Teilweise

- Allgemeine Öffentlichkeit
- persönlicher KI-Gebrauch
- nationale Sicherheit/Militär

Nein

ISACA Germany Chapter EXPERTS TOGETHER

Risikokategorien & Hochrisikosysteme



EU AI Act: Risikokategorien

Inakzeptables Risiko: Verbotene KI-Praktiken

Verbotene KI-Praktiken

Manipulative oder ausbeuterische KI-Systeme

- Einsatz unterschwelliger Techniken zur Verhaltensverzerrung.
- Ausbeutung von Alters-, physischen oder psychischen Schwächen.

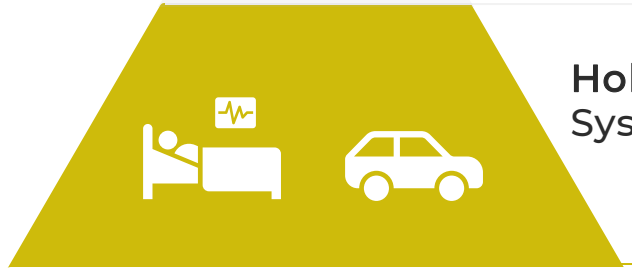
Echtzeit-Biometrieerkennung in öffentlichen Räumen

- Streng limitierter Einsatz gegen Massenüberwachung.
- Ausnahmen für Sicherheit, Vermisstenfälle und schwere Verbrechen mit richterlicher Kontrolle.

Sozialbewertung durch Regierungen und Biometrische Kategorisierung

- Missbrauch biometrischer Daten zur Analyse sensibler Merkmale.
- KI-Bewertung der Vertrauenswürdigkeit nach sozialem Verhalten mit rechtlichen Folgen.

EU AI Act: Risikokategorien



Hohes Risiko: Umfangreiche Auflagen an KI-Systeme und Betreiber

Das Sind Hochriskosysteme

Annex II: EU Harmonisierungsgesetzgebung

- Annex II listet EU Harmonisierungsgesetzgebungen auf
- KI-System ist Produkt oder Sicherheitskomponente eines Produkts
- Konformitätsbewertung durch dritte Partei gefordert
- Z.B.
  - Elektronische und Funkausrüstung
  - Transport und Fahrzeuge
  - Persönliche und öffentliche Sicherheit

Annex III: AI Act Liste

- KI-System ist im Annex III aufgeführt:
- Biometrische Anwendungen
- Management kritischer Infrastrukturen
- Beschäftigung & Mitarbeitermanagement
- Werkzeuge für Strafverfolgungsbehörden
- Migration & Grenzkontrolle

Muss das sein?

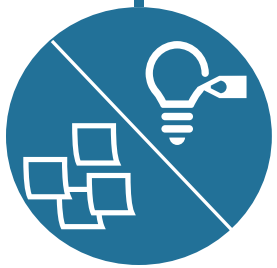
Ausnahmen

Ein System ist doch kein Risikosystem wenn die KI…

- enge prozedurale Tasks löst.
- das Ergebnis früherer menschlicher Aktivitäten verbessert.
- vorbereitende Aufgaben für relevante Bewertungen ausführt.
- Entscheidungsmuster erkennt ohne menschliche Bewertung zu ersetzen.

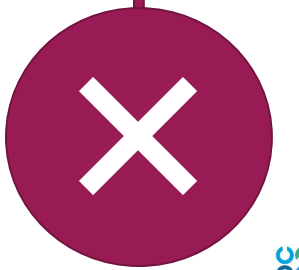
Anbieter Pflichten

- Bewertung dokumentieren vor Markteinführung.
- Registrierung gemäß Artikel 51(1a).
- Dokumentation auf Behördenanfrage bereitstellen.

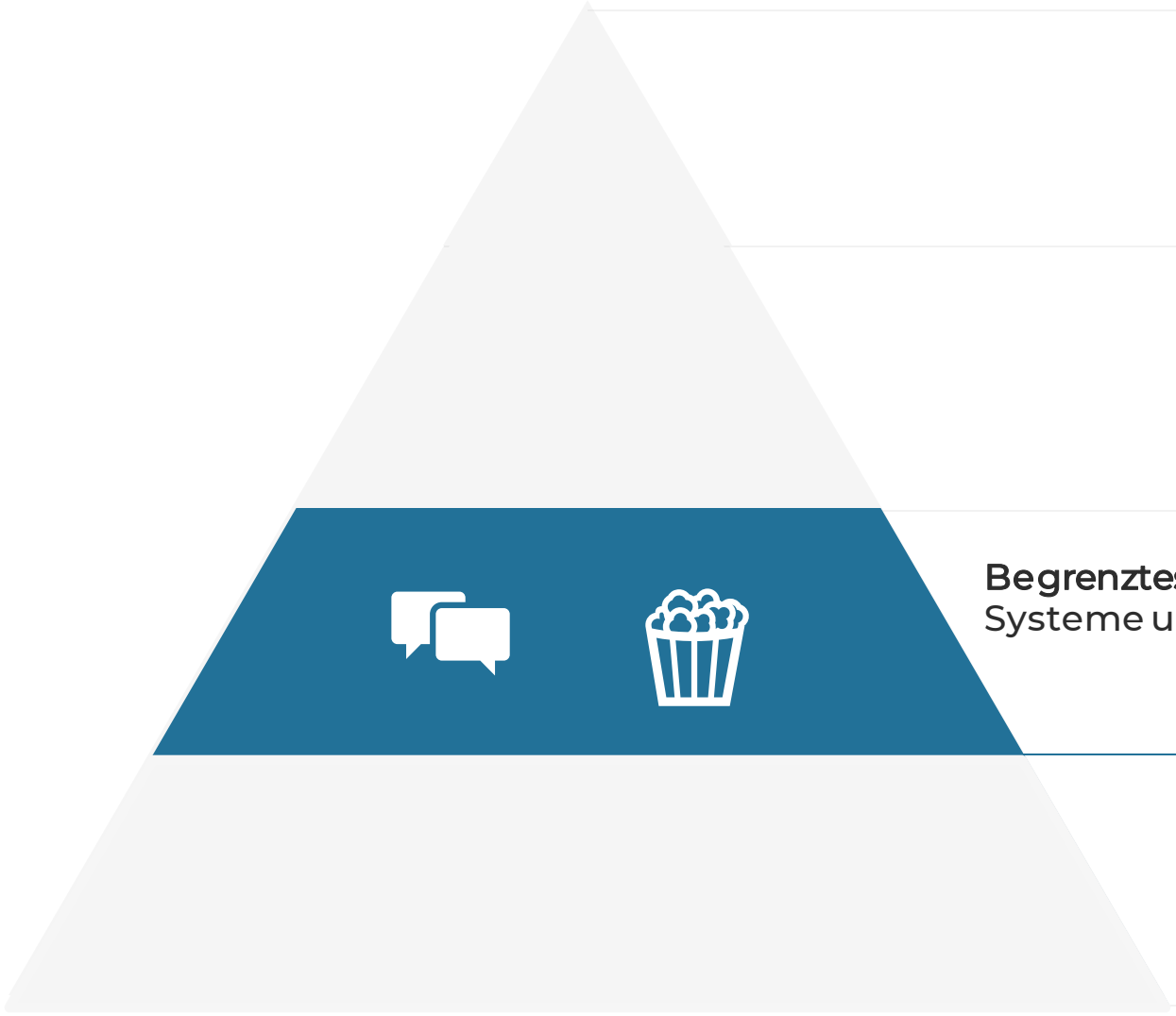


Keine Ausnahme für

- Bei KI-Systemen, die Profiling natürlicher Personen durchführen.



EU AI Act: Risikokategorien



Begrenztes Risiko: Transparenzauflagen für KI-Systeme und Betreiber

ISACA Germany Chapter EXPERTS TOGETHER

Begrenztes Risiko: Transparenzregeln

KI-Transparenz: Mensch-KI-Interaktion -> Offenlegung erforderlich

Kennzeichnung von KI-Inhalten: Synthetische Medien markieren

Emotions- und biometrische KI: Informationspflicht und Datenschutz

Deepfake-Offenlegung: Kennzeichnung erforderlich

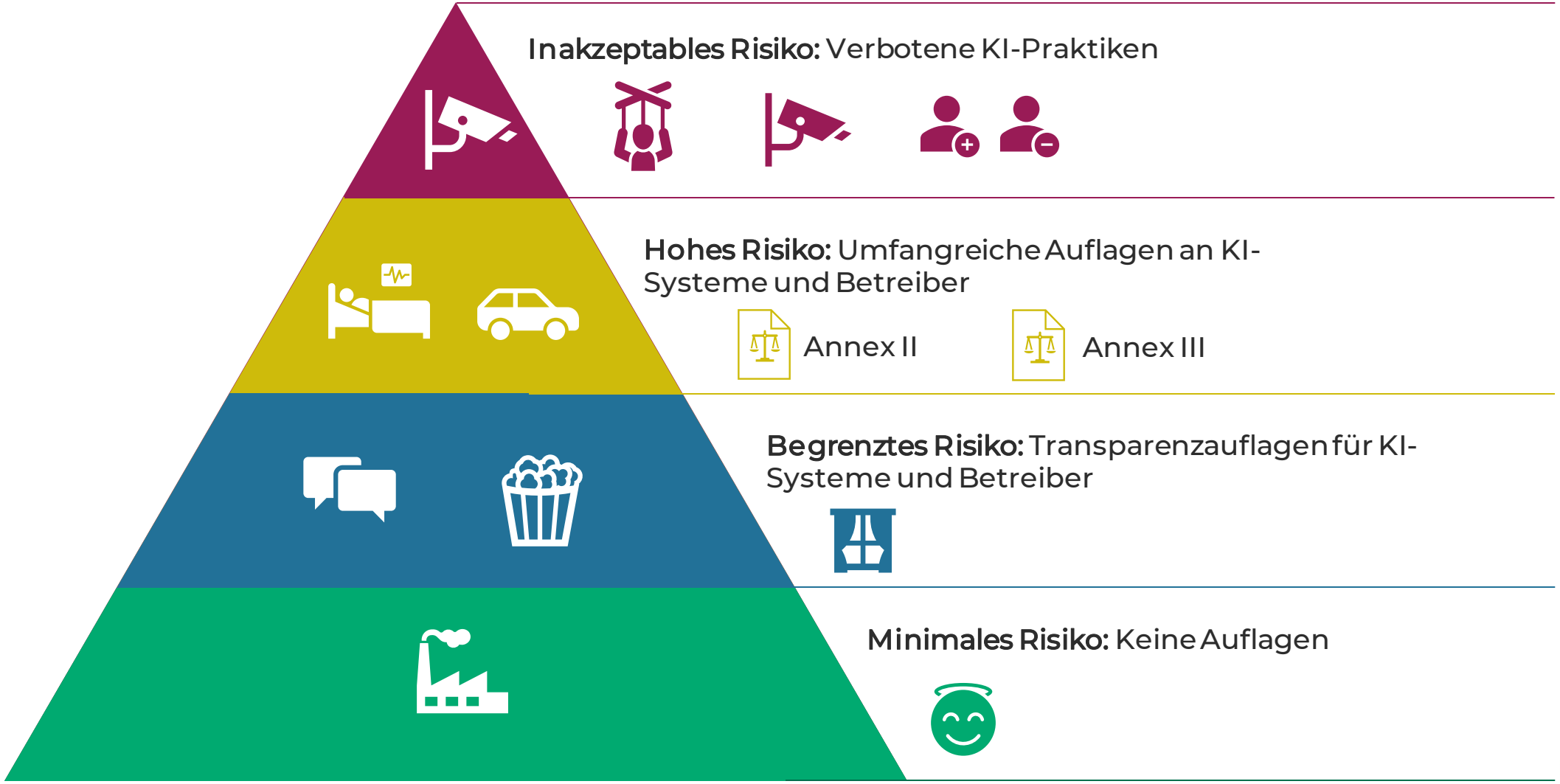
Offenlegung von KI-Texten: Bei öffentlichem Interesse offenlegen

Informationszeitpunkt: Klar und zugänglich bei Erstkontakt.

Zusätzliche Transparenzregeln: Ergänzung bestehender Gesetze und Förderung von Verhaltenskodizes.

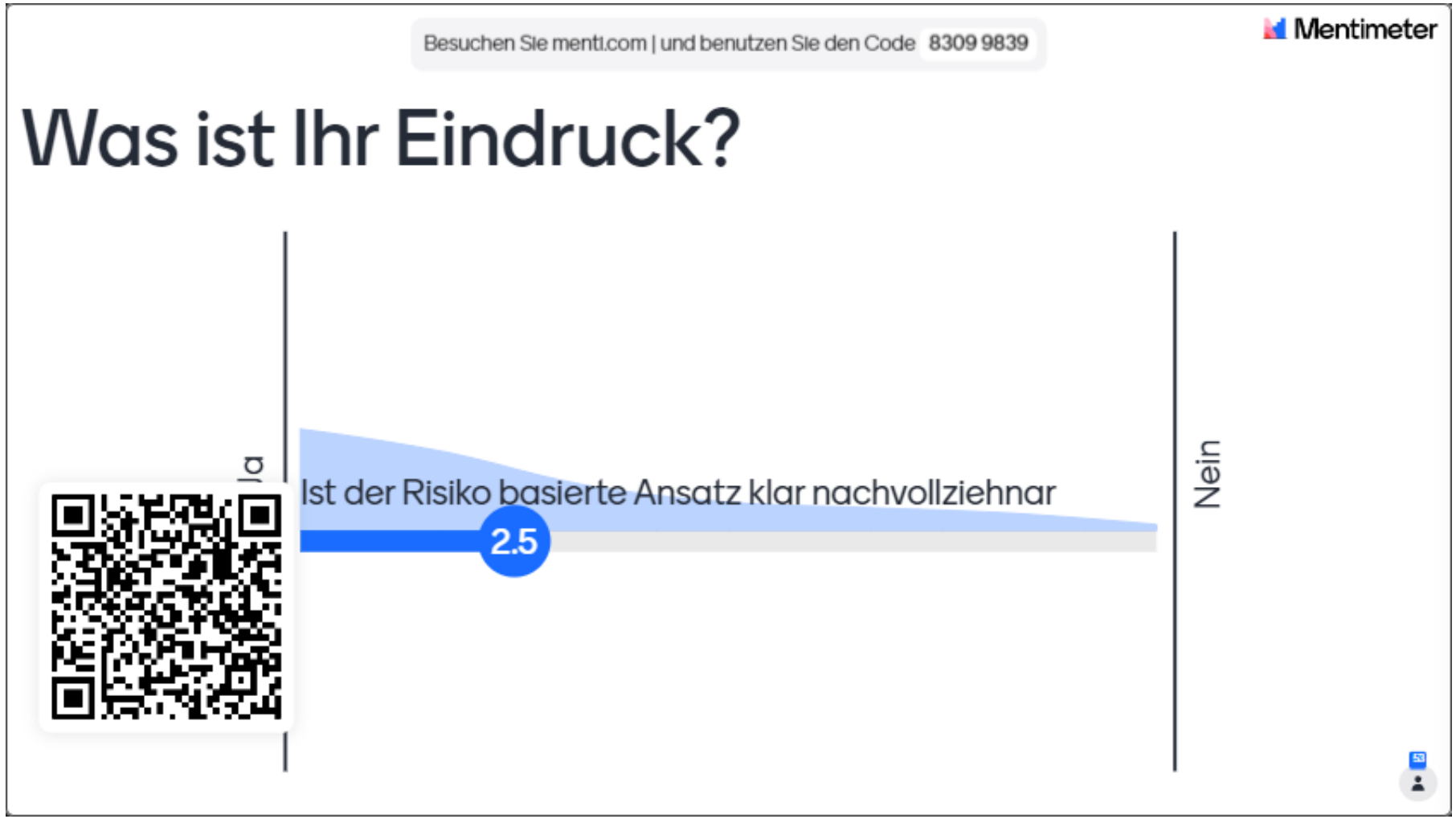
ISACA Germany Chapter EXPERTS TOGETHER

EU AI Act: Risikokategorien



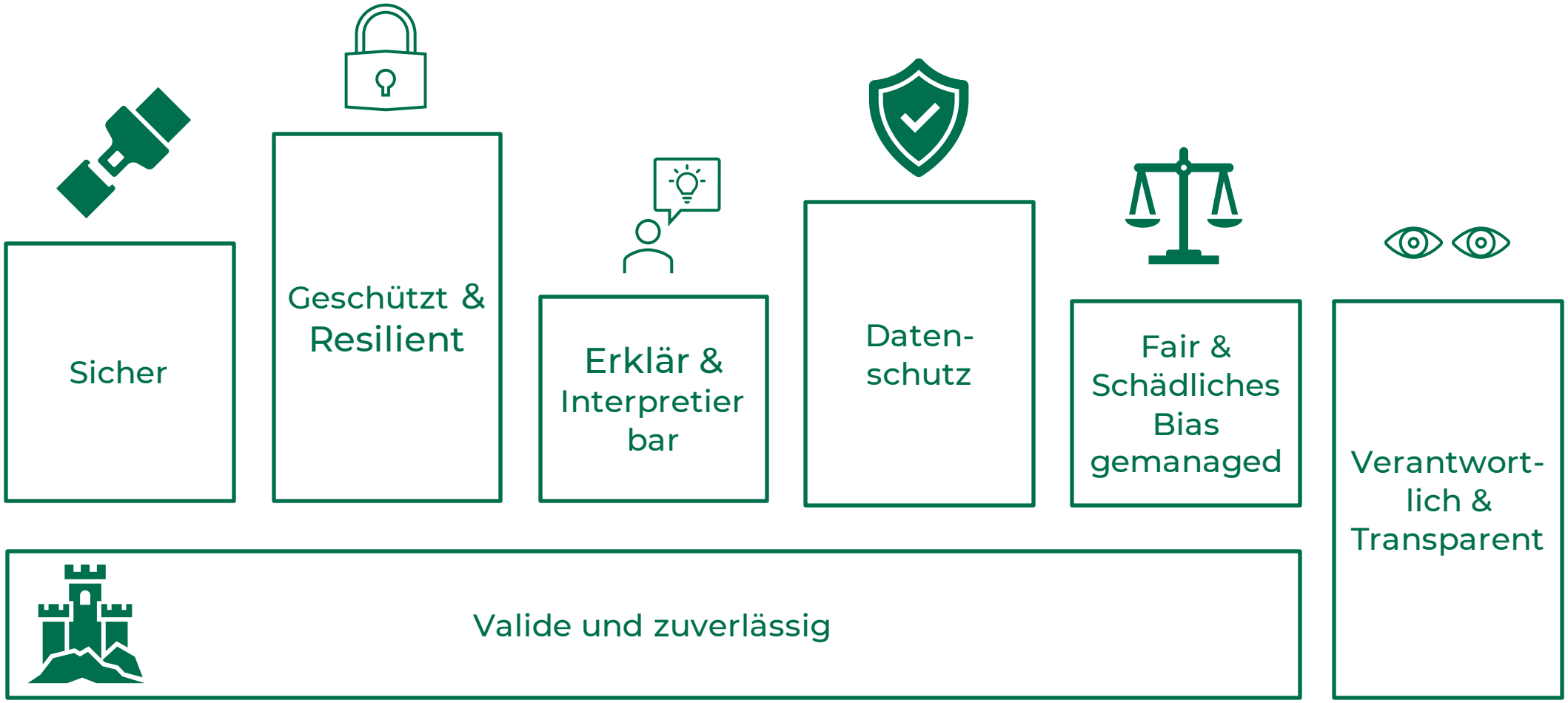
ISACA Germany Chapter EXPERTS TOGETHER

Und Sie?


Besuchen Sie menti.com | und benutzen Sie den Code 8309 9839
Mentimeter
Was ist Ihr Eindruck?
Ja
Ist der Risiko basierte Ansatz klar nachvollziehnar
2.5
Nein

Auflagen für KI-Systeme im Detail

Einschub: Vertrauenswürdige KI



Auflagen für KI-Syteme im Detail

Hochrisiko KI: Systemanforderungen

- Datenverwaltung und -qualität
- Technische Dokumentation
- Datenschutz und -sicherheit
- Transparenz & Informationsbereitstellung
- Robustheit und Genauigkeit
- Menschliche Aufsicht
- Cybersicherheitsmaßnahmen

- **Technische Dokumentation:** Vor Markteinführung erstellen und aktuell halten, mit Details gemäß Anhang IV.
- **Vereinfachung für KMUs:** Möglichkeit der vereinfachten Dokumentation für kleine und mittlere Unternehmen.

Automatisches Logging: Hochrisiko-KI-Systeme müssen Ereignisse lebenslang automatisch aufzeichnen.
Log-Inhalte: Nutzungsdauer, Datenbankabgleiche, Ergebnisse und Nutzeridentifikation.

Möglichkeit zur effektiven Überwachung durch Menschen zur Risikominimierung.

ISACA Germany Chapter EXPERTS TOGETHER

Hochrisiko KI: Organisatorische Anforderungen

Risikomanagementsystem: Kontinuierlicher Prozess über den gesamten Lebenszyklus des KI-Systems.

Qualitätsmanagementsystem: Dokumentiertes System zur Einhaltung der regulatorischen Anforderungen.

Marktüberwachung nach Markteinführung: Aktive Datenerfassung und -analyse zur fortlaufenden Überwachung.

Konformitätsbewertung: Nachweis, dass das KI-System vor Markteinführung den Anforderungen entspricht.

Registrierungspflichten: Registrierung in der EU-Datenbank vor Markteinführung.

Korrekturmaßnahmen: Pflicht zur Ergreifung notwendiger Maßnahmen bei Nichteinhaltung.

- Strategie für regulatorische Konformität
- Nachweis, dass Anforderungen eingehalten werden

- Interner Kontrollverfahren (Anhang VI).
- Qualitätsmanagement- und technische Dokumentationsbewertung durch eine benannte Stelle (Anhang VII).

Und Sie?

Besuchen Sie menti.com | und benutzen Sie den Code **8309 9839**

Welche Herausforderungen sehen Sie hier für Unternehmen?

34 antworten

Oraganisatorische Hürden

Hoher Aufwand für Unternehmen

Welche Anforderungen richten sich an Anwender und welche an Anbieter?

Aufbau eines Managementsystems

Umsetzung der Governance, insb. Dokumentationspflichten

technisches Verständnis

Konformität nachweisen

Trade off zwischen den Anfirderungen entscheiden und dokumentieren

inition.

Nutzung von KI in der Unternehmung

Risiken erkennen

Governance und laufende

> Fehlendes Know-How /

Zusammenfassung der Ergbenisse

1.Organisatorische und Management-Herausforderungen:

1. Aufbau eines effektiven Managementsystems für KI-Anwendungen.
2. Implementierung und Überwachung von Governance-Strukturen, einschließlich Dokumentationspflichten.
3. Klärung und Zuweisung von Zuständigkeiten innerhalb der Organisation.
4. Integration von KI in klassische betriebliche Funktionen.

2.Technisches und Fachwissen:

1. Fehlendes Know-How und Vorerfahrungen im Umgang mit KI.
2. Notwendigkeit technischen Verständnisses und fachlicher Kompetenzen.
3. Verständnis der Systemlogik und Nachvollziehbarkeit von KI-Entscheidungen.
4. Umgang mit der Unschärfe von KI-Definitionen.

3.Compliance und Risikomanagement:

1. Sicherstellung der Konformität mit regulatorischen Vorgaben.
2. Risikomanagement und Fehlervermeidung.
3. Verhältnis von Kosten und Nutzen, Qualitätssicherung.

4.Datenschutz und Sicherheit:

1. Wahrung der Vertraulichkeit von Unternehmensdaten.
2. Einhaltung von Datenschutzbestimmungen.

5.Mitarbeiterentwicklung und Kultur:

1. Weiterbildung und Sensibilisierung von Mitarbeitern und Führungskräften.
2. Schaffung einer unterstützenden Unternehmenskultur.
3. Bewältigung von Herausforderungen bei der Mitarbeiterakzeptanz und -beteiligung.

6.Ethische und soziale Aspekte:

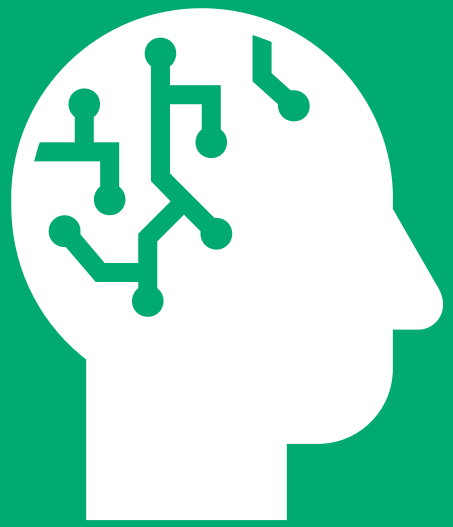
1. Ethische Herausforderungen im Zusammenhang mit dem Einsatz von KI.
2. Umgang mit potenziellem Missbrauch von KI-Systemen wie ChatGPT.

7.Praktische Umsetzungsherausforderungen:

1. Hoher Aufwand und Ressourcenbedarf für die Umsetzung.
2. Balance zwischen Time-to-market und Compliance-Anforderungen.
3. Umgang mit unklaren Anforderungen an Anwender und Anbieter.
4. Nutzung von KI-Technologien bei gleichzeitiger Begrenzung.

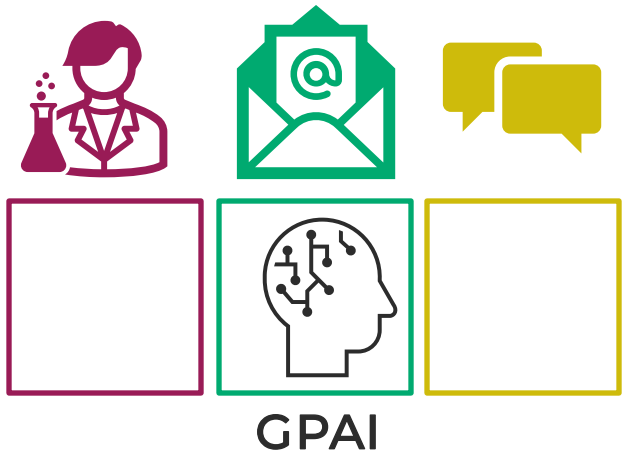
ISACA Germany Chapter EXPERTS TOGETHER

General Purpose AI Systeme

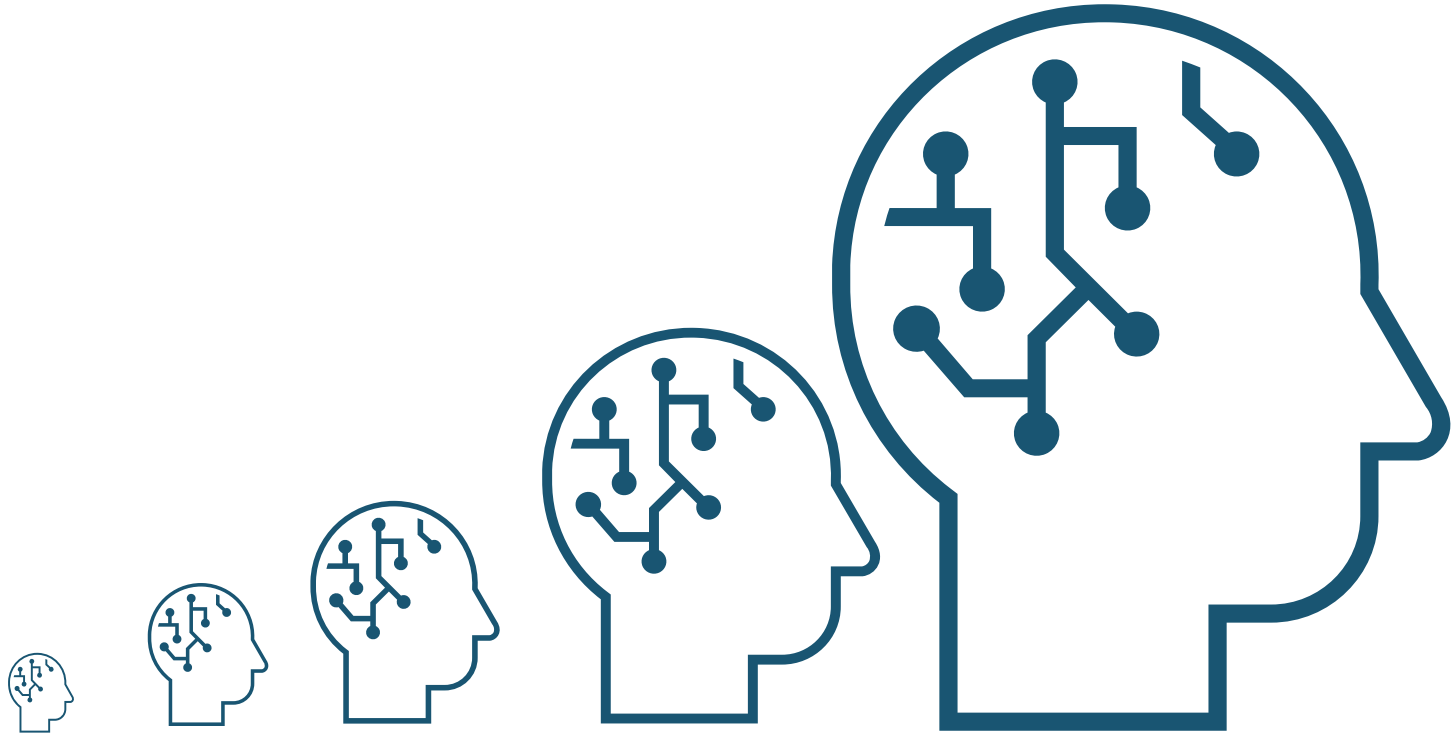


Was ist ein General Purpose AI System

- GPAI Systeme basieren auf GPAI Modellen
- Hohe Allgemeinheit und Vielseitigkeit
- Fähigkeit, diverse Aufgaben kompetent zu erfüllen
- Integration in verschiedene Anwendungssysteme möglich



Was ist Systemisches Risiko



10.000.000.000.000.000.000.000.000

State-of-the-Art KI Hardware
20*10^15 (2024)

High-End Hardware
(Grafikkarte) 100*10^12

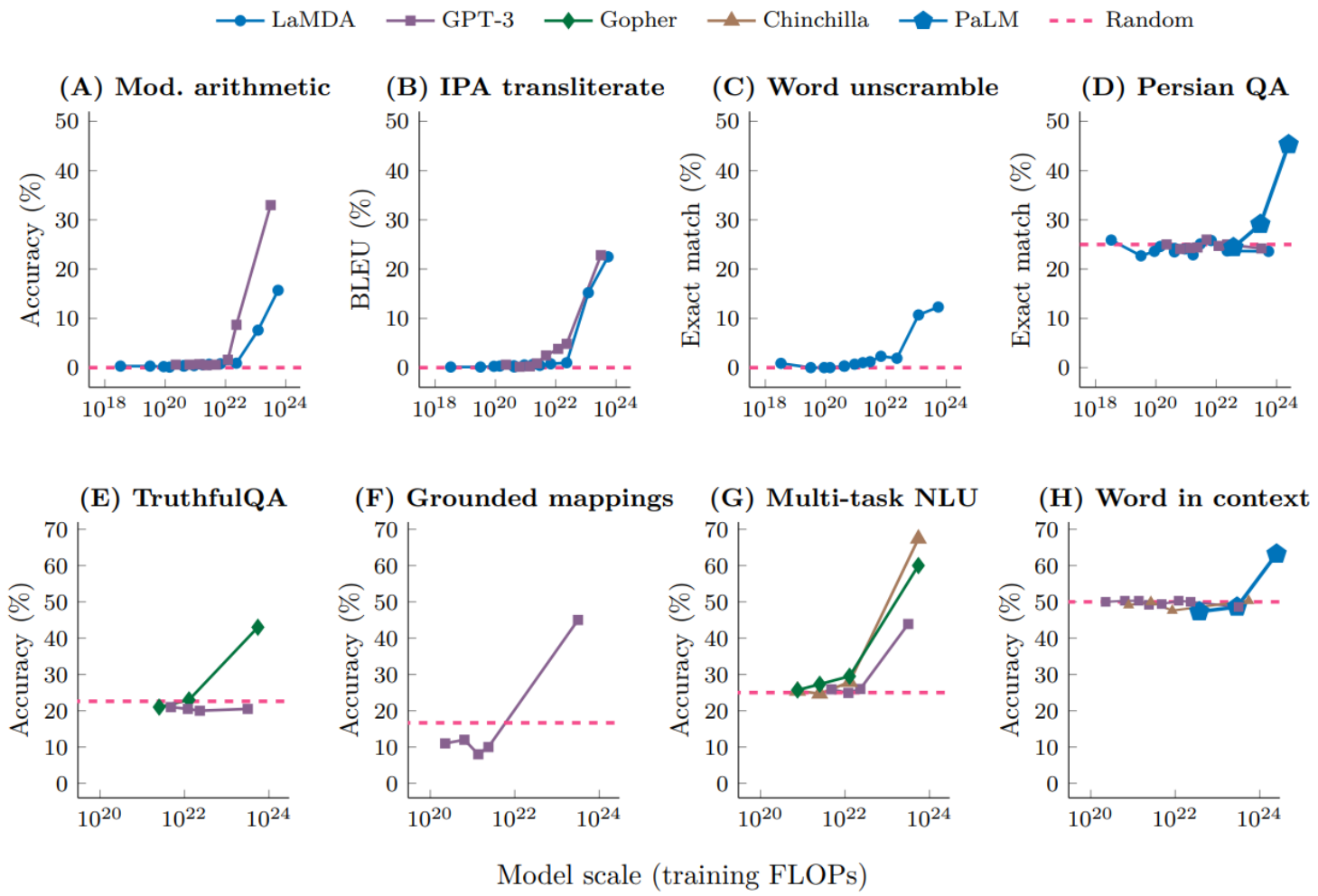
- „High Impact“ Fähigkeiten von General Purpose KI Modellen (State-of-the-Art)
- Signifikanter Einfluss auf den Binnenmarkt und potenzielle negative Auswirkungen auf Gesundheit, Sicherheit, Grundrechte und Gesellschaft
- Auswahl:
  - Durch technische Tools: 10^25 „FLOPs“ für das Training
  - Durch einen Alert des wissenschaftlichen Panels

ISACA Germany Chapter EXPERTS TOGETHER

Was ist Systemisches Risiko

10^25 „FLOPs“

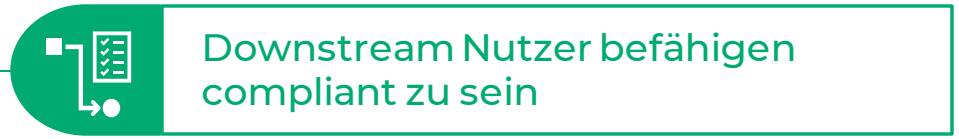
Modelle zeigen emergente Fähigkeiten ab einer gewissen Komplexität



ISACA Germany Chapter EXPERTS TOGETHER

Welche Restriktionen gelten jetzt für GPAI Systeme

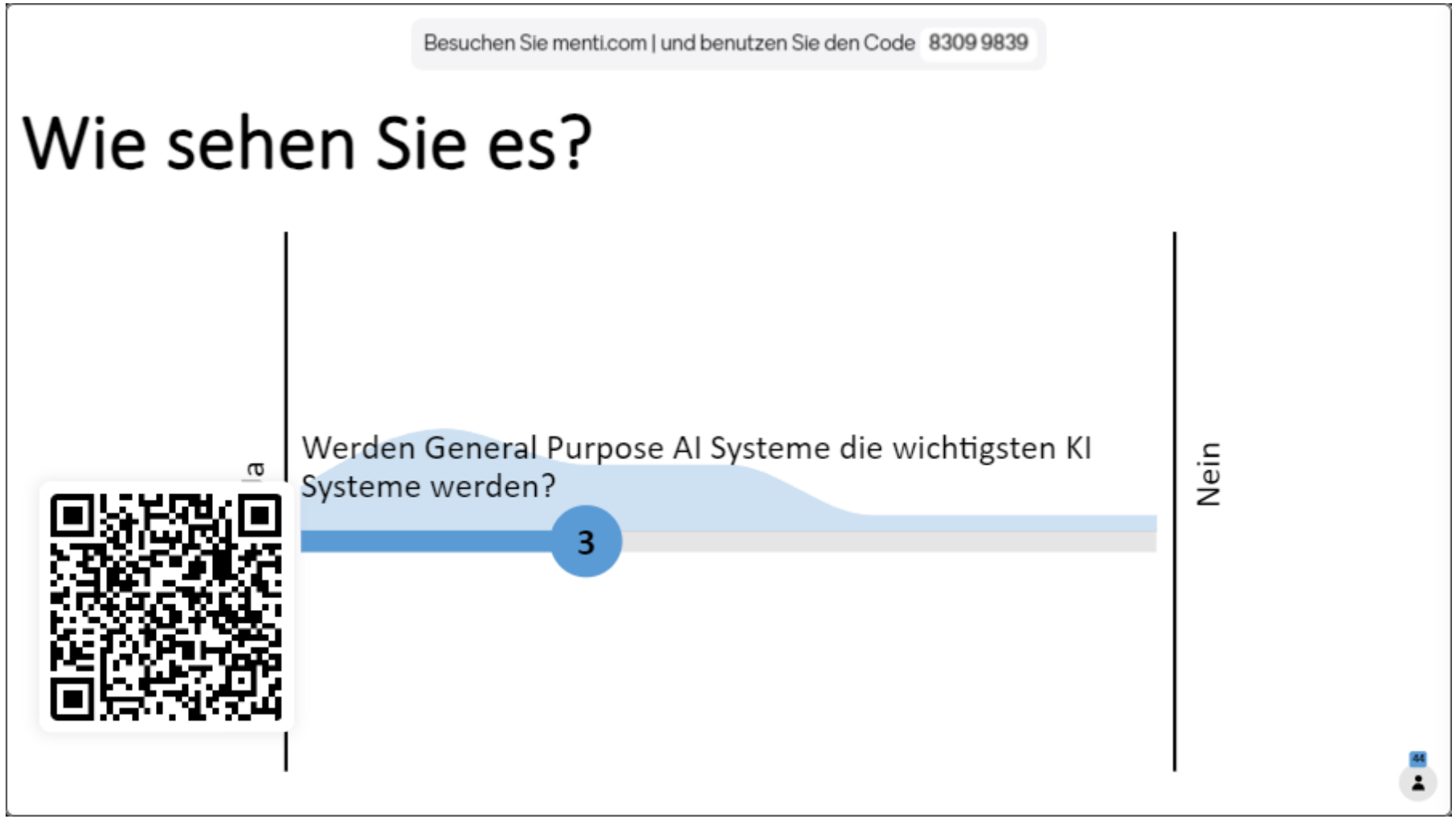
Dokumentation & Compliance: Umfassende Modell-Dokumentation gemäß Anhang IXa; Bereitstellung von Informationen für Integratoren und Behörden.



Urheberrecht & Transparenz: Einhaltung von Urheberrechtsrichtlinien; Veröffentlichung einer Trainingszusammenfassung.

Ausnahmen & Vertretung: Lizenzausnahmen bei freien Modellen; Pflicht zur EU-Vertretung für Nicht-EU-Anbieter.

Und Sie?


Besuchen Sie menti.com | und benutzen Sie den Code 8309 9839
Wie sehen Sie es?
Werden General Purpose AI Systeme die wichtigsten KI Systeme werden?
3
Nein

Strafen & Support

Strafen

Allgemeine Strafen

- Bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes (Artikel 5-Verstöße).
- Bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes (andere Verstöße).

Spezifische Strafen

- Falsche, unvollständige oder irreführende Informationen: Bis zu 7,5 Mio. EUR oder 1 % des weltweiten Jahresumsatzes.
- Reduzierte Strafen für KMUs und Start-ups.

Strafen für EU-Institutionen

- Bis zu 1,5 Mio. EUR (Artikel 5-Verstöße).
- Bis zu 750.000 EUR (andere Verstöße).

ISACA Germany Chapter EXPERTS TOGETHER

Support

KI-Regulierungs-Sandkästen (Regulatory Sandboxes

- **Ziel:** Entwickeln, testen und validieren von KI-Systemen in realen Bedingungen in einer kontrollierten Umgebung.
- **Zielgruppe:** Anbieter von KI-Systemen, bevorzugter Zugang für KMUs und Startups.
- **Unterstützung:** Technische und regulatorische Beratung durch zuständige Behörden.

Europäisches KI-Büro und KI-Rat

- **Ziel:** Überwachung der einheitlichen und effektiven Anwendung des KI-Gesetzes, Förderung der Koordination zwischen nationalen Behörden und Unterstützung bei der Einhaltung der Gesetzgebung und internationaler Kooperation.
- **Zielgruppe:** Mitgliedsstaaten, Anbieter und Nutzer von KI-Systemen.

Wissenschaftliches Gremium unabhängiger Experten

- **Ziel:** Unterstützung bei Durchsetzungsmaßnahmen, Beratung zu systemischen Risiken und Entwicklung von Bewertungstools für KI-Fähigkeiten.
- **Zielgruppe:** KI-Büro, Marktüberwachungsbehörden, KI-Rat.

ISACA Germany Chapter EXPERTS TOGETHER

Woran wir arbeiten

AI Act Zusammenfassung

Risikokategorien

(System)

(Orga)

Auflagen Hochrisikosysteme

GPAI Systeme

Auflagen

Support

Strafen

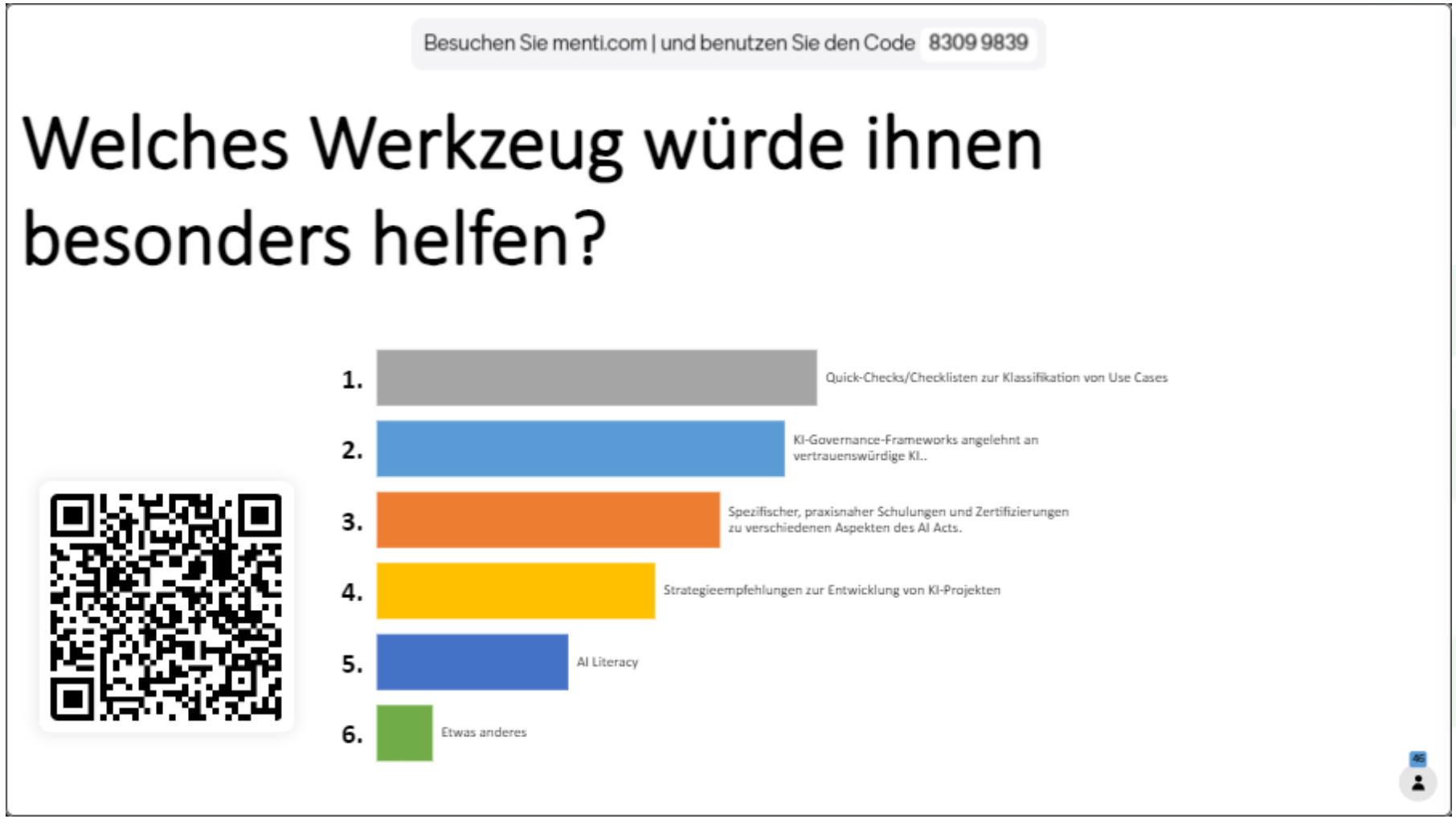
Bedeutung des AI Acts

Wir wollen Unternehmen und Prüfer bei der Adoption des AI Acts unterstützen

Wir denken dabei an die Entwicklung…

- **eines KI-Governance-Frameworks angelehnt an vertrauenswürdige KI.**
- **spezifischer, praxisnaher Schulungen und Zertifizierungen zu verschiedenen Aspekten des AI Acts (AI Literacy fördern).**
- **von Quick-Checks/Checklisten zur Klassifikation von Use Cases**
- **Strategieempfehlungen zur Entwicklung von KI-Projekten**

Und Sie?


Besuchen Sie menti.com | und benutzen Sie den Code 8309 9839
Welches Werkzeug würde ihnen besonders helfen?
1. Quick-Checks/Checklisten zur Klassifikation von Use Cases
2. KI-Governance-Frameworks angelehnt an vertrauenswürdige KI..
3. Spezifischer, praxisnaher Schulungen und Zertifizierungen zu verschiedenen Aspekten des AI Acts.
4. Strategieempfehlungen zur Entwicklung von KI-Projekten
5. AI Literacy
6. Etwas anderes
46

Und Sie?


Besuchen Sie menti.com | und benutzen Sie den Code 8309 9839
Was möchten Sie noch über KI wissen?
59 antworten
anwendungsbeispielr
umsetzungsleitfäden
technische voraussetzunge
datenschutzanforderungen
cybersicherheit
prüfungleitfäden
weitere gpai beispiele
erfahrungsberichte
ai in zukunft
praktische anwendung
grc
use cases
prüfleitfaden
usecases
vorteile
cobit
security
praxisbeispiele
governance
prüfmöglichkeiten
prüfleitfäden
cobit für ki
präzise definition
do and donts
technik
agi wann
auditierungsmöglichkeiten
aktuelle use cases
lessons learnt
transparenz der ki
cross-border ki
definitionen im unternehm
cybersicherheit prüfen
defintorische abgrenzung

Die Fachgruppe Artificial Intelligence

Nora Haberkorn

Fachgruppe

Eric Vogel

ISACA®

Germany Chapter