KI ohne Risiko?

Wie der AI-Act der EU Technologie begegnet und was bei seiner Umsetzung zu beachten ist

metafinanz

technologie. kultur. netzwerke.

Ihre Ansprechpartner*innen

Peggy Jacobs

Expertin für Informations-sicherheit und Third Party Risk Management

peggy.jacobs@metafinanz.de

+49 89 3605316464

Dr. Pia Zachary

Expertin für IT-Regulatorik

pia.zachary@metafinanz.de

+49 89 3605316079

Dr. Gregor Scheithauer

Sales Manager AI & Data-Driven Company

gregor.scheithauer@metafinanz.de

+49 89 3605315533

technologie. kultur. netzwerke.

Wir bringen Zukunftsfähigkeit ans Licht.

Zukunftsmutig, zugewandt, zupackend.

1990 im Schwarzwald gegründet,

… heute in **ganz Deutschland** vertreten.

Mehr als 850 Mitarbeitende

… aus über **50 Nationen.**

Mit mehr als 150 Netzwerk-Partnern

… und **8.000 Expert:innen** für alles gerüstet.

Wir sind ein Mittelständler

… mit **Konzernerfahrung** als Teil der Allianz Group.

Unser NPS: 94,4

… 2024: Rekordwert in der **Kundenzufriedenheit.**

Unser Umsatz: 175 Mio. EUR

… ein **erfolgreiches** Jahr 2024.

Great Place to Work®

… **Platz #1** in drei Kategorien.

Bester IT-Dienstleister

… ausgezeichnet von **brand eins.**

Wir finden Antworten

… auf die Themen unserer Zeit

AI & Data Driven Company

Future Organization

Connected Platforms

Resilient Business

ESG Transformation

Transformation Strategy

metafinanz

AI & Data-Driven Company

Daten, Algorithmen und KI treiben Wirtschaft & Welt in eine neue Ära

Werden Sie zum Vorreiter der daten-basierten Zukunft und steigern Sie Ihre Effizienz und Innovationskraft.

Mit maßgeschneiderten KI-Lösungen schaffen wir echten Mehrwert für Ihr Business und Ihre Kunden. Unsere Expertise in Datenarchitektur und ethischen KI-Leitbildern sichert Ihnen einen nachhaltigen Wettbewerbsvorteil. Treffen Sie klügere Entscheidungen, personalisieren Sie Kundenerlebnisse und entwickeln Sie neue Geschäftsmodelle. Mit uns überwinden Sie den Fachkräftemangel durch Automatisierung und setzen den Grundstein für Ihre langfristige Zukunftsfähigkeit.

Unsere Strahlkraft

- Advanced Analytics & Data Science
- Datenvisualisierung
- KI Legal Tech | Ethik | Automation
- Predictive Maintenance
- Process Mining
- Robotic Process Automation
- Data Engineering
- Business Process Mgmt.
- Cloud Transformation
- Business Intelligence

Resilient Business

Sicherheit schaffen heißt, Risiken erkennen

Stärken Sie Ihre Widerstandsfähigkeit, agieren Sie proaktiv und bauen Sie das Vertrauen Ihrer Stakeholder aus.

In einer Ära voller technologischer und gesellschaftlicher Umbrüche ist Resilienz unerlässlich für Unternehmen. Um Disruptionen und Krisen zu überstehen, müssen Strukturen und Prozesse gestärkt werden. Wir helfen Ihnen, Schwachstellen zu identifizieren, Risiken zu bewerten und maßgeschneiderte Sicherheitskonzepte zu entwickeln. Mithilfe von IT-Lösungen und Ihrem Datenschatz automatisieren wir Geschäftsabläufe und machen Ihr Unternehmen widerstandsfähiger.

Unsere Strahlkraft

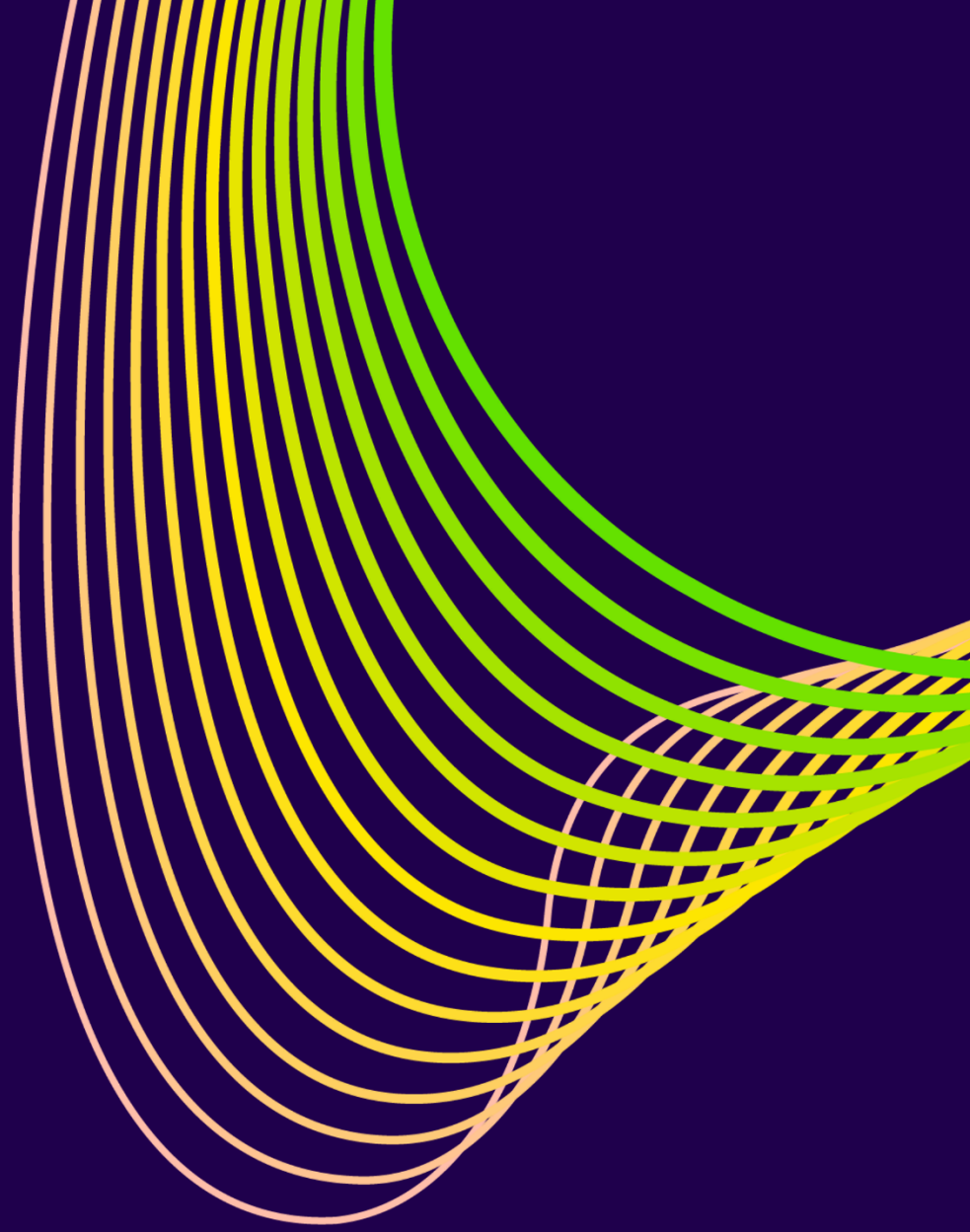
- ICT Governance
- IT Security
- GRC ServiceNow
- Security Awareness & Operations
- Organisation & Personal Resilience
- Information Security
- IT Service Continuity Management
- Business Continuity Management

metafinanz

Agenda

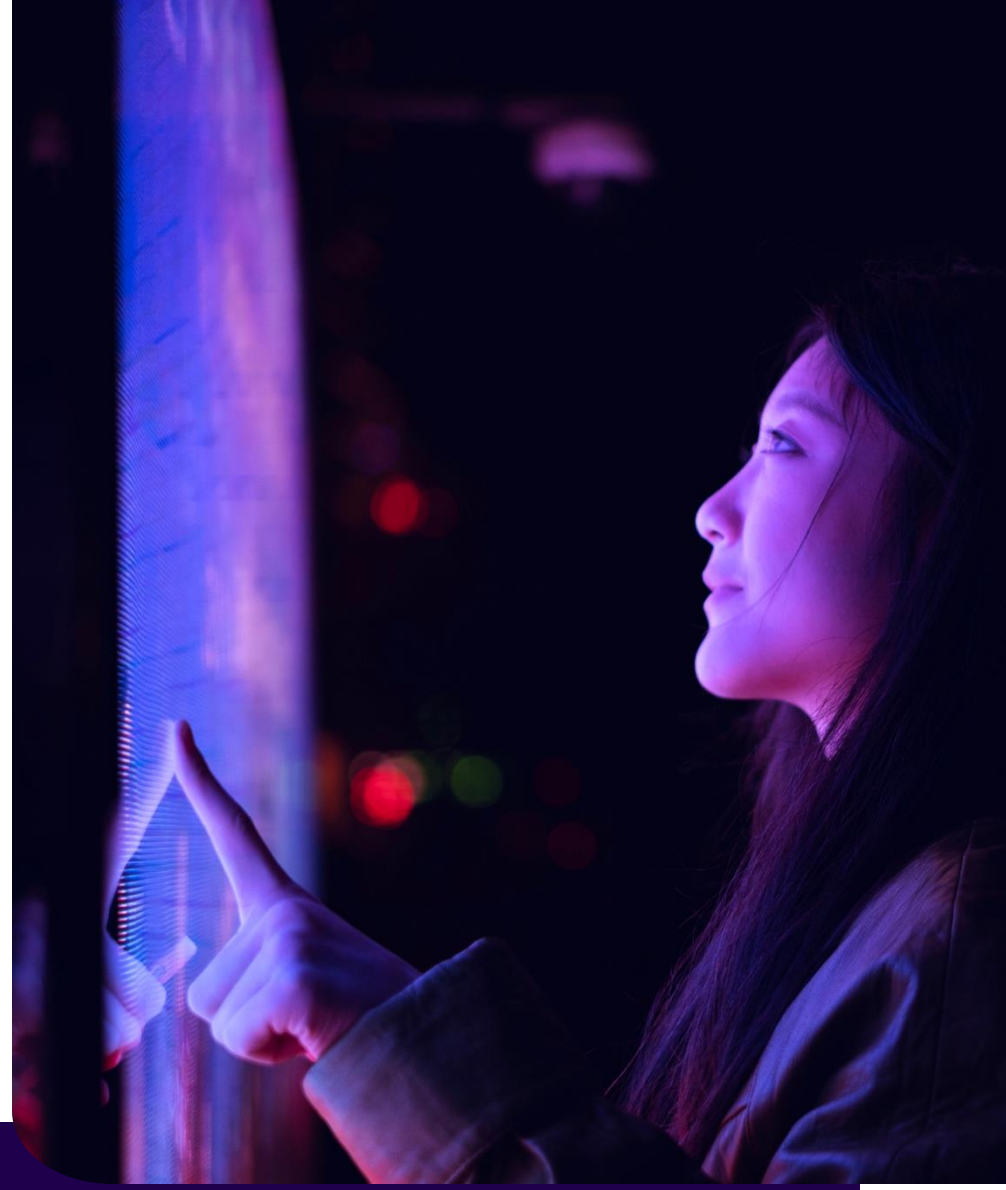
metafinanz

Eckdaten des AI Acts



Eckdaten des AI Acts

Ziel der Verordnung



Das heißt:

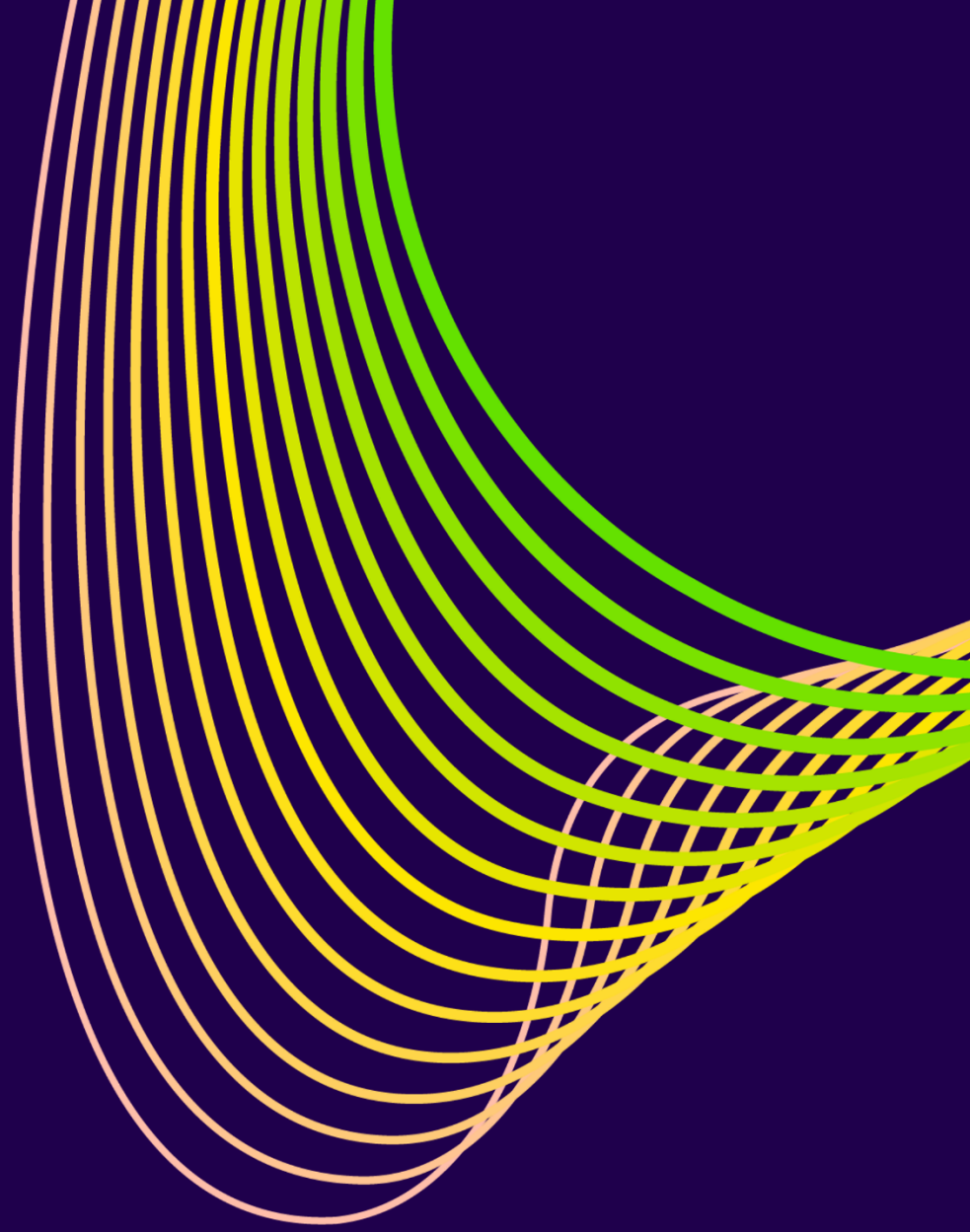
Ein hohes **Schutzniveau** in Bezug auf **Gesundheit**, **Sicherheit** und der in der Charta der EU-Grundrechte verankerten **Grundrechte sicherzustellen.**

Die Einführung von **menschenzentrierter** & **vertrauenswürdiger KI** zu **fördern**, durch besondere **Anforderungen** und **Transparenzpflichten** an den **Anbieter** & **Betreiber** von **KI-Systeme**. Damit wird der **Black-Box Effekt** vermieden.

Das Funktionieren des **KI-Binnenmarkts der EU** zu verbessern, und gleichzeitig die **Entwicklung der KI-Ökosysteme** und die **Innovation** zu **erleichtern** und **unterstützen**.

Ziel der KI-Verordnung ist ein **einheitlicher Rechtsrahmen** für die Entwicklung und **Verwendung** von Systemen künstlicher Intelligenz **(KI-Systeme)** festzulegen.

Geltungsbereich des EU AI Acts



Geltungsbereich

Anbieter, die KI-Systeme in der Europäischen Union in Verkehr bringen/in Betrieb nehmen

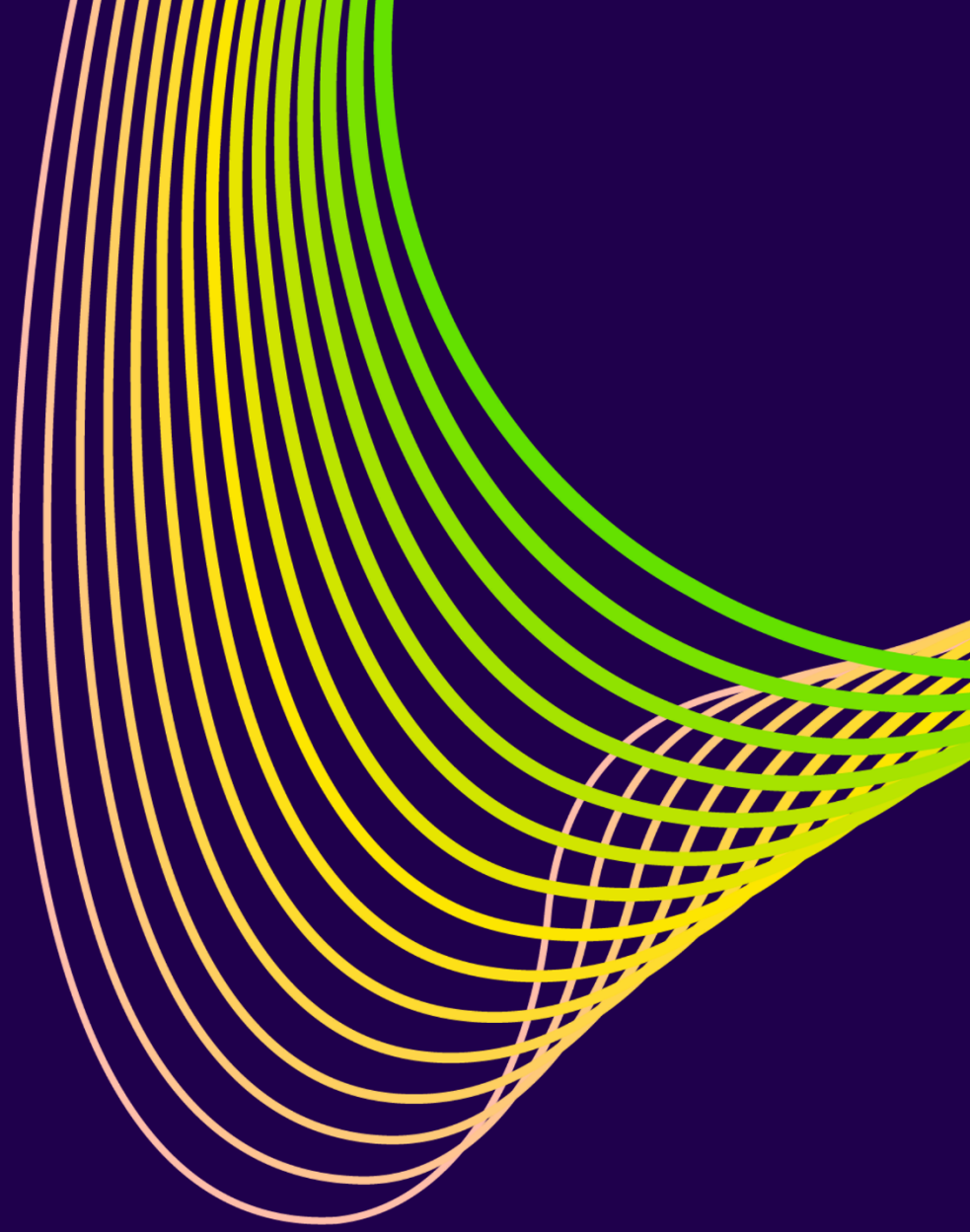
Nutzer von KI-Systemen, die sich in der Union befinden

Anbieter und Nutzer von KI-Systemen in Drittländern, wenn das vom System hervorgebrachte Ergebnis in der Union verwendet wird

Ausnahme bei KI für ausschließlich **militärische Zwecke**

Ausnahme für **Behörden in Drittländern** und **internationale Organisationen** sofern internationale Übereinkunft im Bereich Strafverfolgung und justizieller Zusammenarbeit besteht

Klassifizierung von KI-Systemen



Risiko-basierte Einstellung

Die Verordnung verfolgt eine **Risiko-basierte Einstellung**. Das heißt, als generelles Prinzip:
Je **höher** das Risiko für die **Sicherheit**, die **Gesundheit** und die **Grundrechte**, desto **strenger Regeln** und **Anforderungen** für das KI-Modell.

Das KI-Modell benutzt Praktiken, die in der Liste der **verbotenen Praktiken** gemäß Artikel 5 sind	Absolut **verboten**
Das KI-Modell kann als **hoch-riskantes Modell** gemäß Artikel 6/Anhang III eingestuft werden	Erlaubt unter strengen Anforderungen, gemäß **Kapitel III** der Verordnung
Das KI-Modell wird als **mit allgemeinem Verwendungszweck mit systemischem Risiko eingestuft**	Mit Anforderungen an **Information, Transparenz** und **technische Dokumentation erlaubt**
Das KI-Modell wird als **mit allgemeinem Verwendungszweck** oder als **bestimmtes KI-System eingestuft**	Minimale Anforderungen an der **Information**

Verbotene KI-Systeme

Unterschwellige Beeinflussung

Systeme, die Techniken der unterschwelligen Beeinflussung außerhalb des Bewusstseins einer Person einsetzen, um das Verhalten der Person wesentlich zu beeinflussen, die sich selbst oder anderen dann Schaden zufügen kann.

Ausnutzung Schutzbedürftiger

Systeme, die Schwäche/ Schutzbedürftigkeit einer bestimmten Gruppe ausnutzen, um das Verhalten der Personen wesentlich zu beeinflussen, die sich selbst oder anderen dann Schaden zufügen können.

Social Scoring

Verwendung von Systemen durch Behörden, die natürliche Personen sozial bewerten, um diese ungerechtfertigt/unverhältnismäßig zu benachteiligen.

Echtzeit-Fern-identifizierungssysteme

Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken (definierte Ausnahmen z.B. Schutz der öffentlichen Sicherheit).

Hochrisiko-KI-Systeme

Rechtspflege & demokratische Prozesse (Auslegung Rechtsvorschriften, Ermittlungen)

Migration, Asyl und Grenzkontrolle (Asyl-Entscheidungen, Prüfung von Unterlagen)

Strafverfolgung (Risikobewertungen, Verlässlichkeit von Personen oder Beweismitteln)

Zugänglichkeit und Inanspruchnahme grundl. privater und öffentl. Dienste und Leistungen (z.B. öffentl. Unterstützungsleistungen, Kreditwürdigkeitsprüfung)

Hoch-risiko-Systeme

Biometrische Identifizierung und **Kategorisierung** natürlicher Personen

Verwaltung und Betrieb kritischer Infrastrukturen (Straßenverkehr, Wasser, Gas, Wärme, Strom)

Allgemeine und berufliche Bildung (Zulassung und Bewertung)

Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit (Einstellung, Beförderung, Kündigung, Leistungsüberwachung)

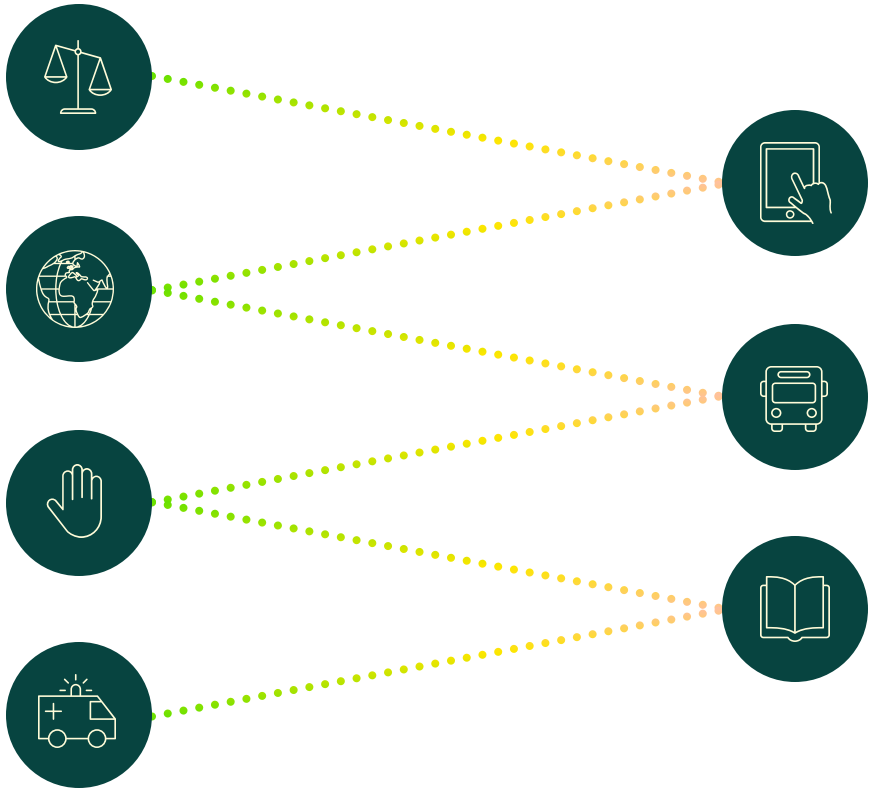
Anforderungen an Hochrisiko-Systeme

Risikomanagementsystem
Einrichtung, Anwendung, Dokumentation und Aufrechterhaltung eines Risiko-managementsystems für das KI-System

Technische Dokumentation
Technische Dokumentation über das System als Nachweis über die Erfüllung des EU AI Acts

Gebrauchsanweisung
Gebrauchsanweisungen für Nutzer zum Betrieb und Interpretation der Ergebnisse

Sicherheit
Angemessenes Maß nach Genauigkeit, Robustheit und Cybersicherheit



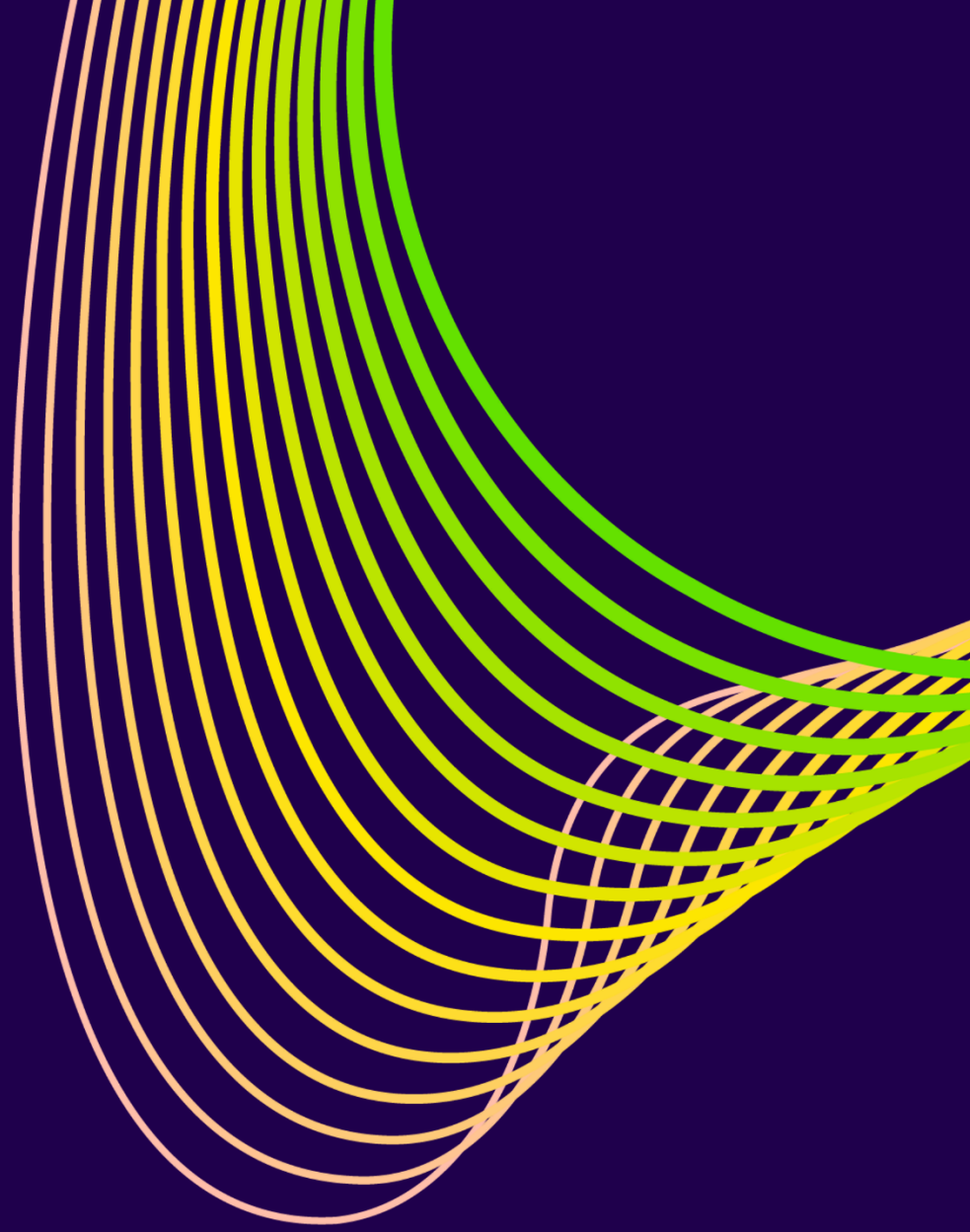
Testdaten
Strenge Anforderungen an Testdaten hinsichtlich Relevanz, Repräsentativität, Fehlerfreiheit und Vollständigkeit sowie an deren Governance

Protokollierung
Pflicht zur automatischen Protokollierung von Vorgängen und Ereignissen

Aufsichtspflicht
Menschliche Aufsichtspflicht

Anforderungen an Betreiber von Hochrisiko-KI-Systemen

Weitere Inhalte des EU AI Acts



Weitere Inhalte des EU AI Acts

Transparenzpflichten für bestimmte KI-Systeme

Mitteilung an natürliche Nutzer, dass sie mit einem KI-System interagieren, sofern nicht offensichtlich

---

Information der Betroffenen bei **Nutzung eines Emotionserkennungssystems** oder eines Systems zur **biometrischen Kategorisierung**

Offenlegung bei Deepfakes, dass Inhalte künstlich erzeugt oder manipuliert wurden

Sanktionen

Gemäß Kapitel XII der Verordnung, verschiedene **Sanktionen** sind für die **Missachtung der Verordnung** vorgegeben.

Die vorgesehen Sanktionen sind verhältnismäßig und abschreckend.

Missachtung des Verbots der in Artikel 5 genannten KI-Praktiken

- Geldbußen von bis zu **35 Millionen €**, oder
- Geldbußen von bis zu **7%** des gesamten weltweiten **Jahresumsatzes**[1]

Missachtung der Anforderungen an Hochrisiko-KI-Systeme

- Geldbußen von bis zu **15 Millionen €**, oder
- Geldbußen von bis zu **3%** des gesamten weltweiten **Jahresumsatzes**[1]

Bereitstellung von falschen, unvollständigen oder irreführenden Informationen

- Geldbußen von bis zu **7,5 Millionen €**, oder
- Geldbußen von bis zu **1%** des gesamten weltweiten **Jahresumsatzes**[1]

[1] Je nachdem, welcher der zwei Beträge höher ist. Für KMU, gilt der jeweils niedrigere Betrag.

Weitere Inhalte

Einrichtung von KI-Reallaboren als **kontrollierte** Umgebung zur Förderung von Innovationen

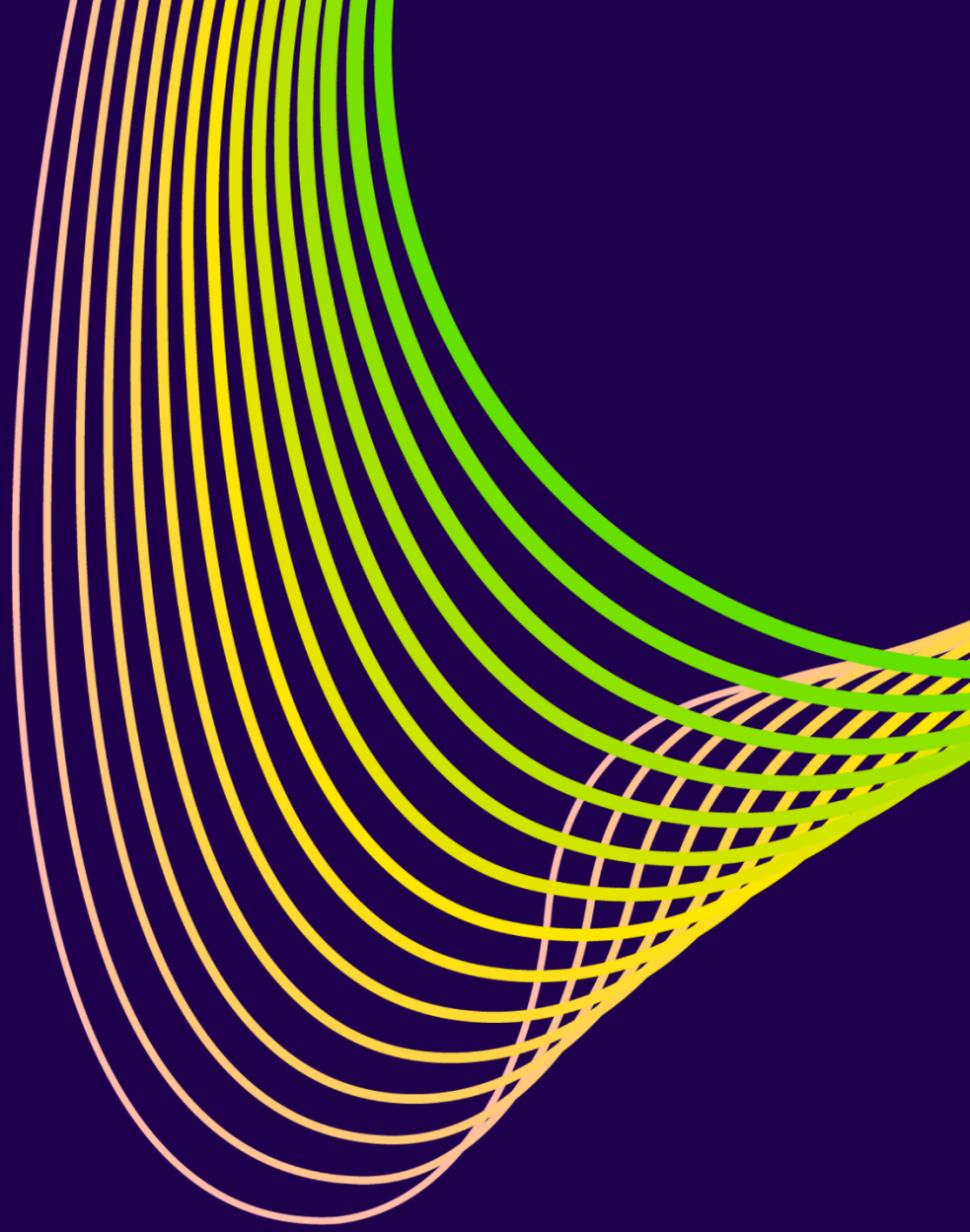
Einrichtung eines **Europäischen Gremiums** für **Künstliche Intelligenz**

- Erleichterung der Zusammenarbeit der nationalen Behörden
- Koordinierung und Mitwirkung an Leitlinien und Analysen
- Unterstützung der nationalen Behörden bei der Umsetzung des EU AI Act

Förderung bei der Erstellung von **Verhaltenskodizes** von KI-Systemen ohne hohes Risiko oder für die freiwillige Anwendung spezifischer Anforderungen

Schulungsverpflichtungen, falls Mitarbeitende mit KI arbeiten (abhängig vom Aufgabenbereich)

Zeitplan



Zeitplan

13.03.2024

EU-Parlament

Verabschiedung des EU AI Acts durch das EU-Parlament

12.07.2024

Veröffentlichung

Veröffentlichung im Amtsblatt der EU

01.08.2024

Inkrafttreten

EU AI Act tritt in Kraft

02.02.2025

Verbot und Kompetenz

- Verbot bestimmter inakzeptablen KI-Systeme
- Anforderung an KI-Kompetenz (Betreiber und Nutzer)

02.08.2025

GPAI, Behörden, Strafen

- Inkrafttreten von Regeln für General-Purpose AI (GPAI) Systeme
- Regeln zur Benachrichtigung von Behörden
- Geldstrafen

02.08.2026

Inkrafttreten

Die übrigen Anforderungen bis auf die Sicherheitsbauteile treten in Kraft

02.08.2027

Sicherheitsbauteile

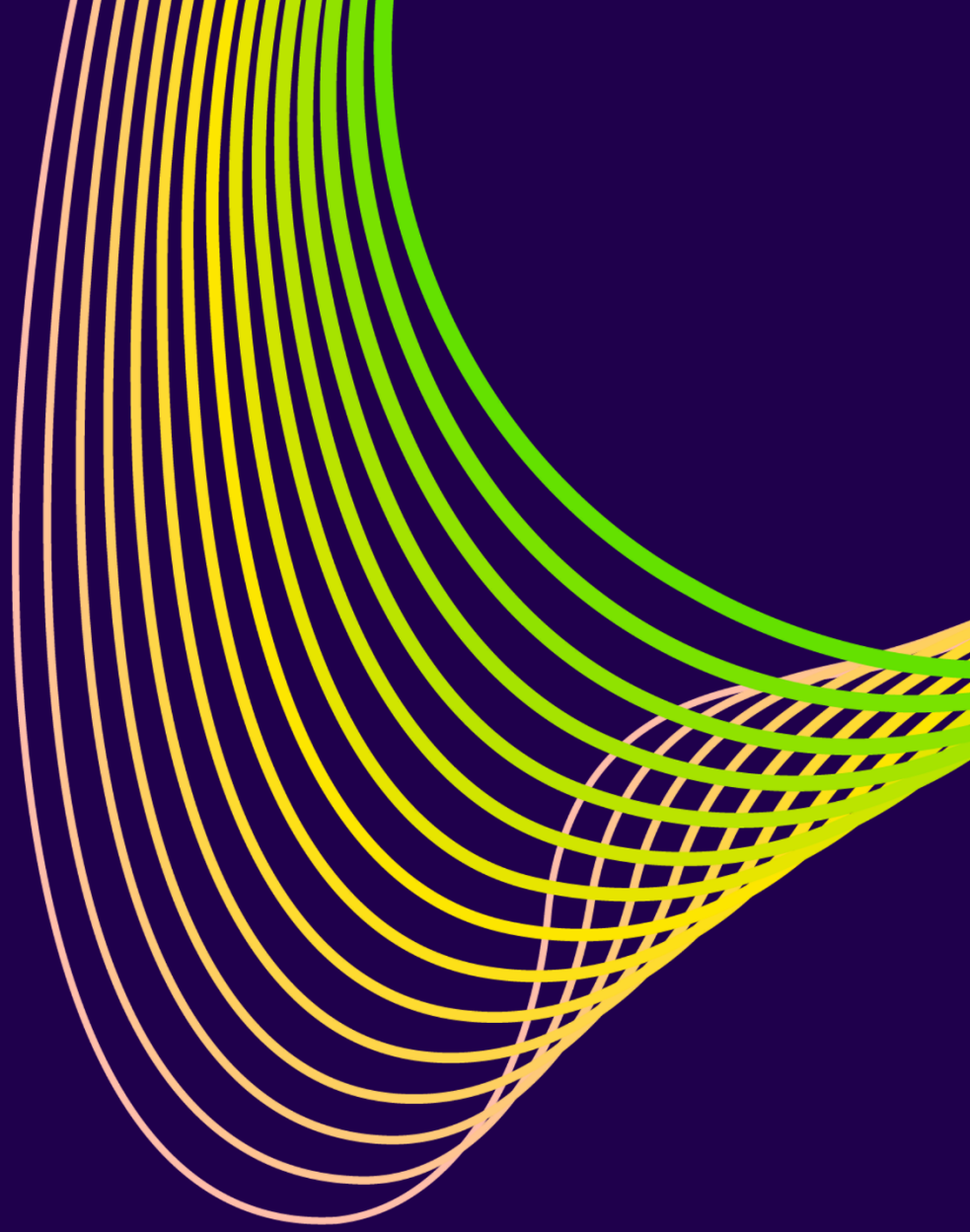
Verpflichtungen für Hochrisiko-Systeme gelten für KI-Systeme als Sicherheitskomponente

2031

Bewertung der Kommission

Bewertung der Durchsetzung der Verordnung und Berichtserstattung

Umsetzung des EU AI Acts



Vorgehen: Etablierung eines KI-Freigabeprozesses Einkauf

- **Start: Unternehmen möchte KI für einen bestimmten Use Case einführen**
- Auswahl bestimmter Anbieter

- Durchführung einer Risikoanalyse über die identifizierten Lösungen
- Einstufung anhand der Klassifizierung des EU AI Acts

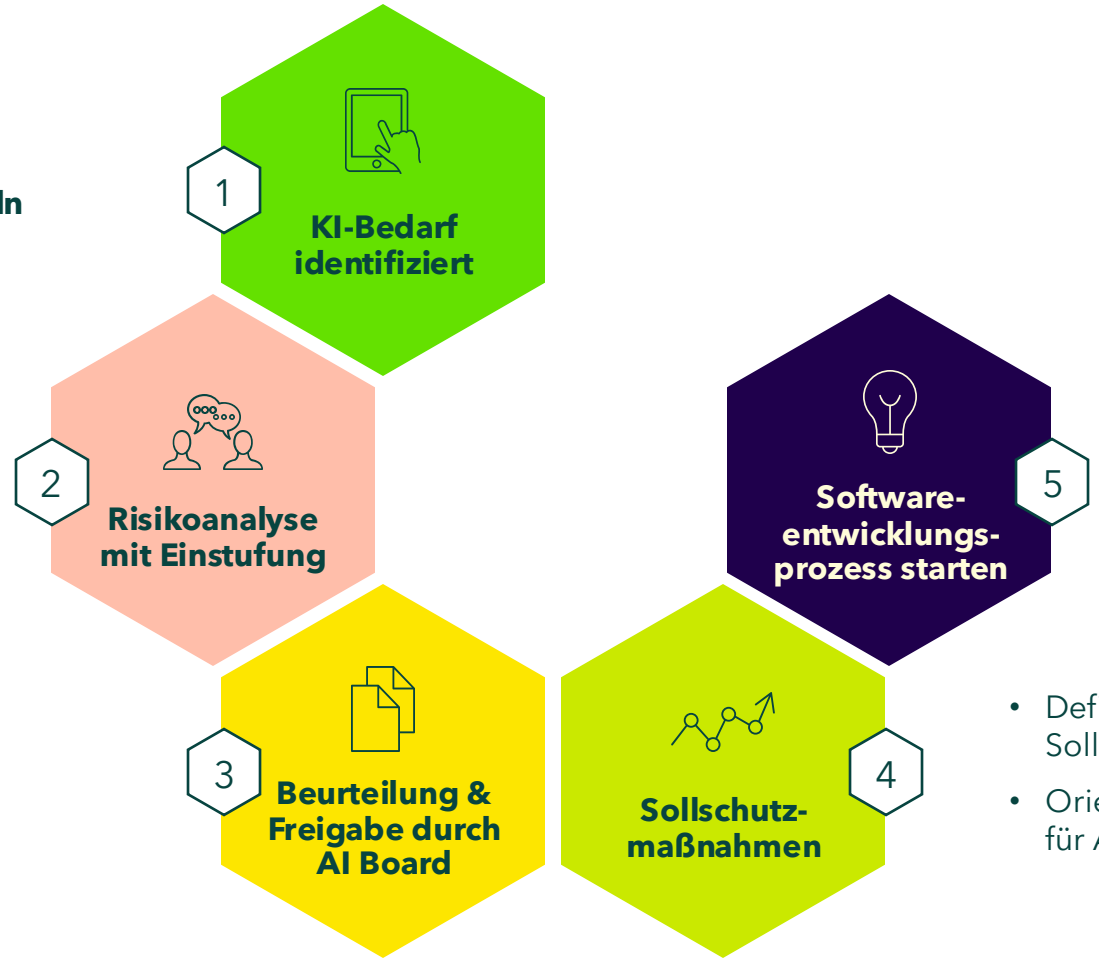
- Beurteilung der geplanten KI-Lösungen anhand der Risikoanalyse
- Erteilung der Freigabe inkl. etwaiger Einschränkungen

Start des regulären Einkaufsprozess

- Definition/Anordnung spezifischer Sollschutzmaßnahmen für die KI
- Orientierung an den Maßnahmen für TPRM

Vorgehen: Etablierung eines KI-Freigabeprozesses Eigenentwicklung für Eigennutzung

Start: Unternehmen möchte KI für einen bestimmten Use Case entwickeln



- Durchführung einer Risikoanalyse über die zu entwickelnde Lösung
- Einstufung anhand der Klassifizierung des EU AI Acts

- Beurteilung der geplanten KI-Lösung anhand der Risikoanalyse
- Erteilung der Freigabe inkl. etwaiger Einschränkungen

- Definition/Anordnung spezifischer Sollschutzmaßnahmen für KI
- Orientierung an den Maßnahmen für Anwendungsentwicklung

Start des regulären Software-entwicklungsprozess

Mögliche Aufgaben eines AI Boards

Unterstützung bei Entwicklung und Umsetzung der KI-Strategie.

Einbindung der KI-Strategien in andere Unternehmensstrategien, wie der IT-Strategie.

Priorisierung der KI-Lösung mit dem größten Nutzen.

Frühzeitiges Schaffen von Transparenz zwischen den beteiligten Fachbereichen und Funktionen.

Sicherstellung von externer Compliance, ethischen Standards und der Einhaltung der unternehmensinternen Vorgaben.

Stärkung des Vertrauens in KI.

Koordinator
Steuerung des AI Boards

Datenschutz	Human Resources	Enterprise Architecture	Informations-sicherheit	Rechts-funktion	Risiko Management	Intellectual Property/ Patentrecht	Weitere Stakeholder
Prüfung der Verarbeitung, Speicherung, Weitergabe pbD und Einhaltung von Datenschutz-anforderungen.	Informations- und Auskunftspflichten an MA, Sicher-stellung von Anti-diskriminierung durch KI, Organisation von Schulungen.	Kompatibilität und Einbindung in IT-Architektur.	Einhaltung der Informationssicher-heitsanforderungen, Risikobewertung und Schutzbedarf.	Überprüfung rechtlicher Implikationen.	Überblick über unternehmens-weites Risiko-management, Identifizierung der Top-Risiken.	Prüfung urheberrechtliche Anforderungen und Konflikte.	

Unsere Leistung

- Gap-Analysen
- Aufbau eines KI-Governance Frameworks
- Anpassung und Neuerstellung von Richtlinien
- Aufbau eines AI-Boards
- Design von Risikoanalysen inkl. Automatisierung
- Definition von Sollschutzmaßnahmen
- Kompetenzentwicklung und Schulungen

Unsere Schulungen

Schulung	Dauer	Zielgruppe	Inhalt	Art
Achieving Responsible AI with SAFe	4	Alle Mitarbeitende	Die Anwendung agiler Werte und Prinzipien zur Umsetzung von Responsible AI in der Organisation	Blended Learning (Einführung + Self Learning + Halbtagesworkshop)
AI Empowerment „Starter“	2	Alle Mitarbeitende	Einführung in GenAI, Einführung ins Prompting, Praktische Übungen	Online
AI Empowerment „Advanced“	2	Alle Mitarbeitende	Aktueller Stand GenAI, Prompting, Anlegen von CustomGPT	Online
GenAI Exitgame	1,5	Alle Mitarbeitende	Leichtes Format zur Aktivierung der Mitarbeiter in Sachen GenAI, erste Kenntnisse in Prompting, Spaß & Teamcoaching	Präsenz WS
GenAI Einführungsworkshop	4	Alle Mitarbeitende	Einführung in GenAI mit Anwendungsbeispielen in Textmanagement, Bild- & Video, Innovationsmanagement, Blick nach draußen	Online
1zu1 GenAI Leadership Coaching	Tbd.	Führungskräfte, Entscheider	Intensive 1zu1 Betreuung von Führungskräften, Einstieg über Hausaufgaben in Verbindung mit 3 – 4 direkten Coachings à ca. 2 Std.	Präsenz & Online
CoPilot Basic Schulung	~2 h	Alle Mitarbeitende	Grundlegendes Verständnis von M365 Copilot, seinen Funktionen und Vorteilen	Präsenz & Online
CoPilot Tailored	Ab 2 h	Alle Mitarbeitende	Nach Absprache und auf die Bedürfnisse des Kunden zugeschnittene Schulung zu M365 Copilot	Präsenz & Online
CoPilot Prompting	Ab 2 h	Alle Mitarbeitenden mit Grundkenntnissen	Prompting für M365 Copilot	Präsenz & Online

Umsetzung des EU AI Acts

Grünes Licht für IT-Dienstleister

Wie ein Versicherungskonzern mit uns Klarheit im Dienstleister-Dschungel schafft und sich widerstandsfähiger gegen IT-Risiken aufstellt.

Kunde: **Versicherungskonzern**

Projektkontext:

Aufbau eines Third Party Risk Managements

Unser Beitrag für den Kunden:

In unseren Projekten beraten wir Kunden zum ganzheitlich im Aufbau des Outsourcing- und IT-Dienstleister Managements. Dank unserer Lösungen können Risiken von neuen Dienstleistern besser eingeschätzt werden und die Dienstleister effizient gesteuert werden. Natürlich alles smart umgesetzt und transparent für die Führungsetage.

Story lesen

metafinanz

Vielen Dank!

metafinanz
technologie. kultur. netzwerke.

metafinanz Informationssysteme GmbH

Leopoldstraße 146
80804 München

Große Gallusstraße 16-18
60312 Frankfurt

Theodor-Heuss-Str. 30
70174 Stuttgart

Linzer Straße 225/3a
1140 Wien