FIDES
Wir sind Vertrauen.

Wirtschaftsprüfer | Steuerberater
IT-Berater | Unternehmerberater

Update: Omnibus-Gesetze Einführung von KI und "Agentic AI" im Mittelstand

Dr. Ralf Kollmann

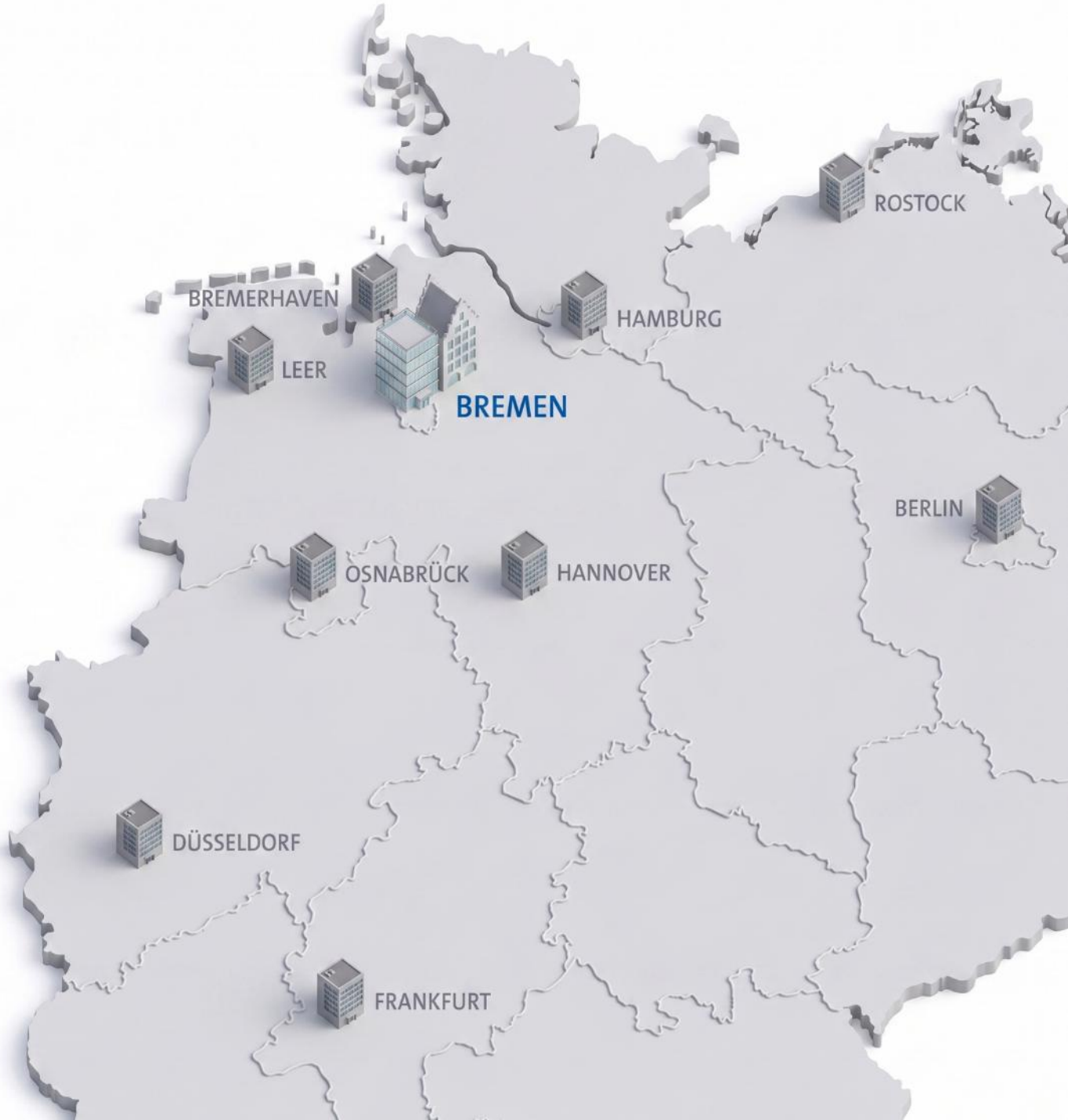
September/Oktober 2026



FIDES im Überblick

- Gegründet 1919
- Die führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Nordwestdeutschland seit über 100 Jahren
- Unter den TOP 25 in Deutschland
- 30 Partnerinnen und Partner,
  350 Mitarbeiterinnen und Mitarbeiter
- Unabhängig und partnergeführt

Beratung individuell und
"vom Unternehmer zum Unternehmer"



FIDES
Wir sind Vertrauen.



Inhalt

1. AI Omnibus Act
2. Digital Omnibus Act
3. KI-Management im Mittelstand
4. Einführung von KI und "Agentic AI" im Mittelstand

FIDES
Wir sind Vertrauen.

Zwei Omnibus-Vorhaben mit unterschiedlichem Rechtsstatus

AI Omnibus



- Verabschiedet als **Verordnung (EU) 2026/1744**
- Veröffentlichung im EU-Amtsblatt **am 24. Juli 2026**
- Inkrafttreten **am 27. Juli 2026**
- Seitdem unmittelbar geltendes EU-Recht

8. Juli 2026 (Beschlossen) → **24. Juli 2026** (Veröffentlicht) → **27. Juli 2026** (In Kraft)

Ziel:

- Vereinfachung, Präzisierung und teilweise zeitliche **Verschiebung von Pflichten** des AI Acts

Digital Omnibus



- Kommissionsvorschlag COM(2025) 837 final vom 19. November 2025
- Betrifft unter anderem DSGVO, Data Act, ePrivacy, NIS-2, DORA, CER und eIDAS

Verfahren 2025/0360(COD)

Status: Awaiting committee decision

- **Beratung in Parlament und Rat dauert an**
- Vorschläge sind daher noch nicht **verbindlich** und können sich **wesentlich ändern**

FIDES
Wir sind Vertrauen.

AI Omnibus Act – neue Fristen

2. August 2026

Grundlegende Geltung der KI-Verordnung



KI-Inhalte

Allgemeine Transparenzpflichten gem. **Art. 50 KIVO**

bspw. Chatbots, KI-generierte Inhalte, Deepfakes, öffentliche Informierung

2. Dezember 2026



Übergangsfrist für vermarktete Systeme zur Erzeugung von synthetischen Inhalten: Transparenzpflicht gemäß Art. 50 Abs. 3 KIVO

Neue verbotene KI-Praktiken: "Nudifyer"-Apps bzw. -Systeme

2. Dezember 2027

Geltung für **Hochrisiko-KI-Systeme** nach Art. 6 Abs. 2 in Verbindung mit Anhang III



Recruiting



Personalentscheidungen und Leistungsbewertung von Mitarbeitenden



Bonitäts-prüfungen



KI-Systeme als Sicherheitsbauteile in kritischen Infrastrukturen (Konkretisierung der Geltung)

2. August 2028

Geltung für **Hochrisiko-KI-Systeme** nach Art. 6 Abs. 1 in Verbindung mit Anhang I



FIDES
Wir sind Vertrauen.

AI Omnibus Act: Erleichterungen der KI-Verordnung

VEREINFACHUNG DER DOKUMENTATION



- KMU, Start-ups und Small Mid-Caps dürfen die in Anhang IV geforderten Inhalte der technischen Dokumentation in vereinfachter Form bereitstellen.
- Die Kommission muss hierfür ein standardisiertes Formular schaffen.

PROPORTIONALES QUALITÄTSMANAGEMENT



- Die Umsetzung des Qualitätsmanagementsystems muss (darf) der Größe des Anbieters angemessen sein, ohne das erforderliche Schutzniveau herabzusetzen.

VEREINFACHTE REGISTRIERUNG



- KI-Systeme, die einem Anwendungsfall gem. Anhang III zuzuordnen sind, aber aufgrund der Ausnahme aus Art. 6 Abs. 3 KIVO als nicht hochriskant eingestuft werden, bleiben grds. registrierungspflichtig. Der erforderliche Datensatz wird jedoch reduziert.

VERARBEITUNG besonderer Kategorien personenbezogener Daten

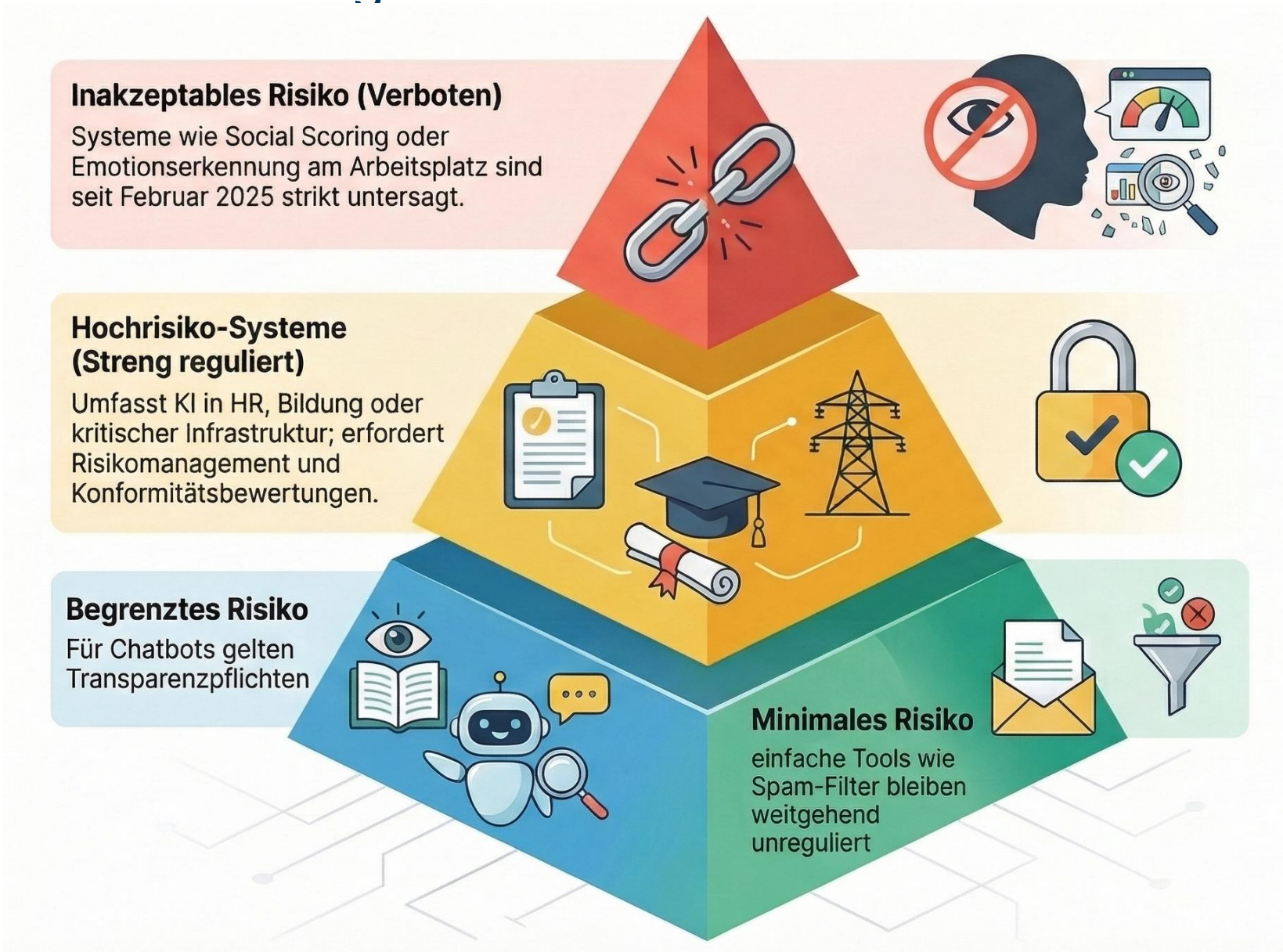


- Die Verarbeitung besonderer Kategorien personenbezogener Daten zur Bias-Erkennung und Bias-Korrektur wird unter bestimmten Bedingungen erlaubt.

Hinweis: Die Nummerierung entspricht der thematischen Gliederung in Anhang 3 der KI-VO

FIDES
Wir sind Vertrauen.

KI-Verordnung: Risikoklassen



- Social Scoring
- Predictive Policing
- Biometrische Echtzeit-Fernidentifikation im öffentlichen Raum zur Strafverfolgung
- nicht wahrnehmbare Manipulation

- Produkte gemäß Europäischer Harmonisierungsvorschriften / Anhang 1 KIVO
- Biometrische Fernidentifizierung,
- Sicherheitsbauteile kritischer Infrastruktur,
- Bildung, Bewerbung / Entscheidungen im Beschäftigungsverhältnis,
- Bewertung der Kreditwürdigkeit

- Chatbots, KI-Ergebnisse, Berichterstattung

FIDES
Wir sind Vertrauen.

Artikel 6 KI-Verordnung: Einstufung als Hochrisiko-KI-System

Ein KI-System gilt als hochriskant, wenn es als Sicherheitsbauteil oder Produkt unter spezifische **EU-Harmonisierungsvorschriften** fällt (Anhang 1) **ODER** einem der acht definierten **kritischen Anwendungsbereiche** (Anhang 3) zuzuordnen ist.

Fokus Unternehmen (Hochrisiko-Fälle)

1 Anhang 1: EU-Harmonisierungsrecht

KI-Systeme, die als Produkt oder Sicherheitsbauteil unter EU-Vorschriften fallen (z. B. Maschinen, Medizinprodukte, Aufzüge, Spielzeug).



2 Anhang 3 (Nr. 4): Beschäftigung & Personal

- KI für **Recruiting** (z. B. gezielte Schaltung von Stellenanzeigen, Screening und Filtern von Bewerbungen).
- KI für Entscheidungen und Bewertungen im Arbeitsverhältnis (z. B. Beurteilung von Leistung und Verhalten, Beförderungen, Kündigungen).



3 Anhang 3 (Nr. 5): Dienstleistungen & Leistungen

- KI zur Bewertung von Bonität und Kreditwürdigkeit von natürlichen Personen.
- (Zusätzlich in Nr. 5: KI zur Zuteilung öffentlicher Hilfsleistungen sowie zur Priorisierung in Notrufzentralen).



Weitere Hochrisiko-Kategorien (Anhang 3)

1 Biometrik

Biometrische Fernidentifizierungs-systeme, biometrische Kategorisierung sowie Emotionserkennung (soweit gesetzlich zulässig).



2 Kritische Infrastrukturen

KI als Sicherheitsbauteile für das Management und den Betrieb kritischer digitaler Infrastrukturen, Straßenverkehr oder Energieversorgung.



3 Bildung & Berufsausbildung

KI zur Entscheidung über den Zugang zu Bildungseinrichtungen, zur Bewertung von Lernergebnissen oder zur Überwachung bei Prüfungen.



7 Migration, Asyl & Grenzkontrolle

KI zur Risikobewertung von Personen, Überprüfung von Asyl- oder Visumanträgen sowie Lügendetektoren im Grenzbereich.



6 Strafverfolgung

KI-Systeme für Profiling, die Bewertung des Rückfallrisikos von Liegendetektoren oder die Analyse im Grenzbereich.



8 Rechtspflege & Demokratie

KI zur Unterstützung von Justizbehörden bei der Recherche und Auslegung von Fakten/Recht sowie KI zur gezielten Ansprache von Wählern in demokratischen Wahlen.



Hinweis: Die Nummerierung entspricht der thematischen Gliederung in Anhang 3 der KI-VO

FIDES
Wir sind Vertrauen.

Kritische Infrastrukturen: Nicht jede KI-Funktion in regulierten Produkten ist eine Sicherheitskomponente



Eine KI-Komponente erfüllt eine **Sicherheitsfunktion**, wenn ihr bestimmungsgemäßer Zweck darin besteht, **Risiken** für **Gesundheit und Sicherheit** von Personen oder Eigentum zu **verhindern** oder zu mindern.

Hochrisiko-Anwendungsfälle (Beispiele)



KI-Systeme zur Überwachung und Erkennung von Situationen in kritischer Infrastruktur, die direkt zu physischen Schäden an Personen oder Eigentum führen können.



KI-Systeme für physischen Perimeterschutz, wie Kameras, Radar und Drohnensteuerung.



KI-Systeme zur Anomalie-Erkennung in Datenmustern kritischer Funktionen wie Lastverteilung, Netzstabilität oder Abschaltverfahren.

Nicht Hochrisiko-Anwendungsfälle (Beispiele)



KI-Systeme **ausschließlich** für **Cybersicherheits-zwecke**, ohne direkte Sicherheitsfunktion.



Honeypot-System zur proaktiven Identifizierung und Neutralisierung von Cyberbedrohungen in Echtzeit.



KI-Technologie zur **aktiven Interaktion mit An-greifern**, um neue Angriffsmuster zu erlernen.



KI-System zur Unterstützung bei der Erkennung von unbefugtem Zugriff (z. B. Benachrichtigung betroffener Kunden).



KI-System zur Erkennung verdächtiger E-Mail-Ad-dressen und Identifizierung gestohlener Daten.

FIDES
Wir sind Vertrauen.



Inhalt

1. AI Omnibus Act
2. Digital Omnibus Act
3. KI-Management im Mittelstand
4. Einführung von KI und "Agentic AI" im Mittelstand

FIDES
Wir sind Vertrauen.

Zwei Omnibus-Vorhaben mit unterschiedlichem Rechtsstatus

AI Omnibus

- Verabschiedet als **Verordnung (EU) 2026/1744**
- Veröffentlichung im EU-Amtsblatt **am 24. Juli 2026**
- Inkrafttreten **am 27. Juli 2026**
- Seitdem unmittelbar geltendes EU-Recht

8. Juli 2026 (Beschlossen) → **24. Juli 2026** (Veröffentlicht) → **27. Juli 2026** (In Kraft)

Ziel:

- Vereinfachung, Präzisierung und teilweise zeitliche **Verschiebung von Pflichten** des AI Acts

Digital Omnibus



- Kommissionsvorschlag COM(2025) 837 final vom 19. November 2025
- Betrifft unter anderem DSGVO, Data Act, ePrivacy, NIS-2, DORA, CER und eIDAS

Verfahren 2025/0360(COD)



Status: Awaiting committee decision

- **Beratung in Parlament und Rat dauert an**
- Vorschläge sind daher noch nicht **verbindlich** und können sich **wesentlich ändern**

FIDES
Wir sind Vertrauen.

Erleichterung bei Meldungen (Datenschutz, Informationssicherheit)

Digital Omnibus Act

Erleichterung der Meldung an Aufsichtsbehörden

Eine Meldung ist nur erforderlich, wenn die Datenschutzverletzung voraussichtlich **ein hohes Risiko für die Rechte und Freiheiten** natürlicher Personen zur Folge hat.



72 Stunden



Die **Meldefrist** soll **von 72 auf 96 Stunden verlängert** werden.

Single-Entry-Point



Die materiellen Melde-tatbestände und Meldefristen der jeweiligen Rechtsakte bleiben grundsätzlich bestehen. Vereinheitlicht wird primär der technische Übermittlungsweg.

Bis zur Einrichtung des Single-Entry-Points sollen Meldungen weiterhin unmittelbar an die zuständige Datenschutzaufsichtsbehörde erfolgen.

FIDES
Wir sind Vertrauen.

Digital Omnibus, Cookies und Einwilligungsmanagement

Wesentliche Anforderungen an das Speichern und Auslesen personenbezogener Daten

Wesentliche Anforderungen an das Speichern und Auslesen personenbezogener Daten auf Endgeräten aus der ePrivacy-Richtlinie werden in die DSGVO überführt.



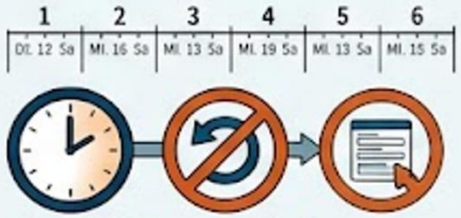
Nutzererfahrung und technische Umsetzung

Ein-Klick-Verfahren zur Ablehnung



Nutzer sollen Einwilligungsanfragen mit einem leicht verständlichen Ein-Klick-Verfahren ablehnen können.

2 Fristen nach Ablehnung



Nach Ablehnung soll eine erneute Anfrage für denselben Zweck grundsätzlich für mindestens sechs Monate ausgeschlossen sein.

3 Verbindliche technische Signale



Einwilligungs-signale

Ablehnung-ssignale

Maschinenlesbare Einwilligungs- und Ablehnungssignale sollen grundsätzlich **24 Monate nach Inkrafttreten verbindlich** werden;



für die technische Bereitstellung durch nicht als KMU einzuseranbieter ist eine Frist von **48 Monaten** vorgesehen.



nicht KMU

FIDES
Wir sind Vertrauen.

Digital-Omnibus 2025

Endgeräte. Einwilligung. Nutzererfahrung.

Weniger Cookie-Banner. Mehr nutzerseitige Kontrolle. Die wichtigsten Änderungen auf einen Blick.

Vorschlag der Europäischen Kommission
vom 19.11.2025
Änderungen u. a. bei Art. 88 ff. DSGVO

EIN EINFACHERES DIGITALES EUROPA

1 Systemwechsel: DSGVO statt Doppelregulierung



- Verarbeitung personenbezogener Daten **in und aus Endgeräten künftig direkt in der DSGVO (Art. 88a).**
- Art. 5 Abs. 3 ePrivacy-RL gilt für natürliche Personen insoweit nicht mehr, wie personenbezogene Daten betroffen sind.

2 Einwilligung bleibt der Grundsatz



- Speicherung personenbezogener Daten auf einem Endgerät oder Zugriff auf dort gespeicherte Daten **nur mit Einwilligung.**
- Ausnahmen nur in den in Art. 88a Abs. 3 DSGVO abschließend genannten Fällen.

3 Diese Zwecke sind einwilligungsfrei

- Übertragung elektronischer Kommunikation
- Ausdrücklich vom Nutzer verlangte Dienstleistung
- **Aggregierte** Reichweiten- und Nutzungsmessung (nur für eigene Nutzung)
- Sicherheit des Dienstes oder des Endgeräts

4 Ablehnen muss einfach sein



- Einwilligungsanfragen müssen mit einem **einzigen Klick** oder gleichwertigen Mitteln abgelehnt werden können (Art. 88a Abs. 4 lit. a).
- Keine manipulativen oder asymmetrischen Designs mehr.

5 „Nein" gilt mindestens 6 Monate



- Nach einer Ablehnung darf für denselben Zweck mindestens sechs Monate lang keine erneute Einwilligungsanfrage gestellt werden (Art. 88a Abs. 4 lit. c).
- Bei erteilter Einwilligung während der gültigen Einwilligungsdauer ebenfalls keine neue Abfrage (Art. 88a Abs. 4 lit. b).

6 Browser als Einwilligungsmanager



- Größere Browseranbieter müssen technische Mittel bereitstellen, mit denen Nutzer Einwilligungen erteilen, Anfragen ablehnen und den Werbewiderspruch (Art. 21 Abs. 2 DSGVO) ausüben können (Art. 88b Abs. 6).
- Ziel: Consent-Management von jeder einzelnen Website auf die Nutzerseite (z. B. Browser) verlagern.

7 Automatisierte und maschinenlesbare Signale



- Online-Schnittstellen müssen technisch ermöglichen, dass Nutzer ihre Entscheidungen (Einwilligung, Ablehnung, Widerspruch) automatisiert und maschinenlesbar übermitteln können (Art. 88b Abs. 1).
- Verantwortliche müssen diese Signale beachten (Art. 88b Abs. 2).
- EU-Standards durch Normungsorganisationen; bei Konformität Konformitätsvermutung (Art. 88b Abs. 4).

8 Sonderregel für Medienanbieter



- Mediendiensteanbieter sind bei der Bereitstellung eines Mediendinestes von den Pflichten nach Art. 88b Abs. 1 und 2 ausgenommen.
- Begründung: Sicherung der Online-Einnahmen für unabhängigen Journalismus.

Zeitplan (geplant)

- **6 Monate** nach Inkrafttreten: Anwendung von Art. 88a (Endgeräte/Einwilligung/Ausnahmen)
- **24 Monate** nach Inkrafttreten: Anwendung von Art. 88b Abs. 1 und 2 (maschinenlesbare Signale, Beachtung durch Verantwortliche)
- **48 Monate** nach Inkrafttreten: Pflichten größerer Browseranbieter gemäß Art. 88b Abs. 6

STARKE RECHTE. STARKE INNOVATION. EIN DIGITALER BINNENMARKT.

Hinweis: Darstellung basiert auf dem Kommissionsvorschlag COM(2025) 837 final vom 19.11.2025. Stand: 11/2025. Noch nicht geltendes Recht.

FIDES
Wir sind Vertrauen.

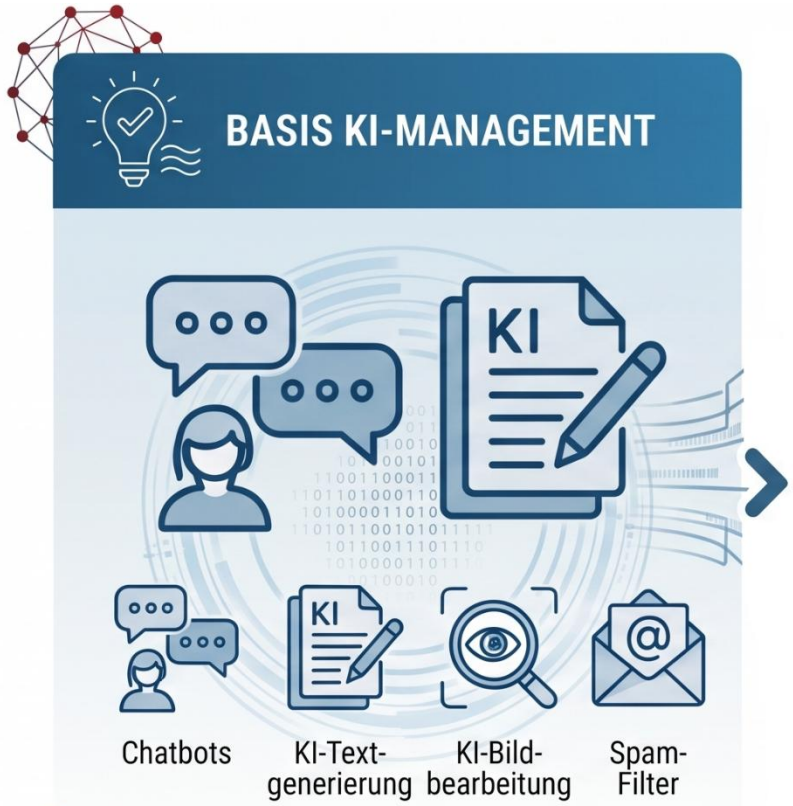


Inhalt

1. AI Omnibus Act
2. Digital Omnibus Act
3. KI-Management im Mittelstand
4. Einführung von KI und "Agentic AI" im Mittelstand

FIDES
Wir sind Vertrauen.

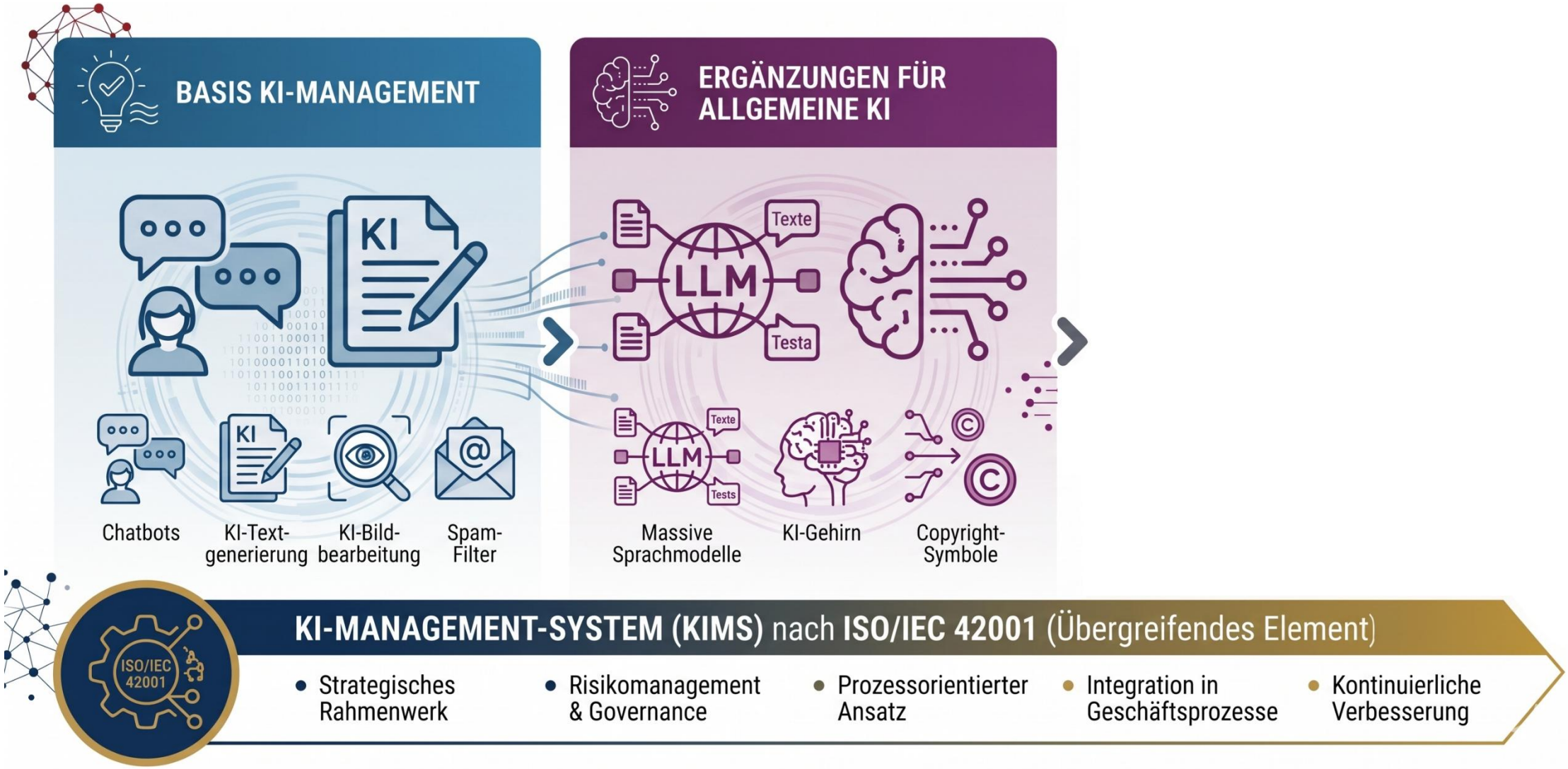
KI-Management: KI-Verordnung vs. ISO/IEC 42001





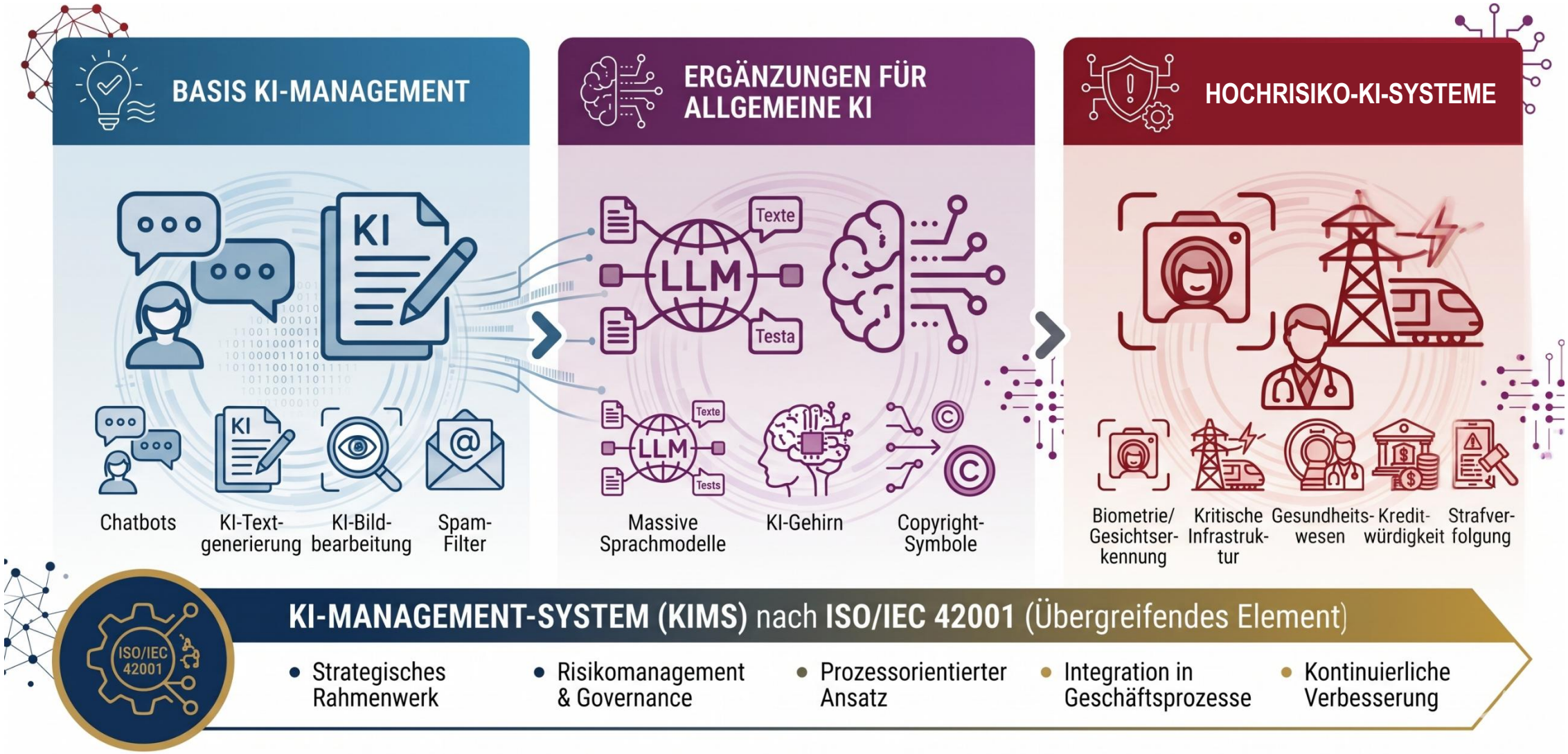
FIDES
Wir sind Vertrauen.

KI-Management: KI-Verordnung vs. ISO/IEC 42001



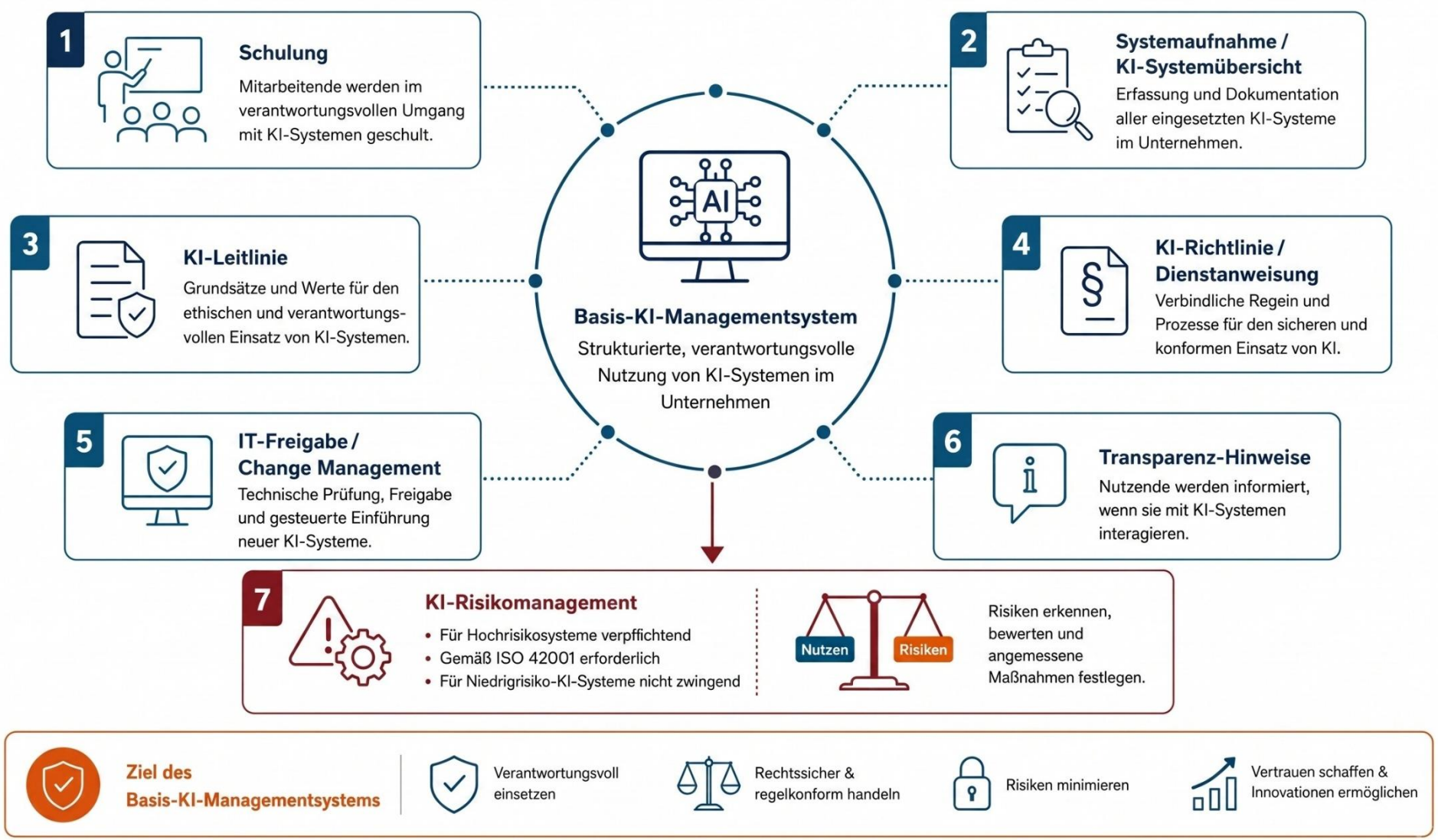
FIDES
Wir sind Vertrauen.

KI-Management: KI-Verordnung vs. ISO/IEC 42001



FIDES
Wir sind Vertrauen.

Basis-Anforderungen für unkritische KI-Systeme



Dieses Basis-KI-Managementsystem gilt für KI-Systeme, die nicht als Hochrisiko-KI-Systeme eingestuft sind.

FIDES
Wir sind Vertrauen.

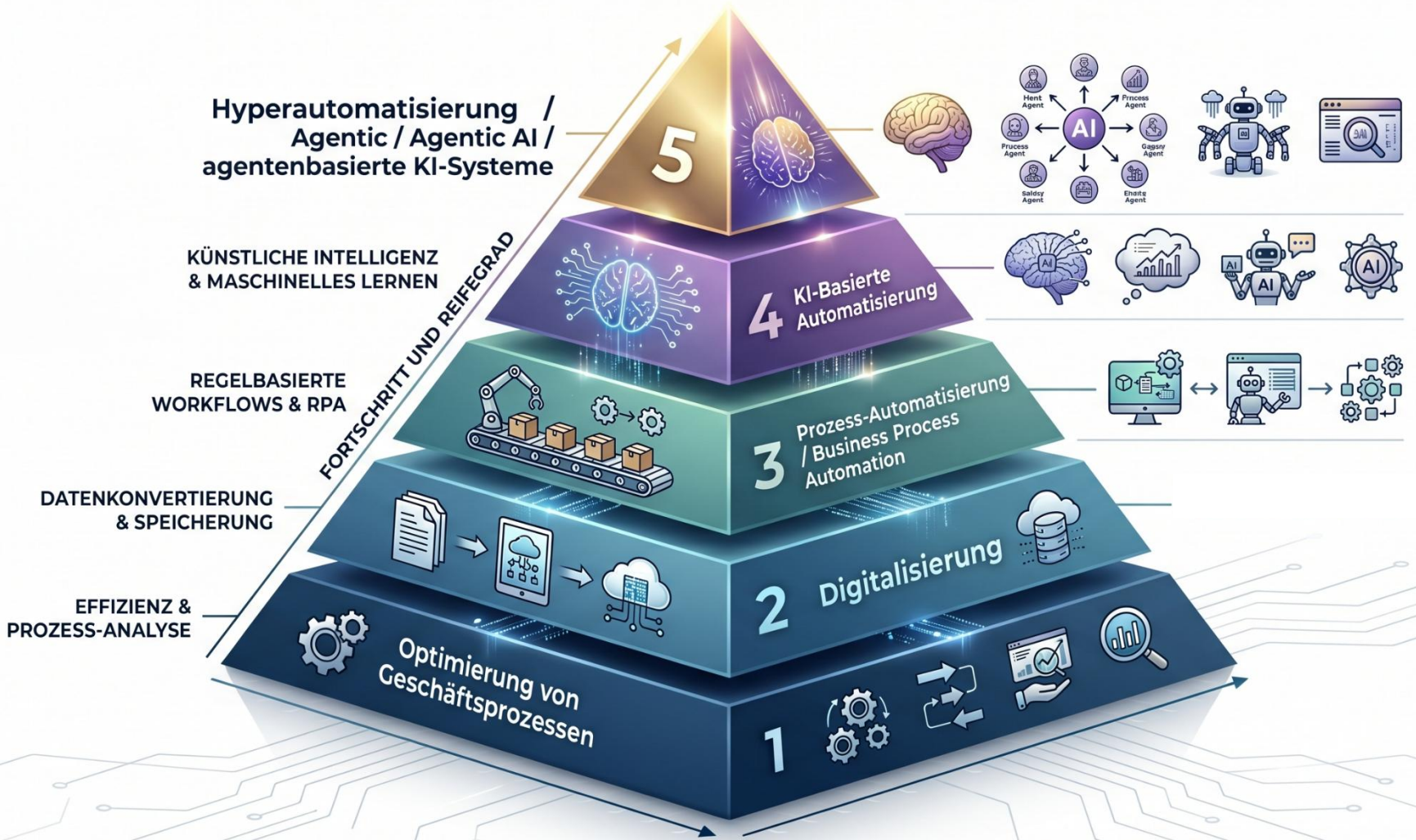


Inhalt

1. AI Omnibus Act
2. Digital Omnibus Act
3. KI-Management im Mittelstand
4. Einführung von KI und "Agentic AI" im Mittelstand

FIDES
Wir sind Vertrauen.

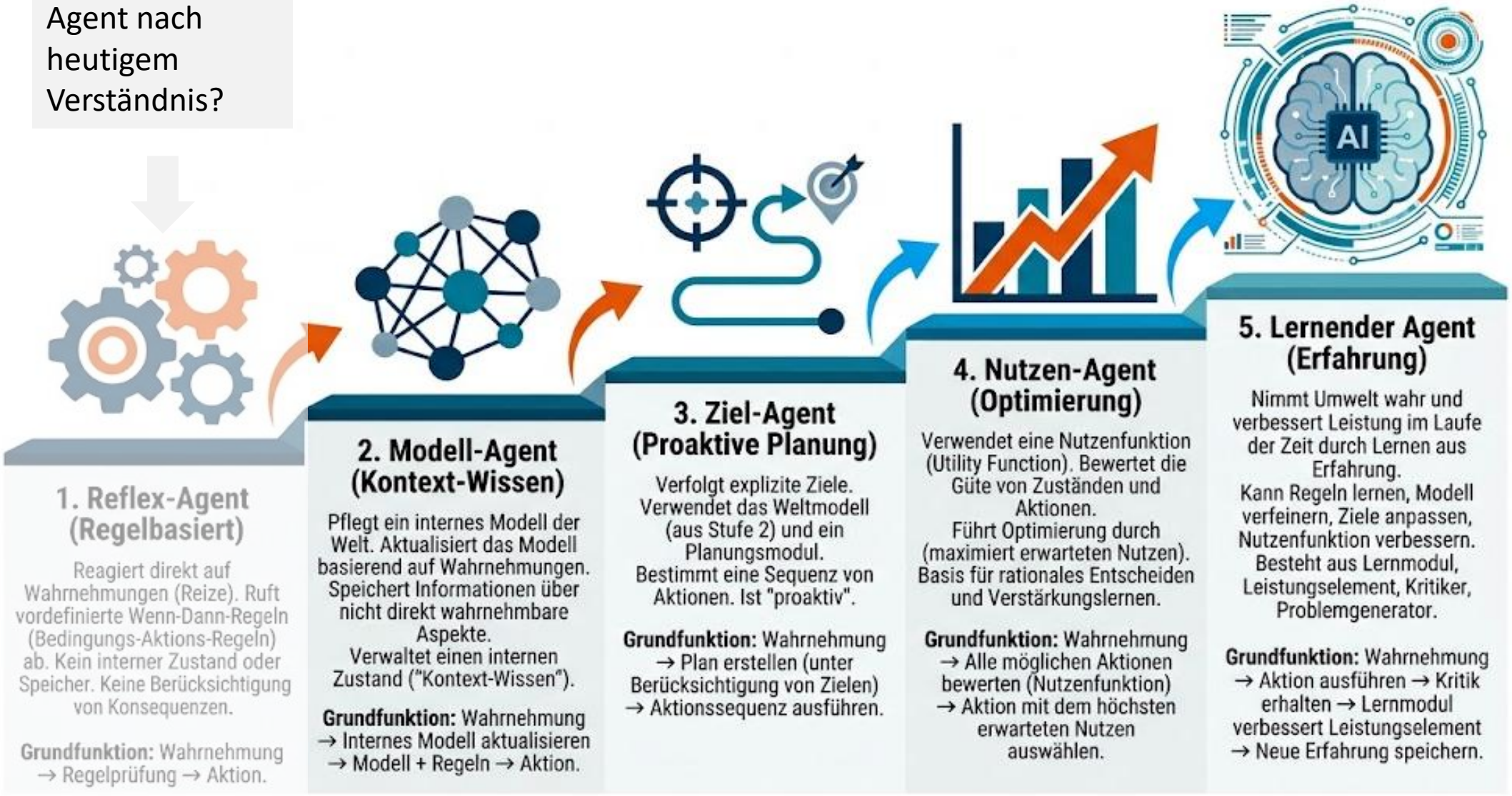
Digitale Transformation mit KI beginnt bei den Prozessen



FIDES
Wir sind Vertrauen.

Was ist Agentic AI?

Agent nach heutigem Verständnis?



Standard-Klassifizierung nach Russell & Norvig, "Artificial Intelligence: A Modern Approach"

FIDES
Wir sind Vertrauen.

Blue Print für eine KI-Strategie im Mittelstand

STUFE 1: INDIVIDUELLE PRODUKTIVITÄTS-ASSISTENZ (Copilot-Prompting)



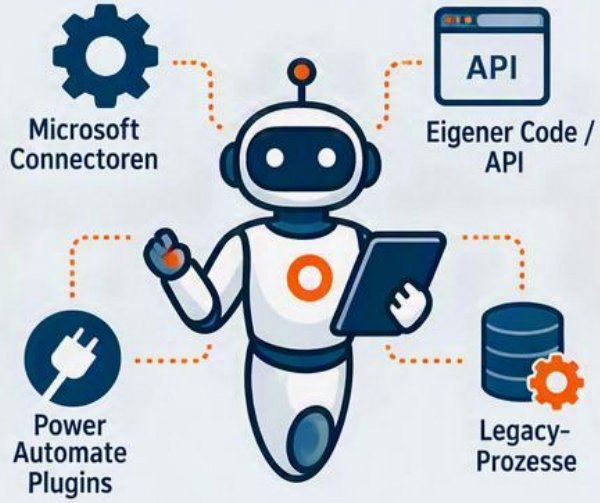
Microsoft Graph & Daten

Copilot / M365 Copilot

Microsoft Firmen-Daten (Shared Teams)

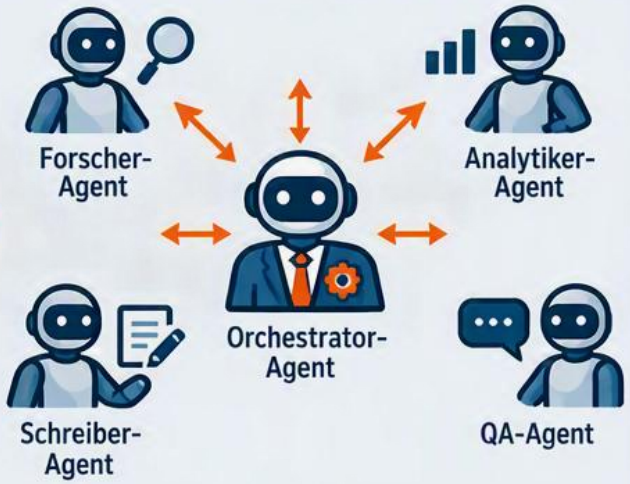
- Prompting im sicheren Unternehmenskontext
- Prompting in sicheren Unternehmensdaten
- RAG ohne Workflow-Logik

STUFE 2: PROZESS-ERWEITERUNG & INTEGRATION (Low-Code Agenten)



- Integration von KI in bestehende Altsysteme
- Sukzessive Ablösung oder Ergänzung von Nicht-KI-Prozessen
- Sichere Konnektoren

STUFE 3: VOLLSTÄNDIGE ORCHESTRIERUNG & AGENTIC SYSTEMS (Multi-Agent Workflows)



- Komplexe Geschäftsprozesse: koordinierte Agenten
- Mit spezifischen Aufgaben und KI-Governance-Kontrollen
- Copilot Plattform für Orchestrierung

INDIVIDUELLE PRODUKTIVITÄT → **PROZESSE ERWEITERN** → **DURCHGÄNGIGE ORCHESTRIERUNG**

LAYER 1: ÄNDERUNGSMANAGEMENT & MITARBEITER-QUALIFIZIERUNG FÜR AGENTIC AI (ADOPTION)

- Bewusstsein & Schulungen
- Low-Code Designer-Training & Rollen
- Kompetenz für AI Ops & Orchestrierung

LAYER 2: IT-SICHERHEIT & DATENSCHUTZ

- Datensicherheit in Unternehmenskontext (M365 DLP)
- Sichere Konnektoren, API-Gateway, Datenfluss-Kontrolle
- Validierung von Workflows, Audit-Trails, KI-Governance-Überwachung

FIDES
Wir sind Vertrauen.

FIDES
Wir sind Vertrauen.

Wirtschaftsprüfer | Steuerberater
IT-Berater | Unternehmerberater

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

FIDES IT Consultants GmbH

Dr. Ralf Kollmann

+49 174 9280 408

r.kollmann@fides-online.de





Dr. Ralf Kollmann



Geschäftsführer FIDES IT Consultants GmbH

+49 (421) 3013-408
r.kollmann@fides-online.de

Ein Gespräch bewegt mehr. Ihr Ansprechpartner

Kurzvita / Qualifikation

Als Geschäftsführer der FIDES IT Consultants GmbH liegt mein Tätigkeitsschwerpunkt in der IT-Beratung mit den Themen Informationssicherheit, Datenschutz sowie IT-Strategie und Einführung von KI-Systemen.

Darüber hinaus halte ich regelmäßig Seminare zu Themen der Informationstechnik bzw. KI und bin als Speaker auf Konferenzen und Fachveranstaltungen tätig.

- Eintritt FIDES 2005
- Diplom-Informatiker
- Diplom-Wirtschaftsinformatiker (Studienschwerpunkt Unternehmensrecht)
- Dr.-Ing. (Promotion im Bereich Softwaretechnik und Datenbanksysteme)

Tätigkeitsfelder

- IT-Strategie und IT-Compliance
- Datenschutz und Informationssicherheit
- Business Continuity Management
- KI-Strategie und KI-Compliance
- Einführung von KI-Systemen

FIDES
Wir sind Vertrauen.

FIDES
Wir sind Vertrauen.

Wirtschaftsprüfer | Steuerberater
IT-Berater | Unternehmerberater

FIDES IT CONSULTANTS GMBH

HAUPTNIEDERLASSUNG
Birkenstraße 37
28195 Bremen
Telefon +49 (421) 3013-400
Fax +49 (421) 3013-449
it@fides-online.de
www.fides-online.de

ZWEIGNIEDERLASSUNG
Hamburg

NÖLLE & STOEVESANDT
Rechtsanwälte -
Partnerschaftsgesellschaft mbB
Birkenstraße 37
28195 Bremen
Telefon +49 (421) 3013-165
Fax +49 (421) 3013-166
info@noelle-stoevesandt.de
www.noelle-stoevesandt.de

FIDES TREUHAND GMBH & CO. KG
Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

HAUPTNIEDERLASSUNG
Birkenstraße 37
28195 Bremen
Postfach 10 57 27
28057 Bremen
Telefon +49 (421) 3013-0
Fax +49 (421) 3013-100
bremen@fides-online.de
www.fides-online.de

ZWEIGNIEDERLASSUNGEN
Berlin
Bremerhaven
Hamburg
Hannover
Osnabrück

FIDES CORPORATE FINANCE GMBH
Wirtschaftsprüfungsgesellschaft
Birkenstraße 37
28195 Bremen
Telefon +49 (421) 3013-400
Fax +49 (421) 3013-449
unternehmerberater@fides-online.de
www.fides-online.de