



IHRE WIRTSCHAFTSKANZLEI



KI-Compliance für Finanzunternehmen – Aktuelles zu KI-VO, Datenschutz, Finanzaufsicht

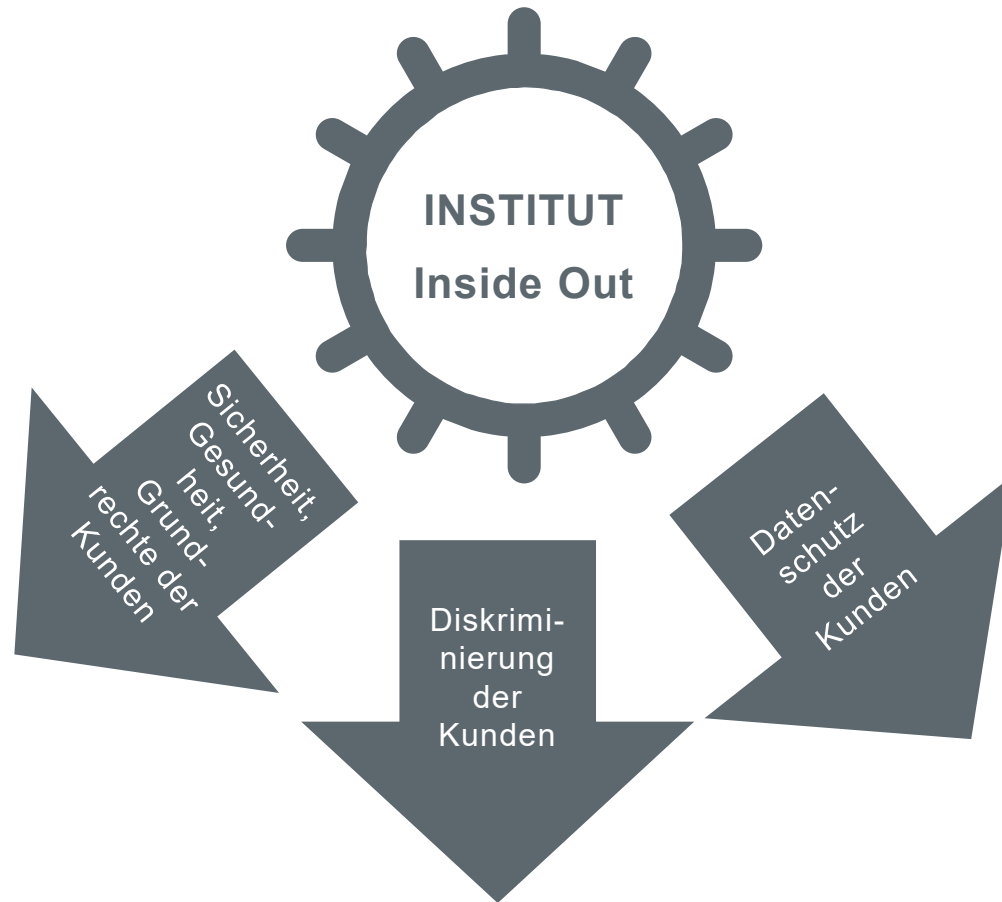
GÖRG KI-Forum | 10. September 2026

Dr. Matthias Terlau | Dilan Mienert | Dr. Valentin Zipfel

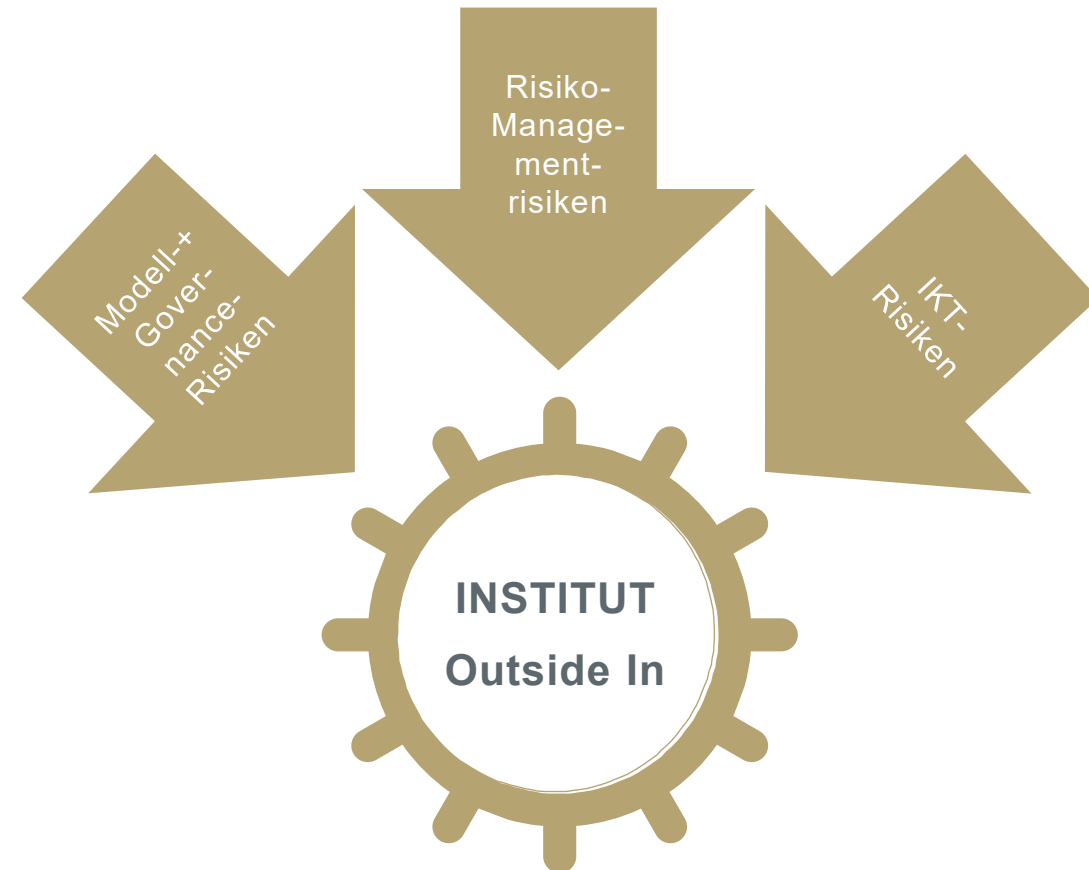
Agenda

- Überblick
- KI-Verordnung – nationale Umsetzung
- Datenschutz
- Finanzaufsicht
- Handlungsempfehlungen

Die verschiedenen Perspektiven der Regulierung von KI-Risiken



KI-Verordnung, AGG, CCD2, DSGVO



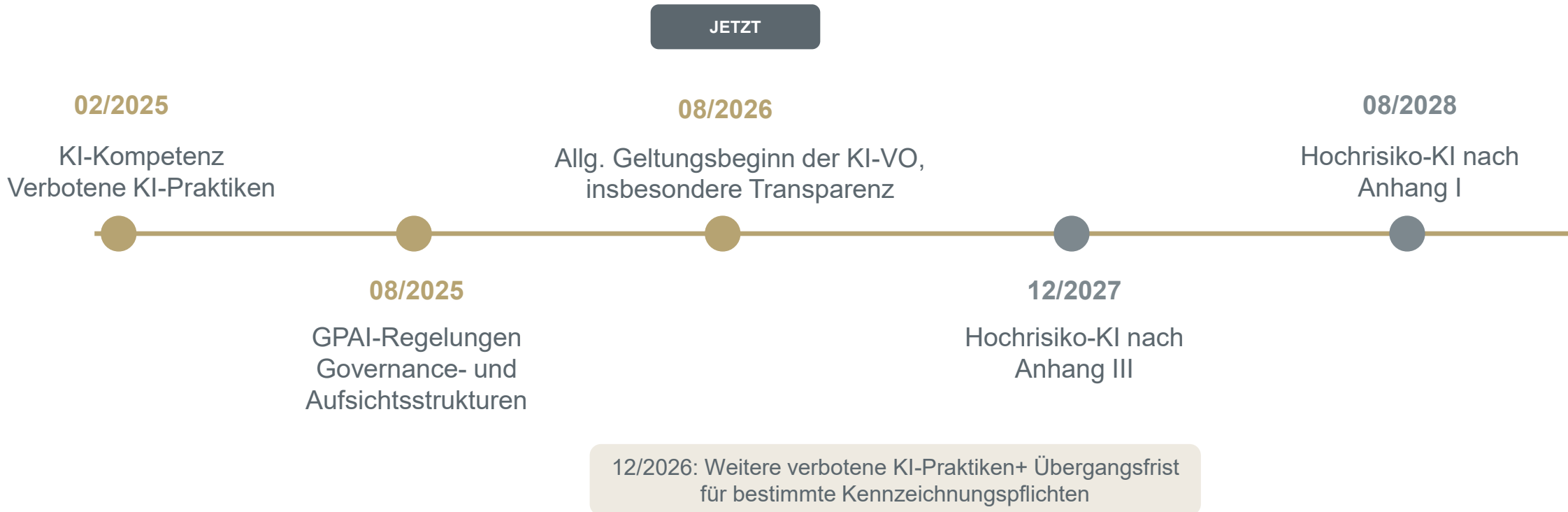
§ 25a KWG, § 27 ZAG, MaRisk, DORA

01

KI-VO

KI-VO: Anwendungszeitpunkte und Übergangsfristen

Digital-Omnibus seit 27. Juli 2026: Hochrisiko-Pflichten auf 2027 / 2028 verschoben



Kernaussage: Nicht „alles seit August 2026“ – sondern Pflichtenpakete mit unterschiedlichen Startpunkten.

Leitlinien, Verhaltenskodizes und Standards

Begriffe & Verbote

KI-System-Definition
(Feb. 2025)

final

Verbotene Praktiken
(Feb. 2025)

final

Generative KI / GPAI

GPAI-Leitlinien + Kodex
(Juli 2025)

final

Art.-50-Leitlinien (Juli 2026)
Transparenzkodex (Juni 2026)

final

Hochrisiko & Umsetzung

Hochrisiko-Klassifizierung
Entwurf (Mai 2026)

Entwurf

Harmonisierte Standards
in Entwicklung

in
Arbeit

1 Recht

KI-VO + Digital-Omnibus

2 Auslegung

Leitlinien / Q&As / Verhaltenskodizes

3 Technik

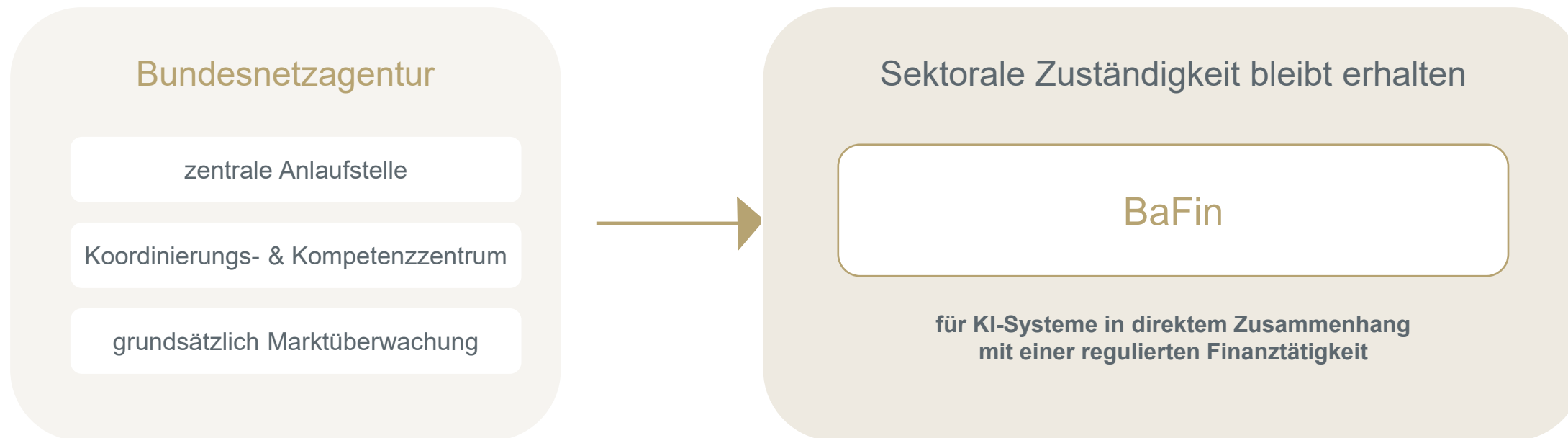
Harmonisierte Standards und technische Nachweise

Umsetzung entsteht heute aus Gesetz, Auslegung und technischen Nachweisen.

Umsetzung und Aufsicht in Deutschland

seit 29.07.2026

KI-MIG ordnet Zuständigkeiten und Zusammenarbeit



Leitidee: zentrale Koordination – sektorale Aufsicht nach Sachnähe und bestehenden Strukturen.

KI-Governance: praktische Anforderungen für Banken

1

Inventar & Klassifizierung

Welche KI nutzen wir – und wofür?

2

Rollen & Lieferkette

Anbieter / Betreiber / Drittanbieter sauber trennen

3

KI-Kompetenz & Nutzungsregeln

risikobasiert schulen, erlaubte Nutzung definieren

4

Bestehende Governance nutzen

Risikomanagement, Compliance, DORA / Auslagerung und IKS verzahnen

Hochrisiko-Vorbereitung parallel aufbauen → z. B. Kreditwürdigkeitsbewertung natürlicher Personen: Pflichten ab 02.12.2027

KI-Kompetenz gilt bereits seit 2025; Art.-50-Transparenzpflichten seit August 2026.

02 | DSGVO und BDSG

Ausgangspunkt: drei EuGH-Urteile

C-634/21

07.12.2023 · SCHUFA (Scoring)

Schon die automatisierte Score-Erstellung ist eine „Entscheidung“ nach Art. 22 Abs. 1 DSGVO, sofern davon maßgeblich die Kreditvergabe oder Vertragsentscheidung eines Dritten abhängt.

„Auslöser“ für § 37a BDSG

C-203/22

27.02.2025 · Dun & Bradstreet

Anspruch auf Erläuterung des konkret angewandten Verfahrens bei automatisierter Bonitätsprüfung (Credit Scoring). Information darüber, wer Urheber des Score-Wertes ist.

C-413/23 P

04.09.2025 · EDSB / SRB

Ob Daten „personenbezogen“ sind, hängt von der jeweiligen Stelle ab. Für den Übertragenden (der über den Schlüssel zur Re-Identifizierung verfügt), bleiben pseudonymisierte Daten personenbezogen.

Noch offen: Ist bereits die Einschränkung der Zahlungsarten aufgrund automatisierter Bonitätsprüfung – auch bei internem Scoring – eine Entscheidung i.S.d. Art. 22 Abs. 1 DSGVO? Vorlage OGH v. 13.8.2025 – 6 Ob 15/25m.

§ 37a BDSG n.F. (Auszug)

(1) Das Recht gemäß Art. 22 Abs. 1 DSGVO, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, besteht über die in Art. 22 Abs. 1 a) und c) DSGVO genannten Ausnahmen hinaus nicht, wenn zu einer natürlichen Person Wahrscheinlichkeitswerte erstellt oder verwendet werden über

- Nr. 1 ein bestimmtes zukünftiges Verhalten der Person zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dieser Person oder
- Nr. 2 ihre Zahlungsfähig- und -willigkeit durch Auskunftfeien und unter Einbeziehung von Informationen über Forderungen.

(...)

§ 37a BDSG n.F. – die Antwort des Gesetzgebers

20.11.
2026

zeitgleich mit den verschärften
§§ 505a, 505b BGB und § 18a KWG

1

Fundstelle

Art. 3 Nr. 4 des Gesetzes v. 12.5.2026 zur Umsetzung der EU-Verbraucherkreditrichtlinie (CCD 2)

2

Weg ins Gesetz

Kabinettsbeschluss 7.2.2024 → BT-Drs. 20/10859 → Diskontinuität
→ Umsetzung im Verbraucherkreditgesetz

3

Rechtsnatur

Keine Rechtsgrundlage. Rechtsgrundlage bleibt Art. 6 DSGVO – § 37a BDSG n.F. nimmt nur aus dem Verbot des Art. 22 DSGVO heraus.

§ 31 BDSG entfällt zeitgleich.

§§ 505 a und 505b BGB sowie § 18a KWG (Kreditvergabe)

Anwendungsbereich und die vier Datenverbote

Abs. 1 – Wen es (be-)trifft

- Nr. 1 – Prognose künftigen Verhaltens für Vertragsentscheidungen. Nicht auf Auskunftseien beschränkt: erfasst internes Scoring, Verhaltens- und Betrugsscoring.
- Nr. 2 – Zahlungsfähigkeit und -willigkeit durch Auskunftseien unter Einbeziehung von Forderungen.

Abs. 2 Nr. 2 und Nr. 3 lit. a

Keine Minderjährigen. Merkmale müssen mit wissenschaftlich anerkanntem Verfahren nachweisbar erheblich sein – faktisch eine Erklärbarkeitspflicht.

Abs. 2 Nr. 1 – nicht nutzbare Daten

- a) Art. 9-DSGVO-Daten
- b) Alter, Geschlecht, Name, Social-Media-Daten
- c) **Zahlungsein- und -ausgänge auf Bankkonten**
- d) **Anschriftendaten**

Kontodatenbasierte Bonitätsmodelle und Geo-Scoring lassen sich auf § 37a BDSG nicht mehr stützen – für die Kreditwürdigkeitsprüfung nach § 505b BGB bleiben Kontodaten aber nutzbar.

Transparenz- und Interventionsrechte

Abs. 4 – Auskunft auf Antrag, Frist des Art. 12 Abs. 3 DSGVO

- genutzte personenbezogene Daten und Kriterien
- Gewichtung der Kategorien und der Einzelkriterien zueinander, die den Wert am stärksten beeinflussen
- Aussagekraft des konkreten Wahrscheinlichkeitswerts
- erstellte Werte und ihre Empfänger

Speicherungspflicht: 1 Jahr → Protokollierung der Score-Bildung auf Einzelfallebene

Abs. 5 – Interventionsrechte

Anfechtung · Darlegung des eigenen Standpunkts · Entscheidung einer natürlichen Person

Digital Omnibus – zwei Pakete



KI-Omnibus

- VO (EU) 2026/1744
- ABl. 24.7.2026, in Kraft seit 27.7.2026
- **Geltendes Recht**



Datenomnibus (Datenrecht)

- COM(2025) 837 v. 19.11.2025 – DSGVO, ePrivacy, Data Act, NIS 2
- Art. 4 Nr. 1 DSGVO: relativer Personenbezug
- Art. 22 DSGVO: „hat das Recht“ entfällt – Ziel ist die automatisierte Kreditentscheidung
- Berechtigtes Interesse für KI-Training
- **Trilog nicht begonnen – Q4/2026 oder später**

EDSA/EDSB, Gemeinsame Stellungnahme 2/2026 v. 11.2.2026: Vereinfachung ja – aber klare Ablehnung der Neudefinition des Personenbezugs; auch der Rat ist zurückhaltend.

03

Outside In – die Risiken der Banken

MaRisk-Novelle 2026 zu KI-Risiken

**AT 4.3.4 NEU:
KI-gestützte Modelle
im Rahmen des
Risikomanagements**

Modelle zur Kredit-
vergabe u -bearbeitung
(z.B. Scoring)

Modelle zur
Risikoklassifizierung

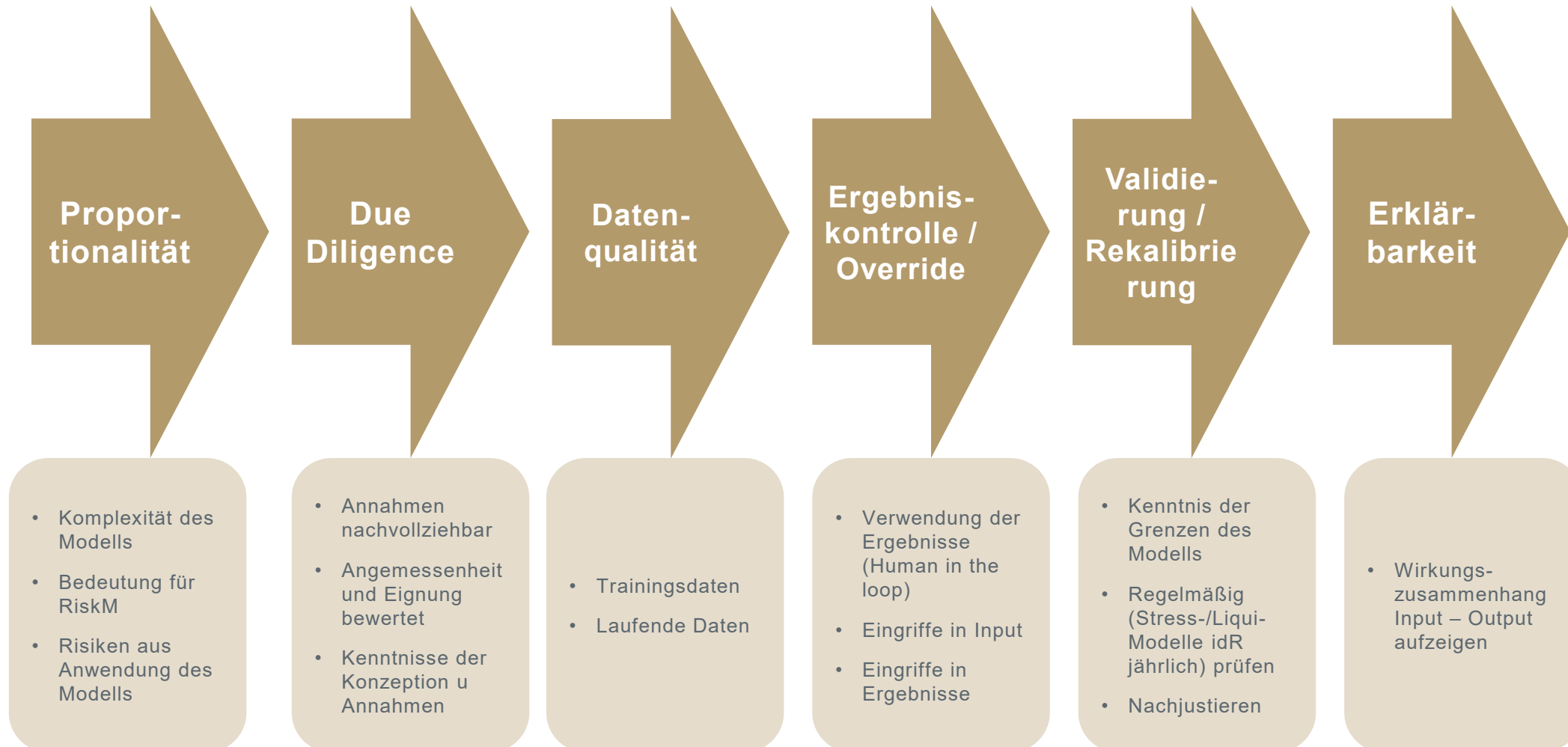
Modelle zur
Risikoquantifizierung

Modelle für
Stresstests

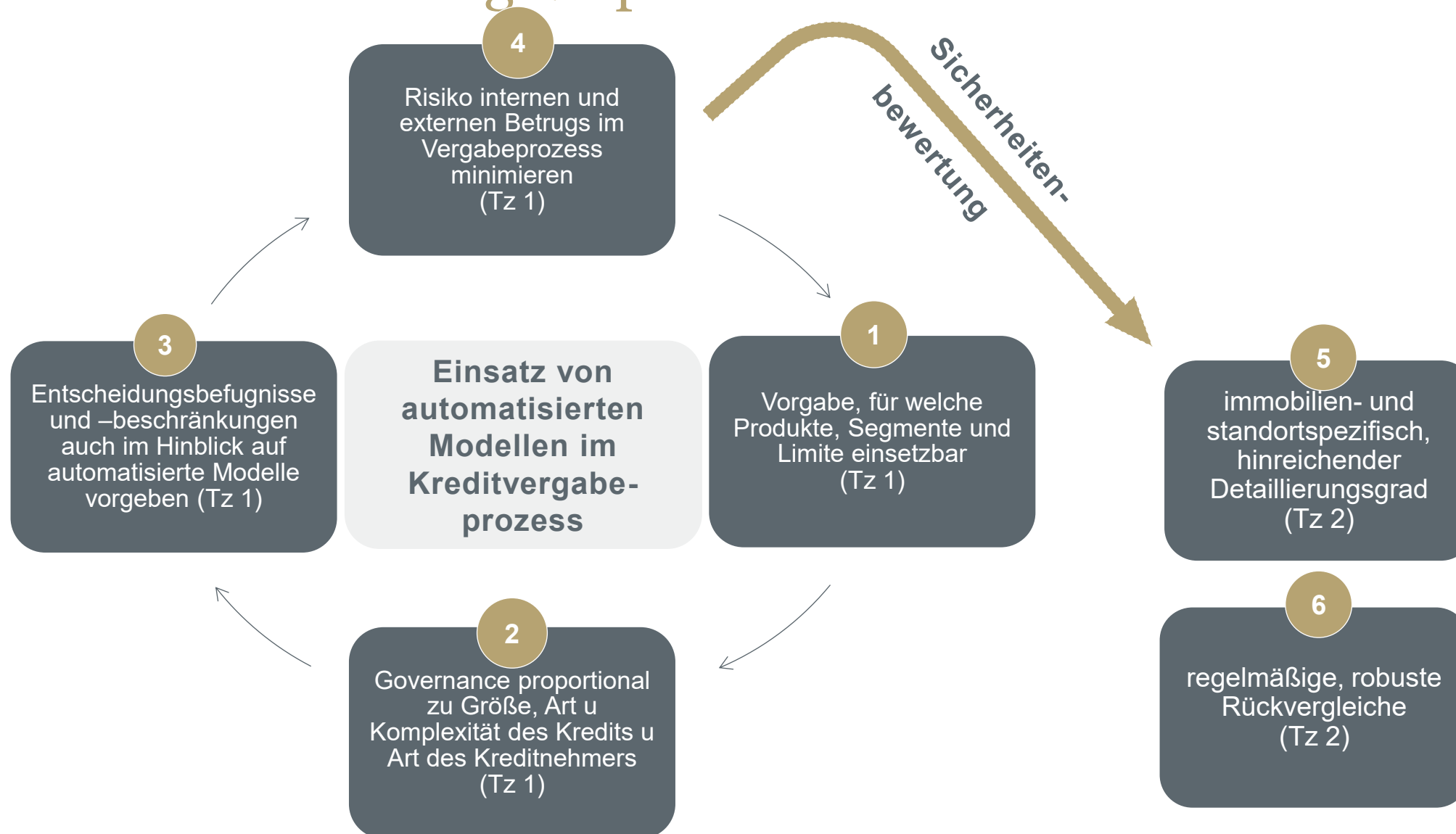
Bewertungs- und
Preisbildungsmodelle

„Ein Modell ist eine quantitative Methode, ein System oder ein Ansatz, der statistische oder mathematische Theorien, Techniken und Annahmen anwendet, um Eingabedaten zu quantitativen Schätzungen zu verarbeiten.“

AT 4.3.4 MaRisk-Novelle 2026 – Anforderungen an KI-Governance



BTO 1.2 MaRisk-Novelle 2026 – Modelle für Kreditvergabeprozess



DORA - Prozesse für KI-Systeme von der „Wiege“ bis zur „Bahre“

- KI-Systeme als **eigenes IKT-Asset**
- Betrachtung des gesamten **KI-Lebenszyklus**
- **Identifikation** und **Dokumentation** – **Explainable AI**
- **Kapazitäten** und **Leistung** des KI-Systems überprüfen
- Errichtung von Vorgaben für die **Deinstallation**
- **Angriffe** auf das KI-System vorhersehen, erkennen
- **Früherkennung** von Anomalien
- **IKT-Geschäftsfortführungsmanagement**: Reaktion, Wiederherstellung und Backup
- **Meldung** von schwerwiegenden IKT-Vorfällen
- **IKT-Dienstleister** (insbesondere Cloud) – Risiken managen



Vielen Dank für Ihre Aufmerksamkeit!

GÖRG

IHRE WIRTSCHAFTSKANZLEI



Dr. Matthias Terlau

Partner

T:+49 221 33660 470

E:mterlau@goerg.de



Dilan Mienert

Rechtsanwältin | Assoziierte Partnerin

T:+49 30 884503 143

E:dmienert@goerg.de



Dr. Valentin Zipfel

Rechtsanwalt | Assoziierter Partner

T:+49 69 170000 202

E:vzipfel@goerg.de