

KI-ready?

Fachinfo zur KI-Compliance
Januar 2026



Sehr geehrte Damen und Herren,

75 % der Vorstände geben an, bereits KI-Werkzeuge zu verwenden (Quelle: www.dz-cp.de/ki-ready). In der Praxis dürfte der Anteil sogar deutlich höher liegen: Nahezu jede Bank nutzt das KI-Modul der Google-Suche oder hat den Microsoft Copilot im MS365 im Einsatz.

Unsere Erfahrung als Mehrmandantendienstleister ist, dass Banken - bewusst oder unbewusst - mehr KI-Technologien im Zugriff bzw. Einsatz haben, als vielleicht zunächst vermutet. Und: **Der aufsichtskonforme Einsatz von KI ist machbar.** Die wichtigsten Stellschrauben sind nachfolgend zusammengefasst.

KI mit System einführen: effizient und nachvollziehbar

Ein regelkonformer Einsatz von KI beginnt mit grundlegender Transparenz: Welche Systeme sind im Einsatz, wie kritisch sind diese aus regulatorischer Sicht – und welche Verantwortung trägt Ihr Institut konkret?

Bewährt haben sich die folgenden drei Schritte für einen sicheren und regelkonformen KI-Einsatz – die im Übrigen auch in Prüfungen zunehmend im Fokus stehen.

1. Vollständiges KI-Inventar erstellen

Erfassen Sie sämtliche im Institut eingesetzten KI-Systeme – einschließlich Pilotanwendungen, Fachbereichslösungen und externer Cloud- oder SaaS-Tools. Dokumentieren Sie insbesondere, welche Daten verarbeitet werden (z. B. Kunden-, Mitarbeiter- oder Risikodaten). Tipp: Schauen Sie in den Informationsverbund

in der Informationssicherheit / ITK-Risikomanagement nach. Suchen Sie dort die IKT-Assets/Objekte mit KI-Bezug.

2. Einordnung in die Risikokategorien der KI-Verordnung vornehmen

Ordnen Sie jedes KI-System den in der KI-Verordnung vorgesehenen Risikoklassen zu. Gerade im Bankenumfeld sind Anwendungen mit Bezug zu Kreditentscheidungen, Betrugsprävention oder Personalprozessen häufig besonders kritisch.

3. Rolle Ihres Instituts nach der KI-Verordnung klären

Prüfen Sie, ob Ihr Institut als Anbieter, Betreiber oder in einer kombinierten Rolle auftritt. Diese Einordnung ist maßgeblich für Governance-Anforderungen, Dokumentationspflichten, Kontrollmechanismen und Haftungsfragen. >

Checkliste KI-Einführung

Die folgenden Fragen helfen Ihnen, wichtige Aspekte in der KI-Bestandsaufnahme und Umsetzung der KI-VO frühzeitig zu berücksichtigen.

Hinweis: Diese Checkliste ersetzt keine Rechtsberatung, unterstützt jedoch dabei, Risiken systematisch zu identifizieren und priorisiert anzugehen.

	Ja	Nein
A. Transparenz		
1. Sind alle KI-Systeme im Institut zentral erfasst – inklusive dezentraler Fachbereichslösungen?		
2. Ist dokumentiert, welche bank- und personenbezogenen Daten durch KI verarbeitet werden?		
B. Regulatorische Einordnung		
3. Wurden alle KI-Systeme korrekt nach den Risikokategorien der KI-Verordnung eingestuft?		
4. Sind die jeweiligen Pflichten aus KI-VO, DSGVO, DORA und Bankaufsichtsrecht eindeutig zugeordnet?		
C. Governance		
5. Sind Rollen und Zuständigkeiten (z. B. Fachbereich, IT, Datenschutz, Compliance) klar definiert?		
6. Existiert ein Freigabeprozess für neue KI-Anwendungen und Modelländerungen		
D. Betrieb		
7. Werden KI-Ergebnisse vor ihrem Einsatz fachlich geprüft (Vier-Augen-Prinzip)?		
8. Sind Protokollierung, Nachvollziehbarkeit und Audit-Trails sichergestellt?		

Sie haben Fragen?

Wir freuen uns auf den Austausch mit Ihnen.
Sprechen Sie uns an!

Mit herzlichen Grüßen



Ihr Björn Blechenberg

Bereichsleiter Marketing & Vertrieb

Telefon: 069 580024-172

E-Mail: bjoern.blechenberg@dz-cp.de,
vertrieb@dz-cp.de



Ihr Benjamin Wellnitz

Bereichsleiter IKT-Compliance & Datenschutz

Telefon: 069 580024-246

E-Mail: benjamin.wellnitz@dz-cp.de

P. S. Weitere Informationen zum sicheren Einsatz von KI im Bankenumfeld finden Sie auch online:

<https://www.dz-cp.de/ki-ready>