#freiraumsichern

Eine Publikation der DZ CompliancePartner GmbH
November 2025

Regulativ sichere Einführung von Künstlicher Intelligenz – Orientierung für Finanzinstitute

Künstliche Intelligenz ist längst im Finanzsektor angekommen: Von der automatisierten Analyse großer Datenmengen über Chatbots bis zu generativen Sprachmodellen wie ChatGPT – viele Mitarbeitende setzen bereits KI-Tools ein, häufig ohne sich der **rechtlichen, regulatorischen und haftungsrechtlichen Folgen** bewusst zu sein.

Mit dem **EU-AI-Act** (KI-Verordnung), der **Datenschutz-Grundverordnung** (DSGVO), den **Bankaufsichtlichen Anforderungen an die IT** (BAIT) sowie den **Mindestanforderungen an das Risikomanagement** (MaRisk) stehen Banken und Finanzdienstleister nun vor einer neuen Herausforderung:

KI-Anwendungen müssen **technisch beherrschbar, auditierbar, transparent und rechtskonform** implementiert werden – andernfalls drohen aufsichtsrechtliche Sanktionen, Bußgelder nach Art. 83 DSGVO, Reputationsschäden und Haftungsrisiken.

Diese Checkliste mit **15 Kernfragen,** ermöglicht es, den **Status quo der KI-Nutzung** im eigenen Haus zu bewerten und zentrale Risiken frühzeitig zu identifizieren.

Die Fragen decken unter anderem folgende Prüfungsfelder ab:

- **Datenschutz & Informationssicherheit** (Rechtsgrundlagen nach Art. 6 DSGVO, Auftragsverarbeitung, Datenminimierung), IKT-Asset-Risikobewertung
- **Bankaufsichtsrechtliche Anforderungen** (DORA, MaRisk AT 7.2 Modellrisikomanagement),
- **AI-Act-Konformität** (Risikoklassifizierung, Transparenz- und Dokumentationspflichten),
- **Haftung & IP-Rechte** (Urheberrecht, Markenrecht, Verantwortlichkeit bei KI-Entscheidungen),
- **Governance & Verantwortlichkeiten** (Einrichtung einer KI-Policy, Benennung eines KI-Officers, Schulung von Mitarbeitenden).

KI-ready?

15 Kernfragen helfen dabei, sich zu Überlick zum Status quo zur KI-Nutzung zu verschaffen. Wenden Sie sich gerne an uns, wenn wir Ihnen mit Ihren Antworten weiterhelfen können.

	Ja	Nein
A. Bestandsaufnahme		
1. Werden in Ihrem Unternehmen bereits KI-Tools genutzt (inkl. Pilotprojekte)?	☐	☐
2. Werden dabei personenbezogene Daten verarbeitet (Kunden, Mitarbeitende, Bewerber)?	☐	☐
3. Werden Daten an Drittanbieter übermittelt (Cloud-/SaaS-Tools), und sind Auftragsverarbeitungsverträge (Art. 28 DSGVO) abgeschlossen?	☐	☐
B. Datensicherheit & Geheimhaltung		
4. Geben Mitarbeitende vertrauliche Informationen (z. B. Geschäftsgeheimnisse, interne Dokumente) in KI-Tools ein?	☐	☐
5. Gibt es interne Policies, welche Informationen in KI-Systeme eingegeben werden dürfen?	☐	☐
C. Governance & Strategie		
6. Existiert eine KI-Strategie mit klaren Zielen und Risikobewertung?	☐	☐
7. Sind Verantwortlichkeiten (KI-Officer, Datenschutz, IT-Sicherheit) definiert?	☐	☐
8. Gibt es eine freigegebene KI-Tool-Liste und einen Prozess zur Zulassung neuer Tools?	☐	☐
D. Compliance & Recht		
9. Liegen für alle KI-Anwendungen Rechtsgrundlagen vor (DSGVO, EU-AI-Act, DORA, Bankaufsichtsrecht)?	☐	☐
10. Wird KI-generierter Content immer durch Menschen geprüft, bevor er verwendet wird (Haftungsprävention)?	☐	☐
11. Gibt es Verfahren, um Rechte Dritter (Urheberrecht, Markenrecht) zu wahren?	☐	☐
12. Werden Audit-Trails/Protokolle geführt, um Entscheidungen nachvollziehbar zu machen?	☐	☐
E. Risiko- und Notfallmanagement		
13. Existiert ein Incident-Response-Plan, falls KI-Entscheidungen fehlerhaft oder rechtswidrig sind?	☐	☐
14. Werden neue KI-Tools vor Einsatz auf Bias, Diskriminierung und Modellrisiken geprüft?	☐	☐
15. Sind Mitarbeitende zu Datenschutz, Prompt-Security und AI-Ethik geschult?	☐	☐

Die Checkliste dient als Grundlage für **interne Audits, Risikoanalysen und Compliance-Prozesse** und unterstützt Entscheidungsträger bei der Entwicklung einer nachhaltigen **KI-Governance-Strategie.** Sie ersetzt keine Rechtsberatung, liefert aber einen strukturierten Rahmen, um regulatorische Pflichten zu identifizieren, Risiken zu priorisieren und Handlungsbedarf klar zu benennen.

DZ ComliancePartner steht Ihnen darüber hinaus als Partner für KI-Produkte und Compliance-Beratung zur Seite – von der technischen Implementierung bis zur juristisch abgesicherten Ausgestaltung Ihrer KI-Projekte. Gerne begleiten wir Sie bei der Umsetzung der notwendigen Maßnahmen für einen rechts- und aufsichtskonformen KI-Einsatz in Ihrem Institut.

Haben Sie Fragen oder wünschen weitere Informationen? Melden Sie sich gerne bei uns.

Wir werden in regelmäßigen Abständen über weitere Aufgaben aus der KI-Verordnung berichten und praxisorientierte Arbeitshilfen zur Verfügung stellen. Wenn Sie interessiert sind, schreiben Sie uns eine E-Mail mit dem Betreff „ KI-VO auf dem neuesten Stand“ an vertrieb@dz-cp.de. wir werden Sie in unseren Verteiler aufnehmen und Ihnen Arbeitshilfen und Hinweise via E-Mail zusenden.

DZ CompliancePartner GmbH
Herr Benjamin Wellnitz

Telefon: 069 580024-246
Fax: 069 580024-900
E-Mail: benjamin.wellnitz@dz-cp.de

Herausgeber: DZ CompliancePartner GmbH, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 580024-0, Telefax 069 580024-900, www.dz-cp.de, Handelsregister HRB 11105, Amtsgericht Offenbach, USt.-IdNr.: DE201150917, Geschäftsführung: Jens Saenger (Sprecher), Dirk Pagel