

KI-ready?

Fachinfo zur KI-Compliance
Februar 2026



Sehr geehrte Damen und Herren,

mit dem zunehmenden Einsatz von KI rückt eine zentrale Frage in den Fokus: **Wie stehen Datenschutz-Grundverordnung (DSGVO) und KI-Verordnung (KI-VO) eigentlich zueinander?**

Die KI-VO setzt dort an, wo die DSGVO endet – beim System selbst:

Sobald KI-Systeme personenbezogene Daten verarbeiten (z. B. Kunden-, Mitarbeiter- oder Trainingsdaten), gilt die DSGVO vollumfänglich. Besonders relevant sind dabei u. a. Zweckbindung, Datenminimierung, Transparenz, Datenqualität, Vertraulichkeit und Sicherheit.

Die KI-VO geht über die Regelungen der DSGVO hinaus und regelt spezifische Aspekte der eingesetzten KI-Systeme. Die Anforderungen an Transparenz, Nachvollziehbarkeit und Datenqualität werden in Bezug auf den Einsatz von KI-Systemen spezifisch geregelt:

- ▶ Die KI-VO regelt den Einsatz von KI-Systemen, indem sie Risikoklassen definiert - viele KI-Anwendungen im Bankenumfeld implizieren gemäß KI-VO ein „hohes Risiko“ (z. B. Kreditentscheidungen oder auch Betrugsprävention).
- ▶ Mit der jeweiligen Risikoklassifizierung sind entsprechende Pflichten verbunden - wie z. B. die Einrichtung eines Risiko-Managementsystem, die Einhaltung von Daten- und Governance-Standards, die technische Dokumentation sowie definierte Kontrollmechanismen.

Verarbeitet also ein KI-System personenbezogene Daten, greift immer die DSGVO. Zusätzlich sind je nach Risikoklasse, die Anforderungen aus der KI-VO umzusetzen. Das heißt auch: Beide Regelwerke können verletzt werden - mit jeweils eigenen Sanktionen.

In der Praxis hat sich Folgendes bewährt:

- I. Integriertes Compliance-Konzept:
Datenschutz-Management und KI-Compliance werden in einem gemeinsamen Governance-Framework gedacht.
- II. Aufbau von Audit-Trails
Eine lückenlose Dokumentation von Trainingsdaten, Modelländerungen, Entscheidungen und Kontrollen erhöhen die Resilienz.
- III. Stringente Steuerung der Dienstleister:
Auftragsverarbeitungsverträge nach DSGVO und Pflichten aus der KI-Verordnung werden aufeinander abgestimmt - insbesondere bei Cloud-SaaS- und KI-Anbietern.

>

Praxistipps für Banken und Finanzdienstleister



Integrierter Compliance-Ansatz

DSGVO & KI-VO in einem gemeinsamen Governance-Framework integrieren



Audit-Trails sicherstellen

Lückenlose Dokumentation gewährleistet hohe Resilienz und Prüfungssicherheit



Dienstleister richtig einbinden

Verträge gemäß DSGVO und KI-VO abgestimmt steuern

Datenschutz und KI-Compliance gemeinsam steuern!

Zusammen genommen bilden beide Regelwerke - DSGVO und KI-VO - eine solide Basis für eine hohe Resilienz und auch Prüfungssicherheit.

Beide Regelwerke gelten parallel und kumulativ: Das heißt auch, Verstöße können gleichzeitig datenschutzrechtliche und KI-regulatorische Konsequenzen nach sich ziehen. In der Praxis hat sich ein integrierter Ansatz, eine lückenlose Dokumentation und die richtige Einbindung der Dienstleister bewährt.

Sie haben Fragen oder möchten Ihre KI-Governance ganzheitlich aufstellen?

Unsere Datenschutz- und KI-Experten unterstützen Sie bei der datenschutzkonformen Entwicklung, Beschaffung und Nutzung von KI-Systemen im Bankenumfeld.

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
oder
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>