



Sehr geehrte Kolleginnen und Kollegen,

generative KI ist längst im Arbeitsalltag angekommen. Sie kann dabei unterstützen, Texte zu formulieren, Inhalte zusammenzufassen, Informationen zu strukturieren oder erste Ideen zu entwickeln. Richtig eingesetzt kann sie Arbeit erleichtern, Prozesse beschleunigen und neue Perspektiven eröffnen.

Gleichzeitig gilt: **KI ist ein Werkzeug – kein Ersatz für Verantwortung, Fachwissen und sorgfältige Prüfung.**

Wer generative KI nutzt, sollte deshalb bewusst entscheiden,

- welche Informationen eingegeben werden,
- wie Ergebnisse bewertet werden und
- ob eine weitere fachliche Prüfung erforderlich ist.

Sensible Informationen schützen

Vertrauliche, personenbezogene oder interne Informationen sollten nicht in öffentlich zugänglichen oder nicht freigegebenen KI-Tools eingegeben werden.

Dazu zählen beispielsweise

- Kundendaten,
- Mitarbeiterdaten,
- Vertragsinhalte,
- interne Strategien,
- nicht veröffentlichte Geschäftsinformationen oder
- sicherheitsrelevante Details.

Der Grund liegt auf der Hand: Bei externen KI-Anwendungen ist häufig nicht vollständig transparent, wie eingegebene Inhalte verarbeitet, gespeichert oder für weitere Zwecke genutzt werden. Nutzen Sie ausschließlich **die vom Unternehmen freigegebenen KI-Anwendungen und beachten Sie die jeweils geltenden Nutzungsbedingungen**. Auch scheinbar anonymisierte Informationen können Rückschlüsse auf Personen, Kunden, Institute oder Geschäftsvorgänge zulassen.

Ergebnisse kritisch prüfen

KI-Systeme generieren in der Regel überzeugend klingende Inhalte – diese sind jedoch nicht automatisch richtig. Antworten können **fehlerhaft, unvollständig, veraltet oder missverständlich** sein. Manchmal sind sie auch **frei erfunden**.

KI-generierte Inhalte sollten daher nicht ungeprüft übernommen werden. Besonders bei rechtlichen, finanziellen, technischen oder sicherheitsrelevanten Themen ist eine fachliche Prüfung erforderlich. **KI-Ergebnisse dürfen nicht als alleinige Entscheidungsgrundlage für rechtliche, regulatorische, finanzielle, technische, sicherheitsrelevante oder kundenbezogene Entscheidungen verwendet werden.**

>

5 Grundregeln für den sicheren KI-Einsatz

1	Keine sensiblen Daten eingeben Vertrauliche, personenbezogene oder interne Informationen gehören nicht in frei zugängliche KI-Tools.
2	Ergebnisse immer prüfen KI-Antworten können fehlerhaft, unvollständig oder veraltet sein.
3	Fachliche Verantwortung behalten KI unterstützt – sie ersetzt nicht die eigene Einschätzung oder notwendige Expertenprüfung.
4	Urheberrechte und Quellen beachten Eine KI ist nur so gut wie die Daten, mit denen sie trainiert wurde.
5	Interne Vorgaben einhalten Datenschutzregelungen, Freigabeprozesse und Unternehmensrichtlinien haben Vorrang.

KI-Einsatz ja – aber bewusst, geprüft und verantwortungsvoll

Urheberrechte und Quellen beachten

KI-generierte Inhalte – Texte, Bilder, Präsentationen, Tabellen oder auch Konzepte – können urheberrechtlich relevante Bestandteile enthalten oder auf Quellen beruhen, die nicht transparent ausgewiesen werden. **Bei extern verwendeten KI-generierten Inhalten ist zu prüfen, ob Kennzeichnungspflichten, Lizenzbedingungen oder Nutzungsrechte betroffen sind.** Dies gilt insbesondere dann, wenn KI-Ergebnisse veröffentlicht, weitergegeben oder geschäftlich genutzt werden sollen.

Fazit

Generative KI kann unterstützen – sie ersetzt aber nicht die eigene fachliche Einschätzung. Entscheidend ist ein bewusster Umgang: Welche Aufgabe soll die KI übernehmen? Welche Informationen dürfen verwendet werden? Wie belastbar ist das Ergebnis? Und wer muss es gegebenenfalls prüfen oder freigeben?

Bei Unsicherheiten sollte Rücksprache mit den zuständigen Ansprechpartnern gehalten werden. So lässt sich das Potenzial generativer KI nutzen, ohne unnötige Risiken einzugehen.

Gerne unterstützen wir Sie mit unseren Expertinnen und Experten bei Ihrem KI-Projekt.

Weitere Fachinformationen zum sicheren Einsatz von KI im Bankenumfeld:
<https://www.dz-cp.de/ki-ready>

Björn Blechenberg
Marketing & Vertrieb
069 580024-172
bjoern.blechenberg@dz-cp.de



Benjamin Wellnitz
IKT-Compliance & Datenschutz
069 580024-246
benjamin.wellnitz@dz-cp.de

