

Vertraulichkeit im KI-Alltag

Sechs Fragen, bevor ein Inhalt in ein KI-Werkzeug eingefügt, hochgeladen oder mitgeschnitten wird. Gedacht als Merkkarte neben dem Bildschirm — nicht zum Ablegen.

Begleitmaterial zum Beitrag „Vertraulichkeit im KI-Alltag“
ki-kompetenz.academy/wissen/vertraulichkeit-im-ki-alltag/

NICHT NUR DAS EINGABEFELD ZÄHLT

Im Eingabefeld tippt jemand bewusst. Mehr Inhalt ist auf den leiseren Wegen unterwegs — die gehören mitgedacht:

Datei-Anhänge

Besprechungsmitschnitte

Browser-Erweiterungen

angeschlossene Ablagen

übernommene Prompts

Zugangsschlüssel

1 Ist der Inhalt bereits für alle zugänglich veröffentlicht?

☐

Was auf der eigenen Website steht, wirft die Geheimhaltungsfrage nicht auf. Alles andere schon.

2 Betrifft er Kategorien, die der Geheimhaltung unterliegen?

☐

Kalkulationen, Konditionen, Entwicklungsstände, Personalangelegenheiten — auch im Anhang darunter.

3 Gehört das Geheimnis überhaupt uns?

☐

Bei Kundenunterlagen liegt die Verfügungsgewalt woanders — oft samt einer schriftlichen Zusage, die älter ist als das erste KI-Werkzeug im Haus.

4 Sind personenbezogene Daten dabei?

☐

Dann geht es zusätzlich um das Datengeheimnis nach § 6 DSG und um die Anordnung des Dienstgebers.

5 Gibt es dafür ein Werkzeug, das bei uns freigegeben ist?

☐

Ein unternehmensinternes oder in Europa gehostetes System ist eine Prüffrage, kein Freibrief.

6 Woher stammt der Prompt, und was hängt am Werkzeug?

☐

Übernommene Anweisungen, angeschlossene Ablagen, Erweiterungen und Zugangsschlüssel entscheiden mit, was tatsächlich übertragen wird.

Bleibt eine Frage offen, wird gefragt — nicht eingefügt

Diese Karte ordnet die Fragen, sie beantwortet sie nicht. Ob eine Information im Einzelfall geheim zu halten ist, ist im eigenen Haus zu klären: bei der Datenschutzstelle, der Rechtsabteilung oder der Unternehmensleitung. Keine Rechtsberatung.

BEI VERTRAULICHEN INHALTEN FRAGEN WIR

BEI UNS FREIGEGBENE KI-WERKZEUGE