

## Sicherer Umgang mit KI

### Wie Sie Word-, Excel- und Outlook-Daten vor dem KI-Upload wirksam pseudonymisieren

Die Potenziale von Künstlicher Intelligenz (KI) im Büroalltag sind enorm: Ob es darum geht, komplexe Excel-Tabellen zu analysieren, lange Word-Berichte zusammenzufassen, Verträge zu prüfen oder einen Entwurf für Antworten auf geschäftliche E-Mails in Outlook zu erstellen – moderne Sprachmodelle (LLMs) sparen wertvolle Zeit.

Doch die Bequemlichkeit hat einen datenschutzrechtlichen Haken. Sobald sensible Unternehmensdaten, Geschäftsgeheimnisse oder personenbezogene Daten ungeschützt in Cloud-KI-Systeme hochgeladen werden, droht Ärger. Wie sieht die rechtliche Lage aus, warum ist Vorsicht geboten und wie lässt sich der Datenabfluss mithilfe smarter Tools verhindern?

#### DSGVO und Geschäftsgeheimnisse

Wer geschäftliche Dokumente unbedacht in kommerzielle Cloud-KI-Dienste füttert, bewegt sich schnell in einer rechtlichen Grauzone – oft sogar im klaren Verstoß gegen geltendes Recht:



**Die DSGVO (Datenschutz-Grundverordnung):** Sobald in Word-Dokumenten, Excel-Tabellen oder E-Mails personenbezogene Daten von Kunden, Partnern oder Mitarbeitern (Namen, E-Mail-Adressen, Telefonnummern, Kontodaten) enthalten sind, greift die DSGVO. Ein Upload an einen Drittanbieter in den USA (oder dessen Cloud) ohne entsprechende Auftragsverarbeitungsverträge (AVV) und ohne Einwilligung der Betroffenen ist unzulässig.

#### Das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG):

Geschäftsdaten behalten ihren rechtlichen Status als Geschäftsgeheimnis nur bei Bestehen angemessener Schutzmaßnahmen. Die Übermittlung vertraulicher Vertragsinhalte an externe KI-Anbieter ohne spezifische Vereinbarungen zur Zweckbindung und zum Ausschluss von Modellschulungen hebt diesen Schutzstatus auf.

Zur Wahrung des Geheimnisschutzes ist die Verarbeitung vertraulicher Daten auf Systeme mit garantierter Datenisolation zu beschränken oder auf zuvor vollständig verschlüsselte Datensätze zu begrenzen.

Viele Cloud-KI-Anbieter nutzen standardmäßig eingegebene Daten (Prompts und Uploads) für das Training ihrer zukünftigen Modelle, sofern man dem nicht ausdrücklich widerspricht (Enterprise-Tarife ausgenommen). Selbst bei striktem Datenschutz der Anbieter verbleiben die Daten auf fremden Servern. Ein unachtsamer Klick, eine unverschlüsselte Schnittstelle oder ein veraltetes Compliance-Setup genügen, und sensible Daten könnten abfließen. Ein effektiver Schutz muss daher vor dem Absenden der Daten ansetzen.

### **Wie funktioniert der Schutz? Pseudonymisierung statt starrer Schwärzung**

Werden Dokumente einfach nur mit schwarzen Balken versehen (geschwärzt), versteht die KI den Kontext oft nicht mehr. Tabellen verschieben sich, Sätze ergeben keinen Sinn.

Eine intelligente Pseudonymisierung – zum Beispiel mit IAS DataHide – erkennt sensible Angaben in Word- und Excel-Dateien sowie E-Mails und ersetzt Namen, Firmen, IBANs oder Kennzahlen durch neutrale Platzhalter. Diese bleiben einheitlich, sodass die KI die Zusammenhänge im Text weiterhin erkennt und die bereinigten Inhalte analysieren, zusammenfassen oder überarbeiten kann. Anschließend lassen sich die Platzhalter auf Knopfdruck und in wenigen Sekunden wieder durch die Originaldaten ersetzen.

Wer E-Mails direkt mit einer KI verarbeiten möchte, kann alternativ auch eine vollständig lokal betriebene Lösung nutzen, sodass die Inhalte das eigene System nicht verlassen.

### **Fazit**

Datenschutz und KI schließen sich nicht aus – vorausgesetzt, man überlässt die Datensicherheit nicht dem Zufall. Durch intelligente Pseudonymisierung, den Einsatz leichtgewichtiger smarter Tools oder den konsequenten Umstieg auf lokale KI-Umgebungen behalten Unternehmen die volle Kontrolle über Ihre Worddokumente, Excel- und Outlook-Daten und nutzen dennoch die vollen Vorteile moderner KI.