

Heikle Daten

KI-Kolumne. Jeder, der Sprachmodelle nutzt, sollte immer erst überlegen, welche Daten dort gespeichert werden sollen – und welche nicht. Ein Überblick.

Autorin: Bettina Bläß

34

Je häufiger man mit ChatGPT, dem Microsoft Copilot oder Mistral arbeitet, desto eher neigt man dazu, zu vergessen, dass es Daten gibt, die dort aus Datenschutz- und Sicherheitsgründen nicht eingegeben werden sollten. Denn üblicherweise nutzt man diese Tools über das Internet. Denn die Informationen, die man hier eingibt, werden bei dem Unternehmen gespeichert, dessen Tool man nutzt. Wer den französischen KI-Assistenten Le Chat von Mistral wählt, hat zwar durch die Einhaltung der europäischen Datenschutzgrundverordnung eine erhöhte Datensicherheit – trotzdem liegen die eingegebenen Informationen dann bei einem Unternehmen. Noch kritischer ist es zu sehen, wenn man zusätzlich weder durch einen Vertrag noch durch eine entsprechende Software oder individuell angepasste Einstellungen das Training der Tools mit den eingegebenen Informationen unterbunden hat.

Bedenkenlos – alles, was auf einer Postkarte steht

Zur Sicherheit sollte man sich deshalb angewöhnen, grundsätzlich nie sensible Daten in ein Large Language Model (LLM) einzugeben. Dazu zählen personenbezogene Daten, etwa die Namen von Patienten, Mitarbeitern, Vorgesetzten oder Kooperationspartnern mitsamt Adressen, Geburtsdaten, Gesundheitsinformationen, Kontodaten oder medizinischen Befunden. Ebenso tabu sollten interne Unternehmensinformationen sein sowie Verträge, nicht veröffentlichte Geschäftszahlen, interne Strategiepapiere, Preislisten, Kalkulationen oder Protokolle aus internen Konferenzen. Besonders heikel wird es bei Betriebs- und Geschäftsgeheimnissen oder anwaltlichen Schriftsätzen. Die einfache Regel lautet: Alles, was man nicht bedenkenlos auf eine Postkarte schreiben und fremden Menschen zeigen würde, gehört nicht in ein KI-Tool, das nicht auf dem eigenen Server betrieben wird. Eine Ausnahme könnte sein, wenn man mit dem Anbieter einen entsprechenden Vertrag geschlossen hat. ■



Doctolib

So vermeiden Sie Zahlücken.

Top Funktionen:

- ✓ Individualisierbarer, KI-gestützter Kalender
- ✓ Automatische Terminbenachrichtigungen an alle Patient:innen
- ✓ Automatische Recalls mit Buchungstracking
- ✓ Digitale Nachrückerliste



**KI-Sprechstundenassistent
jetzt kostenlos testen!**

