**Richtlinien im Umgang mit KI für KMU**

Nutzen Ihre Mitarbeitenden bereits ChatGPT für geschäftliche Zwecke? Wir gehen davon aus, dass das der Fall ist. Deshalb ist es umso wichtig, Richtlinien zu definieren, was sie dürfen und was nicht, wenn sie KI-Tools nutzen. Folgende Fragen sollten dabei berücksichtigt werden:

**Was ist bei der Auswahl des
KI-Tools wichtig?**

Bei vielen kostenlos verfügbaren KI-Tools wie z.B. ChatGPT oder Claude stimmen Sie implizit der Weiterverarbeitung und Nutzung der eingegebenen Daten für Trainingszwecke durch den Anbieter zu. Es gilt: «kostenlos heisst, dass man es mit der Preisgabe der eigenen Daten zahlt». Da in Ländern wie den USA die Datenschutzbestimmungen weniger streng sind als in der Schweiz, kann dies potenzielle Datenschutzrisiken mit sich bringen.

Wenn Sie nicht wollen, dass die eingegebenen Daten weiterverwendet werden, dann empfehlen wir ausschliesslich die Pro-Versionen von KI-Tools zu nutzen, um die Datennutzung für Trainingszwecke zu deaktivieren (siehe Screenshot am Beispiel von ChatGPT in den Einstellungen) und somit eine bessere Datenkontrolle zu gewährleisten, sofern den Versprechungen der Firma OpenAI geglaubt wird.

**Was muss bei der Verwendung von KI-Tools beachtet werden?**

Geben Sie **keine geheimen, vertraulichen personenbezogenen oder andere geschäftsrelevanten Daten sowie Geschäftsprozesse** in KI-Tools ein. Dazu gehören:

* **Sensible Daten**, welche auf Personen zurückgeführt werden können.
* **Finanzdaten** wie z.B. Preisstrategien oderKalkulationsgrundlagen
* **Vertragsdetails / Geschäftsgeheimnisse** mit Infos über Produkte, vertrauliche Projekte, Strategien oder Kunden.

**Welche einfach umsetzbaren Massnahmen gibt es?**

* **Anonymisierung unternehmens- und personenbezogener Daten** (z.B. Namen von Personen oder Firmen ändern).
* Falls keine vollständige Anonymisierung möglich ist, sollten die Daten **pseudonymisiert** werden(z.B. durch das Ersetzen von Bezeichnungen von Scheinunternehmen / Musternamen).

**Sind die erhaltenen Resultate präzise und korrekt?**

KI-Systeme können **falsche Informationen** liefern oder „halluzinieren“ / „fabulieren“. Konkret heisst das, dass unpräzise oder sogar erfundene Aussagen generiert werden können.

**Wichtig:** Resultate und Informationen aus den KI-Tools sollten nur übernommen werden, nachdem diese kritisch hinterfragt und auf ihre Richtigkeit / Zuverlässigkeit überprüft wurden.

**Bestimmungen im Umgang mit KI-Tools**

Die folgenden Ausführungen regeln, wie Mitarbeitende der Firma \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ sich verhalten sollen, wenn sie KI-Tools (z.B. ChatGPT) für geschäftliche Zwecke nutzen.

1. **Unternehmensweite Bestimmungen im Umgang mit KI**

Die Verwendung von KI-Tools wie ChatGPT ist (nicht) gestattet.

1. **Login-Daten**

Die Verwendung der unternehmensbezogenen E-Mail-Adresse zur Registrierung bei KI-Tools für geschäftliche Zwecke ist Mitarbeitenden (gestattet / nicht gestattet).

Bei Erteilung der Erlaubnis müssen Mitarbeitende folgende interne Meldepflichten erfüllen: Die Mitarbeitenden sind verpflichtet, dass sie der IT-Abteilung / den Vorgesetzten mitteilen, falls sie ChatGPT das erste Mal für geschäftliche Zwecke verwenden. Sie sind verpflichtet, alle gesetzlichen Vorgaben sowie arbeits- und datenschutzrechtlichen Bestimmungen und die vorliegenden Bestimmungen einzuhalten.

1. **Gezielte Anwendung von KI- Tools**

Bei der Nutzung kostenloser KI-Tools (z.B. kostenlose Version von ChatGPT) besteht das Risiko, dass die eingegebenen Daten zu Trainingszwecken für die Weiterentwicklung des Systems verwendet werden. Deshalb ist es entscheidend, klare Richtlinien für den Einsatz von KI-Tools festzulegen. Das Unternehmen kann z.B. vorsehen, dass nur Bezahlversionen eingesetzt werden, bei denen die eingegebenen Daten nicht gespeichert werden. Dabei soll eingestellt werden, dass die Daten nicht weiterverwendet werden dürfen (z.B. bei ChatGPT unter Einstellungen, Datenkontrollen, «Das Modell für alle verbessern»). Oder es kann definiert werden, welche Daten nicht eingegeben werden dürfen (siehe nächster Punkt).

1. **Rechtliche Rahmenbedingungen und Datenschutzbestimmungen beachten**

Vertrauliche Unternehmensinformationen und Daten von Dritten dürfen **nicht** in KI-Tools eingegeben werden. Diese umfassen konkret:

* **Sensible Daten**, welche auf Personen zurückgeführt werden können. Die Daten von Personen müssen anonymisiert sein. D.h. es darf kein Rückschluss auf die Person gezogen werden können. Das bedeutet, dass keine Namen von Kunden in ChatGPT und weitere KI-Tools eingegeben werden dürfen. Gleiches gilt für Bilder der Kundschaft.
* **Finanzdaten** wie z.B. Preisstrategien oder Kalkulationsgrundlagen, welche zentral für das Unternehmen sind, dürfen nicht eingegeben werden. Wenn diese Informationen öffentlich werden, kann dies dem Unternehmen schaden.
* **Vertragsdetails / Geschäftsgeheimnisse** mit Infos über Produkte, vertrauliche Projekte, Strategien oder Kunden dürfen nicht eingegeben werden.

Bei der Verwendung von KI-Tools müssen sensible unternehmens- oder personenbezogene Daten anonymisiert oder pseudonymisiert werden. Ansonsten könnten sie in Zukunft durch danach suchende Personen gefunden werden.

1. **Menschliche Überprüfung von KI-generierter Inhalte**

Die Resultate von KI-Tools können unpräzise oder sogar falsch sein. Vor der Verwendung von KI-generierten Inhalten muss eine qualifizierte Person diese auf ihre Richtigkeit, Genauigkeit und Zuverlässigkeit überprüfen.

1. **Kennzeichnung von KI-generierten Inhalten**

Werden Inhalte mit Hilfe von KI-Tools wie ChatGPT generiert, soll dies deklariert werden. Z.B. «künstlich generiert» oder «mit Hilfe von KI generiert».

**Der Mitarbeiter \_\_\_\_\_\_\_\_\_\_\_\_\_\_, die Mitarbeiterin \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ bestätigt, diese Regelungen gelesen und verinnerlicht zu haben.**

**Firmensitz, Datum \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

 **Unterschrift**

Einzelne Elemente dieser Bestimmungen wurden angelehnt an die KI-Guidelines für KMU der WKO (2023). Abgerufen von <https://www.wko.at/oe/digitalisierung/kmu-ki-guidelines.pdf>