Rechtssicherheit beim KI-Einsatz

KI rechtssicher nutzen – Praxistipps für KMU

Künstliche Intelligenz gehört in vielen KMU bereits zum Arbeitsalltag. Rechtliche Risiken entstehen beim Einsatz vor allem durch die Inhalte, die in die KI eingegeben werden, und durch die Art und Weise, wie Ergebnisse anschliessend weiterverwendet werden. Ein Quick-Check schafft Orientierung, ohne den Arbeitsalltag unnötig zu blockieren.

› Reto Fanger, Vera Egli

Montag, 08.30 Uhr im HR: Eine Mitarbeiterin kopiert Auszüge aus einem Bewerbungsdossier sowie Interview-Notizen in ein kostenloses KI-Tool und promptet: «Formuliere mir eine Absage für diese Bewerbung. Hier ist ein Mustertext aus dem Internet. Begründe professionell, aber klar und beziehe dich auf die Gesprächsnotizen und den Mustertext.»

Ein kurzer Prompt, in dem bereits mehrere rechtliche Themen stecken:

- Datenschutz: Bewerbungsunterlagen und Interview-Notizen sind Personendaten. Je nach Tool werden Daten an Dritte weitergegeben und unter Umständen ins Ausland bekannt gegeben.
- Geheimhaltung und Vertraulichkeit: HR-Notizen sind häufig sensibel. Diese Problematik ist jedoch keineswegs nur auf den HR-Bereich beschränkt. Auch in anderen Bereichen werden KI-Tools oft mit vertraulichen Unternehmensinformationen oder vertraulichen Kundendaten gefüttert.
- Urheber-/Lizenzrechte: «Im Internet gefunden» bedeutet nicht, dass das Gefundene frei verwendet werden darf. Urheberrechtlich geschützte Inhalte (z.B. Texte oder Bilder) können schon bei der Eingabe (Input) problematisch werden, wenn keine entsprechenden Nutzungsrechte bestehen oder der Anbieter Inhalte weiterverwenden darf.
- Haftungsrisiken: Sobald ein KI-Output nach aussen geht, wird daraus eine Erklärung des KMU. Die rechtliche Verantwortung verbleibt beim KMU, auch wenn der Inhalt KI-generiert wurde.

Rechtlicher Rahmen

Diese Konstellation ist für KMU typisch. Fehlen freigegebene Tools, weichen Mitarbeitende auf privat genutzte oder kostenlose KI-Versionen aus, die zur sogenannten «Schatten-IT» gehören und vom Unternehmen weder geprüft noch kontrolliert werden. Das erhöht die Risiken von Datenabfluss, fehlender Nachvollziehbarkeit und intransparenten Vertragsgrundlagen.

Der Einsatz von KI erfolgt jedoch nicht in einem rechtsfreien Raum. Auch ohne eigenständige KI-Gesetzgebung gelten bereits heute Normen, insbesondere aus dem Datenschutz-, Urheber-, Vertrags-, Arbeits- und Haftungsrecht. Je nach Geschäftsmodell, Zielmarkt, Datenbearbeitung und Einsatzkontext können zusätzlich europäische Vorgaben relevant werden, wie etwa die KI-Verordnung der Europäischen Union (EU AI Act) oder die Datenschutz-Grundverordnung (DSGVO).

Damit rückt ein risikobasierter Ansatz in den Vordergrund. Je stärker Personen, vertrauliche Informationen, Aussenwirkung oder Entscheidungen über Personen betroffen sind und je weniger das KMU die Datenflüsse und den Output kontrollieren kann, desto vertiefter haben Prüfung, Freigabe und Kontrolle zu erfolgen.

Der Quick-Check für die Praxis

Ein praktikabler Prüfprozess hilft, den Einsatz von KI im Betrieb einzuordnen. Der folgende Quick-Check zeigt, welche Daten eingegeben werden dürfen, wie Ergebnisse zu kontrollieren sind, welche Punkte beim Anbieter abzusichern sind und wie die Nutzung organisatorisch eingebettet werden kann.

Stufe 1: Use-Case-Check
Startpunkt ist stets der konkrete Anwendungsfall. Wofür soll das KI-Tool eingesetzt werden, in welchem Bereich (z.B. HR, Support, Marketing) und mit welcher Aussenwirkung? Zu unterscheiden ist zwischen interner Unterstützung (z.B. Entwurf/Brainstorming) und Anwendungen mit Aussenwirkung oder Entscheidungsbezug. Je näher der Use Case an Personen, sensiblen Themen oder Aussenwirkung liegt, desto höher sollten die Anforderungen an Review und Freigabe sein.

Besondere Vorsicht ist dort angezeigt, wo KI Aussagen über Personen beeinflusst oder Entscheidungen vorbereitet. Im HR kann die Auswertung oder Vorselektion von Bewerberdaten mit KI datenschutzrechtlich heikle Fragen auslösen, insbesondere mit Blick auf Profiling, Transparenz, Verhältnismässigkeit und automatisierte Einzelentscheidungen. Bei ausschliesslich automatisierten Einzelentscheidungen mit Rechtsfolge oder erheblicher Beeinträchtigung können zudem besondere Informationspflichten gelten. Ausserdem kann ein Anspruch auf Überprüfung durch eine natürliche Person bestehen. Im Arbeitsverhältnis gilt zudem, dass Personendaten nur in dem Umfang bearbeitet werden dürfen, der für das Arbeitsverhältnis erforderlich ist. Für solche Anwendungsfälle empfiehlt sich deshalb vorab eine kurze Risikoanalyse, die Datenschutz und Informationssicherheit gemeinsam betrachtet.

Stufe 2: Input-Check
Sobald Zweck und Einsatzbereich des KI-Tools feststehen, sollte das KMU festlegen, welche Datenkategorien in das Tool eingegeben werden dürfen und welche nicht. In der Praxis wird häufig unterschätzt, dass bereits ein scheinbar harmloser Prompt Personendaten, vertrauliche Geschäfts- oder Kundendaten oder urheberrechtlich geschützte Inhalte enthalten kann. Der Input ist deshalb nicht nur datenschutzrechtlich, sondern auch urheber- und lizenzrechtlich zu prüfen. Wird mit Texten, Bildern oder Vorlagen gearbeitet, müssen die erforderlichen Nutzungsrechte vorliegen und die Bearbeitung im Tool muss von diesen Rechten abgedeckt sein.

Ohne klare Vorgaben weichen Mitarbeitende in der Praxis oft auf private oder kostenlose KI-Tools aus, die vom KMU weder geprüft noch freigegeben wurden. Statt pauschaler Verbote braucht es deshalb freigegebene Tools und klare Regeln für die Nutzung. Das KMU sollte freigegebene Tools definieren, klare Richtlinien festlegen und Mitarbeitende zu zulässi-

Abb. 1: Stufen Quick-Check

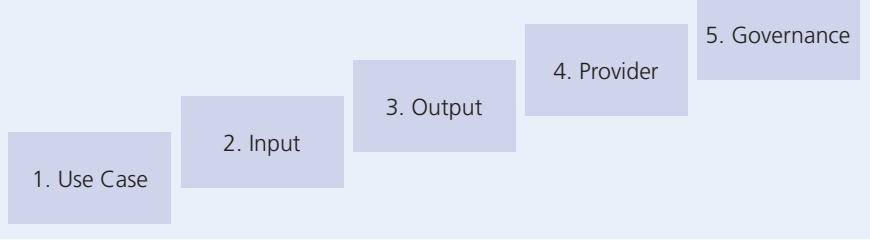
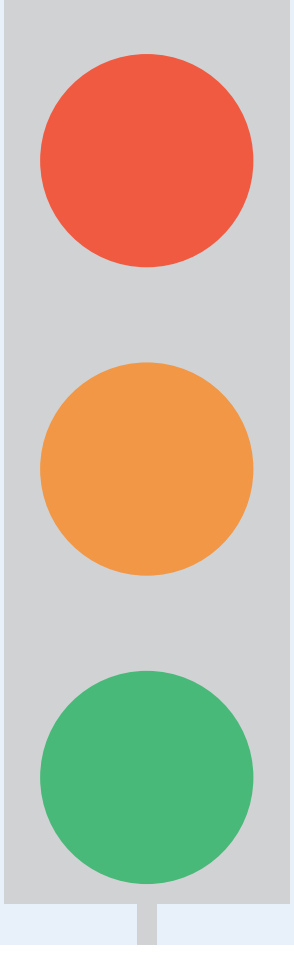


Abb. 2: Prompt-Ampel



Input (Prompt)	Typische Beispiele	Nutzung in KI-Tools
› Besonders schützenswerte Personendaten › Vertrauliche/sensible Daten (Geschäftsgeheimnisse, Amts-/Berufsgeheimnisse) › Zugangsdaten/Sicherheitsinformationen › Urheberrechtlich geschütztes Material (ohne Nutzungsrecht)	› Bewerbungsdossiers › Arbeitszeugnisse › Umsatzzahlen › Passwörter › Bilder/Texte aus dem Internet (ohne Nutzungsrecht)	**Intern und extern:** Nicht in KI-Tools eingeben
› Interne Daten und Richtlinien (ohne Personenbezug) › Interne Unterlagen (ohne geschäftskritische, vertrauliche oder sensible Inhalte) › Personendaten (nach vorgängiger Prüfung)	› Interne Prozessbeschreibungen › Schulungsunterlagen › Interne Mustervorlagen › Anonymisierte Reports	**Intern:** Nur in vom KMU freigegebenen KI-Tools eingeben (Input und Output dennoch zu überprüfen) **Extern:** Nicht in KI-Tools eingeben
› Sachdaten › Anonymisierte Personendaten › Öffentlich verfügbare Inhalte, sofern keine Nutzungsrechts- oder Vertraulichkeitsrisiken bestehen	› Allgemeine Rechercheanfragen › Übersetzungen ohne Personenbezug › Produkttexte ohne Kundennamen	**Intern und extern:** Grundsätzlich in KI-Tools eingebbar (Ergebnisse dennoch überprüfen)

gen Datenkategorien schulen. So lässt sich die Nutzung besser steuern, ohne den praktischen Einsatz unnötig zu erschweren. Für den Alltag empfiehlt sich eine einfache Einteilung in zulässige, heikle und gesperrte Inhalte. Als erster Anhaltspunkt kann die «Prompt-Ampel» dienen (siehe Abb. 2). Sind Use Case, Input und Datenkategorien definiert, stellt sich die Frage, was mit den Ergebnissen passieren darf.

Stufe 3: Output-Check

KI-Output ist stets zu prüfen, bevor er weiterverwendet wird. Ein Review durch einen Fachverantwortlichen oder ein Vier-Augen-Prinzip reduziert das Risiko falscher Tatsachenbehauptungen sowie diskriminierender oder unpassender Formulierungen. Dieser «human in the loop»-Ansatz ist nicht nur Best Practice, sondern ein zentraler Baustein rechtssicherer KI-Nutzung. Denn auch wenn die KI generiert, bleibt die rechtliche Verantwortung beim KMU.

Urheberrechtlich ist Vorsicht geboten, wenn KI fremde Inhalte übernimmt oder Stil, Struktur oder prägende Elemente eines bestehenden Werks nachbildet. Dabei ist nicht nur eine kreative Nähe problematisch. Ein Sprachmodell kann Formulierungen, die es im Training sehr häufig gesehen hat, in passenden Situationen reproduzieren (bis hin zu charakteristischen Slogans). Ein zulässiges Zitat muss als Zitat erkennbar sein und setzt eine inhaltliche Auseinandersetzung voraus.

Datenschutzrechtlich ist zudem zu beachten, dass Verstösse gegen das DSG zu Sanktionen führen können. Zudem kann der EDÖB (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter) Untersuchungen eröffnen und Massnahmen anordnen.

Viele rechtliche Risiken hängen auch vom Anbieter und den vertraglichen Rahmenbedingungen ab.

Stufe 4: Provider- und Vertrags-Check

Ein KI-Tool ist nicht nur eine Anwendung, sondern immer auch ein Dienstleistungs- und Vertragsverhältnis mit einem Anbieter, häufig mit Cloud-Infrastruktur, Unterauftragsbearbeitern und Support-

zugriffen. Viele KMU verlassen sich auf Standardbedingungen und merken erst im Nachhinein, dass zentrale Themen wie die Weiterverwendung von Inhalten nicht ausreichend geregelt sind. Ein Anbieter- und Vertragscheck sollte deshalb bei jedem Tool mit Rot-/Gelb-Daten ein Standardprozess sein.

Geprüft und vertraglich festgelegt werden sollten im Besonderen die folgenden Mindestpunkte:

- Datenschutz und Datenflüsse (einschliesslich Ausland): Zu klären sind Zweck, bearbeitete Daten, Datenstandort, Sicherheitsmassnahmen und Informationspflichten. Auf dieser Grundlage ist zu prüfen, ob ein Vertrag zur Auftragsbearbeitung (ADV/ABV) erforderlich ist, ob eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen ist und ob bei einer Bekanntgabe ins Ausland zusätzliche Garantien sicherzustellen sind.
- Nutzungsrechte: Im KI-Alltag wird häufig übersehen, dass rechtliche Risiken schon bei der Eingabe mit Texten, Bildern, Vorlagen oder sonstigen Daten entstehen. Das KMU sollte daher klären, ob es über die nötigen Rechte am Input verfügt und ob der Output ohne Einschränkungen genutzt oder veröffentlicht werden darf.
- Geheimhaltung und Vertraulichkeit: Beim Einsatz von KI-Providern ist Vertraulichkeit zentral, weil in der Praxis schnell interne Informationen sowie Kunden- oder Partnerdaten in Prompts oder hochgeladene Dokumente gelangen. Zu prüfen ist, ob Geheimhaltungs- oder Vertraulichkeitspflichten auch Subprozessoren, Supportzugriffe, Speicher- und Löschregeln sowie Nachweismöglichkeiten abdecken. Viele Anbieter begrenzen ihre Haftung stark oder formulieren Sicherheitsmassnahmen nur allgemein, wodurch verbleibende Risiken faktisch beim KMU liegen. Kritisch sind insbesondere Klauseln zur Weiterverwendung von Inputs oder Outputs, zu Haftungsbeschränkungen und zu unklaren Lösch- und Kontrollrechten.

Das KMU sollte jederzeit beantworten können, welche Daten im Tool bearbeitet werden, wohin sie fliessen, wofür der Anbieter sie verwenden darf und welche Sicherheiten (vertraglich und technisch) dafür bestehen. Der Vertrag setzt dafür den rechtlichen Rahmen. Die Governance stellt sicher, dass diese Vorgaben im Alltag umgesetzt, verstanden und regelmässig überprüft werden.

Stufe 5: Governance-Check

KI-Governance schafft den organisatorischen Rahmen für einen kontrollierten Einsatz von KI im Unternehmen. Sie übersetzt die Stufen 1 bis 4 in den KMU-Alltag. Gute Governance dient der Risikominderung, der Einhaltung rechtlicher und interner Vorgaben, der Vertrauensbildung und dem Reputationsschutz.

In der Regel genügt ein überschaubares, aber klar definiertes Grundpaket an Governance-Massnahmen. Dazu gehört insbesondere, pro Tool oder Anwendungsfall eine verantwortliche Person (Owner) zu bestimmen, zulässige Datenkategorien festzulegen, einen Freigabeprozess zu definieren, Mitarbeitende zu schulen und ein Verzeichnis der freigegebenen KI-Anwendungen zu führen. Ergänzend sollte ein Prozess für Vorfälle festgelegt werden, damit Risiken möglichst schnell gemeldet und beurteilt und geeignete Massnahmen ergriffen werden können. Diese Punkte lassen sich in einer internen Weisung festhalten. Sämtliche Prozesse und Verzeichnisse sollten dabei regelmässig überprüft und aktualisiert werden.

Fazit

Rechtssicherheit beim KI-Einsatz entsteht durch klare Zuständigkeiten und einen nachvollziehbaren Prüfprozess. Wer Anwendungsfälle, Eingaben, Ergebnisse, Anbieter und Governance systematisch prüft, schafft eine tragfähige Grundlage für den Einsatz von KI im KMU-Alltag. «

Porträt

Reto Fanger
Rechtsanwalt, Dr. iur., Inhaber

Reto Fanger ist als Inhaber der ADVOKATUR FANGER als Rechtsanwalt mit Schwerpunkt ICT-, Daten-, Medien- und Arbeitsrecht in der ganzen Schweiz tätig und lehrt zudem als Dozent an der Hochschule Luzern und an der Richterakademie der Universität Luzern.

Vera Egli
MLaw und Datenschutzberaterin

Vera Egli verfügt über einen Master of Law der Universität Luzern und ein CAS Datenschutzberaterin der ZHAW und arbeitet als Legal Consultant bei der ADVOKATUR FANGER.

Kontakt

reto.fanger@advokatur-fanger.ch
vera.egli@advokatur-fanger.ch
www.advokatur-fanger.ch