Interview mit **Cyril Berger,** Jurist und Experte für Künstliche Intelligenz (KI)

Was KMU bei der Nutzung von KI beachten müssen – Die Integration von KI in alltägliche Softwarelösungen nimmt rasant zu. Ob in Microsoft 365, in CRM-Tools, Buchhaltungssoftware oder sogar in der täglichen Kommunikation via WhatsApp – KI-Funktionen sind überall verfügbar. Für KMUs stellt sich daher vermehrt die Frage: Was bedeutet diese Entwicklung aus juristischer Sicht? Müssen Geschäftsführende rechtliche Risiken fürchten, wenn KI zunehmend in die Tätigkeiten des Arbeitsalltags integriert wird? Wir sprechen mit Cyril Berger, Gründer & Co-CEO von Code Law, über Chancen, Herausforderungen und konkrete Handlungsempfehlungen.

F: Herr Berger, KI-Funktionen tauchen mittlerweile in fast jeder Software auf. Sollte mir das als Inhaber einer Firma aus rechtlicher Sicht schlaflose Nächte bereiten?

A: Nein, schlaflose Nächte brauchen Sie nicht zu haben – aber wachsame Tage sollten Sie einplanen. Die Integration von KI in Softwarelösungen bringt viele Vorteile, birgt jedoch auch neue Risiken, insbesondere im Hinblick auf Datenschutz, Urheberrecht und Haftung. Entscheidend ist, dass Sie sich als Unternehmer bewusst mit der Technologie auseinandersetzen und prüfen, wo und wie KI in Ihrem Betrieb zum Einsatz kommt. Wichtig ist deshalb, die Softwarelösungen, in welchen KI eingesetzt wird, zu kennen, die Vertragsbedingungen der Anbieter sorgfältig zu prüfen und sich im Zweifel rechtlich beraten zu lassen. Wer gut informiert ist und seine Hausaufgaben macht, kann KI verantwortungsvoll und rechtskonform nutzen.

F: Was muss ich und meine Mitarbeitenden bei der Eingabe von Daten in KI-gestützte Systeme besonders beachten?

A: Der zentrale Punkt ist der Datenschutz. Wenn Sie Personendaten – also Informationen, die sich auf eine identifizierbare Person beziehen – in KI-gestützte Systeme eingeben, müssen Sie sicherstellen, dass dies rechtlich zulässig ist. Das bedeutet insbesondere, dass Sie prüfen müssen, ob das System die eingegebenen Personendaten an Dritte übermittelt oder zur Weiterverarbeitung speichert. Viele KI-Tools, insbesondere cloudbasierte, nutzen Daten zur Verbesserung ihrer Modelle – das kann problematisch sein, wenn es sich um Personendaten handelt, aber auch dann, wenn Kundeninformationen, Geschäftsgeheimnisse oder andere sensible Daten betroffen sind.

Zudem sollten Unternehmen intern klare Richtlinien schaffen: Wer darf welche KI-Tools nutzen, zu welchen Zwecken, und welche Daten dürfen dabei eingegeben und bearbeitet werden? Auch Schulungen sind sinnvoll, um das Bewusstsein für Datenschutz und Informationssicherheit im Umgang mit KI-Systemen zu stärken. Der Einsatz von KI ist nicht per se ein Risiko – er sollte jedoch bewusst und kontrolliert erfolgen.

F: Aber wie soll das im Alltag umgesetzt werden? Plötzlich taucht bei einem Software-Update eine neue KI-Funktion auf. Wie sollen Geschäftsführer den Überblick behalten? Wie sollen sie wissen, welche Software oder App welche Daten speichert oder an Dritte übermittelt?

A: Genau dies ist eine der grossen Herausforderungen in der Praxis – und eine, die sich nicht allein mit einer einzelnen Massnahme lösen lässt. In vielen Unternehmen wird Software dezentral angeschafft und verwendet, sei es WhatsApp für die rasche und unkomplizierte Kommunikation, DeepL für Übersetzungen oder ChatGPT für Textvorschläge. Und oft bemerkt man gar nicht, dass eine neue Funktion KI-basiert ist – sie ist nach einem Update einfach da.

Deshalb braucht es eine Kombination aus Sensibilisierung, klaren Prozessen und technischer Unterstützung. Sinnvoll ist es, ein Verzeichnis der eingesetzten und zugelassenen Tools zu führen – idealerweise ergänzt um Informationen, wie diese Anwendungen mit Daten umgehen. Auch ein interner KI-Leitfaden kann helfen: Er definiert, welche Tools zulässig sind, welche Daten darüber nicht bearbeitet werden dürfen und welche Freigaben notwendig sind.

Zudem lohnt es sich, die Datenschutzerklärungen und Nutzungsbedingungen regelmässig der KI-gestützten Tools zu prüfen. Ich bin mir bewusst, dass dies mühsam klingt, denn gerade bei weit verbreiteten Tools ändern sich die Datenschutzerklärungen und Nutzungsbedingungen oft, ohne dass die Nutzer aktiv informiert werden. Wer hier keine Kontrolle einführt, läuft Gefahr, unbeabsichtigt in Datenschutz- oder Geheimhaltungsprobleme zu geraten.

Wichtig ist also: Nicht alles im Detail selbst überwachen – aber die richtigen Strukturen und Zuständigkeiten im Unternehmen schaffen. Dann lässt sich der Überblick behalten, auch wenn die Zahl der KI-Funktionen weiter zunimmt.

F: Welche vertraglichen Punkte soll ich beim Einsatz von KI-gestützter Software mit dem Anbieter unbedingt klären?

A: Sobald ein Unternehmen Software nutzt, die Personendaten bearbeitet – darunter insbesondere über eigene Mitarbeitende, aber auch über Mitarbeitende von Kunden, Partnern und Lieferanten – muss eine sog. Vereinbarung zur Auftragsdatenbearbeitung (ADV)

abgeschlossen werden. Dies ist sowohl gemäss Schweizer Datenschutzgesetz als auch gemäss EU-DSGVO Pflicht. Viele Softwareanbieter stellen die ADV online zur Verfügung, meist im Kundenportal oder auf der Website. Wichtig ist, dass die ADV sorgfältig gelesen und dann – gemäss den eigenen internen Vorgaben – aktiv akzeptiert bzw. abgeschlossen wird und dies auch dann, wenn es sich bloss um ein Update zu einer bereits bestehenden ADV handelt.

Die ADV sollte klar regeln, welche Daten bearbeitet werden und zu welchem Zweck, wo die Daten gespeichert werden (z. B. Schweiz, EU, USA) und für wie lange, welche Sicherheitsmassnahmen der Anbieter zum Schutz der Daten trifft, ob Unterauftragsbearbeiter (Subunternehmer) eingesetzt werden, und was am Ende der Vertragsbeziehung mit den Daten passiert. Auch der Umgang mit Datenschutzverletzungen muss geregelt sein.

Gerade bei weit verbreiteten Tools von grossen Anbietern ist eine inhaltliche Diskussion und Verhandlung der ADV-Inhalte nicht möglich. Dies führt zu einem klassischen «take it or leave it»: Kommt man bei der Prüfung der ADV zum Schluss, dass die betreffende Software nicht eingesetzt werden sollte, ist auf deren Einsatz zu verzichten und eine andere Lösung zu suchen.

F: Kann ich die Inhalte, die mir eine KI liefert – z. B. Textvorschläge, Bilder oder Analysen – einfach so verwenden?

A: Aktuell bewegen wir uns hier in einer rechtlichen Grauzone. Es gibt bislang kaum gefestigte Rechtsprechung dazu, ob und in welchem Umfang KI-generierte Inhalte wie Texte, Bilder oder Analysen urheberrechtlich geschützt sind – oder ob bei ihrer Nutzung Rechte Dritter verletzt werden könnten. Juristisch ist somit vieles noch umstritten.

Das heisst: Was eine KI ausgibt, darf nicht automatisch wie eigenes geistiges Eigentum behandelt werden. Besonders bei Bildern oder Texten, die stark an bestehende Werke erinnern, besteht das Risiko, dass unbeabsichtigt gegen Urheberrechte verstossen wird. Auch bei vertraulichen Informationen oder sensiblen Daten, die in die KI eingegeben wurden, ist Vorsicht geboten – es kann nicht ausgeschlossen werden, dass Ähnliches später anderen Nutzern wieder angezeigt wird.

F: Wo sehen Sie die grössten Risiken für KMU im Umgang mit KI?

A: Die grössten Risiken für KMU sehe ich beim Datenschutz und bei der Geheimhaltung von vertraulichen Daten. Viele Tools senden Daten an Server im Ausland – wer dabei Personen- oder Kundendaten eingibt, riskiert Datenschutzverstösse oder die Verletzung von Geheimhaltungspflichten.

Ein weniger rechtliches, sondern eher Business-bezogenes Risiko sehe ich bei der Verlässlichkeit von KI-Ergebnissen bzw. deren inhaltlichen Genauigkeit: KI kann überzeugend klingen, aber auch falsche oder irreführende Informationen liefern. Wer sich blind auf Ergebnisse verlässt, trifft womöglich falsche Entscheidungen.

Deshalb braucht es klare interne Richtlinien, Schulungen und ein Mindestmass an Kontrolle, um diesen Risiken zu begegnen.

F: Welche Informationen sollten meine Mitarbeitenden zur Nutzung von KI erhalten und was muss vertraglich geregelt werden?

A: Mitarbeitende sollten verstehen, dass KI-Tools keine Spielerei sind, sondern damit Daten bearbeitet werden – damit können rechtliche Folgen verbunden sein. Deshalb ist Aufklärung zentral: Welche Daten dürfen eingegeben werden? Welche Tools sind erlaubt? Was muss kritisch geprüft werden, bevor KI-generierte Inhalte verwendet werden?

Wie bereits erwähnt, empfehlen sich diesbezüglich klare interne Richtlinien zur KI-Nutzung. Solche Richtlinien gelten nach Schweizer Recht als Weisungen des Arbeitgebers (Art. 321d OR) und sind damit grundsätzlich verbindlich – auch ohne ausdrückliche Erwähnung im Arbeitsvertrag. Wichtig ist aber, dass sie verständlich formuliert und den Mitarbeitenden klar kommuniziert werden, damit sie dann im Arbeitsalltag auch gelebt werden. Wer zusätzliche Sicherheit möchte, etwa bei besonders sensiblen Daten oder in regulierten Branchen, kann KI-bezogene Regelungen auch im Personalreglement oder als Ergänzung zum Arbeitsvertrag verankern.

F: KI-Systeme entscheiden zunehmend mit, etwa bei Bewerbungen oder Bonitätsprüfungen. Wo lauern hier rechtliche oder ethische Fallstricke für KMU?

A: Sobald KI im Personalwesen oder bei geschäftskritischen Entscheidungen zum Einsatz kommt, wird es heikel – etwa wenn Bewerbungen KI-gestützt vorsortiert oder Absagen automatisiert werden. Solche Prozesse müssen transparent, nachvollziehbar und diskriminierungsfrei sein. Dies verlangt nicht nur das Datenschutzrecht, sondern auch das Gleichstellungsgesetz. KMU tragen hier die Verantwortung, auch wenn sie eine externe Lösung nutzen. Deshalb gilt: KI darf unterstützen – entscheiden sollte am Ende der Mensch.

FAZIT: Künstliche Intelligenz (KI) bietet auch für KMU grosse Chancen – von effizienteren Arbeitsabläufen bis hin zu neuen Geschäftsmodellen. Doch der rechtssichere Einsatz von KI-gestützter Software erfordert Aufmerksamkeit: Datenschutz, Geheimhaltung, Urheberrecht und Transparenz müssen mitgedacht werden. Wer Mitarbeitende sensibilisiert, interne Leitplanken setzt und sich im Zweifelsfalle rechtlich beraten lässt, kann KI verantwortungsvoll nutzen – und dabei von ihren Stärken profitieren, ohne unnötige Risiken einzugehen.

Zur Person

Cyril Berger ist ein erfahrener Wirtschaftsjurist mit besonderer Expertise an der Schnittstelle von Recht, Technologie und Unternehmertum. Er war mehrere Jahre als Senior Legal Counsel bei einem grossen Schweizer ICT-Unternehmen tätig – mit Fokus auf Vertrags-, IT-, Telekommunikations-, Gesellschafts- und Datenschutzrecht. Heute berät er mit Code Law insbesondere KMU und Startups umfassend zu rechtlichen Fragestellungen.