Künstliche Intelligenz II

Wie Unternehmen KI ohne Risiko nutzen können

Wenn ein Unternehmen die KI- Nutzung nicht ausdrücklich verbietet, nutzen viele Mitarbeiter bestimmte KI-Tools, um ihre Arbeit zu vereinfachen. Damit es für die Arbeitgeber nicht teuer wird, ist es wichtig, dass dabei die Grundregeln für eine sichere und erlaubte Nutzung beachtet werden ganz generell und speziell für die Standorte in der EU. Der Beitrag bringt eine Übersicht.

› Gabriele Ochner, Stefanie Luckert

Tatsächlich gibt es kaum noch ein Unternehmen, in dem die Mitarbeiter nicht die Möglichkeiten der künstlichen Intelligenz nutzen. Dabei gibt es zwei Seiten der Medaille: die rechtlichen EU-Grundlagen zur künstlichen Intelligenz (KI-VO bzw. AI-Act) auf der einen Seite und die mit der Nutzung der KI durch die Mitarbeiter verbundenen Risiken auf der anderen.

Grundregeln zur KI-Nutzung

Die Beachtung der folgenden Grundregeln ist dabei essenziell.

Verantwortlichkeit festlegen
Innerhalb des Unternehmens sollte eine zentrale Zuständigkeit für die Koordination der Thematik KI festgelegt werden. Es sollte klar geregelt werden, wer in Bezug auf den Einsatz von KI und die Umsetzung von KI-Projekten welche Aufgaben, Kompetenzen und Verantwortlichkeiten hat. Unternehmensintern sind dabei diverse Zuständigkeiten bzw. Themen betroffen (unter anderem Datenschutz, Datensicherheit etc.). Die konkrete Ausgestaltung der Zuständigkeiten hängt im Einzelnen von der Grösse und der konkreten internen Organisation eines Unternehmens ab. Soweit bereits eine interne Zuständigkeit für den Bereich «Datenschutz» vorhanden ist, bietet es sich an, diese um die Koordination der KI zu erweitern, da es hier normalerweise bereits fundierte Sachkenntnisse in den Bereichen Datenschutz und (idealerweise auch) Datensicherheit gibt.

Inhalte prüfen, Kontrolle behalten
Weil die KI hervorragend darin ist, Texte und Inhalte zu generieren, diese aber nicht versteht, können Antworten beziehungsweise Lösungen für bestimmte Anwendungen unpassend oder falsch sein. Die Mitarbeiter müssen im Rahmen der Unternehmensvorgaben vor diesem Hintergrund dazu verpflichtet werden, den Output der KI zu kontrollieren, um der Reputation des Unternehmens oder anderer betroffener Parteien, zum Beispiel Kunden, Lieferanten oder anderen Vertragspartnern, nicht zu schaden und die Kontrolle über die Nutzung innerhalb des Unternehmens dauerhaft zu gewährleisten.

kurz & bündig

- Innerhalb des Unternehmens sollte eine zentrale Zuständigkeit für die Koordination der Thematik KI festgelegt werden.
- Seit dem 2. Februar 2025 müssen Anbieter und Betreiber (also unter anderem Unternehmen) von KI-Systemen gemäss Artikel 4 der KI-VO Massnahmen ergreifen, um ein ausreichendes Niveau an KI-Kompetenzen bei ihrem Personal sicherzustellen.

Ausschliesslich intern freigegebene KI-Tools einsetzen
Da nicht alle Anbieter vertrauenswürdig und sicher sind, sollten Mitarbeiter zumindest bei Personendaten, anderen vertraulichen, beziehungsweise sensiblen Daten und Werken Dritter nur jene Tools nutzen, deren Einsatz zuvor von hierfür qualifizierten und sachkundigen Personen (zum Beispiel IT-Abteilung oder externe Sachverständige) geprüft und freigegeben wurde.

Bestehende Regeln zum KI-Einsatz beachten
Aktuell gibt es bereits viele konkrete gesetzliche Vorgaben, die bei KI-Vorhaben

zu beachten sind. So gelten zum Beispiel die datenschutzrechtlichen Regelungen uneingeschränkt auch für die Nutzung von KI. Diese bereits bestehenden Vorgaben sollten vor der Umsetzung von Projekten geprüft werden. Alle arbeitsrechtlichen Regelungen, wie zum Beispiel Vertraulichkeits- und Verschwiegenheitspflichten (interne und gesetzliche Regelungen), gelten selbstverständlich gleichermassen für die Nutzung von KI-Tools im Rahmen der Tätigkeitsausübung durch die Mitarbeiter.

Schulung und Sensibilisierung der Mitarbeiter

Es ist wichtig, dass die Mitarbeiter dafür sensibilisiert werden, wie generative KI-Anwendungen funktionieren und wie diese in die Arbeit integriert werden können. Seit dem 2. Februar 2025 müssen Anbieter und Betreiber (also unter anderem Unternehmen) von KI-Systemen in der EU gemäss Artikel 4 der KI-VO Massnahmen ergreifen, um ein ausreichendes Niveau an KI-Kompetenzen bei ihrem Personal sicherzustellen. KI-Kompetenzen sind dabei sowohl Fähigkeiten als auch Kenntnisse und Verständnis, die es Beschäftigten ermöglichen, «KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden».

Gemäss der KI-VO haben Anbieter und Betreiber von KI-Systemen nach bestem Wissen und Gewissen dafür zu sorgen, dass eigenes Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI Systemen befasst sind, über die notwendigen KI-Kompetenzen verfügen. Mögliche Massnahmen sind Schulungen, KI-Guidelines, Weiterbildungs- und Zertifizierungsprogramme etc.

Datenschutz

Die Datenverarbeitung von ChatGPT oder anderen bekannten KI-Systemen ist bislang recht intransparent. Es ist nicht klar, auf welcher Rechtsgrundlage personenbezogene Daten dabei in die USA übermittelt werden. Ebenso wenig gibt es eine Rechtsgrundlage für die Verarbeitung und Speicherung personenbezogener Daten auf Servern in den USA. Aus diesem Grund sollte beim Einsatz generativer KI-Systeme stets geprüft werden, wo die Datenverarbeitung ganz konkret stattfindet.

Ganz wichtig: Auf die Eingabe und Nutzung von personenbezogenen und auch anderen sensiblen beziehungsweise vertraulichen Daten sollte bei der Anwendung generativer KI-Systeme aus unserer Sicht generell verzichtet werden! Das Gleiche gilt für Daten Dritter (wie zum Beispiel Vertragspartner), die in anderen Zusammenhängen entweder bezogen und/oder verarbeitet wurden. Insgesamt ist unsere Empfehlung an alle nutzenden Unternehmen, sorgfältig abzuwägen, welche Informationen in die Systeme eingespeist werden, da diese Informationen wiederum genutzt werden können, um die KI zu trainieren und zu verbessern. Seit Kurzem können immerhin ChatGPT-Nutzende über eine Opting-out-Funktion entscheiden, dass ihre Daten nicht mehr zum Trainieren der KI eingesetzt werden.

Datenqualität

Arbeitsergebnisse von KI-Tools hängen stark von der Qualität, der Quantität und Gewichtung der einzelnen Datensätze ab, mit denen sie trainiert werden. Generative KI kann möglicherweise ungenaue, irreführende oder nicht aktuelle Aussagen generieren. Bei vielen generativen KI-Systemen ist nicht transparent, welche Datenquellen genutzt werden.

Geistiges Eigentum

Daten, mit denen die KI gefüttert wurde, können urheberrechtlich geschützt sein – zum Beispiel Textbausteine, Begriffe oder Bilder. Dadurch stellt der KI-generierte Output unter Umständen eine Urheberrechtsverletzung dar. Die Vervielfältigung kann strafbar sein. Insofern ist bei von KI generiertem Output grundsätzlich immer Vorsicht geboten.

Transparenz

Wir empfehlen generell, den Einsatz von generativen KI-Modellen gegenüber den Vertragspartnern und Kunden offenzulegen, einschliesslich der Information, in welchen Abläufen sie zum Einsatz kommen. Dies kann dazu beitragen, Vertrauen bei Zulieferern, Kunden, Mitarbeitenden oder Aktionären etc. zu stärken. Diese Informationen können zum Beispiel im Rahmen einer bereits bestehenden Datenschutzerklärung des Unternehmens auf der Homepage eingefügt werden.

Haftung und Risikomanagement

Als Unternehmen sollte man mögliche rechtliche und finanzielle Risiken im Zusammenhang mit dem Einsatz von generativer KI berücksichtigen. Dazu gehört auch die Klärung der Haftungsfrage im Falle von Fehlern oder Schäden, die durch die Nutzung der KI verursacht werden. In der Regel trifft die Verantwortlichkeit für die unternehmenskonforme Nutzung die sog. Datenverantwortlichen, das heisst die Geschäftsführung. Andere Haftungsfolgen sind dabei explizit (rechtskonform) festzulegen.

Ethische Überlegungen

Als Unternehmen sollte man die potenziellen Auswirkungen des Einsatzes von generativer KI auf verschiedene Betroffene wie Kunden, Mitarbeitende und die Gesellschaft als Ganzes berücksichtigen. Es sollte sichergestellt werden, dass die Nutzung im Einklang mit den ethischen Prinzipien des Unternehmens steht. Soweit für das Unternehmen ein Code of Conduct oder andere schriftliche Leitlinien bestehen, sollte die Nutzung bestimmter KI-Tools nicht im Widerspruch zu diesen Regelungen stehen.

Coding

Falls Unternehmen generative KI im Bereich von Programmierung und Coding einsetzen, sollte man sich zuvor mit der Syntax und den Befehlen des Tools vertraut machen und die Erklärungen gründlich lesen. Fehler im Code können sich auf die Performance, Funktionalität und Sicherheit der Anwendungen auswirken.

Plug-ins und Datensicherheit

Seit Anfang April 2024 ermöglicht zum Beispiel das hinter ChatGPT stehende

Unternehmen OpenAI über neue Plug-ins die direkte Einbindung von ChatGPT in Unternehmenssysteme. So können zum Beispiel (Echtzeit-)Datensätze von Unternehmen über Schnittstellen gezielt durchsucht werden oder Aufgaben von der KI wahrgenommen werden, zum Beispiel die Buchung von Reisen. Zwar sind die Plug-in-Features aktuell noch sehr begrenzt, KI-Experten rechnen jedoch damit, dass mittelfristig ein eigenes System ähnlich dem Apple App-Store entstehen könnte. Auch bei der Nutzung von KI über solche Plug-ins sollten sich interessierte Unternehmen unbedingt intensiv mit Fragen zu Datenschutz, Urheberrecht und Datensicherheit auseinandersetzen.

KI-Policy empfohlen

Vor dem Hintergrund der vielen zu berücksichtigenden Aspekte gibt es bisher noch keine für jedes Unternehmen passenden Regularien, die man als ausreichend und umfassend empfehlen kann. Im Ergebnis ist die sichere Implementierung und Nutzung eines KI-Systems von seiten einer IT-Abteilung oder eines externen IT-Beraters zu gewährleisten, da es insbesondere technische Details, vor allem die Gewährleistung der Sicherheit vor Cyberkriminalität, zu beachten gibt, denn ein KI-Tool ist ein «Zutrittstor» für Hacker. Wir empfehlen daher, die rechtlich massgeblichen Grundsätze zur Nutzung von KI im Unternehmen festzuhalten und in nachvollziehbare, alltagstaugliche Handlungsanweisungen für die Mitarbeiter im Unternehmen umzusetzen, zum Beispiel in Form einer Richtlinie (KI-Policy) oder Arbeitsanweisung. Dafür braucht es im Vorfeld

- eine Bestandsaufnahme aller im Unternehmen eingesetzten KI-Anwendungen, um mögliche Verstösse frühzeitig zu erkennen.
- die Prüfung, ob eingesetzte oder entwickelte KI-Systeme als verbotene KI oder Hochrisiko-KI einzustufen sind. Für die letzteren Systeme gelten in der EU in späteren Umsetzungsphasen des KI-Gesetzes umfangreiche Dokumentations- und Compliance-Anforderungen.
- die Anpassung bzw. Ergänzung interner Richtlinien, insbesondere in den Bereichen Datenschutz und Ethik, um auf künftige Transparenz- und IT-Sicherheitsanforderungen vorbereitet zu sein, idealerweise durch einen Verhaltenskodex für die Mitarbeiter.
- den Aufbau einer internen Compliance-Struktur zur Überwachung und Einhaltung der regulatorischen Anforderungen. «

Veranstaltung zum Thema

Was Unternehmen beim Einsatz von KI-Systemen beachten müssen
KI als Gamechanger – aber welche Spielregeln gelten?

Eine Online-Veranstaltung der Vereinigung Schweizerischer Unternehmen in Deutschland (VSUD)

Zeit: 21. Oktober 2025, 10.30 bis 12.15 Uhr, Online
Anmeldung: Heike Würth, veranstaltungen@vsud.ch, +41 61 375 95 00

Mehr Informationen:
www.vsud.ch/beratung-service/veranstaltungen/veranstaltungskalender

Porträt

Gabriele Ochner
Rechtskonsulentin, Vereinigung Schweizerischer Unternehmen in Deutschland (VSUD)

Stefanie Luckert
Geschäftsführerin, Vereinigung Schweizerischer Unternehmen in Deutschland (VSUD)

Als branchenübergreifendes Wirtschaftsnetzwerk, politische Interessenvertretung und Fachberatung unterstützt die VSUD Schweizer Unternehmen aller Branchen und Grössenordnungen bei ihrer Marktpräsenz in Deutschland.

Kontakt

gabriele.ochner@vsud.ch
stefanie.luckert@vsud.ch
www.vsud.ch