

ChatGPT und seine Tücken

DIGITALISIERUNG *Die zunehmende Nutzung von Künstlicher Intelligenz im beruflichen Umfeld fordert Betriebsräte heraus. Zwei Fragen sind dabei zentral: Welche Haftungsrisiken bestehen für Beschäftigte und welche Mitbestimmungsrechte hat der Betriebsrat? Antworten am Beispiel der bekanntesten KI-Anwendung.*

VON ESTHER BECKHOVE

Künstliche Intelligenz (KI) wie ChatGPT wird zunehmend in Unternehmen eingesetzt, um Texte zu generieren, Informationen bereitzustellen oder Arbeitsabläufe zu erleichtern. Doch während KI-Anwendungen Effizienzgewinne bringen, bergen sie auch erhebliche Risiken – vor allem im Bereich Datenschutz und Haftung.

Für Betriebsräte stellt sich die Frage: Wie können Beschäftigte den Einsatz von ChatGPT sicher und verantwortungsvoll gestalten? Welche Haftungsrisiken bestehen für Arbeitnehmer, wenn durch die Nutzung Fehler passieren? Und welche Rolle spielt der Betriebsrat bei der Regulierung von KI-gestützten Systemen im Unternehmen? Dieser Leitfaden gibt eine praxisorientierte Übersicht über die wesentlichen Risiken und mögliche Schutzmaßnahmen für Arbeitnehmer.

Warum ist der Einsatz von ChatGPT im Betrieb problematisch?

Datenschutz- und Geheimhaltungsrisiken

ChatGPT verarbeitet Texteingaben extern, und je nach Version kann es Nutzerdaten speichern oder für das Training weitere KI-Modelle verwenden. Unternehmen und Beschäftigte laufen daher Gefahr, gegen Datenschutzvorgaben – vor allem die Datenschutz-Grundverordnung (DSGVO) – zu verstoßen.

Beispiel: Ein Mitarbeiter aus der Personalabteilung nutzt ChatGPT, um eine profes-

sionelle Formulierung für eine Kündigung zu erstellen und gibt dabei Name und Kündigungsgrund eines Beschäftigten ein. Falls diese Daten gespeichert oder verarbeitet werden, liegt ein Datenschutzverstoß vor.

Fehlerhafte oder irreführende Inhalte

ChatGPT kann Falschinformationen generieren oder veraltete bzw. ungenaue Daten liefern. Arbeitnehmer, die sich blind darauf verlassen, riskieren, fehlerhafte oder sogar rechtswidrige Inhalte weiterzugeben.

Beispiel: Ein IT-Mitarbeiter fragt ChatGPT nach einer Anleitung zur Konfiguration eines Servers. Die KI liefert eine falsche oder veraltete Anleitung, wodurch das System ausfällt und der Geschäftsbetrieb gestört wird.

Verstöße gegen betriebliche Regelungen

Nicht jedes Unternehmen erlaubt die Nutzung von KI-Anwendungen. Wer gegen unternehmensinterne Vorgaben verstößt, riskiert arbeitsrechtliche Konsequenzen.

Beispiel: Ein Mitarbeiter einer Bank nutzt ChatGPT zur Analyse von Finanzdaten, obwohl das Unternehmen den Einsatz externer KI-Tools ausdrücklich untersagt.

Unter welchen Umständen haften Beschäftigte bei Schäden durch ChatGPT?

Die Haftung von Arbeitnehmern für Fehler beim Einsatz von ChatGPT richtet sich nach

DARUM GEHT ES

1. KI-Anwendungen bringen Effizienzgewinne, bergen aber auch erhebliche Risiken – vor allem im Bereich Datenschutz und Haftung.
2. Die Haftung von Arbeitnehmern für Fehler beim Einsatz von ChatGPT richtet sich nach den Grundsätzen der beschränkten Arbeitnehmerhaftung.
3. Betriebsräte können diese Haftungsrisiken mindern, indem sie sich frühzeitig mit ChatGPT auseinandersetzen und ihr Mitbestimmungsrecht ausüben.

AUF EINEN BLICK

Die Grundlagen Künstlicher Intelligenz (KI) wurden bereits vor Jahrzehnten entwickelt, doch erst seit November 2022 gibt es einen Hype um die Technologie. Damals stellte das US-Unternehmen OpenAI seine generative KI ChatGPT vor, die als Sprachmodell rasch populär wurde. Heute sind neben dem Pionier weitere Textgeneratoren stark gefragt, auch in der Arbeitswelt, denn viele von ihnen sind in der Basisversion kostenlos und ihre Nutzung erfordert kaum technisches Wissen.

Die bekanntesten Lösungen sind sogenannte Large Language Models (LLM), also große Sprachmodelle. Dafür gibt es etwa eine Handvoll mehr oder weniger bekannter Anbieter, neben OpenAI etwa Google (mit Gemini), Meta (Llama), Anthropic (Claude) und Microsoft, dessen Copilot genanntes Sprachmodell auf ChatGPT basiert. Zuletzt debattierten Tech-Welt und Politik zudem das Potenzial und die Risiken, die mit dem Einsatz der chinesischen Open-Source-Anwendung DeepSeek verbunden sind. Aus deutscher Sicht verdient außerdem Aleph Alpha Erwähnung. Das Unternehmen wird von namhaften Geldgebern wie SAP und der Stiftung von Dieter Schwarz unterstützt, Inhaber von Lidl und Kaufland. Es hat seinen Sitz in Heidelberg und wirbt mit der Einhaltung europäischer Datenschutznormen.

den Grundsätzen der beschränkten Arbeitnehmerhaftung. Das bedeutet, dass Arbeitnehmer nicht automatisch in voller Höhe für Schäden aufkommen müssen. Die Haftung unterscheidet sich je nach Grad der Fahrlässigkeit:

Leichte Fahrlässigkeit – keine Haftung

Leichte Fahrlässigkeit liegt vor, wenn einem Beschäftigten ein geringfügiges Versehen oder ein alltäglicher Fehler unterläuft.

Konsequenz: Der Arbeitnehmer haftet nicht.

Mittlere Fahrlässigkeit – anteilig begrenzt-**te Haftung**

Mittlere Fahrlässigkeit bedeutet, dass der Arbeitnehmer zwar nicht grob unachtsam war, aber dennoch gegen seine Sorgfaltspflichten verstoßen hat.

Konsequenz: Je nach Schaden kann der Arbeitnehmer anteilig haften, oft unter Berücksichtigung seines Einkommens.

Grobe Fahrlässigkeit – volle oder überwiegende Haftung

Grobe Fahrlässigkeit liegt vor, wenn ein Arbeitnehmer seine Sorgfaltspflichten in außergewöhnlich hohem Maß verletzt und einen Schaden billigend in Kauf nimmt.

Konsequenz: Der Arbeitnehmer kann in voller Höhe haftbar gemacht werden.

Vorsatz – volle Haftung

Bei vorsätzlichem Handeln (z. B. absichtlicher Geheimnisverrat oder bewusst falsche Information) haftet der Arbeitnehmer in vollem Umfang.

Beispiel: Ein Mitarbeiter gibt bewusst vertrauliche Geschäftsgeheimnisse in ChatGPT ein, um eine interne Analyse zu erleichtern, obwohl ihm bekannt ist, dass die Daten extern verarbeitet werden.

Konsequenz: Dies kann neben zivilrechtlichen Schadensersatzforderungen auch eine fristlose Kündigung und strafrechtliche Konsequenzen nach sich ziehen.

Abgrenzung der verschiedenen Arten von Fahrlässigkeit

Wann welche Form der Fahrlässigkeit vorliegt, ist in der Praxis schwer zu entscheiden. Es kommt auf die Einzelheiten an und oft liegen Versehen, mangelnde Sorgfalt und Pflichtverletzung nah beieinander.

Ungenaue Übersetzung

Ein Mitarbeiter nutzt ChatGPT, um eine geschäftliche E-Mail an einen ausländischen Geschäftspartner zu übersetzen. Durch eine ungenaue Übersetzung entsteht ein Missverständnis, das zu Verzögerungen in einer Lieferkette führt. Der Arbeitgeber muss daraufhin zusätzliche Maßnahmen ergreifen, um das

Problem zu lösen.

Einstufung: Leichte Fahrlässigkeit

Begründung: Der Mitarbeiter hätte die Übersetzung sorgfältiger prüfen oder sie von einem Kollegen gegenlesen lassen können. Hier hingegen hat der Mitarbeiter vermutlich geglaubt, dass die KI-Übersetzung ausreichend ist, und das Missverständnis war nicht unmittelbar vorhersehbar. Die Fehlinterpretation ist ein »alltägliches Missgeschick«, das durch eine zusätzliche Kontrolle vermeidbar gewesen wäre. Die Verzögerung in der Lieferkette ist zwar ärgerlich, aber kein schwerwiegender Schaden (z. B. keine Vertragsstrafe oder erhebliche finanzielle Verluste). Der Arbeitgeber muss zwar reagieren, aber es entstehen keine katastrophalen Konsequenzen.

Grobe Fahrlässigkeit würde im Gegensatz dazu vorliegen, wenn der Mitarbeiter eine naheliegende und offensichtliche Sorgfaltspflicht verletzt. Das wäre dann der Fall, wenn der Mitarbeiter eine geschäftliche E-Mail ohne jegliche Prüfung aus einer KI übernimmt, obwohl er weiß, dass es sich um einen besonders kritischen oder rechtsverbindlichen Vertragstext handelt.

Falsche Produktbeschreibung

Ein Mitarbeiter im E-Commerce nutzt ChatGPT, um eine Produktbeschreibung für einen neuen Artikel zu erstellen. ChatGPT beschreibt das Produkt als »wasserdicht«, obwohl es tatsächlich nur »wasserabweisend« ist. Der Mitarbeiter überprüft den Text nicht gründlich und stellt die Beschreibung online. Nach einiger Zeit reklamieren einige Kunden, weil das Produkt nicht den Erwartungen entspricht. Das Unternehmen muss einige Rückstattungen leisten.

Einstufung: Mittlere Fahrlässigkeit

Begründung: Der Mitarbeiter hätte die Produktbeschreibung sorgfältig prüfen müssen, da er für die Richtigkeit der veröffentlichten Informationen verantwortlich ist. Die Begriffe »wasserdicht« und »wasserabweisend« haben eine klare Bedeutung im Produktmarketing und ein solcher Fehler kann für Kunden kaufentscheidend sein. Zwar handelt es sich nicht um eine absichtliche Täuschung, aber der Feh-

ler hätte durch eine einfache Kontrolle leicht vermieden werden können. Der entstandene Schaden (Rückstattungen) ist begrenzt, aber nicht unerheblich.

Wie kann der Betriebsrat zur Regulierung der ChatGPT-Nutzung beitragen?

Mitbestimmungspflichten des Betriebsrats

Nach § 87 Abs. 1 Betriebsverfassungsgesetz (BetrVG) hat der Betriebsrat bei der Einführung und Anwendung von technischen Systemen, die das Verhalten oder die Leistung der Beschäftigten erfassen können, ein Mitbestimmungsrecht. Auch ChatGPT fällt in diese Kategorie, wenn das Unternehmen Vorgaben zur Nutzung macht oder soweit KI-Systeme zur Überwachung von Verhalten oder Leistung der Arbeitnehmer geeignet sind.

Betriebsvereinbarungen zu KI-Nutzung

Betriebsräte sollten darauf hinwirken, dass klare Regelungen für den Umgang mit ChatGPT und anderen KI-Tools getroffen werden. Eine Betriebsvereinbarung könnte folgende Punkte regeln:

- **Zulässige und unzulässige Anwendungsfälle** (z. B. kein Einsatz für vertrauliche Dokumente)
- **Datenschutzkonforme Nutzung** (z. B. keine Eingabe personenbezogener Daten)
- **Qualitätssicherung** (z. B. Pflicht zur Überprüfung von KI-generierten Inhalten)
- **Haftungsregelungen** (z. B. Begrenzung der Arbeitnehmerhaftung bei Fehlern, besonders für die Fälle der mittleren Fahrlässigkeit und hinsichtlich der Höhe des Anspruchs gegen den Arbeitnehmer)
- **Klärung der Verantwortlichkeiten** (wer haftet für Fehler in KI-generierten Inhalten)

Sensibilisierung und Schulung der Beschäftigten

Viele Beschäftigte nutzen ChatGPT, ohne die Chancen und Risiken der Software zu kennen. Der Betriebsrat kann auf Schulungen und klare Leitlinien drängen, um die Belegschaft für den Datenschutz zu sensibilisieren, sie auf Haftungsrisiken hinweisen und ihr zu vermitteln, wie wichtig eine Überprüfung KI-generierter Texte und Empfehlungen ist. Dies kann

eine sichere Nutzung von Sprachmodellen gewährleisten und ist im Übrigen ein Erfordernis der KI-Verordnung der EU: Seit Februar dieses Jahres müssen Unternehmen ihren mit KI-Systemen arbeitenden Beschäftigten »ausreichende« KI-Kompetenz vermitteln (s. auch Beitrag auf S. #####).

das verantwortungsvoll tun zu können. Das liegt nicht nur im Interesse des Gesetzgebers, sondern auch in dem des Betriebs und vor allem im Interesse der Beschäftigten.◀

Esther Beckhove, Fachanwältin für
Arbeitsrecht.
www.beckhove.de



AUF EINEN BLICK

Checkliste für eine Betriebsvereinbarung zu ChatGPT

1. **Zulässige Nutzung:** In welchen Arbeitsbereichen darf ChatGPT eingesetzt werden?
2. **Verbotene Eingaben:** Wie ist die Übermittlung sensibler Daten und vertraulicher Informationen an die KI zu verhindern?
3. **Überprüfungspflicht:** Wer trägt die Verantwortung für den Umgang mit KI-generierten Inhalten?
4. **Haftungsregelungen:** Wer haftet wann und wie sind Beschäftigte vor unweisentlichem Fehlverhalten zu schützen?
5. **Schulungsmaßnahmen:** Der sichere Umgang mit KI verlangt verpflichtende Trainings.
6. **Mitbestimmungsrechte:** Bei Einführung und Nutzung von KI-Tools wird der Betriebsrat eingebunden.

Quintessenz: Was Betriebsräte tun können

Der Einsatz von ChatGPT im Arbeitsumfeld ist nicht per se problematisch, birgt aber erhebliche Haftungs- und Datenschutzrisiken für die Beschäftigten. Betriebsräte können diese Risiken mindern, indem sie sich frühzeitig mit dem Thema auseinandersetzen und ihr Mitbestimmungsrecht ausüben. Die Einführung und Nutzung von ChatGPT und anderen KI-Anwendungen verlangt erstens klare, in einer Betriebsvereinbarung verankerte Regeln. Zweitens gilt es, die Schulung der Beschäftigten sicherzustellen: Wer KI einsetzt, braucht bestimmte Kenntnisse und Kompetenzen, um

