ChatGPT: Was Unternehmen rechtlich beachten sollten

ChatGPT ist seit Ende des vergangenen Jahres in aller Munde. Die KI des US-Unternehmens OpenAI wird unterdessen bereits in einigen Unternehmen eingesetzt. Was diese beachten müssen, weiss Isabelle Wildhaber, Professorin für Privat- und Wirtschaftsrecht an der Universität St.Gallen.

Isabelle Wildhaber, ChatGPT ist eigentlich nichts anderes als ein Chatbot, wie er in vielen Unternehmen und Behörden bereits eingesetzt wird. Beispielsweise für die Beantwortung von Standardfragen im Kundendienst. Was also macht diesen «Super-Bot» so interessant für Unternehmen?

ChatGPT, ein generatives KI-Sprachmodell von OpenAI, bewegt die Welt seit Ende letzten Jahres. Er kann Aufsätze schreiben, Codierungen vornehmen oder komplexe Forschungsaufträge strukturieren – und das alles in Sekundenschnelle. Die Qualität der Antworten von ChatGPT schickte Schockwellen durchs Silicon Valley. Google hat dann Anfang Februar seinen eigenen KI-Chatbot «Bard» präsentiert. ChatGPT ist durchaus etwas anderes als herkömmliche Chatbots!

«Die Qualität der Antworten schickte Schockwellen durchs Silicon Valley.»

Wie funktioniert ChatGPT denn?

ChatGPT basiert auf einem Deep-Learning-Modell, welches mit einem riesigen Datensatz trainiert wird. Die Daten stammen aus Webscraping, Büchern, Wikipedia und anderen Textquellen. ChatGPT ist aber nicht direkt mit dem Internet verbunden, das bedeutet, er kann nur auf seine eigenen Trainingsdaten zurückgreifen und nicht auf externe Informationen im Internet. Das Modell wurde mit dem Ziel trainiert, jeweils das nächste Wort vorherzusagen.

Die Digitalisierung ist bekanntlich gekommen, um zu bleiben. Welchen Stellenwert könnte ChatGPT in Zukunft in der Arbeitswelt einnehmen?

Das Auftauchen von ChatGPT ist ein Schlüsselmoment, das mit der Erfindung des Internets vergleichbar ist. Es wird in Zukunft nicht mehr wegzudenken sein und die Art, wie wir arbeiten, überall beeinflussen und ändern, genauso wie es das Internet in den vergangenen 20 Jahren getan hat. Eine Nutzung von ChatGPT im geschäftlichen Kontext könnte z. B. darin bestehen, ChatGPT als integrierten Kunden-Support Chatbot auf der eigenen Website oder als Recherchetool zu verwenden.

ChatGPT verwendet sowohl die Eingaben als auch den Output für die Entwicklung oder Verbesserung seiner Dienste. Kann der Bot unter diesen Voraussetzungen überhaupt seriös in Unternehmen eingesetzt werden?

ChatGPT kann sehr hilfreich sein. Aber wir müssen tatsächlich lernen, bei unseren Eingaben keine Betriebs- und Geschäftsgeheimnisse oder sonst Vertrauliches preiszugeben. Bei ChatGPT können Nutzer ihre Fragen oder Befehle an die KI in ein Suchfeld eingeben und diese Eingaben nennt man «Prompts». Nutzer dürfen sich nicht zu einer Erwähnung von Betriebs- und Geschäftsgeheimnissen in den Prompts verleiten lassen. Ein Nutzer könnte etwa ein Geschäftsgeheimnis erwähnen, um Anregungen für weitere Produktideen oder Ideen für neue Dienstleistungen zu bekommen.

Wie sieht das mit dem Datenschutz aus bei ChatGPT?

Der Datenschutz spielt bei ChatGPT gleich in mehrfacher Hinsicht eine wichtige Rolle. Werden in den Prompts Angaben gemacht, die auf eine Person direkt oder indirekt schliessen lassen, werden über ChatGPT personenbezogene Daten verarbeitet. Die Mitarbeiter von Unternehmen sollten sensibilisiert werden, keine Prompts bei ChatGPT einzugeben, die personenbezogenen Daten von einem ihrer Kunden, Lieferanten, Geschäftspartner oder Arbeitskollegen enthalten. Ausserdem müssen Unternehmen darauf achten, welche datenschutz-

Isabelle Wildhaber: Der Datenschutz spielt eine wichtige Rolle.

rechtlichen Vereinbarungen abgeschlossen werden müssen, um Datentransfers in unsichere Drittländer zu legitimieren.

Wie kann man als Unternehmen sicherstellen, dass Antworten des Bots, die man ggf. für PR-Texte verwendet, nicht gegen Urheberrecht verstossen?

ChatGPT ist nicht Urheber des vom KI-Sprachmodell erzeugten Outputs, weil er kein Mensch ist. Deshalb können die Texte durch den ChatGPT-Nutzer frei verwendet werden. Das ergibt sich auch aus den Terms and Conditions von OpenAI. Es ist aber nicht auszuschliessen, dass bei der Verwendung von ChatGPT-Output urheberrechtliche Ansprüche von Dritten entstehen. Denn als Nutzer hat man ja keinen näheren Einblick in die Trainingsdaten. Wenn die KI mehrere Sätze oder Absätze aus vorhandenen, menschengeschaffenen Texten zitiert, könnte das eine zustimmungspflichtige Vervielfältigung sein.

«Wir müssen lernen, bei unseren Eingaben nichts Vertrauliches preiszugeben.»

Im digitalen Zeitalter werden AGB nur noch selten wirklich gelesen und meist einfach so akzeptiert. Das ist bei einem so mächtigen Tool wie ChatGPT wohl nicht ratsam, oder?

Terms and Conditions der Anbieter von KI-Einwendungen sowie die Lizenzvereinbarungen müssen geprüft und eingehalten werden. Unternehmen sollten darauf achten, welche Rechte sich die Anbieter der KI-Anwendungen an den Prompts einräumen lassen und wie es sich mit der kommerziellen Verwertung der Outputs verhält. Ausserdem unterscheidet ChatGPT z. B. private und gewerbliche Nutzung und verlangt eine «Corporate Membership» für Arbeitgeber.

Es gibt also einige Stolpersteine bei der Nutzung von ChatGPT in Unternehmen. Bereits wird deshalb auch schon vereinzelt der Ruf laut, ihn für die Nutzung in Unternehmen zu verbieten. Kann man das überhaupt?

Ich fände es nicht sinnvoll, ChatGPT zu verbieten. Ich würde eher dazu raten, die eigenen Mitarbeiter zu schulen.

Und wie konkret?

Wir müssen alle lernen, wie wir unsere Suchanfragen und Befehle an ChatGPT und die vielen anderen generativen KI-Tools (z. B. DALL-E oder Midjourney für KI-generierte Bilder) möglichst präzise und für die KI erkennbar formulieren, um einen qualitativ hochwertigen und verwertbaren Output zu erzielen. Die Mitarbeiter müssen dafür sensibilisiert werden, dass der Output von ChatGPT & Co. kritisch hinterfragt werden muss. Die Fakten müssen selbst recherchiert werden, da der Output unvollständig oder gar falsch sein kann. Des Weiteren würde ich die Mitarbeiter aufklären, was für ein rechtssicheres Prompting notwendig ist, d. h. über Themen wie Datenschutz und Betriebs- und Geschäftsgeheimnisse informieren.

Interview: Patrick Stämpfli Bild: zVg