



Weiterchatten mit Hubert – neue rechtliche Entwicklungen zu KI-Chatbots



Das Problem – Warum Chatbots?

Das Ausgangsproblem bleibt auch mit Inkrafttreten der KI-Verordnung unverändert. Eine Website mit vielen wichtigen Informationen ist für Kunden hilfreich, aber nur soweit sie die Informationen auch gut auffinden können. Selbst wenn die Webseiten gut durchdacht und ordentlich strukturiert sind, bleiben die Kunden oftmals unzufrieden, da sie aufgrund der Menge an Informationen das für sie Richtige nicht finden können. Hier wünschen sie sich dann doch das kurze Gespräch mit einem Gegenüber, in welchem die konkreten Fragen geklärt werden können. Die Unternehmen wissen dies und richten häufig einen Kundensupport ein; letzterer wird – wie bereits in unseren [Praxistipp Chatten mit Hubert](#) dar-

gestellt kommen immer häufiger Chatbots zum Einsatz, um Support-Mitarbeitende zu entlasten..

Was ist ein Chatbot?

Solche Chatbots wie „Hubert“ basieren auf Künstlicher Intelligenz (KI). Hubert, als Chatbot-Applikation mit einer anwenderfreundlichen Benutzeroberfläche, kann Fragen, die ihm in einem „Support-Chat“ gestellt werden, erkennen und beantworten. Für dieses Anwendungsszenario wird zuvor ein generatives Sprachmodell in das unternehmenseigene System integriert und zumeist mit Daten aus unternehmenseigenen Vorgängen trainiert. Auf diese Weise wird es möglich, verfü-

Gefördert durch:



Bundesministerium
für Wirtschaft
und Klimaschutz

Mittelstand-
Digital

aufgrund eines Beschlusses
des Deutschen Bundestages



bare text-generierende KI-Modelle an die eigenen Bedürfnisse des Unternehmens anzupassen (sog. „Pre-Prompt-Engineering“). Stellt ein Kunde eine Anfrage (setzt einen Prompt), kann diese vom Chatbot sofort und unternehmensbezogen beantwortet werden.

Sofern ein solches Vorhaben seitens des Unternehmens umgesetzt wird, stellt sich die Frage, welche Rolle das Unternehmen nach der KI-Verordnung einnimmt. Ist es Anbieter und/oder Betreiber?

Chatbots als Allzweck-KI

Im [Parxistipp Chatten mit Hubert](#) haben wir bereits verschiedene rechtliche Anforderungen beleuchtet, die bei Planung und Einsatz von Chatbots beachtet werden müssen. Hier fokussierten wir insbesondere die Lizenzbedingungen der beigezogenen KI-Modelle/Systeme sowie datenschutzrechtliche Anforderungen. Beides bleibt auch weiter von hoher Relevanz.

Hinzu treten nun allerdings die Anforderungen der KI-Verordnung, die seit August 2024 in Kraft sind. Dies betrifft auch große Sprachmodelle die generative KI nutzen (sog. GPAI-Modelle bzw. „Allzweck-KI“), zu denen auch Chatbots gehören. Die Regelungen der KI-Verordnung für diese Allzweck-KI, gelten allerdings frühestens ab dem 2. August 2025 (Art. 113 KI-Verordnung)¹, weshalb auch noch etwas Zeit bleibt, sich auf die neuen Regelungen einzustellen.

Die KI-Verordnung formuliert Anforderungen an KI-Modelle mit allgemeinem Verwendungszweck (GPAI bzw. Allzweck-KI). Dabei wird nach Modellen mit und ohne systemisches Risiko unterschieden. Für erstere wird vor allem Transparenz und die Einhaltung des Urheberrechts gefordert (Art. 53 KI-Verordnung). Modelle mit systemischem Risiko müssen auch Anforderungen an Risiko-Ermittlung und -Minderung genügen (Art. 55 KI-Verordnung). Die Pflichten treffen dabei den Anbieter (≈ Entwickler) nicht jedoch den Betreiber (≈ Nutzer).

¹ Wurde das Allzweck-KI-Modell vor dem 2. August 2025 in Verkehr gebracht, muss der Anbieter die Pflichten aus dem AI-Act erst zum 2. August 2027 erfüllen (Art. 111 KI-Verordnung).

Wichtige Abgrenzungsfrage: Anbieter oder Betreiber?

Insofern muss die Frage beantwortet werden, in welcher Rolle das betroffene Unternehmen in Bezug auf das KI-System sowie das dahinterstehende KI-Modell auftritt. In der Regel wird das Unternehmen, das nur ein fremdes KI-Modell in die eigene Anwendung integriert, es also auf ein „geschlossenes System“ zugreift, kein Entwickler sein, sondern nur Betreiber. Findet allerdings im Rahmen eines Trainingsprozesses – wie in unserem Beispiel – ein Training mit unternehmenseigenen Daten statt, wird also das KI-System im Rahmen des „Finetuning“ womöglich verändert, kann sich ein zuvor entwickeltes „geschlossenes System“ weiterentwickeln und womöglich zu einem eigenständigen (neuen) KI-Modell werden. Dann würde das Unternehmen in die Rolle eines Anbieters verfallen, dessen Pflichtenlage nach der KI-Verordnung deutlich umfassender ist. Diese Grenzziehung ist vom Einzelfall abhängig und die „Kippunkte“ sind aufgrund der in hohem Maße auslegungsbedürftigen Regelungen der KI-Verordnung noch unklar.

Allerdings soll die KI-Verordnung künftig durch Praxisleitfäden erläutert werden (Art. 56 KI-Verordnung), die sich diesen schwierigen Auslegungs- und Abgrenzungsfragen annehmen. Die Entwicklung dieser Praxisleitfäden hat auf europäischer Ebene bereits begonnen.

Fazit

Die Nutzung von Chatbots im Kunden-Support bleibt weiterhin eine gute Möglichkeit, die Kundenzufriedenheit zu erhöhen und die eigenen Mitarbeitenden zu entlasten. Dennoch kann es sein, dass zu den bereits existierenden rechtlichen Anforderungen (Lizenzen, Datenschutz) weitere hinzutreten. Wie diese genau ausgestaltet sind und ob sie auch mittelbar den Betreiber oder lediglich den Anbieter treffen, wird in Zukunft mit der Veröffentlichung von Praxisleitfäden weiter konkretisiert werden. Wir empfehlen, die Entwicklungen weiterhin aufmerksam zu verfolgen.