KI-Chatbots auf Unternehmenswebseiten

Rechtliche Rahmenbedingungen, Risiken und Gestaltungsempfehlungen

Executive Summary

Überblick

Der Einsatz von KI-Chatbots auf Unternehmenswebseiten bietet erhebliche Chancen zur Effizienzsteigerung, birgt aber zugleich komplexe rechtliche Risiken. Die Technologie hat sich von einfachen regelbasierten Systemen zu hochentwickelten Large Language Models (LLM) entwickelt, die Dialoge führen und kontextbezogen auf komplexe Anfragen reagieren können. Noch riskanter wird es, wenn KI-Agenten untereinander kommunizieren und autonom Geschäftsprozesse abwickeln.

Zentrale rechtliche Herausforderungen bei KI Chatbots auf Webseiten

- **Datenschutzrecht (DSGVO):** Jede KI-Chatbot-Interaktion verarbeitet personenbezogene Daten (IP-Adresse, Gesprächsinhalte). Erforderlich sind Rechtsgrundlagen nach Art. 6, 9 DSGVO, umfassende Informationspflichten, Auftragsverarbeitungsverträge (AVV) mit Anbietern sowie ggf. Datenschutz-Folgenabschätzungen (DSFA). Zudem ist Art. 22 DSGVO (menschliche Letztentscheidung) sicherzustellen.
- **KI-Verordnung (AI Act):** Ab 02.08.2026 gilt eine Transparenzpflicht nach Art. 50 KI-VO: Nutzer müssen vor Interaktionsbeginn darauf hingewiesen werden, dass sie mit einer KI kommunizieren. Die Risikoklassifizierung bestimmt weitere Pflichten: Systeme mit geringem Risiko unterliegen primär Transparenzanforderungen, Hochrisiko-KI erfordert Risikomanagementsysteme, technische Dokumentation, Aufnahme ins KI-Register des Unternehmens und Konformitätsbewertungen.
- **Vertragsrecht: KI** Chatbot-Erklärungen können unter Umständen dem Unternehmen als Willenserklärungen zugerechnet werden. Ein vom KI Chabot genannter Preis oder eine Lieferzusage kann rechtsverbindlich sein. Dies gilt auch bei Fehlern durch Halluzinationen. Besonders kritisch: Agent-to-Agent-Kommunikation ohne menschliche Kontrollinstanz.
- **Haftungsrisiken:** Fehlerhafte Auskünfte können zu Schadensersatzansprüchen führen, Verträge mit nachteiligem Inhalt können geschlossen werden, irreführende Aussagen können zu wettbewerbsrechtlichen Abmahnungen nach UWG führen; daneben bestehen Pflichten aus dem Fernabsatz. Auch muss darauf

RAin Michaela Berger, LL.M.
Fachanwältin für IT-Recht
Datenschutz-Auditorin · Datenschutzbeauftragte
michaela.berger@rdp-law.de

geachtet werden, dass keine unzulässige Beratung z.B. aus den Bereichen Recht, Medizin oder Finanzen stattfindet.

Empfohlene Schutzmaßnahmen beim Einsatz von KI-Chatbots

Technische Maßnahmen:

- Strikte Funktionsbegrenzung: Bot darf keine rechtsverbindlichen Erklärungen abgeben
- Festlegung von Wissensquellen und Zugriffsberechtigungen;
- Outputfilter
- Festlegung fit / unfit for purpose
- keine Preisnennung durch den Bot (Verweis auf Webseite/Kundenservice)
- Logging und (stichprobenartiges) Monitoring aller Chatverläufe
- Regelmäßige Tests und Kontrolle

Rechtliche Maßnahmen:

- Haftungsbeschränkungen im Rahmen des AGB-Rechts (§§ 305 ff. BGB)
- Auftragsverarbeitungsvertrag (AVV) mit Verbot der Datenweiterverwertung zu eigenen Zwecken
- Prüfung und ggf. Anpassung des Versicherungsschutzes

Fazit: Rechtssicherheit als Schlüssel für den erfolgreichen Einsatz von KI-Chatbots

KI-Chatbots erfordern sorgfältige rechtliche Planung. Eine Kombination aus technischen Guardrails, durchdachter Nutzungsrechts-Gestaltung, transparenter Kommunikation und kontinuierlicher Überwachung ermöglicht rechtssicheren Einsatz. Unternehmen, die diese Aspekte systematisch adressieren, können die Vorteile der Technologie nutzen, ohne sich unkalkulierbaren Haftungsrisiken auszusetzen.

www.rdp-law.de
RAin Michaela Berger, LL.M.
Fachanwältin für IT-Recht
Datenschutz-Auditorin · Datenschutzbeauftragte
michaela.berger@rdp-law.de

Einleitung

Immer mehr Unternehmen setzen KI-gestützte Chatbots auf ihren Webseiten ein, um Kunden rund um die Uhr zu betreuen, Anfragen zu beantworten oder sogar Geschäftsprozesse zu automatisieren.

Während frühere Chatbots lediglich auf vordefinierte Antwortbäume zurückgriffen, sind moderne Systeme auf Basis großer Sprachmodelle (Large Language Models, LLM) in der Lage, frei formulierte Dialoge zu führen und dabei kontextbezogen auf komplexe Anfragen einzugehen.

Rechtlich komplexer und ungleich riskanter wird es, wenn KI-Agenten nicht mehr nur mit Menschen, sondern auch untereinander kommunizieren: Der Chatbot eines Kunden stimmt automatisch mit dem KI-System eines Lieferanten Bestellungen ab oder handelt Vertragskonditionen und Rabatte aus.

Mit den wachsenden Einsatzmöglichkeiten steigen auch die rechtlichen Anforderungen und Risiken. Unternehmen müssen eine Vielzahl von Regelungen beachten, die vom Datenschutzrecht über das Vertragsrecht, das Wettbewerbsrecht bis hin zur europäischen KI-Verordnung (KI-VO) reichen.

Dieser Beitrag gibt einen Überblick über die wesentlichen Rechtsfragen, die beim Einsatz von KI-Chatbots auf Unternehmenswebseiten zu beachten sind, und zeigt Gestaltungsmöglichkeiten auf, um rechtliche Risiken zu minimieren.

Einsatzszenarien von KI-Chatbots

KI-Chatbots auf Webseiten lassen sich in verschiedenen Konstellationen einsetzen, die jeweils unterschiedliche rechtliche Fragen aufwerfen:

KI CHATBOTS IN KUNDENSERVICE UND SUPPORT

Der KI-Chatbot beantwortet Fragen zu Produkten, Dienstleistungen, Lieferzeiten oder Rückgabebedingungen. Er kann Nutzer durch FAQ-Bereiche führen, Störungsmeldungen entgegennehmen oder an den passenden Ansprechpartner weiterleiten. Denkbar ist aber auch der Einsatz in Bereichen der Stammdatenänderungen (Bankverbindung, Kontaktdaten) oder typische kundenvertragsbezogene Anfragen: Entgegennahme von Kündigungen von Abos, Zählerstandsmeldungen im Energiesektor.

BERATUNG UND PRODUKTEMPFEHLUNGEN DURCH KI CHATBOTS

Chatbots können Nutzer bei der Produktauswahl beraten, individuelle Empfehlungen aussprechen oder Konfigurationen vorschlagen. Hier bewegt sich der KI Chatbot bereits in einem Bereich, in dem fehlerhafte oder irreführende Aussagen Haftungsfragen auslösen können, insbesondere wenn die Empfehlung als verbindliche Zusicherung verstanden werden kann. Auch können Beratungen erfolgen, die bestimmten rechtlichen Schranken unterliegen, wie z.B. unzulässige Rechtsberatung, Beratung im Bereich Medizin oder Finanzen.

RAin Michaela Berger, LL.M.
Fachanwältin für IT-Recht
Datenschutz-Auditorin · Datenschutzbeauftragte
michaela.berger@rdp-law.de

KI CHATBOTS BEI VERTRAGSANBAHNUNG UND VERTRAGSSCHLUSS

Rechtlich noch kritischer ist die Einbindung des KI-Chatbots in den Bestellprozess. Der Chatbot kann diesbezüglich Preise nennen, Angebote unterbreiten, Bestellungen entgegennehmen oder sogar Verträge abschließen. Unternehmen müssen in diesem Bereich besonders die Frage klären, ob der Chatbot wirklich rechtswirksame Verträge schließen soll und wie sich dies ggf. verhindern lässt oder konform gestaltet werden kann.

WEITERE EINSATZGEBIETE VON KI CHATBOTS

Darüber hinaus sind zahlreiche weitere Einsatzgebiete für Chatbots denkbar und auch in der Praxis bereits im Einsatz, wie z.B. im Beschwerdemanagement, bei der Terminvereinbarung, im internen Wissensmanagement mit Kundenschnittstelle oder bei der Lead-Generierung im Vertrieb. Jedes Szenario bringt spezifische rechtliche Herausforderungen mit sich.

Datenschutzrechtliche Anforderungen beim Einsatz von KI Chatbots auf Webseiten

Beim Einsatz eines KI-Chatbots auf einer Webseite werden immer personenbezogene Daten verarbeitet, was den Anwendungsbereich der DSGVO eröffnet. Bereits die IP-Adresse des Nutzers, seine Eingaben im Chat und die daraus generierten Gesprächsverläufe stellen personenbezogene Daten im Sinne der DSGVO dar. Unternehmen müssen daher eine Reihe von datenschutzrechtlichen Anforderungen erfüllen:

RECHTSGRUNDLAGE DER DATENVERARBEITUNG

Für jede Verarbeitung personenbezogener Daten ist eine Rechtsgrundlage nach DSGVO erforderlich. Welche Rechtsgrundlage einschlägig ist, hängt vom konkreten Einsatzszenario und dem Zweck der Datenverarbeitung ab. Dient der KI Chatbot ausschließlich der Beantwortung allgemeiner Fragen, kann Rechtsgrundlage das berechtigte Interesse des Unternehmens an einem effizienten Kundenservice sein. Auch kommt in Angelegenheiten des Kundenservices regelmäßig die Rechtsgrundlage Art. 6 Abs. 1 lit. b) DSGVO in Betracht, wenn der KI Chatbot Daten zur Begründung oder Durchführung eines Vertragsverhältnisses mit dem Nutzer verarbeitet. Es wird aber auch Verarbeitungen personenbezogener Daten geben, die nur mit ausdrücklicher vorheriger Einwilligung des Nutzers zulässig sind.

INFORMATIONSPFLICHTEN NACH DSGVO

Gemäß Art. 12, 13 und 14 DSGVO sind Nutzer umfassend über die Datenverarbeitung zu informieren. Die Datenschutzerklärung der Webseite muss daher um Angaben zur Datenverarbeitung bei Nutzung des KI-Chatbots ergänzt werden.

RAin Michaela Berger, LL.M.
Fachanwältin für IT-Recht
Datenschutz-Auditorin · Datenschutzbeauftragte
michaela.berger@rdp-law.de

AUFTRAGSVERARBEITUNG MIT ANBIETERN VON KI-CHATBOTS

Wird der KI-Chatbot über einen externen Dienstleister betrieben, etwa über eine Cloud-basierte KI-Plattform, liegt in der Regel eine Auftragsverarbeitung nach Art. 28 DSGVO vor. In diesem Fall ist ein Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO (AVV) mit dem Anbieter abzuschließen. Neben den üblichen rechtlichen Themen, die in einer AVV geregelt werden, muss ausdrücklich geregelt sein, dass der Auftragsverarbeiter (Anbieter) die über den KI Chatbot verarbeiteten Daten nicht zu eigenen Zwecken nutzen darf, insbesondere nicht zum Training der eigenen KI-Modelle. Auch beim Thema Datenlöschung bestehen KI-spezifische Herausforderungen.

Zudem stellen sich diesbezüglich oft Fragen der Datenverarbeitung in unsicheren Drittstaaten, die gelöst werden müssen.

DATENSCHUTZ-FOLGENABSCHÄTZUNG BEIM EINSATZ VON KI-CHATBOTS

Abhängig vom Umfang der Datenverarbeitung und den eingesetzten Technologien kann eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO erforderlich sein. Dies gilt insbesondere dann, wenn der Chatbot umfangreiche Nutzerprofile erstellt, besondere Kategorien personenbezogener Daten verarbeitet oder automatisierte Einzelentscheidungen im Sinne des Art. 22 DSGVO trifft.

KI Chatbots und KI-Verordnung (KI-VO, AI Act)

IST WEBSEITENBETREIBER ANBIETER ODER BETREIBER EINES KI-SYSTEMS IM SINNE DER KI VO

An die Stellung als Anbieter oder Betreiber eines KI-Systems werden in der KI VO unterschiedliche und teilweise für Anbieter sehr weitreichende Verpflichtungen geknüpft.
Webseitenbetreiber müssen somit in einem ersten Schritt klären, welche Stellung sie bei Einsatz des KI Chatbots auf der eigenen Webseite innehaben.
Dies ist eine umfangreiche rechtliche Bewertung, die den Einsatzzweck, das Maß an Modifikation und weitere Merkmale mit einbezieht. Die Grenzen zwischen Anbieter und Betreiber sind in diesem Bereich schnell überschritten, weswegen eine sichere rechtliche Beurteilung unumgänglich ist.

Wird der KI-Chatbot im KI-Modell mit eigenen Daten trainiert und/oder für den Webseitenbetreiber direkt entwickelt und als z.B. „DerWebseitenbetreiberBot“ mit eigenem Namen des Unternehmens betrieben, kann der Webseitenbetreiber zum Anbieter werden.

RAin Michaela Berger, LL.M.
Fachanwältin für IT-Recht
Datenschutz-Auditorin · Datenschutzbeauftragte
michaela.berger@rdp-law.de

Bei einem KI-Chatbot, der auf einem Template eines anderen Anbieters aufsetzt, keinen eigenen „Webseitenbetreibernamen" erhält und nur auf die Websuche, feste interne Datenquellen oder RAG-Systeme zurückgreift, ist der Webseitenbetreiber in der Regel nur Betreiber.

TRANSPARENZPFLICHT NACH ART. 50 KI-VO BEI KI CHATBOTS

Art. 50 Abs. 1 KI-VO verpflichtet den Anbieter eines KI-Systems, das zur direkten Interaktion mit natürlichen Personen bestimmt ist, sicherzustellen, dass die betroffenen Personen darüber informiert werden, dass sie mit einem KI-System interagieren. Für KI Chatbots auf Webseiten bedeutet dies, dass der Nutzer klar und unmissverständlich darauf hingewiesen werden muss, dass er mit einer Künstlichen Intelligenz kommuniziert und nicht mit einem Menschen. Dieser Hinweis muss rechtzeitig, also vor Beginn der Interaktion, erfolgen.

Die Transparenzpflicht gilt ab dem 02.08.2026. Verstöße sind bußgeldbewehrt.

RISIKOKLASSIFIZIERUNG

Die KI-VO verfolgt einen risikobasierten Ansatz. somit muss jeder Einsatz eines KI-Chatbots nach Risikostufen klassifiziert werden.
KI Chatbots, die ausschließlich im Kundenservice eingesetzt werden, dürften in der Regel als KI-Systeme mit geringem Risiko einzustufen sein, für die primär die Transparenzpflichten gelten. Wird der Chatbot jedoch in Bereichen eingesetzt, die unter die Hochrisiko-KI nach Art. 6 KI VO fallen, etwa im Bereich der Kreditwürdigkeitsprüfung, der Personalauswahl oder der Zugangsentscheidung zu wesentlichen Dienstleistungen, greifen zusätzlich die umfangreichen Anforderungen der Art. 8 ff. KI-VO. Dazu gehören unter anderem ein Risikomanagementsystem, Anforderungen an die Datenqualität, eine technische Dokumentation, menschliche Aufsicht und Konformitätsbewertungen.

Die Einstufung ist somit ein wichtiger Schritt der Unternehmens-Compliance, um sämtliche Pflichten in Zusammenhang mit dem Einsatz eines KI-Chatbots identifizieren und umsetzen zu können.

Rechtliche Risiken beim Einsatz von KI Chatbots auf Webseiten

Neben oben genannten Verpflichtungen kommen rechtliche Risiken beim Einsatz von KI-Chatbots ins Spiel, wenn der KI Chatbot z.B. eigenständig Erklärungen abgeben kann, die als rechtsverbindliche Willenserklärungen des Unternehmens qualifiziert werden.

VERTRAGSSCHLUSS: ZURECHNUNG VON KI CHATBOT-ERKLÄRUNGEN

Erklärungen, die von automatisierten Systemen im Geschäftsverkehr abgegeben werden, werden dem Betreiber des Systems als dessen Willenserklärungen zugerechnet. Dies gilt unabhängig davon, ob der Betreiber die konkrete Erklärung kannte oder wollte. Wer ein automatisiertes System im Rechtsverkehr

RAin Michaela Berger, LL.M.
Fachanwältin für IT-Recht
Datenschutz-Auditorin · Datenschutzbeauftragte
michaela.berger@rdp-law.de

einsetzt, muss sich die von diesem System generierten Erklärungen grundsätzlich zurechnen lassen, so wie er sich auch die Erklärungen eines Erfüllungsgehilfen zurechnen lassen muss.

Für den Einsatz von KI-Chatbots bedeutet dies: Wenn der Bot einem Kunden einen bestimmten Preis nennt, eine Lieferzusage macht oder ein Sonderangebot unterbreitet, kann diese Erklärung grundsätzlich als verbindliches Angebot oder als Annahme eines Vertragsangebots gewertet werden. Das Unternehmen wäre dann an diese Erklärung gebunden, auch wenn der Chatbot aufgrund einer Halluzination oder Fehlkonfiguration fehlerhaft arbeitet.

Auch müssen fernabsatzrechtliche Regelungen beachtet / erfüllt sein.

BESONDERE RISIKEN BEI DER KOMMUNIKATION VON KI-AGENTEN UNTEREINANDER

Eine besondere Risikolage entsteht, wenn nicht ein Mensch mit einem KI Chatbot interagiert, sondern zwei KI-Systeme verschiedener Unternehmen autonom miteinander kommunizieren. Anwendungsbereiche sind automatisierte Beschaffungsprozesse, bei denen der KI-Agent eines Kunden eigenständig mit dem KI-System eines Lieferanten Verfügbarkeiten prüft, Preise verhandelt und Bestellungen auslöst, auch Flug- oder Reisebuchungen. In der agent-to-agent Situation fehlt die menschliche Kontrollinstanz auf beiden Seiten, was die Gefahr potenziert, dass rechtsverbindliche Verträge zu Konditionen geschlossen werden, die keines der beteiligten Unternehmen so gewollt hat. Unternehmen, die ihre KI-Agenten für die automatisierte Kommunikation mit externen Systemen einsetzen, sollten daher besonders strenge Wertgrenzen, Freigabemechanismen und automatische Plausibilitätsprüfungen implementieren und vertraglich mit ihren Geschäftspartnern klare Regelungen für den Fall fehlerhafter Agent-zu-Agent-Kommunikation treffen.

In diesen Situationen kommen auch diesbezügliche Regelungen in Unternehmens-AGB eine wichtige Rolle zu. Oftmals wird hier schon streitig sein, wessen AGB überhaupt einbezogen worden sind.

HAFTUNG FÜR FEHLERHAFTE AUSKÜNFTE VON KI CHATBOTS

Selbst wenn kein Vertrag zustande kommt, kann das Unternehmen für fehlerhafte Auskünfte des Chatbots haften. Denkbar sind Ansprüche, wenn der Nutzer im Vertrauen auf eine falsche Auskunft des KI Chatbots eine nachteilige Entscheidung trifft oder Handlung vornimmt.

WETTBEWERBSRECHTLICHE HAFTUNG BEI AUSSAGEN VON KI CHATBOTS

Auch wettbewerbsrechtliche Ansprüche nach dem UWG kommen in Betracht, wenn der KI Chatbot irreführende Angaben über Produkte, Preise oder Eigenschaften macht oder Regelungen wie die Preisangabenverordnung (PAngV) missachtet. Diese können dann Gegenstand von kostspieligen wettbewerbsrechtlichen Abmahnungen z.B. durch Mitbewerber sein.

RAin Michaela Berger, LL.M.
Fachanwältin für IT-Recht
Datenschutz-Auditorin · Datenschutzbeauftragte
michaela.berger@rdp-law.de

Schutzmaßnahmen und Gestaltungsempfehlungen beim Einsatz von KI Chatbots

Um die dargestellten Risiken zu minimieren, sollten Unternehmen beim Einsatz von KI-Chatbots auf ihren Webseiten eine Reihe von technischen und rechtlichen Schutzmaßnahmen ergreifen:

TECHNISCHE MAßNAHMEN

- Thematische Begrenzung: Der KI-Chatbot sollte so konfiguriert werden, dass er ausschließlich zu den definierten Themengebieten Auskunft gibt und fachfremde Anfragen höflich ablehnt oder an einen menschlichen Ansprechpartner weiterleitet.
- System-Prompts und Guardrails: Über gezielte Systemanweisungen (System-Prompts) kann das Verhalten des KI-Chatbots gesteuert werden, beispielsweise durch die Anweisung, keine rechtsverbindlichen Zusagen zu machen, keine medizinischen oder rechtlichen Ratschläge zu erteilen oder stets auf die Notwendigkeit einer individuellen Beratung hinzuweisen.
- Ausgabe-Filter: Technische Filter können verhindern, dass der KI-Chatbot unangemessene, diskriminierende oder schädliche Inhalte ausgibt.
- Menschliche Eskalation: Für komplexe oder sensible Anfragen sollte ein Eskalationspfad zu menschlichen Mitarbeitern vorgesehen werden.
- Logging und Monitoring: Sämtliche Chatverläufe sollten protokolliert und stichprobenartig kontrolliert werden, um Fehlfunktionen frühzeitig zu erkennen und die Qualität der Antworten kontinuierlich zu verbessern. Selbstverständlich müssen die Nutzer auch hierüber informiert werden.
- Regelmäßige Tests: Der Chatbot sollte vor dem Einsatz und fortlaufend im Betrieb systematisch getestet werden, einschließlich Tests, bei denen gezielt versucht wird, den Bot zu fehlerhaften Aussagen zu verleiten.

RECHTLICHE MAßNAHMEN

- Disclaimer und Haftungshinweise: Im Chat-Interface sollte ein deutlich sichtbarer Hinweis darauf erfolgen, dass es sich um einen KI-gestützten Assistenten handelt und die Antworten keine rechtsverbindlichen Auskünfte darstellen.
- AGB-Gestaltung: Die Allgemeinen Geschäftsbedingungen sollten klarstellen, dass Äußerungen des Chatbots keine verbindlichen Angebote darstellen und Verträge nur über den regulären Bestellprozess zustande kommen.
- Haftungsbeschränkung: Im Rahmen des rechtlich Zulässigen sollten Haftungsbeschränkungen für fehlerhafte Auskünfte des Chatbots aufgenommen werden. Dabei sind die Grenzen des

RAin Michaela Berger, LL.M.
Fachanwältin für IT-Recht
Datenschutz-Auditorin · Datenschutzbeauftragte
michaela.berger@rdp-law.de

AGB-Rechts (§§ 305 ff. BGB) zu beachten, insbesondere kann die Haftung für Vorsatz und grobe Fahrlässigkeit nicht ausgeschlossen werden.

- Vertragliche Absicherung mit dem Anbieter: Im Vertrag mit dem Chatbot-Anbieter sollten klare Regelungen zu Service Level Agreements, Haftungsverteilung, Datenschutz und dem Verbot der Datenweiterverwertung getroffen werden.
- Versicherungsschutz: Unternehmen sollten prüfen, ob ihre bestehende Betriebs- und Vermögensschadenhaftpflichtversicherung auch Schäden durch fehlerhafte KI-Systeme abdeckt, und den Versicherungsschutz gegebenenfalls anpassen.

Fazit: Compliance und Kontrolle sichern den nachhaltigen Chatbot-Einsatz

Der Einsatz von KI-Chatbots auf Unternehmenswebseiten bietet erhebliches Potenzial zur Effizienzsteigerung und Verbesserung der Kundenkommunikation. Die rechtlichen Rahmenbedingungen sind jedoch vielschichtig und erfordern eine sorgfältige Planung. Unternehmen müssen datenschutzrechtliche Vorgaben einhalten, die Anforderungen der KI-Verordnung beachten und insbesondere das Risiko ungewollter Vertragsbindungen oder andere Rechtsfolgen durch fehlerhafte KI-Chatbot-Erklärungen aktiv steuern.

Eine Kombination aus technischen Guardrails, durchdachter AGB-Gestaltung, klarer Kommunikation gegenüber den Nutzern und regelmäßiger Überwachung des Chatbot-Verhaltens ist der Schlüssel zu einem rechtssicheren Einsatz. Unternehmen, die diese Aspekte frühzeitig und systematisch adressieren, können die Vorteile der Technologie nutzen, ohne sich unkalkulierbaren Haftungsrisiken auszusetzen.

Als Rechtsanwälte und Fachanwälte für IT-Recht können wir für den von Ihnen geplanten KI-Chatbot diese rechtlichen Fragen beantworten und sichere Lösungen für Sie finden. Wir freuen uns auf Ihr Projekt!

RAin Michaela Berger, LL.M.
Fachanwältin für IT-Recht
Datenschutz-Auditorin · Datenschutzbeauftragte
michaela.berger@rdp-law.de

(FAQ)

1. Was sind die typischen Einsatzszenarien von KI-Chatbots auf Unternehmenswebseiten?

KI-Chatbots werden in verschiedenen Konstellationen eingesetzt:

- **Kundenservice und Support:** Beantwortung von Fragen zu Produkten, Dienstleistungen, Lieferzeiten, Rückgabebedingungen; Störungsmeldungen; Weiterleitung an Ansprechpartner; Stammdatenänderungen (Bankverbindung, Kontaktdaten); Entgegennahme von Kündigungen oder Zählerstandsmeldungen.
- **Beratung und Produktempfehlungen:** Unterstützung bei Produktauswahl, individuelle Empfehlungen, Konfigurationsvorschläge.
- **Vertragsanbahnung und Vertragsschluss:** Preisnennung, Angebotsunterbreitung, Entgegennahme von Bestellungen, Vertragsabschluss.
- **Weitere Anwendungen:** Beschwerdemanagement, Terminvereinbarung, internes Wissensmanagement mit Kundenschnittstelle, Lead-Generierung.

2. Welche rechtlichen Bereiche sind beim Einsatz von KI-Chatbots besonders relevant?

Die wesentlichen Rechtsbereiche umfassen: Datenschutzrecht (DSGVO, BDSG), KI-Verordnung (AI Act), Vertragsrecht (BGB), Wettbewerbsrecht (UWG), Haftungsrecht sowie branchenspezifische Regelungen. Jeder Einsatzbereich erfordert die Beachtung unterschiedlicher Schwerpunkte innerhalb dieser Rechtsgebiete.

3. Ist die DSGVO für KI Chatbots anwendbar?

Bei jeder Chatbot-Interaktion werden personenbezogene Daten im Sinne der DSGVO verarbeitet, insbesondere: IP-Adresse des Nutzers, Eingaben im Chat (Textnachrichten, Anfragen), generierte Gesprächsverläufe, Zeitstempel der Interaktion, ggf. weitere technische Daten (Browser-Informationen, Gerätekennungen). Diese Datenverarbeitung eröffnet zwingend den Anwendungsbereich der DSGVO.

4. Welche Rechtsgrundlage benötige ich für die Datenverarbeitung durch den KI Chatbot?

Die Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO hängt vom konkreten Einsatzszenario ab:

- **Art. 6 Abs. 1 lit. f) DSGVO (berechtigtes Interesse):** Wenn der Chatbot ausschließlich der Beantwortung allgemeiner Fragen dient und das berechtigte Interesse an effizientem Kundenservice überwiegt.
- **Art. 6 Abs. 1 lit. b) DSGVO (Vertragserfüllung):** Wenn der KI Bot Daten zur Begründung oder Durchführung eines Vertragsverhältnisses verarbeitet (z.B. Stammdatenänderungen, Vertragsanfragen).
- **Art. 6 Abs. 1 lit. a) DSGVO (Einwilligung):** Für bestimmte Verarbeitungen, die nicht unter die vorgenannten Rechtsgrundlagen fallen, ist eine ausdrückliche vorherige Einwilligung des Nutzers erforderlich.

RAin Michaela Berger, LL.M.
Fachanwältin für IT-Recht
Datenschutz-Auditorin · Datenschutzbeauftragte
michaela.berger@rdp-law.de

5. Benötige ich eine Datenschutzerklärung für einen KI Chatbot?

Ja. Gemäß Art. 12, 13 und 14 DSGVO müssen Nutzer umfassend informiert werden. Die Datenschutzerklärung muss mindestens folgende Angaben zum Chatbot enthalten:

- Verantwortlicher für die Datenverarbeitung
- Kontaktdaten des Datenschutzbeauftragten / für Datenschutz
- Zweck der Datenverarbeitung durch den Chatbot
- Rechtsgrundlage der Verarbeitung
- Kategorien der verarbeiteten personenbezogenen Daten
- Empfänger oder Kategorien von Empfängern (insbesondere externe Chatbot-Anbieter)
- Dauer der Speicherung bzw. Kriterien für die Festlegung
- Profiling
- Herkunft der Daten
- Hinweis auf Betroffenenrechte (Auskunft, Berichtigung, Löschung etc.)
- Ggf. Information über Datenübermittlung in Drittstaaten

6. Wann brauche ich einen Auftragsverarbeitungsvertrag (AVV) für einen KI-Chatbot?

Wird der KI-Chatbot über einen externen Dienstleister betrieben (z.B. Cloud-basierte KI-Plattform), liegt regelmäßig eine Auftragsverarbeitung nach Art. 28 DSGVO vor. In diesem Fall ist zwingend ein AVV mit dem Anbieter abzuschließen. Der AVV muss insbesondere regeln, dass der Auftragsverarbeiter die über den Chatbot verarbeiteten Daten nicht zu eigenen Zwecken nutzen darf, insbesondere nicht zum Training eigener KI-Modelle. Zudem müssen Fragen der Datenverarbeitung in unsicheren Drittstaaten geklärt werden.

7. Wann ist eine Datenschutz-Folgenabschätzung (DSFA) erforderlich?

Eine DSFA nach Art. 35 DSGVO ist erforderlich, wenn die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Dies gilt insbesondere, wenn der KI-Chatbot: umfangreiche Nutzerprofile erstellt, eine große Mengen an personenbezogenen Daten verarbeitet, besondere Kategorien personenbezogener Daten verarbeitet (z.B. Gesundheitsdaten), automatisierte Einzelentscheidungen im Sinne des Art. 22 DSGVO trifft, oder umfangreiche Verhaltensbewertungen vornimmt.

8. Bin ich als Webseitenbetreiber Anbieter oder Betreiber des KI-Chatbots?

Die Einordnung als Anbieter oder Betreiber eines KI-Systems nach der KI-VO ist komplex und erfordert eine umfassende rechtliche Bewertung. Diese berücksichtigt den Einsatzzweck, das Maß an Modifikation des Systems, die Kontrolle über das System und weitere Merkmale. Die Grenzen zwischen Anbieter und Betreiber sind fließend. An beide Rollen knüpfen unterschiedliche und teilweise sehr weitreichende Verpflichtungen an. Eine sichere rechtliche Beurteilung ist daher unumgänglich.

RAin Michaela Berger, LL.M.
Fachanwältin für IT-Recht
Datenschutz-Auditorin · Datenschutzbeauftragte
michaela.berger@rdp-law.de

9. Was bedeutet die Transparenzpflicht nach Art. 50 KI-VO für meinen KI Chatbot?

Art. 50 Abs. 1 KI-VO verpflichtet den Anbieter eines KI-Systems, das zur direkten Interaktion mit natürlichen Personen bestimmt ist, sicherzustellen, dass die betroffenen Personen darüber informiert werden, dass sie mit einem KI-System interagieren.

Konkret bedeutet dies für Chatbots:

- Der Nutzer muss klar und unmissverständlich darauf hingewiesen werden, dass er mit einer Künstlichen Intelligenz kommuniziert und nicht mit einem Menschen
- Der Hinweis muss rechtzeitig erfolgen, also vor Beginn der Interaktion
- Die Transparenzpflicht gilt ab dem 02.08.2026
- Verstöße gegen diese Pflicht sind bußgeldbewehrt

10. Wie wird mein KI Chatbot risikoklassifiziert?

Die KI-VO verfolgt einen risikobasierten Ansatz. Die Klassifizierung hängt vom konkreten Einsatzzweck ab:

- **Geringes Risiko:** Chatbots, die ausschließlich im Bereich der Informationsvermittlung eingesetzt werden, gelten in der Regel als KI-Systeme mit geringem Risiko. Für diese gelten primär die Transparenzpflichten nach Art. 50 KI-VO.
- **Hochrisiko-KI:** Wird der Chatbot in Bereichen eingesetzt, die unter Art. 6 KI-VO fallen (z.B. Kreditwürdigkeitsprüfung, Personalauswahl, Zugangsentscheidungen zu wesentlichen Dienstleistungen), greifen umfangreiche Anforderungen der Art. 8 ff. KI-VO.

Zu den Anforderungen an Hochrisiko-KI gehören: Risikomanagementsystem, Anforderungen an Datenqualität, technische Dokumentation, menschliche Aufsicht (Human Oversight), Konformitätsbewertungen.

11. Ist mein Unternehmen an Aussagen des KI Chatbots gebunden?

Ja, grundsätzlich werden Erklärungen automatisierter Systeme dem Betreiber als Willenserklärungen zugerechnet. Es gelten die ganz normalen Regelungen des BGB zur Gültigkeit von Willenserklärungen. Wer ein automatisiertes System im Rechtsverkehr einsetzt, muss sich die vom System generierten Erklärungen zurechnen lassen. Wenn der KI Chatbot einem Kunden einen bestimmten Preis nennt, eine Lieferzusage macht oder ein Angebot unterbreitet, kann dies als verbindliches Angebot oder als Annahme eines Vertragsangebots gewertet werden. Das Unternehmen ist dann grundsätzlich an diese Erklärung gebunden, auch wenn der Bot aufgrund einer Halluzination oder Fehlkonfiguration falsche Aussagen tätigt. Anders ist dies ggf. dann zu beurteilen, durch anderweitige Maßnahmen rechtlich sichergestellt ist, dass der KI Chatbot keine Willenserklärungen abgibt.

12. Wie kann ich verhindern, dass der KI Chatbot versehentlich Verträge abschließt?

Folgende technische und rechtliche Maßnahmen minimieren das Risiko:

RAin Michaela Berger, LL.M.
Fachanwältin für IT-Recht
Datenschutz-Auditorin · Datenschutzbeauftragte
michaela.berger@rdp-law.de

Technische Maßnahmen:

- Strikte Funktionsbegrenzung: Der Chatbot sollte so konfiguriert werden, dass er keine rechtsverbindlichen Erklärungen abgeben kann
- Keine Preisnennung durch den Bot: Verweis auf die Webseite oder den Kundenservice für konkrete Preisauskünfte
- Bestellvorgänge ausschließlich über den regulären Bestellprozess der Webseite, nicht über den Chat

Rechtliche Maßnahmen:

- AGB-Klausel: Klarstellung, dass Äußerungen des Chatbots keine verbindlichen Angebote darstellen und Verträge nur über den regulären Bestellprozess zustande kommen
- Disclaimer im Chatverlauf

13. Was sind die besonderen Risiken bei Agent-to-Agent-Kommunikation?

Besonders riskant wird es, wenn zwei KI-Systeme verschiedener Unternehmen autonom miteinander kommunizieren (z.B. automatisierte Beschaffungsprozesse, bei denen der KI-Agent eines Kunden mit dem System eines Lieferanten Verfügbarkeiten prüft, Preise verhandelt und Bestellungen auslöst).

Besondere Gefahren:

- Fehlende menschliche Kontrollinstanz auf beiden Seiten
- Potenzierte Gefahr rechtsverbindlicher Verträge zu ungewollten Konditionen
- Komplexe Beweislage bei Fehlern

Empfohlene Schutzmaßnahmen:

- Besonders strenge Wertgrenzen für autonome Transaktionen
- Freigabemechanismen für kritische Geschäftsvorfälle
- Automatische Plausibilitätsprüfungen
- Vertragliche Regelungen mit Geschäftspartnern für den Fall fehlerhafter Agent-zu-Agent-Kommunikation
- Klare Regelungen in Unternehmens-AGB

14. Hafte ich für fehlerhafte Auskünfte des KI Chatbots?

Ja, selbst wenn kein Vertrag zustande kommt, kann das Unternehmen für fehlerhafte Auskünfte haften. Denkbar sind Schadensersatzansprüche, wenn der Nutzer im Vertrauen auf eine falsche Auskunft eine nachteilige Entscheidung trifft oder Handlung vornimmt. Zudem kommen wettbewerbsrechtliche Ansprüche nach dem UWG in Betracht, wenn der KI Chatbot irreführende Angaben über Produkte, Preise oder Eigenschaften macht. Diese können Gegenstand wettbewerbsrechtlicher Abmahnungen unter anderem durch Mitbewerber sein.

RAin Michaela Berger, LL.M.
Fachanwältin für IT-Recht
Datenschutz-Auditorin · Datenschutzbeauftragte
michaela.berger@rdp-law.de

15. Kann ich die Haftung für KI Chatbot-Fehler in den AGB ausschließen?

Nur eingeschränkt. Im Rahmen des rechtlich Zulässigen sollten Haftungsbeschränkungen für fehlerhafte Auskünfte des Chatbots in die AGB aufgenommen werden. Dabei sind jedoch die Grenzen des AGB-Rechts (§§ 305 ff. BGB) zu beachten:

- **Nicht ausschließbar:** Haftung für Vorsatz und grobe Fahrlässigkeit
- **Nicht ausschließbar:** Haftung für Verletzung von Leben, Körper, Gesundheit
- **Nicht ausschließbar:** Haftung für Verletzung wesentlicher Vertragspflichten
- **Beschränkbar:** Haftung für einfache Fahrlässigkeit bei Nebenpflichten auf den vorhersehbaren, vertragstypischen Schaden

Eine sorgfältige AGB-Gestaltung unter Berücksichtigung dieser Grenzen ist empfehlenswert.

Dies gilt aber nur, wenn sichergestellt ist, dass die AGB wirksam einbezogen wurden.

16. Was sollte in den Nutzungsbedingungen für den Chatbot stehen?

Spezifische Nutzungsbedingungen für den Chatbot sollten mindestens folgende Punkte umfassen:

- Klarstellung, dass es sich um ein KI-System handelt (Transparenzpflicht Art. 50 KI-VO)
- Information über die Funktionsweise des Chatbots
- Hinweis auf die Grenzen des Systems (keine rechtsverbindlichen Auskünfte)
- Klarstellung, dass Verträge nur über den regulären Bestellprozess zustande kommen
- Datenschutzhinweise (Verweis auf Datenschutzerklärung)

17. Ab wann gelten die Transparenzpflichten der KI-Verordnung für KI Chatbots?

Die Transparenzpflicht nach Art. 50 KI-VO gilt ab dem 02.08.2026. Ab diesem Datum müssen Nutzer vor Interaktionsbeginn darauf hingewiesen werden, dass sie mit einem KI-System kommunizieren. Andere Bestimmungen der KI-VO gelten teilweise bereits früher oder später. Unternehmen sollten ihre Compliance-Strategie zeitnah entwickeln, um rechtzeitig konform zu sein.

18. Was passiert bei Verstößen gegen die KI-VO?

Verstöße gegen die KI-VO sind bußgeldbewehrt. Die Höhe der Bußgelder orientiert sich am weltweiten Jahresumsatz des Unternehmens und kann erheblich sein. Neben Bußgeldern drohen auch Anordnungen der zuständigen Aufsichtsbehörden, etwa zur Einstellung des Betriebs des KI-Systems oder zur Nachbesserung. Zudem können Verstöße zu zivilrechtlichen Schadensersatzansprüchen Betroffener führen.

19. Wie kann mir ein Fachanwalt für IT-Recht bei KI Chatbots helfen?

Ein Fachanwalt für IT-Recht kann Sie umfassend beim rechtssicheren Einsatz von KI-Chatbots unterstützen:

RAin Michaela Berger, LL.M.
Fachanwältin für IT-Recht
Datenschutz-Auditorin · Datenschutzbeauftragte
michaela.berger@rdp-law.de

- Rechtliche Bewertung Ihres spezifischen Einsatzszenarios
- Einordnung als Anbieter oder Betreiber nach KI-VO
- Risikoklassifizierung und Identifikation aller Compliance-Pflichten
- Erstellung und Prüfung von AGB, Nutzungsbedingungen und Datenschutzerklärungen
- Vertragsgestaltung mit Chatbot-Anbietern (inkl. AVV)
- Durchführung von Datenschutz-Folgenabschätzungen (DSFA)
- Entwicklung von Compliance-Strategien zur Erfüllung der KI-VO
- Laufende rechtliche Begleitung und Aktualisierung bei Rechtsänderungen

20. Welche Unterlagen sollte ich für eine rechtliche Beratung zu einem KI Chatbot bereithalten?

Für eine effiziente rechtliche Beratung sind folgende Unterlagen hilfreich:

- Beschreibung des geplanten oder bestehenden Einsatzszenarios des Chatbots
- Technische Dokumentation des KI Chatbot-Systems
- Bestehende AGB, Nutzungsbedingungen und Datenschutzerklärung
- Verträge mit dem Chatbot-Anbieter
- Beispiel-Chatverläufe oder Protokolle
- Übersicht über verarbeitete Datenarten
- Darstellung der Schnittstellen zu anderen Systemen (insbesondere bei Agent-to-Agent-Kommunikation)

RAin Michaela Berger, LL.M.
Fachanwältin für IT-Recht
Datenschutz-Auditorin · Datenschutzbeauftragte
michaela.berger@rdp-law.de