Leitfaden:

ChatGPT im Unternehmen: Wie Sie den Chatbot auf keinen Fall nutzen sollten

Das müssen Unternehmen beachten, die ChatGPT im Team nutzen

DATENSCHUTZ EXPERTE.DE

Seit November 2022 hält ChatGPT die Welt in Atem. Täglich chatten Millionen Nutzer weltweit mit der Künstlichen Intelligenz des US-amerikanischen Anbieters OpenAI oder nutzen das schier unendliche Wissen des Chatbots für ihre Arbeit. Nur wenige Monate nach dem Go-Live der KI, im März 2023, entbrannte in Europa eine Diskussion um die Frage, wie gefährlich ChatGPT für den Datenschutz ist.

Unternehmen sind verunsichert:

- Ist die rechtssichere Nutzung von ChatGPT im Unternehmen überhaupt möglich?
- Was passiert mit Mitarbeiterdaten, die im Hintergrund erhoben werden und mit den eingegebenen Daten?
- Welche Stolperfallen gibt es?
- Wie kann der KI-Einsatz bis zur Verabschiedung einer KI-Richtlinie möglichst sicher gestaltet werden?

Dieser Leitfaden erklärt die beiden größten Gefahrenquellen für Unternehmen und zeigt anwendungsnah, was Sie jetzt beachten müssen, um Unternehmens- und Mitarbeiterdaten zu schützen.

Check-in: Die wichtigsten Fakten, die Sie über ChatGPT wissen sollten

- ChatGPT steht für **Chatbot Generative Pre-trained Transformer**.
- Die Anwendung ist **sprachbasiert**: Die Nutzer kommunizieren über Texteingaben mit der KI.
- Der Chatbot basiert auf dem **Deep-Learning-Prinzip**, einem Teilgebiet des maschinellen Lernens.
- Hinter ChatGPT steckt ein **künstliches neuronales Netz**, das ähnlich wie das menschliche Gehirn funktioniert.
- Die KI ist in der Lage, zu lernen, Texte zu verstehen und bestimmte **Entscheidungen zu treffen**.
- Um besser zu werden, greift ChatGPT auf frei verfügbare Informationen im Internet zu und nutzt zusätzlich die Eingaben **von mehr als 100 Millionen Usern**.
- **Privatpersonen und Unternehmen** verwenden die KI.
- Es ist nicht auszuschließen, dass auch **personenbezogene Daten** verarbeitet werden.

Status quo beim Datenschutz

Bisher ist der DSGVO-konforme Einsatz von ChatGPT in Unternehmen **nicht möglich**. Zum einen mangelt es an **Transparenz** für die Nutzer. OpenAI arbeitet zwar daran, das zu ändern. Bis dahin ist für die User jedoch nicht nachvollziehbar, wie ihre Daten von der KI verarbeitet werden.

Zum anderen fehlen **gesetzliche Grundlagen** für den Umgang mit KI in Europa. Die EU-Kommission entwickelt deshalb seit April 2021 harmonisierte Vorschriften. Ein Vorschlag für ein „Gesetz über künstliche Intelligenz“ liegt vor.

Allerdings hat die Entwicklung bei Künstlicher Intelligenz seit 2021 einen **Quantensprung** gemacht. ChatGPT hat gezeigt, wie vielseitig die Möglichkeiten von KI sind. Da viele der Anwendungen im Gesetzesvorschlag **nicht berücksichtigt** sind, ist eine schnelle Verabschiedung der Richtlinie nicht absehbar.

Fest steht jedoch:

Mit der KI-Verordnung (KI-VO) kommen eine Reihe von Regeln auf Anwender und Betreiber von KI-Systemen zu. Diese Vorgaben müssen zusätzlich zur DSGVO umgesetzt werden. Es lohnt sich, die Entwicklungen zu verfolgen und vorbereitet zu sein.

Gefahrenquelle #1: Was passiert mit den erhobenen Nutzerdaten?

Der KI-Chatbot von OpenAI ist für Nutzer und Datenschützer eine Blackbox. Im Unternehmensumfeld ist diese Tatsache in doppelter Hinsicht kritisch: Zum einen ist der Schutz der eingegebenen Daten nicht gewährleistet, zum anderen ist unklar, was mit erhobenen Nutzungsdaten passiert.

Problem: Wenn Angestellte im beruflichen Kontext ChatGPT nutzen, erlauben sie dem Anbieter, Nutzungsdaten zu verarbeiten. Für Arbeitgeber und Arbeitnehmer ist jedoch nicht abzusehen, welche Daten konkret erhoben werden und was damit passiert.

Hintergrund: Wenn Mitarbeiter mit ChatGPT arbeiten, benötigen sie ein Nutzerkonto, für das eine E-Mail-Adresse und eine Mobilfunknummer angegeben werden müssen. Mit der Einrichtung eines Nutzerkontos erlauben Mitarbeiter dem Anbieter außerdem, Nutzungsdaten zu erfassen, auszuwerten und sogar an Dritte weiterzugeben. Wie OpenAI die Daten genau nutzt, bleibt teilweise unklar.

Laut der OpenAI-Datenschutzbestimmung gehören zu den Nutzerdaten unter anderem die Aktionen, die Nutzer ausführen, Informationen über ihre Zeitzone und ihr Land und IP-Adressen. Allerdings erfolgt seitens OpenAI keine Aufklärung darüber, zu welchem Zweck und in welchem Umfang Daten weitergegeben werden.

Beispiel: OpenAI kann also theoretisch tracken, dass Mitarbeiter X den Chatbot jeden zweiten Tag für Recherchen zum Thema Y verwendet.

Konsequenzen: Unternehmen können aktuell nicht absehen, in welchem Umfang die Daten ihrer Mitarbeiter von ChatGPT getrackt, verarbeitet und an Dritte weitergegeben werden oder was damit passiert.

Unternehmen, die ihren Mitarbeitern ChatGPT als Tool zur Verfügung stellen, müssen **eine datenschutzkonforme Verarbeitung der Daten** Ihrer Mitarbeitenden gewährleisten und u.a. in der Datenschutzinformation für Mitarbeiter darüber informieren, welche Nutzungsdaten dabei verarbeitet werden. Aktuell ist jedoch unklar, welche Daten von OpenAI zu welchem Zweck erhoben werden. Davon abgesehen entstehen für Unternehmen **Cybersecurity-Risiken**, wenn Mitarbeiter ihre berufliche E-Mail-Adresse und Mobilfunknummer für die Anmeldung bei ChatGPT verwenden.

Gefahrenquelle #2: Wo lauern Stolperfallen bei Daten, die eingegeben werden?

Die folgenden Praxisbeispiele verdeutlichen, worauf Teams verschiedener Abteilungen achten sollten, wenn sie mit ChatGPT arbeiten und dabei nicht gegen die DSGVO oder andere Gesetze verstoßen wollen.

Abteilung	Einsatz	Gefahreneinschätzung
Marketing	Im Bereich Marketing und Kommunikation hat ChatGPT sich bereits bewährt. Texte für **E-Mail-Strecken oder Google-Anzeigen** sind mit der KI in Sekundenschnelle formuliert.	**Gering** Marketingexperten können ChatGPT als Inspirationsquelle nutzen, solange sie **keine personenbezogenen Daten** eingeben und die Ergebnisse auf Richtigkeit prüfen. **Achtung:** Soll die KI genutzt werden, um Muster in Nutzerdaten auszuwerten, müssen diese Daten anonymisiert sein.
Content Marketing	Manchmal fehlt Content-Profis die zündende Idee für einen Blogartikel oder einen Social Media Post. ChatGPT ist in der Lage, in kurzer Zeit verschiedene **Textvarianten** zu schreiben und Content Teams **Inspiration** für Inhalte zu liefern.	**Gering** Solange **keine personenbezogenen** Daten im Chat verwendet werden, ist die Nutzung von ChatGPT im Content-Bereich unbedenklich. **Achtung:** Bei KI-generierten Texten ist das **Urheberrecht** oft nicht nachvollziehbar. Um **Plagiatsvorwürfe** zu vermeiden, sollten die Texte der KI höchstens als Basis für **eigene Formulierungen** oder als Inspiration für die weitere Beschäftigung mit einem Thema dienen.
Software-entwicklung	ChatGPT erstellt nicht nur Texte, sondern auch Programmiercode. Viele Entwickler greifen deshalb gern auf die KI zurück, um ihren **Code-entwicklungsprozess** zu beschleunigen oder zu optimieren.	**Moderat** Die Softwareentwicklung mithilfe von KI stellt keine unmittelbare Gefährdung für personenbezogene Daten dar. Jedoch können dabei andere **schützenswerte Daten** in unbefugte Hände geraten und **Geschäftsgeheimnisse** preisgegeben werden. Gemäß **Geschäftsgeheimnisgesetz** (GeschGehG) müssen Unternehmen nachweisen, dass sie ihr Know-how durch Maßnahmen schützen, die extern erkennbar und angemessen sind. **Beispiel aus der Praxis:** Beim Tech-Konzern Samsung haben Ingenieure ChatGPT genutzt, um Fehler im Quellcode eines proprietären Programms zu identifizieren. So gelangten die sensiblen Daten in den Trainingsdatensatz der KI – und in den KI-Chat der Konkurrenz.

Abteilung	Einsatz	Gefahreneinschätzung
Human Resources	ChatGPT hat das Potenzial, Personalabteilungen zu entlasten. Prozesse wie das **Bewerbungsverfahren** oder das Schreiben von **Arbeitsverträgen** und **Stellenbeschreibungen** können durch KI effizienter werden.	**Hoch** HR-Abteilungen in Unternehmen arbeiten täglich mit besonders sensiblen Daten, etwa Gesundheitsdaten oder Informationen zur Konfession. Diese Daten haben in KI-Systemen wie ChatGPT, die datenschutzrechtlich noch immer schwer einschätzbar sind, grundsätzlich nichts zu suchen. Darüber hinaus ist **Art. 22 DSGVO** zu beachten, wenn Unternehmen einer KI wichtige **HR-Entscheidungsprozesse** überlassen, ohne dass daran eine natürliche Person mitwirkt. Eine betroffene Person hat das Recht, nicht einer Entscheidung unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht. Das ist zum Beispiel bei automatisiert erstellten Arbeitszeugnissen der Fall. **Achtung:** KI-Prozesse im HR-Bereich könnten gegen das **Allgemeine Gleichbehandlungsgesetz** (AGG) verstoßen – etwa, wenn diskriminierende Datensätze Grundlage für die Entscheidungen des Chatbots sind. **Beispiel:** Die Bewerbungs-KI von Amazon hat Frauen benachteiligt, da die eingespeisten Datensätze mehr Zusagen für Männer enthielten.
Kundensupport	Chatbots sind im Customer-Support vieler Unternehmen bereits eine feste Größe. Sie beantworten häufig gestellte Fragen und führen personalisierte Gespräche mit Kunden. Mit ChatGPT könnten Kundenanfragen noch **natürlicher und individueller** beantwortet werden, da die KI stets dazulernt.	**Hoch** Im Customer Support ist die Eingabe sensibler Daten wie Adressdaten, E-Mail-Adressen oder gar Zahlungsinformationen durch die Kunden nicht auszuschließen. Deshalb birgt diese Anwendung **hohe datenschutzrechtliche Risiken.** **Hinweis:** Bei „Kundensupport mittels künstlicher Intelligenz“ empfiehlt die Datenschutzkonferenz die Durchführung einer **Datenschutz-Folgenabschätzung** (DSFA) nach Art. 35 Abs. 1 S. 1 DSGVO.

Unternehmen fragen, Datenschützer antworten

So vielfältig wie der Alltag in Unternehmen sind die Anwendungsmöglichkeiten von ChatGPT. Um Ihnen Orientierung zu geben, stellen wir Ihnen drei praxisnahe Fragen und Antworten aus unserem Beratungsalltag vor und erklären, welche Überlegungen wichtig sind.

Wir möchten mit ChatGPT Präsentationen für interne Zwecke erstellen. Was müssen wir beachten, wenn dabei auch Namen von Mitarbeitenden und Umsatzzahlen verarbeitet werden?

In diesem Fall ist von ChatGPT abzuraten, da in unternehmensinternen Meetings vertrauliche KPIs, Unternehmensziele, Mitarbeiterinformationen und Geschäftsgeheimnisse diskutiert werden. Diese personenbezogenen Daten und sensible Geschäftsinformationen würden durch die Eingabe in den Chatbot in die KI-Trainingsdaten gelangen und könnten in die falschen Hände geraten.

Ich möchte ChatGPT nutzen, um damit Produkttexte für meinen Shop zu erstellen. Darf ich das?

Produkttexte können ohne Eingabe personenbezogener Daten erstellt werden und erfordern keine betriebsinternen Informationen, die nicht an die Öffentlichkeit gelangen dürfen. Dem Einsatz von ChatGPT steht nichts im Weg.

Darf ich ChatGPT für die Recherche über Bewerber einsetzen?

Von der Recherche über Kandidaten im Bewerbungsprozess sollten HR-Abteilungen absehen. Zum einen wäre hierfür die Eingabe personenbezogener Daten der Bewerber erforderlich. Zum anderen kann die Richtigkeit der von ChatGPT recherchierten Daten nicht sichergestellt werden. Hinzu kommt, dass die Quellen der KI-Recherche nicht klar sind. Das ist aus datenschutzrechtlicher Sicht problematisch, da Unternehmen z. B. keine Informationen aus privaten sozialen Netzwerken über Bewerber erheben dürfen.

3 Fragen an Prof. Dr. Boris Paal

Professor Dr. Boris P. Paal forscht und lehrt an der Juristenfakultät der Universität Leipzig. Außerdem berät und veröffentlicht er im gesamten Zivil- und Wirtschatssrecht mit einem besonderen Schwerpunkt auf Daten(schutz)-, Informations-, Medien- und Wettbewerbsrecht. datenschutzexperte.de hat mit ihm über ChatGPT gesprochen.

Herr Prof. Paal, wie beurteilen Sie die aktuelle Debatte um ChatGPT und Datenschutz?

Die Debatte um ChatGPT zeigt die Notwendigkeit einer Regulierung für KI-Systeme. Die Regulierung muss sicherstellen, dass hoch leistungsfähige KI-Systeme rechtskonform trainiert und eingesetzt werden, sodass sie den Menschen nützen. Aktuell wird auf EU-Ebene über den Entwurf einer KI-Verordnung verhandelt, die den Einsatz von KI-Technologie sicher, transparent und grundrechtskonform machen soll. Zu diesem Zweck ist eine Kategorisierung von KI-Technologien nach Risikopotenzial und Auswirkungen für Grundrechte vorgesehen. Je nach Einstufung sollen dann Verbote, Einschränkungen oder Transparenzpflichten greifen.

Welchen Impact hat ChatGPT Ihrer Meinung nach auf die Wirtschaft und die Gesellschaft?

ChatGPT stellt uns vor neue Herausforderungen, vor allem weil KI-Systeme replizieren und skalieren können. Diese neuartigen Fähigkeiten betreffen sowohl generative Prozesse als auch zivilgesellschaftliche Grundfragen, zum Beispiel wenn es um Hassrede, Fake News und die Beeinflussung von Wahlen geht.

Vor welche Herausforderung stellt ChatGPT den Datenschutz in Europa?

In datenschutzrechtlicher Hinsicht stellt sich die Frage, ob die DSGVO-Vorgaben für die umfangreiche Erhebung und Verarbeitung personenbezogener Daten beim Training und Einsatz von KI gewahrt werden. Darüber hinaus ist darauf zu achten, dass KI-Betreiber ihren Informationspflichten hinreichend nachkommen.

Checkliste für den (risikoreduzierten) Einsatz von ChatGPT im Unternehmen

Die folgende Checkliste bietet einige Empfehlungen, um Datenschutzrisiken zu minimieren. Wichtig ist dabei insbesondere, die Verarbeitung personenbezogener Daten möglichst auszuschließen und die Benutzer transparent über die Verarbeitung ihrer Daten zu informieren.

Hinweis:

Diese Checkliste garantiert keine DSGVO-konforme Nutzung von ChatGPT und schützt Ihr Unternehmen nicht vor Bußgeldern. Wer 100%ige Sicherheit wünscht, sollte ChatGPT vorerst suspendieren und die Verabschiedung der KI-Richtlinie auf EU-Ebene abwarten.

So reduzieren Sie Datenschutzrisiken mit ChatGPT, bis die KI-Richtlinie in Kraft tritt

- **Zweck festlegen:** Prüfen Sie, ob der KI-Einsatz notwendig ist. Sollte das der Fall sein, definieren Sie klare Ziele und Zwecke, für die Sie ChatGPT einsetzen möchten. Stellen Sie sicher, dass Sie nur die personenbezogenen Daten erheben und verarbeiten, die für den spezifischen Zweck erforderlich sind.
- **Zweck und Nutzung dokumentieren:** Wenn die Ziele und der Zweck der ChatGPT-Nutzung formuliert sind, müssen Sie diese in Ihrer Datenschutzrichtlinie oder der Datenschutzerklärung Ihres Unternehmens sowie in Ihrem internen Verzeichnis von Verarbeitungsprozessen dokumentieren.
- **Risikomaßnahmen ergreifen:** Der Anbieter von ChatGPT, OpenAI, ist ein in den USA ansässiges Unternehmen. Die in dem Chatbot verarbeiteten Daten werden mutmaßlich in die USA übertragen. Bei einer Datenübertragung in Länder außerhalb der Europäischen Union müssen Unternehmen eine Datenschutz-Folgenabschätzung und ein Transfer Impact Assessment durchführen.
- **Einwilligung einholen:** Müssen bei der Nutzung von ChatGPT personenbezogene Daten verarbeitet werden, benötigen Sie vor der Sammlung und Verarbeitung die Einwilligung der betroffenen Personen.
- **Transparenz schaffen:** Unternehmen sollten transparent sein und den Benutzern klare und leicht verständliche Informationen über die Art und Weise geben, wie ihre Daten verarbeitet werden. Dazu gehört auch die Offenlegung, dass ChatGPT eingesetzt wird, und welche Daten möglicherweise erfasst und verarbeitet werden.
- **Datensicherheit gewährleisten:** Stellen Sie sicher, dass Sie angemessene technische und organisatorische Maßnahmen ergreifen, um personenbezogene Daten zu schützen, die mit KI-Systemen wie ChatGPT erfasst und verarbeitet werden.
- **Vertraglich absichern:** Prüfen Sie, ob die Verantwortlichkeit für die Verarbeitung personenbezogener Daten bei OpenAI, Ihrem Unternehmen oder auf beiden Seiten liegt. Je nach Konstellation ist es notwendig, einen Auftragsverarbeitungsvertrag oder andere vertragliche Vereinbarungen abzuschließen.

- **Betroffenenrechte schützen:** Grundsätzlich müssen Unternehmen sicherstellen, dass Betroffene ihre Rechte gemäß der DSGVO ausüben können. Zu diesen Rechten gehört das Recht auf Zugang, Berichtigung, Löschung und Einschränkung der Verarbeitung.
- **Spielregeln festlegen:** Legen Sie klare Richtlinien für die Nutzung von KI-Systemen wie ChatGPT in Ihrem Unternehmen fest. Ein Datenschutzexperte unterstützt Sie dabei und sorgt dafür, dass die Richtlinie stets auf dem aktuellen Stand ist.
- **Transparent sein:** Informieren Sie Ihr Team über Gefahren und Risiken im Umgang mit KI. Wenn möglich, sollten Ihre Mitarbeiter auf die Eingabe personenbezogener Daten verzichten oder auf anonymisierte Daten zurückgreifen und die generierten Antworten genau prüfen.
- **Konsequent sein:** Sind personenbezogene Daten, diskriminierende oder falsche Aussagen enthalten, dürfen die Antworten nicht verwendet werden.

So bereiten Sie sich auf die KI-VO vor

Solange klare gesetzliche Regelungen für die Nutzung von KI fehlen, sollten Sie beim Einsatz von ChatGPT alle DSGVO-Vorgaben so weit wie möglich erfüllen, eng mit Ihrem Datenschutzbeauftragten zusammenarbeiten und die Entwicklungen rund um den KI-Datenschutz aufmerksam verfolgen.

Unternehmen sind gut beraten, sich auf die KI-Verordnung vorzubereiten: Der aktuelle Entwurf sieht Bußgelder vor, die sogar noch über Strafen der DSGVO liegen. Es drohen unter anderem Bußgelder in Höhe von bis zu **30 Millionen Euro oder 6 Prozent** des gesamten weltweiten Jahresumsatzes.

Schützen Sie sich vor Strafzahlungen – mit einem externen Datenschutzbeauftragten. Unsere Datenschutzexperten sind für Sie da und informieren Sie umfassend zu den Stolperfallen und dem richtigen Einsatz von ChatGPT. Lassen Sie sich unverbindlich zu unserem Angebot beraten.

Faktenlage ändert sich ständig

Unternehmen, die ChatGPT nutzen, sollten die Augen offenhalten. Sowohl auf Seiten der Datenschützer als auch bei OpenAI gibt es ständig neue Entwicklungen, die unter Umständen in Ihre unternehmensinternen KI-Richtlinien einfließen sollten. So ist es den ChatGPT-Usern inzwischen möglich, selbst zu entscheiden, ob Chatverläufe gespeichert und für das Training des Sprachmodells benutzt werden dürfen. Nicht gespeicherte Chats löscht OpenAI eigenen Angaben zufolge innerhalb von 30 Tagen.

Sie haben Fragen?
Wir helfen Ihnen weiter!

Sie wünschen eine kostenlose und unverbindliche Beratung zum Datenschutz-Management in Ihrem Unternehmen und dem Thema externer Datenschutzbeauftragter?

Rufen Sie uns gerne an oder schreiben Sie uns eine E-Mail!

datenschutzexperte.de
+49 (0)89 2500 392 20
info@datenschutzexperte.de

Alexander Ingelheim
Geschäftsführung

datenschutzexperte.de ist einer der digitalen Marktführer im Bereich Datenschutz. Mit einem wachsenden Team aus über 70 Experten unterstützt datenschutzexperte.de Unternehmen mit einer „All-in-one"-Lösung dabei, die Herausforderungen der europäischen Datenschutz-Grundverordnung (EU-DSGVO) problemlos zu meistern. Die eigens entwickelte SaaS-Kundenplattform „Proliance 360" ermöglicht Unternehmen, den Unternehmensdatenschutz vollständig digital und somit intuitiv, sicher und schnell zu verwalten.

DATENSCHUTZ EXPERTE.DE

PROVEN EXPERT EMPFEHLUNG