

Do'S und Don'ts für die Nutzung von ChatGPT



Inhaltsverzeichnis

- **Einleitung**
- **Was ist zu wissen?**
- **Zu beachten**
- **Legende**
- **Do's, Check, Don'ts**
 - Compliance-Grundsätze
 - Nutzung von ChatGPT



Einleitung

Die frei im Internet verfügbare Chat-GPT-Version, zzt. von der Firma OpenAI, („ChatGPT für „Generative Pre-trained Transformer“) kann auf Textfragen antworten, Texte formulieren und dient in erster Linie als Inspirationsquelle, ähnlich wie die Verwendung von Suchmaschinen. In diesem Szenario ist es wichtig zu beachten, dass geschäftsrelevante, sensible, vertrauliche und personenbezogene Daten nicht eingegeben werden dürfen. ChatGPT kann in solchen Fällen als Werkzeug dienen, um Ideen zu generieren oder allgemeine Informationen bereitzustellen. Die hier beschriebenen Regeln sollten auch auf andere KI-Chatbots analog angewandt werden.

In jedem Fall ist sicherzustellen, dass die Verwendung von ChatGPT den internen Richtlinien und gesetzlichen Anforderungen entspricht, um die angemessene Verwendung von geschäftsrelevanten Daten sicherzustellen.

Die WBD stellt gegenwärtig keinen Unternehmens-Account, allerdings kann Chat-GPT mit einem individuellen Account genutzt werden. Hierfür kann auch die WBD-E-Mailadresse verwendet werden. Allerdings ist die Nutzung nicht ganz ohne Risiken. Diese beziehen sich zum einen auf den Datenschutz und zum anderen darauf, dass es schwieriger ist als beispielsweise bei einer Suchmaschinensuche die Ergebnisse zu bewerten. Mit dieser Guideline soll ein kurzer Überblick darüber gegeben werden, was zu beachten und bedenken ist.

Was ist zu wissen?

Grundsätzlich zu beachten ist, dass ChatGPT zwar detaillierte Antworten auf Fragen geben kann, diese aber nicht immer korrekt sein müssen. Prüfen Sie daher die Antworten. Darüber hinaus ist das Wissen über die Welt und Ereignisse nach 2021 begrenzt.

ChatGPT ist nicht mit dem Internet verbunden und kann keine externen Datenquellen abrufen. Die Datenverarbeitung richtet sich ausschließlich nach den eingegebenen Texten und Abfragen.

Es sollte beachtet werden, dass ChatGPT als Modell der künstlichen Intelligenz keine Daten für die User speichert oder Informationen für lange Zeit aufbewahrt. Es verarbeitet Daten in Echtzeit, um angemessene und relevante Antworten zu generieren.

Eingegebene Texte und Abfragen werden vorübergehend im Speicher des Systems vorgehalten, um die Konversation zu unterstützen und ihre Kontinuität sicherzustellen. Eine dauerhafte Speicherung und Verwendung der eingegebenen Daten zur Weiterentwicklung des Algorithmus behält sich ChatGPT vor. Es kann also sein, dass die von Usern eingegebenen Daten anderen Usern bereitgestellt werden.

Was ist zu wissen?

Die Kontoinformationen und Benutzerinhalte werden von ChatGPT erfasst und können an Dritte weitergegeben werden.

Konversationen können ebenso von den KI-Trainern überprüft werden, um die Systeme zu verbessern. Es besteht keine Möglichkeit, spezifische Anfragen aus Ihrem Verlauf zu löschen.

Die IT der WBD kann keine Gewähr für die Verfügbarkeit von ChatGPT übernehmen, ebenso ist kein technischer Support möglich.

Damit die Nutzung von ChatGPT sicher abläuft, wurden einige Aspekte für alle Beschäftigten der WBD-AÖR in Form einer „Do's/ Check/ Don'ts-Liste“ übersichtlich zusammengestellt. Damit schützen Sie sich und das Unternehmen dadurch unter anderem vor Datenmissbrauch.

Zu beachten

Die reguläre Anmeldung bei ChatGPT ist kostenlos. Es gibt mittlerweile jedoch auch eine kostenpflichtige Version, die per upgrade als ChatGPT Plus aufgestockt werden kann.

Diese Aktualisierung würde monatliche Kosten verursachen, die nicht von den Wirtschaftsbetrieben Duisburg übernommen werden.

Compliance- Grundsätze



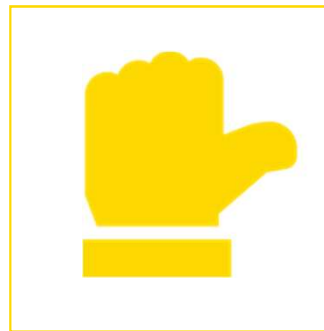
Nutzung von ChatGPT



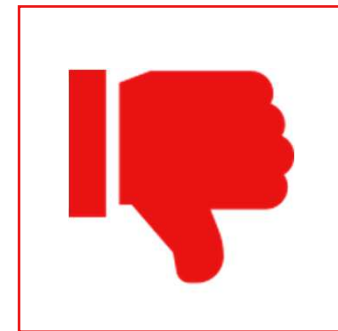
Legende



Do's (Machen): Diese Dinge sind zu empfehlen oder zu befolgen.



Check (Prüfen!): Diese Sachverhalte sind im Einzelfall sorgfältig zu prüfen und abzuwägen.



Don'ts (Lassen!): Diese Dinge müssen unterlassen werden bzw. sind für unternehmensinterne Zwecke nicht erlaubt.

Compliance – Grundsätze



- Gesetze und Vorschriften einhalten
- Interne Regelungen beachten
- Erstellung von Texten ohne Nutzung eines Chatbots (z.B. ChatGPT)



- Bei der Eingabe von unternehmensbezogenen Daten ist kritisch zu prüfen, ob es sich um Betriebs- und Geschäftsgeheimnisse handelt
- Im Zweifel mit Vorgesetzten, C oder der IT Rücksprache halten



- Eingabe von personenbezogenen Daten und jeglichen unternehmensbezogenen Daten wie z.B. Betriebs- und Geschäftsgeheimnisse

Nutzung von ChatGPT



- Texte bzw. die Ergebnisse sollten nur als Inspiration dienen
- Überblick für Themen verschaffen (d. h. beispielsweise um zu ermitteln, welche anderen Themen mit einem Thema verwandt sein könnten)
- ChatGPT kann als Hilfsmittel z.B. für komplexe Themen verwendet werden
- **Wichtig:** Nutzung immer ohne personenbezogene, sensible, unternehmensbezogene oder kundenbezogene Daten sowie Betriebs- und Geschäftsgeheimnisse.



- Kontrolle aller Textvorschläge, da diese nicht immer richtig sind. Eine Überprüfung ist zwingend notwendig.
- ChatGPT gibt keine Quellen an. Werden Texte von ChatGPT eins zu eins veröffentlicht, könnten diese als Plagiat gelten.
- ChatGPTs Wissen ist auf dem Stand von 2021
- Richtigkeit der Texte unbedingt mit vertrauenswürdigen und seriösen Quellen im Internet gegenprüfen



- Blind vertrauen
- Falsche Information veröffentlichen
- Texte einfach kopieren und veröffentlichen = Verstoß gegen Urheberrecht
- Antworten nicht überprüfen / kontrollieren

Noch Fragen?

KONTAKT

Bei Fragen zu ChatGPT

Roman Aiyer

Tel.: (0203) 283 – 7976

E-Mail: r.aiyer@wb-duisburg.de

Bei allgemeinen Fragen zu den Themen

Datenschutz, Datensicherheit und Compliance

Martin Giesen

Tel.: (0203) 283 – 3506

E-Mail: m.giesen@wb-duisburg.de

