Richtlinie zur Verwendung von ChatGPT und anderer Large Language Modells (LLM) im Unternehmen

Inhaltsverzeichnis

1. Zweck und Zielgruppe

Zweck

Diese Richtlinie legt die Bedingungen für die Nutzung von ChatGPT, Gemini, Copilot und anderer Large Language Models (zusammengefasst bezeichnet als LLM) im Unternehmen fest. Ziel ist es, insbesondere gesetzliche Regelungen einzuhalten und die Nutzung für die Mitarbeitenden sicher zu gestalten.

Zielgruppe

Diese Richtlinie richtet sich an alle Mitarbeitenden des Unternehmens, die ChatGPT, Gemini, Copilot oder andere LLMs im Rahmen ihrer beruflichen Tätigkeit nutzen möchten.

2. Was sind LLM?

LLM sind Tools, die durch die Analyse großer Mengen an Text gelernt haben, Sprache zu „verstehen“ und zu erzeugen. Sie werden trainiert, indem sie riesige Datenmengen, wie Bücher oder Webseiten, durchlaufen und dabei Muster und Zusammenhänge in der Sprache erkennen. Durch dieses Training können sie auf Fragen antworten, Texte schreiben und Aufgaben erledigen, für die es Sprachverständnis bedarf.

3. Wie kommuniziert man mit einem LLM?

Die Kommunikation mit einem LLM, beginnt mit der Eingabe einer klaren und spezifischen Anfrage, auch "Prompt" genannt. Der Prompt kann Fragen, Anweisungen oder Szenarien enthalten, die dem LLM helfen, den gewünschten Kontext zu verstehen und relevante Informationen bereitzustellen. Je präziser und strukturierter der Prompt ist, desto genauer und nützlicher ist der Output (die Antwort des LLM).

4. Wer trägt die Verantwortung für die Verwendung der durch LLM generierten Inhalte?

Sofern Sie LLM-generierte Inhalte nutzen, sind Sie allein für die Richtigkeit und die Einhaltung relevanter Gesetze verantwortlich. Sie sollten daher überprüfen, ob die Inhalte den gesetzlichen Rahmenbedingungen und ethischen Standards Ihres Unternehmens entsprechen.

5. Achtsames Teilen von Inhalten

Bitte beachten Sie, dass Anbieter von LLM diese nur kostenlos anbieten, da sie einen eigenen Vorteil hierdurch haben.

Der Preis, den Sie für kostenlose Tools zahlen, sind die Informationen und Daten, die Sie in das LLM eingeben!

LLM können eingegebene Informationen und Daten dazu verwenden, ihr „Wissen“ zu erweitern. Das bedeutet auch, dass das LLM Informationen oder Daten, die Sie eingeben, möglicherweise bei der Beantwortung von Fragen anderer Personen ausgeben.

Zudem wird in jedem Chat mit der LLM auch die Kommunikation an sich trainiert. Das bedeutet, dass das LLM auch die Art und Weise, wie Sie kommunizieren, lernt z. B. durch ihren Schreibstil.

Was Sie tun sollten:

- Beschränken Sie Ihre Eingaben auf Informationen und Inhalte, die Sie auch auf Social-Media oder auf anderen öffentlichen Plattformen teilen würden.

6. Datenschutz

Abhängig von dem Standort Ihres Unternehmens müssen Sie Datenschutzgesetze wie bspw. die Datenschutz-Grundverordnung (DSGVO) in der EU, die UK General Data Protection Regulation (UK GDPR) in Großbritannien oder das Bundesgesetzes über den Datenschutz (DSG) in der Schweiz einhalten, um den Schutz personenbezogener Daten zu gewährleisten.

Personenbezogene Daten sind Angaben, durch die eine Person identifiziert werden kann oder identifizierbar wird, z.B. Name, Adresse, Geburtsdatum, Telefonnr., E-Mail-Adresse (sofern der Vor- und Nachname enthalten sind).

Bereits die Registrierung bei einem LLM kann dazu führen, dass Sie personenbezogene Daten preisgeben, wenn Ihre E-Mail-Adresse Vor- und Nachnamen enthält.

Sofern Sie Texte in den Chat eingeben (prompten), die personenbezogenen Daten von anderen enthalten, verstoßen Sie möglicherweise gegen Datenschutzgesetze.

Was Sie tun sollten:

- Um Ihre Privatsphäre zu schützen, verwenden Sie bei der Registrierung eine E-Mail-Adresse, die nicht Ihren vollen Namen (Vorname und Nachname) enthält.
- Geben Sie keine personenbezogenen Daten an LLM weiter. Anonymisieren Sie diese Daten, z.B. indem Sie statt der Daten ein X als Platzhalter verwenden.
- Nennen Sie darüber hinaus zum Schutz Ihres Unternehmens und von Geschäftspartnern keine Firmennamen.

7. Schutz geistigen Eigentums und Einhaltung von Nutzungsrechten

Bei der Verwendung von LLM müssen der Schutz geistigen Eigentums und die Einhaltung von Nutzungsrechten berücksichtigt werden.

Unter geistigem Eigentum sind kreative, intellektuelle Leistungen zu verstehen, aus denen ein vermögenswertes, aneignungsfähiges Resultat hervorgeht. Es wird u.a. durch das Urheberrechtsgesetz geschützt. Zum geistigen Eigentum zählen z.B. Software Codes, Bücher, Artikel, Gedichte und Liedtexte.

Sie sollten keine urheberrechtlich geschützten Inhalte in ein LLM eingeben.

Zudem ist es möglich, dass durch das LLM generierte Inhalte das Urheberrecht Dritter verletzen.

Es müssen darüber hinaus Nutzungsrechte an Werken, die Ihnen vertraglich oder auf andere Weise eingeräumt wurden, beachtet werden. Wenn bspw. ein Unternehmen einen Text von einer Werbeagentur für ein Prospekt erstellen lässt, sind die Nutzungsrechte oft auf einen speziellen Verwendungszweck beschränkt. Das bedeutet, dass der Text nicht ohne weiteres in ein LLM eingegeben werden darf, um bspw. eine weitere Bearbeitung oder Analyse durchzuführen.

Was Sie tun sollten:

- Geben Sie keine urheberrechtlich geschützten Inhalte an ein LLM weiter.
- Beachten Sie Nutzungsrechte aus Verträgen mit Ihren Geschäftspartnern.
- Prüfen Sie die generierten Inhalte auf Einhaltung der relevanten Urheberrechts-schutzgesetze und den Schutz geistigen Eigentums, bevor sie verwendet werden. Oder lassen Sie sie durch eine fachkundige Person prüfen.

8. Irreführende Werbung und Greenwashing

Bei der Nutzung von LLM generierten Inhalten zu Marketingzwecken bestehen Risiken hinsichtlich irreführender Werbung und Greenwashing.

Dies ist der Fall, sofern die generierten Inhalte in übertriebener Weise oder mit falschen Behauptungen Produkte und Dienstleistungen beschreiben, insbesondere in Bezug auf Umweltfreundlichkeit oder -verträglichkeit.

Solche irreführenden Aussagen können nicht nur das Vertrauen Ihrer Kunden schwächen, sondern auch rechtliche Konsequenzen nach sich ziehen. Es kann hierdurch u.a. zu Verstößen gegen das Wettbewerbsrecht kommen.

Was Sie tun sollten:

- Minimieren Sie diese Risiken, indem Sie alle mit LLM erstellten Inhalte sorgfältig überprüfen, um sicherzustellen, dass sie transparent und wahrheitsgemäß sind.
- Holen Sie die Einschätzung durch eine fachkundige Person ein, ob der Inhalt, den Sie veröffentlichen wollen, ein rechtliches Risiko darstellt.

9. Schutz von Geschäftsgeheimnissen und vertraulicher Informationen

Der Schutz vertraulicher Informationen und von Geschäftsgeheimnissen muss bei der Nutzung von LLM im Unternehmen berücksichtigt werden. Geschäftsgeheimnisse sind Informationen, die für ein Unternehmen einen wirtschaftlichen Wert haben, geheim gehalten werden und nicht allgemein bekannt sind. Dies umfasst, aber ist nicht beschränkt auf, strategische Pläne, finanzielle Daten, Kundendaten und interne Berichte.

Der Schutz dieser Informationen ist entscheidend, um Wettbewerbsvorteile zu bewahren sowie um das Vertrauen von Kunden und Geschäftspartnern zu erhalten.

Was Sie tun sollten:

- Geben Sie LLM keine Informationen, die Geschäftsgeheimnisse oder vertrauliche Informationen enthalten könnten.

10. Halluzinationen

LLM können sogenannte Halluzinationen erzeugen. So werden Inhalte genannt, die plausibel klingen, aber in Wirklichkeit inkorrekt oder ungenau sind. Dieses Risiko macht es erforderlich, dass Sie alle von LLM erzeugten Inhalte kritisch hinterfragen und überprüfen sollten.

Was Sie tun sollten:

- Nutzen Sie LLM nur in Themenbereichen, in denen Sie sich auskennen und die Antwort überprüfen können.
- Überprüfen Sie immer die durch ein LLM bereitgestellten Informationen.
- Um das Risiko von Missverständnissen zu reduzieren, stellen Sie dem LLM klare spezifische Fragen und geben Sie bei unklaren oder widersprüchlichen Antworten zusätzliche Details an.
- LLM sollten als hilfreiches Werkzeug betrachtet werden, aber nicht als alleinige Informationsquelle. Es ist daher ratsam, mehrere Quellen heranzuziehen.

11. Vertragliche Vereinbarungen

Vertragliche Vereinbarungen mit Geschäftspartnern und Geheimhaltungsvereinbarungen (Non Disclosure Agreements = NDAs), müssen beachtet werden, wenn LLM im Unternehmen verwendet werden. Diese könnten neben der Eingabe von Geschäftsgeheimnissen die Eingabe weiterer Informationen in LLM einschränken.

Auf der anderen Seite gehen Sie bei der Nutzung von LLM evtl. auch vertragliche Vereinbarungen ein, z.B. indem Sie bei der Registrierung den Allgemeinen Geschäftsbedingungen zugestimmt haben.

Was Sie tun sollten:

- Prüfen Sie vor der Nutzung von LLM, ob dies gegen vertragliche Vereinbarungen mit Geschäftspartnern Ihres Arbeitsgebers verstößt und welche Beschränkungen bei der Nutzung eingehalten werden müssen.
- Geben Sie keine Informationen weiter, die den Inhalt vertraglicher Vereinbarungen enthalten.
- Prüfen Sie die AGB und eventuelle, andere Nutzungsvereinbarungen daraufhin, welche Nutzungsrechte der LLM bzw. deren Anbieter an Ihren Daten und Informationen eingeräumt werden und wie sie verarbeitet werden (Speicherort, Weiterleitung/Verarbeitung an/durch Dritte).
- Stellen Sie sicher, dass Sie diese Vereinbarungen einhalten.

12. Cybersicherheit

LLM selbst stellt kein direktes Cyberrisiko dar, sofern es nicht auf unternehmensinterne Systeme zugreifen kann. Allerdings kann es indirekt zu Risiken führen, wenn Angreifer das Modell missbrauchen, z.B. durch Social Engineering. Ein mögliches Angriffsszenario **wäre, dass** Cyberkriminelle eine gefälschte Webseite erstellen, die aussieht wie ChatGPT oder ein anderes LLM, um Nutzer zu täuschen. Durch solche Phishing-Seiten könnten Angreifer dann gezielt versuchen, sensible Informationen von den Nutzern zu erlangen, indem sie das System so aussehen lassen, als würden die Antworten von einem vertrauenswürdigen LLM kommen.

Was Sie tun sollten:

- Achten darauf, die Internetadresse korrekt einzugeben. Schon ein einzelnes falsches Zeichen kann dafür sorgen, dass Sie auf eine andere Webseite geleitet werden.
- Melden Sie jede ungewöhnliche verdächtige Aktivität sofort der in Ihrem Unternehmen zuständigen Stelle.

13. Bias und Diskriminierung

Bitte seien Sie sich bewusst, dass LLM sogenannte Bias (voreingenommene Ansichten) enthalten können, da sie mit großen Datensätzen trainiert wurden, die (unbewusste) Vorurteile der Gesellschaft widerspiegeln können. Dies könnte zu diskriminierenden oder unangebrachten Inhalten beim Output führen.

Was Sie tun sollten:

- Stellen Sie sicher, dass LLM generierte Texte keine diskriminierenden Inhalte enthalten, die gegen Gesetz oder den Verhaltenskodex Ihres Unternehmens verstoßen, bevor Sie die Texte nutzen.
- Geben Sie dem LLM für diskriminierenden Output ein negatives Feedback.
- Geben Sie in LLM keine Prompts ein, die als beleidigend, diskriminierend oder illegal angesehen werden könnten.

14. Fehlerhafter oder unangemessener Output

Bei der Verwendung von Inhalten, die durch LLM generiert wurden, ist es wichtig, die Anwendung auf Themen zu beschränken, die in Ihrem Fachgebiet liegen. Diese Vorsichtsmaßnahme garantiert, dass Sie die Richtigkeit der bereitgestellten Informationen persönlich überprüfen können. Auf diese Weise halten Sie den Standard aufrecht, Ihrem Publikum oder Ihren Stakeholdern zuverlässige Informationen zu liefern.

ChatGPT beantwortet die Frage, wie LLM die Richtigkeit des Outpus gewährleisten folgendermaßen: " LLMs (Large Language Models) können die Richtigkeit des Outputs nicht garantieren, da sie auf Wahrscheinlichkeiten basieren und nicht über ein Verständnis oder eine Verifizierung des Wissens verfügen. Sie erzeugen Antworten, indem sie aus riesigen Datenmengen lernen, aber sie führen keine externe Überprüfung der Fakten durch."

Das Korrekturlesen von Inhalten, die mit LLM generiert werden, ist unerlässlich, um inhaltliche oder sprachliche Inkonsistenzen, Rechtsschreibfehler, grammatikalische Fehler sowie

unangemessene Sprache zu korrigieren. Zwar werden LLM kontinuierlich trainiert, um solche Fehler zu minimieren, bei fehlerhaften oder widersprüchlichen Trainingsdaten kann es jedoch sein, dass trotz Modelloptimierungen Fehler bestehen bleiben.

Was Sie tun sollten:

- Verwenden Sie LLM-generierte Inhalte nur für Themenbereiche, in denen Sie über Fachwissen verfügen, sodass Sie die Richtigkeit des Outputs überprüfen können.
- Überprüfen Sie den generierten Inhalt vor der Nutzung auf Fehler.

15. Schulung und Sensibilisierung

Schulung und Sensibilisierung sind für Mitarbeitende, die LLM verwenden, von entscheidender Bedeutung, um sicherzustellen, dass sie die Fähigkeiten, Grenzen und ethischen Standards der Technologie kennen. Eine Schulung befähigt dazu, das Tool verantwortungsbewusst zu nutzen, potenzielle Fallstricke zu vermeiden und fundierte Entscheidungen zu treffen, wenn sie Inhalte erstellen. Es fördert auch eine Kultur des ethischen Einsatzes von KI innerhalb des Unternehmens und hilft, unbeabsichtigte Folgen oder Compliance-Verstöße zu verhindern, die sich aus Missbrauch oder mangelndem Bewusstsein ergeben könnten.

Was Sie tun sollten:

- Bleiben Sie auf dem Laufenden! Informieren und bilden Sie sich hinsichtlich der Nutzung und Entwicklung von LLM weiter.
- Nehmen Sie an den Compliance-Schulungen Ihres Arbeitgebers teil, um einen verantwortungsvollen und sicheren Umgang mit LLM zu gewährleisten.

Anhang I: Hinweise zur Nutzung von LLM

- Beschränken Sie Ihre Eingaben auf Informationen und Inhalte, die Sie auch auf Social-Media oder auf anderen öffentlichen Plattformen teilen würden.
- Abhängig von dem Standort Ihres Unternehmens müssen Sie Datenschutzgesetze wie bspw. die Datenschutz-Grundverordnung (DSGVO) in der EU, der UK General Data Protection Regulation (UK GDPR) in Großbritannien und des Bundesgesetzes über den Datenschutz (DSG) in der Schweiz.
- Um Ihre Privatsphäre zu schützen, verwenden Sie bei der Registrierung eine E-Mail-Adresse, die nicht Ihren vollen Namen (Vorname und Nachname) enthält.
- Geben Sie keine personenbezogenen Daten an LLM weiter. Anonymisieren Sie diese Daten, z.B. indem Sie statt der Daten ein X als Platzhalter verwenden.
- Nennen Sie darüber hinaus zum Schutz Ihres Unternehmens und von Geschäftspartnern keine Firmennamen.
- Geben Sie keine urheberrechtlich geschützten Inhalte oder geistiges Eigentum an ein LLM weiter.
- Beachten Sie Nutzungsrechte aus Verträgen mit Ihren Geschäftspartnern.
- Prüfen Sie die generierten Inhalte auf Einhaltung der relevanten Urheberschutzgesetze und den Schutz geistigen Eigentums, bevor Sie verwendet werden. Oder lassen Sie sie durch eine fachkundige Person prüfen.
- Minimieren Sie diese Risiken, indem Sie alle mit LLMs erstellten Inhalte sorgfältig überprüfen, um sicherzustellen, dass sie transparent und wahrheitsgemäß sind.
- Holen Sie eine Einschätzung durch eine fachkundige Person ein, ob der Inhalt, den Sie veröffentlichen wollen, ein rechtliches Risiko darstellt.
- Geben Sie LLM keine Informationen, die Geschäftsgeheimnisse oder vertrauliche Informationen enthalten könnten.
- Nutzen Sie LLM nur in Themenbereichen, mit denen Sie sich auskennen und die Antwort überprüfen können.
- Überprüfen Sie immer die durch ein LLM bereitgestellten Informationen.
- Um das Risiko von Missverständnissen zu reduzieren, stellen Sie dem LLM klare spezifische Fragen und geben Sie bei unklaren oder widersprüchlichen Antworten zusätzliche Details an.
- LLM sollten als hilfreiches Werkzeug betrachtet werden, aber nicht als alleinige Informationsquelle. Es ist daher ratsam, mehrere Quellen heranzuziehen.
- Prüfen Sie vor der Nutzung von LLM, ob dies gegen vertragliche Vereinbarungen mit Geschäftspartnern Ihres Arbeitsgebers verstößt und welche Beschränkungen bei der Nutzung eingehalten werden müssen.
- Geben Sie keine Informationen weiter, die den Inhalt unserer vertraglichen Vereinbarungen enthalten.
- Stellen Sie sicher, dass Sie die Nutzungsbedingungen und Benutzervereinbarungen für KI einhalten, wenn Sie KI-Tools verwenden.
- Prüfen Sie die AGB daraufhin, welche Nutzungsrechte der LLM bzw. deren Anbieter an Ihren Daten und Informationen eingeräumt werden und wie sie verarbeitet werden (Speicherort, Weiterleitung/Verarbeitung an/durch Dritte).
- Achten darauf, die Internetadresse korrekt einzugeben. Schon ein einzelnes falsches Zeichen kann dafür sorgen, dass Sie auf eine andere Webseite geleitet werden.

- Melden Sie jede ungewöhnliche verdächtige Aktivität sofort der in Ihrem Unternehmen zuständigen Stelle.
- Stellen Sie sicher, dass LLM generierte Texte keine diskriminierenden Inhalte enthalten, die gegen Gesetz oder den Verhaltenskodex Ihres Unternehmens verstoßen, bevor Sie die Texte nutzen.
- Geben Sie der LLM für diskriminierenden Output ein negatives Feedback.
- Geben Sie in LLM keine Prompts ein, die als beleidigend, diskriminierend oder illegal angesehen werden könnten.
- Verwenden Sie LLM-generierte Inhalte nur für Themenbereiche, in denen Sie über Fachwissen verfügen, sodass Sie die Richtigkeit des Outputs überprüfen können.
- Überprüfen Sie den generierten Inhalt vor der Nutzung auf Fehler.
- Bleiben Sie auf dem Laufenden! Informieren und bilden Sie sich hinsichtlich der Nutzung und Entwicklung von LLM weiter.
- Nehmen Sie an den Compliance-Schulungen Ihres Arbeitgebers teil, um einen verantwortungsvollen und sicheren Umgang mit LLM zu gewährleisten.

Disclaimer:

Dieses Dokument stellt ausschließlich eine kostenlose Information dar und ist keine Rechtsberatung. Insbesondere ist zu beachten, dass abhängig von der Branche und Geschäftstätigkeit Ihres Unternehmens weitere Gesetze durch die Nutzung von LLM verletzt werden können.

Zur Erstellung dieses Dokuments wurde teilweise ein LLM genutzt.

Möchten Sie Ihr Unternehmen und Ihre Mitarbeiter schützen oder benötigen Sie Rechtsberatung?

Dann kontaktieren Sie mich über das Kontaktformular unter https://torkilegal.de/kontakt/ , per E-Mail unter info@torkilegal.de oder telefonisch unter +49 1577 8867 520.