

Was versteht man unter Legal Prompting

Konversation mit OpenAI ChatGPT - März 2024

 Unter Legal Prompting versteht man die effiziente Fragestellung an ein LLM im rechtlichen Kontext. Für die Qualität der generierten Antworten sind eine richtige Strukturierung und eine klare, präzise Formulierung des Prompts ausschlaggebend.

Lese ich irgendwo geschrieben durch jemand, der/die es wissen muss, jedenfalls meint, es zu wissen.

Weißt du, ChatGPT, was *Legal Prompting* genau bedeutet. Ich meine rein begrifflich?

 'Legal Prompting' bezieht sich im Kontext von großen Sprachmodellen (Large Language Models, LLMs) auf die Technik, wie Fragen und Anweisungen formuliert werden, um juristisch relevante und präzise Antworten zu erhalten. Diese Technik umfasst die folgenden Aspekte:

Strukturierung des Prompts: Der Aufbau des Prompts muss klar und logisch sein, um das Modell auf die relevanten Informationen zu lenken und Missverständnisse zu vermeiden. Dies kann durch die Einteilung in Absätze oder Punkte erfolgen und sollte alle notwendigen Informationen und Kontext liefern.

Präzise Formulierung: Die Fragen und Anweisungen müssen spezifisch und eindeutig sein, um sicherzustellen, dass das Modell die Anfrage korrekt versteht. Unklare oder mehrdeutige Formulierungen können zu ungenauen oder irrelevanten Antworten führen.

Juristischer Kontext: Der Prompt sollte den rechtlichen Rahmen und den spezifischen Kontext der Anfrage beinhalten, einschließlich relevanter Gesetze, Vorschriften oder juristischer Prinzipien. Dies hilft dem Modell, die Anfrage im richtigen Zusammenhang zu interpretieren.

Beispiele und Szenarien: Gezielte Beispiele oder hypothetische Szenarien können hilfreich sein, um die Anfrage zu verdeutlichen und spezifische Aspekte eines rechtlichen Problems hervorzuheben.

Ein gut konstruierter legaler Prompt könnte also folgendermaßen aussehen:

- a) **Einleitung und Kontext:** Einführung des rechtlichen Themas und des spezifischen Kontexts.
- b) **Konkrete Fragestellung:** Eine klar definierte Frage oder Aufgabe.
- c) **Relevante Details:** Alle notwendigen Informationen, Fakten und rechtlichen Rahmenbedingungen, die für die Beantwortung der Frage wichtig sind.

Beispiel für einen gut strukturierten legalen Prompt:

Einleitung:

Bitte erläutere die rechtlichen Anforderungen an einen Arbeitsvertrag in Deutschland.

Konkrete Fragestellung:

Welche Mindestangaben muss ein schriftlicher Arbeitsvertrag nach deutschem Recht enthalten?

Relevante Details:

Berücksichtige dabei die Vorschriften des Bürgerlichen Gesetzbuchs (BGB) und des Nachweisgesetzes (NachwG).

Durch diese Herangehensweise wird sichergestellt, dass das Sprachmodell relevante, präzise und kontextbezogene Antworten generieren kann.



Danke soweit. Nun, ich gehe davon aus, dass eigentlich alle Prompts legal sind.

Allerdings, ob du auf bestimmte Prompts reagierst und wie du darauf reagierst, kann sich dann an der Sphäregrenze des Legalen zum Illegalen bewegen, dich somit in justiziables Fahrwasser geraten lassen.



Ja, du hast recht, dass die Gestaltung von Prompts, insbesondere im rechtlichen Kontext, entscheidend ist, um sicherzustellen, dass die generierten Antworten nicht nur hilfreich und präzise, sondern auch legal und ethisch vertretbar sind. Bei der Arbeit mit großen Sprachmodellen wie GPT-4 gibt es wichtige Überlegungen, um rechtliche und ethische Fallstricke zu vermeiden:

Einhaltung rechtlicher Grenzen: Prompts sollten innerhalb der gesetzlichen Vorschriften und ethischen Standards formuliert werden. Dies bedeutet, dass Anfragen, die zu illegalen Aktivitäten ermutigen oder rechtlich bedenkliche Ratschläge liefern könnten, vermieden werden müssen.

Datenschutz und Vertraulichkeit: Prompts sollten keine sensiblen persönlichen Daten oder vertrauliche Informationen enthalten, um den Datenschutz und die Privatsphäre der Betroffenen zu wahren.

Vermeidung von Rechtsberatung: Während GPT-4 hilfreiche Informationen zu rechtlichen Themen liefern kann, sollte klargestellt werden, dass es keine qualifizierte Rechtsberatung ersetzt. Nutzer sollten ermutigt werden, bei komplexen rechtlichen Fragen professionelle Rechtsberatung in Anspruch zu nehmen.

Ethik und Verantwortung: Prompts und die darauf basierenden Antworten sollten ethischen Grundsätzen folgen, wie Fairness, Unvoreingenommenheit und Respekt vor allen Beteiligten.

Beispiel eines unethischen Prompts, der vermieden werden sollte:

Wie kann ich eine rechtliche Grauzone ausnutzen, um Steuern zu hinterziehen?

Beispiel eines ethisch vertretbaren und rechtlich einwandfreien Prompts:

Welche legalen Steuersparmöglichkeiten gibt es für Selbstständige in Deutschland gemäß den geltenden Steuerregelungen?

Zusammengefasst, während jeder Prompt grundsätzlich legal sein kann, ist es entscheidend, dass Prompts so formuliert werden, dass sie weder gegen Gesetze noch gegen ethische Richtlinien verstoßen. Dies trägt dazu bei, dass die Nutzung von Sprachmodellen verantwortungsbewusst und sicher erfolgt.



Danke für die Ausführung. Aber darum ging es mir eigentlich gar nicht.

Mir ging es nur darum herauszustellen, dass das, was Englisch als ‚*Legal Prompt*‘ bzw. als ‚*Legal Prompting*‘ bezeichnet wird, eben etwas ganz anderes ist, als das, was auf Deutsch als ein ‚*legaler Prompt*‘ oder ein ‚*legales Prompting*‘ zu bezeichnen wäre.



Ah, ich verstehe. Du wolltest auf den Unterschied zwischen dem englischen Begriff ‚*Legal Prompting*‘ und der möglichen deutschen Interpretation von ‚*legaler Prompt*‘ oder ‚*legales Prompting*‘ hinweisen. Das ist ein wichtiger Unterschied:

Legal Prompting (Englisch):

Bezieht sich spezifisch auf die Technik der Formulierung von Anfragen an ein Sprachmodell im rechtlichen Kontext, um präzise und relevante juristische Antworten zu erhalten.

Hat nichts mit der Legalität der Anfrage selbst zu tun, sondern mit der Art und Weise, wie juristische Fragen effektiv gestellt werden.

Legal(er) Prompt (Deutsch):

Würde sich allgemein auf einen Prompt beziehen, der innerhalb der gesetzlichen Vorschriften liegt, also auf eine legale Fragestellung oder Anweisung.

Fokussiert sich auf die rechtliche Zulässigkeit des Inhalts der Anfrage und nicht auf den spezifischen rechtlichen Kontext oder die Effektivität der Fragestellung.

Dieser Unterschied ist bedeutend, da „*Legal Prompting*“ im Englischen eine spezielle Methodik im juristischen Bereich beschreibt, während „*legales Prompting*“ im Deutschen einfach eine rechtlich einwandfreie Fragestellung bedeuten könnte, unabhängig vom Kontext oder der Spezialisierung.

Zusammengefasst:

Legal Prompting (Englisch): Effektive Fragestellung im rechtlichen Kontext.

Legal(er) Prompt (Deutsch): Eine Frage oder Anweisung, die gesetzeskonform ist.

Das zeigt, wie wichtig es ist, kontextbezogen zu übersetzen und Begriffe genau zu verstehen, um Missverständnisse zu vermeiden.



Genau, wobei ich abschließend einwenden möchte, dass die Frage nach der rechtlichen Zulässigkeit von Prompts bisher so weder in der Rechtswissenschaft, noch in Gesetzen, geschweige denn in der Rechtsprechung überhaupt gestellt wurde, anzunehmenderweise aber entscheidend davon abhängen wird, wie das jeweilige Sprachmodell auf Anfragen wie der zur Ausnutzung rechtlicher Grauzonen reagiert, nicht? Ich bitte um eine kurze, schlagende Antwort.



Richtig, die rechtliche Zulässigkeit von Prompts ist ein bisher unerforschtes Gebiet, aber die Reaktion des Sprachmodells auf bestimmte Anfragen kann potenziell Auswirkungen auf die rechtliche Beurteilung haben.