

## Mag. Novotny: Wozu stimmen Sie zu, wenn Sie ChatGPD oder sonstige KI-Applikationen nutzen?

Was sollten Sie vorab prüfen? Sind Ihre Mitarbeiter bereits geschult und instruiert?

---

KI ist aktuell in aller Munde. Die wenigsten wissen aber, was „im Hintergrund“ passiert, wenn man solche Anwendungen nutzt. Daher möchten wir mit unserem Beitrag heute Problembewusstsein dafür schaffen, dass man KI-Anwendungen (wie etwa **ChatGPD** von Open AI, **Copilot** von Microsoft, Übersetzungs-Tools, etc) nicht **„ungeschaut“ im Unternehmen einsetzen darf**. Da gibt es **Datenschutz-, aber auch Urheberrechtsprobleme, bedenkliche Haftungsszenarien**, einiges ist definitiv verboten, für anderes muss man seine **Mitarbeiter schulen** etc.

Heute wollen wir uns näher ansehen, **was im Hintergrund passiert, wenn Sie eine KI-Anwendung nutzen** und warum das datenschutz-, urheberrechtlich bedenklich sein kann. Wohl zumeist auch ist. Daher baten wir **Mag. Novotny uns zu erklären**, was das juristisch bedeutet und **wie man sich möglichst gut „absichern“ kann**.

**ACHTUNG:** Ein immer größer werdendes Problem ist, wenn Mitarbeiter – ohne Schulung und ohne Zustimmung des Unternehmens – **KI-Anwendung selbstständig in der Firma nutzen**, nur um rascher die Arbeit erledigen zu können (und da beziehen wir uns nicht auf die Richtigkeit der Arbeit – das schauen wir uns bei anderer Gelegenheit näher an – „Schlagwort: halluzinierende KI“).

### ChatGPD & sonstige KI-Applikationen: Wozu geben Sie Ihre Zustimmung bei der Nutzung?

Wer Kinder im schulpflichtigen Alter zu Hause hat, wird schon in den letzten Monaten mit einer **KI-Anwendung namens ChatGPD** in Berührung gekommen sein. Dieses Programm möchten wir heute „als Musterbeispiel“ verwenden, weil man daran vieles erklären kann, was eine KI tut bzw. wie eine KI dabei vorgeht. Dabei handelt es sich um ein „**Large Language Model**“, auf Deutsch ein „riesiges Sprachmodell“, also ein Computer der mit Milliarden von Dokumenten, ganzen Bibliotheken (nicht immer unter Beachtung von Urheber-Rechten) **trainiert** wurde und dadurch – richtige, aber auch falsche – Zusammenhänge gelernt hat. Und z.B. erkannt hat, dass bestimmte Wörter und Sätze oft zusammen vorkommen oder dass nach einem Beistrich oftmals ein „dass“ mit Doppel-S vorkommt. Usw. Usw.

### Das hat nichts mit Intelligenz zu tun, sondern nur mit Wahrscheinlichkeiten.

Wenn Sie also in ChatGPD eine Frage stellen, dann **durchsucht die KI alle gelesenen Daten und sucht die wahrscheinlichste Antwort**, ob diese aber stimmt oder nicht, lässt sich nicht immer feststellen. Zur Bestätigung dieser Aussage zitiere ich aus der Datenschutzerklärung von ChatGPD, [hier nachzulesen...](#)

Am Ende von Punkt 5 „Ihre Rechte“, schreibt Open AI (Unterstreichung durch Redaktion):  
*„Eine Anmerkung zur Genauigkeit: Dienste wie ChatGPT generieren Antworten, indem sie die Anfrage eines Nutzers lesen und als Antwort die Wörter vorhersagen, die wahrscheinlich als nächstes erscheinen werden. In einigen Fällen sind die am wahrscheinlichsten als nächstes erscheinenden Wörter nicht unbedingt die faktisch genauesten. Aus diesem Grund sollten Sie sich nicht auf die faktische Genauigkeit der Ergebnisse unserer Modelle verlassen“.*

**Also warnt ChatGPD vor seinen eigenen Ergebnissen. Daher: Niemals blind vertrauen.**

**Egal:** Die Schüler merkten sehr schnell, dass sich diese Software ganz hervorragend eignet, um kurze Zusammenfassungen von Büchern zu erstellen und damit die **Hausarbeit blitzschnell erledigen** zu

können. Oder Texte in eine andere Sprache zu übersetzen. Oder einen Lebenslauf für eine Bewerbung zu erstellen und und und.

### **Nun ist ChatGPD bei uns Erwachsenen und in den Unternehmen angekommen.**

Dem Problembereich „Richtigkeit“ von Ergebnissen, die die KI liefert, werden wir einen eigenen Beitrag widmen.

Heute möchten wir Sie auf die **Probleme hinweisen**, die dadurch entstehen, **weil Sie die KI nutzen und damit die Nutzungsbedingungen stillschweigend akzeptiert haben**.

Um die **Gefahren aus der Nutzung von KI leicht verstehen zu können**, ein **Beispiel** mit Infos, was da passiert. Ganz simpel erklärt.

Nehmen wir an, Sie wollen einen **Bericht über das Geschäftsjahr 2024 für Ihren Vorstand** erstellen, sich aber durch Nutzung von KI wie ChatGPD oder Copilot (um zwei beispielhaft zu benennen) Arbeit ersparen.

Dann geben Sie genau diese Vorgabe ein (das kann man so formulieren, wie ich es oben getan habe oder kompliziert in Form von Prompts, die die Maschine besser versteht). Danach müssen Sie das **KI-System noch mit jenen Zahlen und Fakten füttern**, die dann im Bericht, Vortrag, etc. für den Vorstand aufscheinen sollen. Etwa Umsatz, Gewinn, Mitarbeiter-Zahl, Referenz-Kunden, gewonnene und verlorene Projekte, Klagsfälle, Schwierigkeiten und Rauswürfe von Mitarbeiter, usw..

**Diese Zahlen und Fakten hätten Sie Word oder Powerpoint auch „mitgeteilt“**, nur waren diese Zahlen nur lokal auf Ihrem PC (eventuell in Ihrer – hoffentlich passwortgesicherten – Cloud), um den Bericht oder den Vortrag erstellen zu können.

**Nutzen Sie jedoch eine KI**, dann verlassen diese personenbezogenen, vielleicht geheimen, auf jeden Fall firmenspezifischen Informationen Ihren Rechner. Und gelangen in die Hände des KI-Betreibers. Der erstellt damit den von Ihnen gewünschten Bericht **UND nutzt Ihre Inputs dazu, um die KI zu verbessern**, d.h. diese Inputs werden in die KI-eigene Datenbank aufgenommen, verarbeitet und **gelangen in den „weltweiten Topf“**. Und werden auch für irgendwelche andere Zwecke genutzt.

### **WOLLEN Sie das? DÜRFEN SIE DAS? Ich sage als Jurist: Sicher nicht!**

Wir wollen hier kein Rechts-Seminar abhalten, aber doch für Problembewusstsein sorgen.

**Und Tipps für die Praxis geben**, daher:

- Studieren Sie die **Nutzungsbedingungen** jener KI-Anwendungen, die Sie im Unternehmen einsetzen möchten. Was steht dort genau?
- **Was darf der KI-Betreiber mit Ihren Inputs**, Ihren personenbezogenen Daten tun? Wem gibt er sie weiter?
- Stimmen Sie laut Nutzungsbestimmungen – durch die bloße Nutzung – zu, **dass Sie selbst „geltendes Recht“ einhalten?**  
Das kann z.B. problematisch werden, wenn Sie ein Foto in Ihrer Anfrage hochladen, um eben z.B. den Vorstand im Bericht mit Namen und Bild herzuzeigen. Damit haben Sie das Foto „dem Internet zur Verfügung gestellt“, wozu Sie kein Recht haben und damit das Urheber- / Nutzungsrecht des Fotografen, Ihrer Firma, etc. geschädigt haben. Millionenklagen können die Folge sein.

- **Schließt der KI-Betreiber die Haftung komplett aus und beschränkt sie auf Mini-Beträge?** Bei ChatGPT findet sich die relevante Passage ganz am Ende der Nutzungsbedingungen:  
Wörtliches Zitat, nur die Unterstreichung stammt von uns. [Nachzulesen hier...](#)  
***Haftungsbeschränkung.** WEDER WIR NOCH UNSERE VERBUNDENEN UNTERNEHMEN ODER LIZENZGEBER HAFTEN FÜR INDIREKTE, ZUFÄLLIGE, BESONDERE, FOLGE- ODER EXEMPLARISCHE SCHÄDEN, EINSCHLIESSLICH SCHÄDEN FÜR ENTGANGENEN GEWINN, FIRMENWERT, NUTZUNG ODER DATEN ODER ANDERE VERLUSTE, SELBST WENN WIR AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDEN. UNSERE GESAMTHAFTUNG IM RAHMEN DIESER BEDINGUNGEN ÜBERSTEIGT NICHT DEN BETRAG, DEN SIE IN DEN LETZTEN 12 MONATEN VOR ENTSTEHUNG DES SCHADENS FÜR DEN DIENST, DER DEN ANSPRUCH AUSGELÖST HAT, BEZAHLT HABEN, ODER EINHUNDERT DOLLAR (\$100), JE NACHDEM, WELCHER BETRAG HÖHER IST.*
- **Erfüllt der KI-Anbieter die Datenschutz-Grundverordnung?**  
Da sind wir wieder bei Fragen wie: Wo ist der Sitz des KI-Betreibers und wo werden die Daten verarbeitet (innerhalb, außerhalb der EU)?  
Gehen die Daten in die USA? Ist z.B. Open AI registriert beim EU-US-Framework?  
Gibt es einen Auftragsverarbeitervertrag und entspricht der der DSGVO?  
Gibt es TOMs?
- **Urheberrechts-Bedenken:**  
Dass Sie keine urheberrechtlichen Werke im Zuge Ihrer Anfrage an die KI hochladen dürfen, haben wir oben bereits besprochen. Aber was passiert, wenn das Ergebnis der KI-Anfrage das Urheberrecht von Dritten verletzt, und Sie nutzen das? Der KI-Betreiber hat seine Haftung auf maximal 100 \$ eingeschränkt. Urheberrechtsverletzungen können aber mit zigtausenden, hunderttausenden Euro bestraft werden (da gibt es schon zahlreiche Urteile).

## WAS ALSO TUN, um diese Problembereiche bei Nutzung von KI möglichst zu bereinigen?

1. Identifizieren Sie, **ob bzw. wo bereits KI-Anwendungen im Unternehmen verwendet** werden.
2. Lesen Sie die **Nutzungsbedingungen**, Datenschutzerklärungen, etc. des Anbieters genau.  
Die Hilfe eines mit der DSGVO-vertrauten Fach-Juristen in Anspruch nehmen...
3. Entscheiden Sie, ob das KI-Produkt **im Interesse des Unternehmens** liegt. Zustimmung oder verbieten.
4. Bei OK: Versuchen Sie die **Einstellungen im KI-Produkt** möglichst datenschutzfreundlich zu gestalten.  
**Tipp: Auf Gratis-Versionen verzichten.** Dort kann man meist nicht einstellen, dass die Daten nicht zum Trainieren der KI verwendet, also weitergegeben werden. Somit landen alle Ihre Inputs im weltweiten „Wissens-Topf“.
5. **Interne Nutzungsregeln für KI definieren** und als zwingende Mitarbeiter-Vorgabe aussenden:  
Darin u.a. **verbieten, dass Mitarbeiter „privat auf Firmengeräten“ eine Gratis-KI-Version nutzen.**
6. Mitarbeiter für die KI-Nutzung **schulen (das ist bereits PFLICHT seit Anfang dieses Jahres)!**
7. **KI-Koordinator** im Unternehmen definieren, als 1. Ansprechpartner für Fragen, Probleme etc.
8. Regelmäßig überprüfen, ob obige Punkte im Unternehmen eingehalten werden und den – sicherlich noch mehr werdenden – rechtlichen Vorgaben entsprechen...

Beste Grüße von [RA Mag. Stephan Novotny](#) und [Mag. Günter Wagner, B2B-Projekte](#)

Sollten Sie noch keinen Anwalt haben: **Mag. Stephan Novotny**, ein auf **Versicherungs- und Datenschutzrecht spezialisierter Fachanwalt** steht gerne zur Verfügung. Für Zurich-Newsletter-Leser sogar zum **Spezialpreis**.



RA Mag. Stephan Novotny, Foto: Stephan Huger

**RA Mag. Stephan Novotny**

1010 Wien, Landesgerichtsstraße 16/12

[kanzlei@ra-novotny.at](mailto:kanzlei@ra-novotny.at)

<https://www.ra-novotny.at>