Blogartikel vom 14.08.2024
Rechtsgebiet: IT-Recht
Autor: Rechtsanwalt Christian Geißler

Künstliche Intelligenz und Geschäftsgeheimnisse

Zuletzt haben wir in einem Beitrag die rechtliche Problematik hinsichtlich des Urheberrechts und das Datenschutzrechts bei der Verwendung von Künstlichen Intelligenzen betrachtet.

In diesem Beitrag stellen wir uns der Frage, ob Unternehmen auch im Hinblick auf Betriebs- und Geschäftsgeheimnisse besondere Vorkehrungen bei der Verwendung von Künstlichen Intelligenzen treffen müssen und ob die Nutzung sogar gegen das Geschäftsgeheimnisschutzgesetz (GeschGehG) verstoßen kann.

Denn die Eingabe bei ChatGPT oder einer anderen Künstliche Intelligenz führt regelmäßig dazu, dass diese Daten von der jeweiligen Künstlichen Intelligenz weiterverwendet werden können. OpenAI, der Betreiber von ChatGPT, erklärt z.B. in seinen Nutzungsbedingungen ausdrücklich, dass bei einer (Non-API) Nutzung seiner Dienste, die eingegebene Daten von OpenAI weiterverwendet werden dürfen, sofern der Nutzer nicht ausdrücklich seinen Widerspruch erklärt hat (Opt-Out).

Das hat zur Folge, dass auch eventuelle Betriebs- oder Geschäftsgeheimnisse, welche bei ChatGPT oder einer anderen Künstliche Intelligenz eingegeben werden, vom Betreiber ggf. weiterverwendet werden und somit vom Nutzer „verraten" werden könnten.

Die Definition von Geschäftsgeheimnissen

Seit dem Jahr 2019 ist in Deutschland das Geschäftsgeheimnisgesetz (GeschGehG) in Kraft. Dieses Gesetz ist Ausfluss der EU-Richtlinie 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen.

Das Geschäftsgeheimnis wird in § 2 Nr. 1 lit. a) – c) GeschGehG definiert und umfasst Informationen, die:

1. Nicht allgemein bekannt oder zugänglich sind und daher wirtschaftlichen Wert haben,
2. Angemessene Geheimhaltungsmaßnahmen unterliegen,
3. Ein berechtigtes Interesse an der Geheimhaltung besteht.

Inhaber eines Geschäftsgeheimnisses, gemäß § 2 Nr. 2 GeschGehG, ist die natürliche oder juristische Person, die rechtmäßige Kontrolle über das Geschäftsgeheimnis hat, in der Regel also das Unternehmen bzw. der Arbeitgeber.

Geschäftsgeheimnisse können vielfältige Informationen umfassen, von bestimmten Kundendaten über Konstruktionszeichnungen, Prototypen, Finanzierungsinformationen, Arbeitsanweisungen, Rezepturen usw. bis hin zu kalkulatorischen Grundlagen für Preisstrategien oder Hintergrundinformationen für Marketingkampagnen.

Geheimhaltungsmaßnahmen sind notwendig

Damit ein Geschäftsgeheimnis als solches Schutz genießt, setzt das deutsche Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) u.a. voraus, dass die fragliche Information „Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen" sein müssen. Der Inhaber des Geschäftsgeheimnisses muss also aktiv Maßnahmen ergreifen, um das betreffende Geheimnis vor dem Zugriff Dritter zu schützen. Diese Maßnahmen müssen auch dokumentiert werden, um sie (z.B. im Streitfall) nachweisen zu können.

Zum Schutz von Geschäftsgeheimnissen können Unternehmen verschiedene Maßnahmen ergreifen:

- **Vertragliche Maßnahmen:** Die Verpflichtung der Mitarbeiter oder Dienstleister mittels Vertraulichkeits- und Verschwiegenheitsvereinbarungen (auch NDA)
- **Organisatorische Maßnahmen:** Die Festlegung von Verantwortlichkeiten (Berechtigungskonzept) oder die Einrichtung von Schutzkonzepten
- **Technische Maßnahmen:** Die Einrichtung von Firewalls, Safes, Passwortschutz oder anderen Schutzvorrichtungen

Stellt die Nutzung von ChatGPT oder anderen Künstlichen Intelligenzen bereits eine Rechtsverletzung im Sinne des GeschGehG dar?

Der Nutzer als Rechtsverletzer

Wenn Mitarbeiter eines Unternehmens als Nutzer Geschäftsgeheimnisse in das Dialogfenster von ChatGPT eingeben, könnte der Mitarbeiter als Rechtsverletzer im Sinne des § 2 Nr. 3 GeschGehG gelten, sofern dies eine unrechtmäßige Offenlegung darstellt. OpenAI, das Unternehmen hinter ChatGPT, speichert nach eigener Aussage Eingaben (außer über die API) und nutzt diese zur Verbesserung ihrer Dienste. Dementsprechend könnten die eingegebenen Informationen nicht nur gegenüber OpenAI offengelegt werden, sondern evtl. sogar gegenüber anderen Nutzern von ChatGPT, wenn die Geschäftsgeheimnisse diesen gegenüber als Folge eines „Prompts" wieder ausgegeben werden. In einem solchen Fall kann die Nutzung von ChatGPT als eine Offenlegung im Sinne der §§ 2 Nr. 3, 4 Abs. 2 Nr. 3

GeschGehG gewertet werden, da die Offenlegung und somit die Preisgabe der geheimen Information gegenüber einem unberechtigten Dritten erfolgt.

Für eine Rechtsverletzung im Sinne des § 2 Nr. 3 GeschGehG ist aber auch notwendig, dass die betreffende Offenlegung rechtswidrig war. Dies kann der Fall sein, wenn der Mitarbeiter gemäß § 4 Abs. 2 Nr. 3 GeschGehG „gegen eine Verpflichtung verstößt, das Geschäftsgeheimnis nicht offenzulegen". Relevant ist also, ob der Mitarbeiter einer **Verpflichtung unterliegt**, das Geschäftsgeheimnis nicht offenzulegen.

Hat der Inhaber des Geschäftsgeheimnisses (Unternehmen) in die Offenlegung eingewilligt, so ist kein rechtswidriges Handeln des Mitarbeiters gegeben.

An dieser Stelle drängt sich die Frage auf: Wann liegt eine Einwilligung des Inhabers vor?

Wenn im Unternehmen eine grundsätzliche Erlaubnis zur Nutzung von ChatGPT oder anderen Künstlichen Intelligenzen besteht, könnte darin bereits eine Einwilligung des Unternehmens in die Offenlegung von Geschäftsgeheimnissen gesehen werden. Anders könnte die rechtliche Einschätzung ausfallen, wenn der Mitarbeiter eine Verschwiegenheits- oder Vertraulichkeitsvereinbarung hinsichtlich der Geschäftsgeheimnisse des Unternehmens unterschrieben hat.

Zwar ist davon auszugehen, dass diese einer ausdrücklichen Einwilligung entgegensteht, rechtlich eindeutig, ist dies aber nicht. Sollte es zu einer rechtlichen Auseinandersetzung kommen, könnte es dennoch zu einer Abwägung der widerstreitenden Interessen kommen.

Daher sollten Unternehmen vorab Klarheit schaffen und betriebsintern genau regeln, ob einerseits ChatGPT und andere Künstliche Intelligenzen genutzt werden dürfen und andererseits in welchem Umfang, insbesondere in Bezug auf die Eingabe von Geschäftsgeheimnissen.

An dieser Stelle ist auch genau darauf zu achten, dass eventuelle Verschwiegenheitsverpflichtungen (auch NDA), welche das Unternehmen abgeschlossen hat, nicht verletzt werden. Denn werden Informationen bei ChatGPT und andere Künstliche Intelligenzen eingegeben, welche unter eine solche Verpflichtung fallen, stellt dies grundsätzlich eine Offenlegung gegenüber einem Dritten dar. Ist diese Offenlegung nicht gestattet, liegt ein Verstoß vor. Gegebenenfalls ist deshalb eine genaue Arbeitsanweisung zum Umgang mit derartigen Informationen notwendig.

Wie kann ich mich gegen die Verletzung von Geschäftsgeheimnissen wehren?

Kommt es dennoch zu einer Verletzung eines Geschäftsgeheimnisses, so stehen dem Inhaber Abwehrrechte gegen den Rechtsverletzer zu.

So kann der Geheimnisinhaber Unterlassung- und Beseitigungsansprüche geltend machen, aber auch Auskunfts- und Schadensersatzansprüche geltend machen.

Je nach Art der Rechtserletzung kann auch die Vernichtung oder die Herausgabe von Gegenständen, Dokumenten, Materialien, elektronischen Daten etc. verlangt werden.

Grundsätzlich ist für die Geltendmachung der Abwehrrechte aus dem GeschGehG kein Verschulden des Rechtsverletzers notwendig. Auch bei einer unabsichtlichen Offenlegung sollen dem Geheimnisinhaber nach dem Gesetzeszweck Abwehrrechte an die Hand gegeben werden, damit dieser seine Geheimnisse (wieder) schützen kann und die Offenlegung (soweit möglich) wieder rückgängig gemacht werden kann.

Liegt aber sogar ein Verschulden seitens des Rechtsverletzers vor, so kann der Geheimnisinhaber zusätzlich Schadensersatz verlangen. In einem solchen Fall könnten auch arbeitsrechtliche Konsequenzen wie eine Abmahnung bis hin zu einer fristlosen Kündigung drohen.

In Ausnahmefällen kann sogar eine Strafbarkeit nach § 23 GeschGehG gegeben sein, wenn der Rechtsverletzer bei der Offenlegung zu Eigennutz, zugunsten eines Dritten oder mit Schadensabsicht gegenüber dem Inhaber gehandelt hat.

Empfehlungen für Schutzmaßnahmen im Unternehmen

Um eine sichere Nutzung von ChatGPT oder anderen Künstliche Intelligenzen zu gewährleisten, sollten Unternehmen vorab folgende Maßnahmen in Betracht ziehen:

1. **Interne Kategorisierung von Informationen:** Betriebs- und Geschäftsgeheimnissen sollten eindeutig und für die Mitarbeiter leicht erkennbar also solche gekennzeichnet werden. (z.B. durch den jeweiligen Zusatz „Geheim", „Vertraulich").
2. **Implementierung interner technischer Vorgaben:** Die Nutzung sollte nur mit Einstellungen erfolgen, die eine Speicherung der Daten und Nutzung zu trainingszwecken ausschließt.
3. **Aufklärung der Mitarbeiter:** Die eigenen Mitarbeiter sollten über die Risiken aufgeklärt werden. Hilfreich ist hier die Einführung von Nutzungsrichtlinien.
4. **Erwägung eines Verbots:** Besteht ein hohes Risiko bezüglich der Offenlegung von Betriebs- und Geschäftsgeheimnissen, so sollte die Nutzung von ChatGPT oder anderen Künstlichen Intelligenzen komplett verboten und technisch blockiert werden.

Künstliche Intelligenz und Berufsgeheimnisträger

Sogenannte Berufsgeheimnisträger müssen sich aber nicht nur um den Datenschutz und eventuelle Geschäftsgeheimnisse Gedanken machen. Sie treffen darüber hinaus noch

verschärfte Pflichten aufgrund Ihres Berufsstandes, wobei sogar in Ausnahmefällen eine Strafbarkeit nach Strafgesetzbuch relevant sein kann.

Konkret ist in § 203 StGB die Verletzung von Privatgeheimnissen unter Strafe gestellt. Demnach wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm z.B. als Arzt, Rechtsanwalt, Wirtschaftsprüfer oder Steuerberater (und ggf. deren Angestellte) anvertraut wurde.

Kann die Eingabe von unter das Berufsgeheimnis fallendender Informationen in ChatGPT oder einer anderen Künstlichen Intelligenz bereits den Straftatbestand des § 203 StGB verwirklichen?

Tatsächlich sollten Berufsgeheimnisträger besondere Vorsicht bei der Nutzung von ChatGPT und anderen Künstlichen Intelligenzen walten lassen. Zwar erfolgt immer eine Prüfung im Einzelfall, auch im Hinblick auf die Art des Geheimnisses, jedoch ist grundsätzlich davon auszugehen, dass die Eingabe von z.B. Gesundheitsdaten oder Daten aus einem Mandatsverhältnis einen Verstoß gegen das Berufsrecht darstellt. Je nach Vorsatz des Handelnden (absichtliches Handeln oder nur fahrlässig) liegt zudem die Verwirklichung des Straftatbestandes aus § 203 StGB auf der Hand.

Fazit

Nicht nur im Hinblick auf den Datenschutz und das Urheberrecht bestehen rechtliche Risiken beim Einsatz von ChatGPT und anderen Künstlichen Intelligenzen in Unternehmen. Um diesen vorzubeugen, sollten Unternehmen daher vorab klare Richtlinien zur Nutzung festlegen und die eigenen Mitarbeiter auf die Risiken hinweisen.