EXKLUSIVE LESEPROBE
technology research hub

Heidrich · Wegener · Werner

Inkl. Data Privacy Framework und generative KI

Datenschutz und IT-Compliance

Das Handbuch für Admins und IT-Leiter

- Entscheidungshilfen und Leitfaden für die Praxis
- Grundlagen, Umgang mit Daten, Sanktionen und Haftung
- Anforderungen der DSGVO an den IT-Betrieb

Rheinwerk Computing

Kapitel 12

Generative KI: Was bei der Nutzung von ChatGPT& Co. zu beachten ist

In diesem Kapitel nehmen wir eine Einordnung der bestehenden rechtlichen Fragen bei der Nutzung generativer KI wie ChatGPT, DALL-E, Github Copilot oder Midjourney vor. Neben urheberrechtlichen Besonderheiten gibt es hier vor allem datenschutzrechtliche Fragestellungen.

KI-Angebote schicken sich an, die Welt der Texte, Bilder und Grafiken unwiderruflich zu verändern. ChatGPT& Co. trainieren mit Milliarden von Inhalten im Netz, die anderen Personen oder Unternehmen gehören. Die Frage bei der rechtlichen Bewertung ist, welche Auswirkungen dies auf die von der KI ausgegebenen Inhalte hat – und wer wiederum Rechte an diesen Inhalten geltend machen kann.

Zwar fehlt es in diesem Bereich noch an Gerichtsurteilen. Erste eindeutige Ergebnisse hinsichtlich der rechtlichen Bewertung stehen jedoch bereits fest. Diese umfassen in erster Linie die beiden Bereiche Urheber- und Datenschutzrecht und sollen nachfolgend erläutert werden.

12.1 Grundlagen: Wie funktioniert ChatGPT eigentlich?

ChatGPT basiert auf der Generative Pre-trained Transformer-Architektur, kurz GPT-Architektur, die wiederum auf der Transformer-Architektur aufbaut. Um ein tieferes Verständnis von ChatGPT zu vermitteln, gehen wir auf die Schlüsselkonzepte und Komponenten ein:

Die Transformer-Architektur wurde 2017 eingeführt und hat die Art und Weise, wie sequenzielle Daten in neuronalen Netzwerken verarbeitet werden, revolutioniert. Der Transformer verwendet den sogenannten Self-Attention-Mechanismus, um Beziehungen zwischen Wörtern in einem Text effizient zu erfassen. Dieser Mechanismus erlaubt es dem Modell, alle Eingabewörter eines Prompts[1] gleichzeitig zu betrachten und somit den Kontext jedes Wortes effizient zu verarbeiten.

1 Der Begriff »Prompt« stammt aus dem Englischen und meint ursprünglich vor allem eine klassische »Eingabeaufforderung«, beispielsweise die DOS-Eingabeaufforderung. Im Kontext von (generativen) KI-Systemen – wie beispielsweise ChatGPT oder Midjourney – wird damit die (beschreibende) Eingabe des Benutzers bezeichnet, zu dem das System dann einen passenden Output erzeugt.

Um dies zu erreichen, berechnet der Self-Attention-Mechanismus Ähnlichkeiten zwischen den Eingabewörtern und ermittelt, wie wichtig ein Wort für ein anderes ist. Diese Gewichtungen werden dann zur Modifikation des Prompts verwendet, um eine bessere Repräsentation des Kontextes zu erhalten. Um Texteingaben zu verarbeiten, zerlegt ChatGPT den Text in kleinere Einheiten, sogenannte Tokens. Diese Tokens repräsentieren Wörter oder Teilwörter. Die Tokenisierung erfolgt durch Byte-Pair Encoding (BPE), das einen Kompromiss zwischen der Abdeckung seltener Wörter und der Länge der Vokabelliste bietet.

ChatGPT wird in zwei Phasen trainiert: Pre-Training und Fine Tuning. Während der Pre-Training-Phase wird das Modell auf große Textdatenmengen trainiert, um die Struktur, Grammatik und den Zusammenhang von Wörtern und Sätzen zu erfassen. In dieser Phase wird das Modell als Sprachmodell trainiert, bei dem es versucht, das nächste Wort in einer Sequenz vorherzusagen.

Im Fine Tuning wird das Modell auf spezifischere Aufgaben angepasst, indem es auf kleinere, zielgerichtete Datensätze trainiert wird. Diese Datensätze enthalten häufig menschliche Dialoge oder Frage-Antwort-Paare, die dem Modell beibringen, wie es auf bestimmte Benutzeranfragen oder Aufgaben reagieren soll.

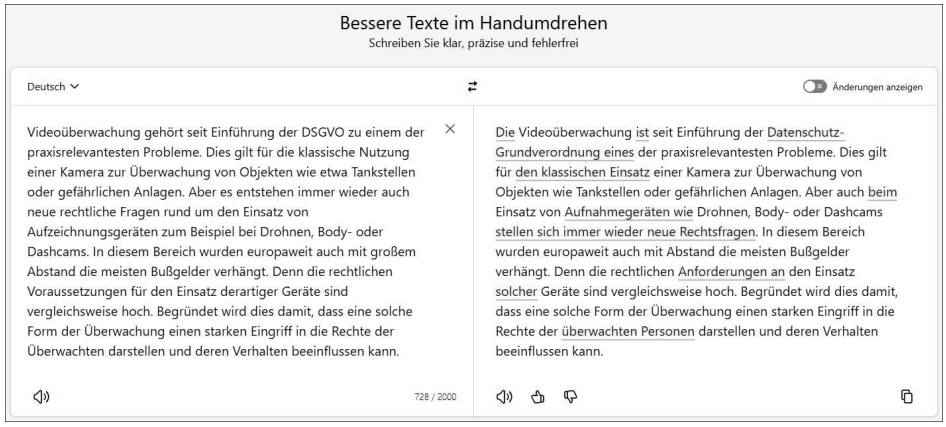


Abbildung 12.1 Wandelt Werke von Juristen in lesbare Texte um: die KI von DeepL Write (Quelle: www.deepl.com/de/write)

Bei der Generierung von Antworten verwendet ChatGPT den trainierten Kontext und das gelernte Wissen, um Wort für Wort Antworten zu erzeugen. Dieser Prozess basiert auf der Wahrscheinlichkeitsverteilung über alle möglichen Wörter, die das Modell erlernt hat. Die Antwortgenerierung kann auf verschiedene Weise gesteuert werden, z. B. durch die Verwendung von sogenannten Temperaturen: Die Temperatur ist ein Hyperparameter, der zur Verarbeitung natürlicher Sprache verwendet wird, um den Grad der Zufälligkeit oder Kreativität im generierten Text zu steuern.

Höhere Temperaturen führen zu einer vielfältigeren und unvorhersehbareren Ausgabe. Umgekehrt führen niedrigere Temperaturen zu einer konservativeren und vorhersehbareren Ausgabe.

Die Daten, die für das Training von ChatGPT verwendet werden, stammen aus einer Vielzahl von Quellen, darunter Bücher, Artikel, Websites und menschliche Dialoge. Die genauen Datenquellen sind nicht öffentlich und werden von den Entwicklern sorgfältig ausgewählt und aufbereitet, um sicherzustellen, dass das Modell ein breites Spektrum an Themen und Stilen abdeckt (vgl. dazu auch Abbildung 12.1). Da die Trainingsdaten aus dem Internet stammen, können sie jedoch auch Verzerrungen und Voreingenommenheit (Bias) enthalten, die sich auf das Verhalten des Modells auswirken können.

ChatGPT besteht aus mehreren Schichten von Transformerblöcken, die jeweils mehrere Attention Heads enthalten. Jeder Attention Head fokussiert auf unterschiedliche Aspekte des Kontexts innerhalb des Eingabetextes. Diese mehrschichtige Architektur ermöglicht es dem Modell, eine tiefere und komplexere Repräsentation der Eingabedaten zu erlernen.

12.2 KI-Generatoren und das Urheberrecht

Das deutsche Urheberrechtsgesetz (UrhG) stammt aus den Anfängen des 20. Jahrhunderts und wurde in den letzten Jahren an die Digitalisierung angepasst. Das Gesetz schützt persönliche geistige Schöpfungen, wie Grafiken, Gemälde, Filme, Texte und Fotografien. Es deckt jedoch keine Ergebnisse ab, die von einer Maschine bzw. einem Algorithmus erzeugt werden.

Das Urheberrecht wird durch die neuen Entwicklungen bis an seine Grenzen strapaziert, und einige Juristen rufen insoweit schon das Ende des Copyrights aus.[2] Doch wie genau sind KI-generierte Werke zu bewerten?

12.2.1 Welche Rechte bestehen an KI-Ergebnissen?

Das Urheberrechtsgesetz schützt Grafiken ebenso wie Gemälde, Filme, Code, Texte und Fotografien. § 2 UrhG bestimmt: Nur persönliche geistige Schöpfungen können Werke im Sinne des Urheberrechts sein und dessen Schutz genießen. Doch schon hier beginnt die Problematik, das über hundertjährige UrhG auszulegen und zu interpretieren. Denn das Gesetz schützt nur das Ergebnis einer menschlichen Schöpfung, nicht aber das Ergebnis eines Algorithmus, der von einer Maschine ausgeführt wird.

2 Lesen Sie dazu beispielsweise Hoeren, »Geistiges Eigentum ist tot – lang lebe ChatGPT«, MMR 2023, 81.

Die Nutzung einer Software zur Bildbearbeitung wird beispielsweise als menschliche Schöpfung betrachtet, da sie von Menschen geplant und ausgeführt wird, wobei der Computer lediglich unterstützt. In diesem Fall ist das Ergebnis urheberrechtlich geschützt. Ähnliches gilt für das Schreiben eines Textes. Auch hier handelt es sich um eine kreative Tätigkeit des Menschen, die zu einer persönlichen geistigen Schöpfung führt. Das Ergebnis ist dann urheberrechtlich geschützt, und nur der Schöpfer kann darüber verfügen. Allerdings ist nur die konkrete Umsetzung einer Idee geschützt, nicht die Idee selbst. Ebenso sind Stilmittel von Künstlern oder Autoren nicht geschützt.

Der Erstellungsprozess durch KI ist aber anders: Bei der Verwendung einer textuellen oder grafischen KI generiert der Computer das Ergebnis vollständig ohne menschliches Zutun. Der Nutzer gibt durch seinen Prompt allenfalls eine grobe Richtung vor, das Endergebnis bleibt zufällig und ist meist nicht einszu einsreproduzierbar. Solche automatisch generierten Ergebnisse sind nicht durch das Urheberrecht geschützt, da dieses nicht die Idee selbst, sondern nur deren konkrete Umsetzung schützt. Es fehlt an der Schöpfung durch den menschlichen Geist.

Auch andere Personengruppen kämen für ein Urheberrecht infrage: Könnten vielleicht KI-Entwickler Urheberrechte an den Schöpfungen ihrer Maschine anmelden? Zwar ist der Code einer Software durch das Urheberrecht geschützt. Das gilt aber nicht für die Produkte, die aus der Software entstehen. Zum gleichen Ergebnis kommt eine rechtliche Prüfung auch im Hinblick auf andere an der Entstehung Beteiligte, wie beispielsweise den Eigentümern der Geräte.

Im Endeffekt, da sind sich die meisten Juristen einig, fallen KI-generierte Texte und Grafiken im Normalfall nicht unter das Urheberrecht. Sie sind vielmehr ungeschützt und für jedermann frei nutzbar. Dies hat zu Kontroversen geführt, bei denen einige Unternehmen aus der Stock-Foto-Branche gegen die neue Technologie vorgehen und Anbieter verklagen. Andere Unternehmen suchen hingegen Kooperationen, wie z. B. Shutterstock, das einen KI-Generator im Angebot hat.

Fallbeispiel: Die Entscheidung des US-Copyright-Amtes

Eine erste Entscheidung zur urheberrechtlichen Einordnung von KI-generierten Bildern lieferte im Februar 2023 das U.S. Copyright Office (USCO)[3]. Das Amt musste über den Urheberrechtsschutz für die Bildergeschichte »Zarya of the Dawn« der KI-Künstlerin Kris Kashtanova entscheiden, bei dem die Bilder mithilfe von Midjourney erstellt worden waren.

3 Mehr Infos zu diesem Urteil lesen Sie beispielsweise unter www.heise.de/news/Entscheidung-KI-generierter-Comic-kann-Copyright-erhalten-Einzelbilder-nicht-7526295.html (zuletzt aufgerufen am 15. Juni 2023).

Im Ergebnis wurde dem Comic zwar grundsätzlich Urheberrechtsschutz gewährt. Dieser bezog sich aber nur auf die Texte und die Zusammenstellung der einzelnen Elemente. Für die mit KI erstellten Bilder wurde der Schutz jedoch abgelehnt, da diese nicht auf menschlicher Kreativität basierten. Entscheidend sei dabei, dass die Ergebnisse von Midjourney unvorhersehbar seien und ein menschlicher Nutzer das Tool nicht ausreichend kontrollieren und steuern könne, um ein bestimmtes Bild zu erzeugen.

Insoweit sei ein Vergleich zu einer Beauftragung eines Künstlers angemessen. Denn der Auftraggeber werde auch nicht Urheber des Auftragswerkes, auch wenn er noch so genaue Vorgaben macht, wie das Bild auszusehen habe.

Aber was ist das Resultat dieser Überlegungen? Nicht weniger als eine gehörige Portion Anarchie in der Welt von Kreativen und Rechteinhabern. Das Urheberrecht hatte sich in den letzten zwei Jahrzehnten – auch mithilfe mächtiger Lobbyorganisationen – immer mehr zu einer Art Superrecht entwickelt, in dem die Befugnisse der Rechteinhaber immer weiter zulasten der Allgemeinheit ausgedehnt wurden. Das Ergebnis ist, dass Fotografen teure Abmahnungen versenden können, wenn jemand nur ein Bildmotiv auf einer Fototapete auf Facebook[4] wiedergibt.

Auf die Welt von Autoren, Grafikern, Illustratoren und Stockfoto-Anbietern kommt eine gehörige Portion Disruption[5] zu. Denn wenn KI-generierte Bilder und Texte nicht urheberrechtlich geschützt sind, können sie von jedermann lizenzfrei genutzt werden – umsonst und ohne zu fragen!

12.2.2 Gemischte Platte: Wie viel KI darf in einem Werk stecken?

In der Praxis stellen sich noch weitergehende Fragen, die von enormer praktischer Relevanz sind: Wie viel KI darf in einem Werk stecken, damit es noch in den Schutzbereich des Urheberrechts fällt? Dies gilt zunächst für selbst erstellte Inhalte, z. B. Texte, die mit KI-Tools wie DeepLWrite[6] bearbeitet werden. Die Software überarbeitet Texte, korrigiert Fehler und schärft Formulierungen. Ein Service, den gerade Juristen mit dem ihnen eigenen Schreibstil schätzen dürften – und den auch der Autor dieses Textes in Anspruch genommen hat.

4 Siehe dazu beispielsweise: »Foto von Fototapete verletzt Urheberrecht des Fototapeten-Fotografen«, online verfügbar unter https://heise.de/-7524441 (zuletzt aufgerufen am 15. Juni 2023) und das zugrundeliegende Urteil des LG Köln (Az 14 O 350/21), online verfügbar unter www.justiz.nrw.de/nrwe/lgs/koeln/lg_koeln/j2022/14_O_350_21_Urteil_20220818.html (zuletzt aufgerufen am 15. Juni 2023).

5 Mit »Disruption« ist hier der Prozessgemeint, bei dem neue Produkte und Dienstleistungen bzw. allgemein Geschäftsmodelle bereits bestehende Alternativen – schlussendlich häufig vollständig – verdrängen.

6 Mehr Informationen zu DeepLWrite gibt es beispielsweise unter www.deepl.com/de/write (zuletzt aufgerufen am 15. Juni 2023).

Solange es dabei nur um den Feinschliff geht, dürfte das kein Problem sein. Besteht der Text am Ende aber überwiegend aus Formulierungen, die aus dem Computer stammen, dürfte das eigene Urheberrecht mit den Überarbeitungen verloren gegangen sein. Umgekehrt stellt sich die Frage, wie umfangreich beispielsweise ein Text umgeschrieben oder ein Bild bearbeitet werden muss, damit an dieser Umgestaltung ein eigenes Recht entsteht. Hier hat das Urheberrecht schon immer hohe Anforderungen gestellt, sodass der Prozentsatz von Eigenerstelltem zu KI-Generiertem recht hoch sein muss.

Hinweis: Das Leistungsschutzrecht

Immerhin tun sich hier einige in der Praxis etwas leichter, weil ihnen ein Leistungsschutzrecht zu Hilfe kommt. Darunter versteht man Rechte, die bestimmten Rechteinhabern in der Medien- und Kreativbranche gewährt werden. Sie schützen nicht das ursprüngliche Werk selbst (wie z. B. das Urheberrecht), sondern die wirtschaftlichen und kreativen Interessen derjenigen, die an der Verbreitung, Vermarktung oder anderweitigen Nutzung des Werkes beteiligt sind. Dieses Leistungsschutzrecht schützt u. a. KI-Grafiken, wenn sie beispielsweise in Computerspielen oder Filmen verwendet werden.

Die Auswirkungen dieser Einstufung als schutzwürdig oder eben nicht schutzwürdig sind von großer praktischer Relevanz. Nicht nur sind KI-Inhalte hinsichtlich ihrer Nutzung plötzlich frei nutzbar, was bislang nahezu unvorstellbar war. Auch Verwertungsgesellschaften wie die VG Wort und die VG Bild-Kunst, die für das Einkommen der Kreativen eine nicht unerhebliche Rolle spielen, stehen vor großen Problemen. Letztere vergüten natürlich nur menschliche Produkte, wobei die Unterscheidung in der Praxis schwierig bis unmöglich sein wird.

Tatsächlich könnte es sogar als Betrug angesehen werden, wenn dort Werke aus dem Computer zur Vergütung angemeldet werden. Und mit dem kaum durchführbaren Nachweis von KI-generierten Texten dürfte das gesamte Verteilungs- und Vergütungsmodell der VG Wort mit dieser Disruption durch amorphe Urheberschaft mittelfristig infrage stehen. Letztlich werden sich auch die Reichweiten von Websites, das Lese- und Suchverhalten von Internetnutzern und das Internet als Ganzes verändern.

Die bahnbrechenden neuen Möglichkeiten der KI-Generatoren stellen nicht nur Berufsgruppen wie Illustratoren, Fotografen, Journalisten oder auch Anwälte vor schwierige neue Herausforderungen. Auch das Recht erfährt eine gehörige Portion Disruption. Das gilt vor allem für das bisher so omnipräsente Urheberrecht. Auch Haftungsfragen, Datenschutz oder der Umgang mit Fälschungen und Deepfakes treffen das Rechtssystem, seine Vertreter, aber auch die Künstler und Interessengruppen hart und müssen zeitnah beantwortet werden. Eine große Herausforderung für alle Akteure!

12.2.3 Besonderheiten bei der Nutzung von KI für Code

ChatGPT und spezifischen Code generierende KI-Instanzen wie Alpha Code und GitHub Copilot werden inzwischen von vielen Softwareentwicklern zum Erstellen oder Überprüfen von Code verwendet (siehe Abbildung 12.2).

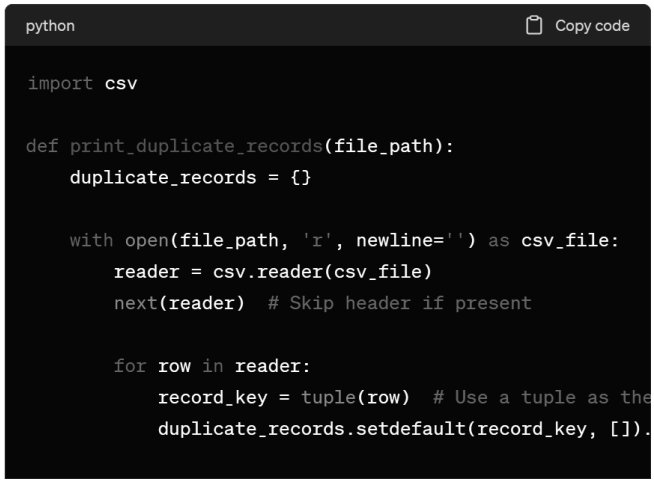


Abbildung 12.2 Coden mit ChatGPT, hier mit folgendem Prompt: »Act as a Python developer. Write code to read and print duplicate records from the provided CSV file«

Viele Rechtsfragen rund um die Nutzung von KI-Generatoren im Bereich der Programmierung sind noch gänzlich ungeklärt. So war es am Anfang der Nutzung dieser Angebote immer wieder aufgefallen, dass bereits bekannte und dokumentierte Code-Zeilen verwendet werden, die möglicherweise urheberrechtlich geschützt sind. Andererseits sind aber bei vielen Aufgaben die Anzahl möglicher Lösungswege beispielsweise im Vergleich zu generiertem Text endlich, sodass es für die KI möglicherweise keinen anderen Weg gab, als die bekannten Zeilen zu nutzen.

Noch gänzlich unbearbeitet ist die Frage, wie sich die Lizenzen der zahlreichen, im Rahmen des Trainings ausgelesenen Programme auswirken. Hier ist es nicht auszuschließen, dass die Nutzung verschiedener Software möglicherweise zur Folge hat, dass ChatGPT & Co. deren Lizenzen zu berücksichtigen haben – oder die Lizenz sogar infizierend hinsichtlich der weiteren Nutzung wirkt.

Wer generative KI in größerem Umfang zur Programmierung nutzt, sollte diese sich gerade erst anbahnende Diskussion aufmerksam verfolgen.

12.2.4 KI von der eigenen Website aussperren?

Kreative und Rechteinhaber sorgen sich um die Nutzung ihrer Werke durch KI-Generatoren. Gibt es eine Möglichkeit, die eigenen Bilder dort löschen zu lassen? Und wie verhindert man einen zukünftigen Zugriff auf das eigene Angebot?

Fremde Werke dürfen im Grundsatz nicht ohne die Zustimmung des Rechteinhabers durch Dritte genutzt werden. Es läge auch im Bereich KI nahe, dass diese Regelung auch für das Auslesen von Bildern oder Texten von der eigenen Website gilt. Allerdings sieht das Recht hier eine folgenschwere Ausnahme vor. Denn tatsächlich erlaubt das Urheberrechtsgesetz das Auslesen von fremden Inhalten zur Nutzung durch KI. Und zwar sowohl für den wissenschaftlichen als auch für den gewerblichen Bereich. Und damit nicht genug: Der Gesetzgeber hat hierfür nicht einmal eine Vergütungspflicht vorgesehen.

Dies ergibt sich aus den §§ 44b und 60d UrhG. Ersterer sieht vor, dass Vervielfältigungen von rechtmäßig zugänglichen Werken für das Text und Data Mining zulässig sind. Darunter versteht der Gesetzgeber die automatisierte Analyse von einzelnen oder mehreren digitalen oder digitalisierten Werken, um daraus Informationen insbesondere über Muster, Trends und Korrelationen zu gewinnen.

Rechtmäßig zugänglich sind Bilder, Grafiken, Code oder Text z. B. dann, wenn sie frei verfügbar im Netz zu finden sind. Die Vervielfältigungen sind zwar zu löschen, wenn sie für das Mining nicht mehr erforderlich sind. Das hilft den Urhebern aber wenig, denn in der Praxis ist in aller Regel nur ein Zugriff auf das Werk notwendig, aber keine dauerhafte Speicherung. Dauerhaft bereitgehalten werden nur die Ergebnisse der KI-Auswertung, die aber ihrerseits im Normalfall nicht geschützt sind.

Was bedeutet das praktisch? Nach § 44b UrhG dürfen fremde Werke, die sich frei zugänglich online befinden, von jedermann ohne Entschädigung oder Lizenz zu Zwecken des Trainings von KI genutzt werden. Diese Vorschrift ist keine Idee des deutschen Gesetzgebers, sondern sie entstammt der Digital Single Market Copyright Directive, der DSM-Richtlinie der EU.

Die damit verbundene Änderung des Urheberrechts war zwar überwiegend sehr vorteilhaft für industrielle Rechteinhaber. So brachte es der Film- und Musikindustrie die erhofften Uploadfilter und den Verlagen ihr Leistungsschutzrecht. Die Auswirkung der Regelungen zu KI wurde aber offenbar nicht so recht vorhergesehen. Ziel der Regelung ist es nach der Gesetzesbegründung, Innovationen in der Privatwirtschaft anzuregen.

Noch weiter gehen die Freiheiten, die der Gesetzgeber der Nutzung von urheberrechtlich geschützten Inhalten zu wissenschaftlichen Zwecken im KI-Bereich gewährt. Voraussetzung ist hier allerdings eine streng nicht kommerzielle Nutzung. Dieser Gruppe ist nach § 60d UrhG eine Vervielfältigung für Text und Data Mining für Zwecke der wissenschaftlichen Forschung gestattet. Die dabei gewonnenen Inhalte dürfen so lange

aufbewahrt werden, wie dies für Zwecke der wissenschaftlichen Forschung oder zur Überprüfung wissenschaftlicher Erkenntnisse erforderlich ist.

Dabei müssen die fremden Inhalte mit angemessenen Sicherheitsvorkehrungen gegen unbefugte Benutzung geschützt werden. Mehr Voraussetzungen gibt es allerdings nicht, und den Rechteinhabern wird weder eine Vergütung noch ein Widerruf vorbehalten.

Immerhin hat das Gesetz die Kreativen nicht völlig rechtslos gelassen. In § 44b UrhG hat der Gesetzgeber einen Interessenausgleich vorgesehen, der sich in Absatz 3 dieser Vorschrift befindet. Die Formulierung ist etwas umständlich: Nutzungen sind danach nur zulässig, wenn der Rechteinhaber sich diese nicht vorbehalten hat. Diesen Nutzungsvorbehalt müsse der Rechteinhaber oder auch der Betreiber der Website ausdrücklich erklären – und zwar in maschinenlesbarer Form.

Denn Sinn und Zweck der Regelung ist es ausweislich der Gesetzesbegründung, einerseits Rechteinhabern die Möglichkeit zu eröffnen, die Nutzung auf Basis der gesetzlichen Erlaubnis zu untersagen. Gleichzeitig bezweckt die Regelung, bei online zugänglichen Inhalten sicherzustellen, dass durch die Maschinenlesbarkeit automatisierte Abläufe, die typisches Kriterium des Text- und Data Mining sind, tatsächlich auch automatisiert durchgeführt werden können.

Diese Formulierung ist etwas irritierend, denn natürlich ist jeder Bestandteil einer Website in irgendeiner Form maschinenlesbar. Allerdings hat sich bei einer ganzen Reihe von Anbietern ein Standard gebildet, den auch die Gesetzesbegründung ausdrücklich nennt: Danach kann der Hinweis auch im Impressum oder in den Allgemeinen Geschäftsbedingungen stehen. Tatsächlich finden sich bei zahlreichen Verlagen inzwischen entsprechende Hinweise im Impressum. Ein solcher Nutzungsvorbehalt für eine Website darf nicht dazu führen, dass dieses Angebot ohne sachliche Rechtfertigung ungleich behandelt wird, beispielsweise bei der Anzeige als Suchmaschinentreffer.

Praxistipp: Musterformulierung für ein Opt-out hinsichtlich der Erfassung der eigenen Seite durch KI

Wer die Erfassung seiner eigenen Werke durch eine KI verhindern möchte, kann beispielswiese die nachfolgende Erklärung in das eigene Impressum aufnehmen:

Der Betreiber dieses Angebots behält sich eine Nutzung der Inhalte dieser Website für kommerzielles Text- und Data Mining (TDM) im Sinne von § 44b UrhG ausdrücklich vor. Für den Erwerb einer Nutzungserlaubnis wenden Sie sich an XY@example.com.

Wichtig zu wissen ist, dass ein solcher Vermerk nur für künftige Zugriffe, aber nicht rückwirkend gilt. Es gibt keinen Anspruch darauf, dass bereits eingelesene Werke rückwirkend entfernt werden müssen oder können. Da das Auslesen rechtmäßig

war, gibt es also derzeit keine Möglichkeit, seine Inhalte aus den Daten der KI entfernen zu lassen.

12.3 KI-Generatoren und der Datenschutz

Neben dem Bereich des Urheberrechts steht vor allem der Datenschutz rund um die Nutzung der neuen KI-Angebote im Mittelpunkt der Diskussion. Hier ist inzwischen ChatGPT im Visier der Datenschutzbehörden. Doch was ist bei der Nutzung der Dienste hinsichtlich der DSGVO zu beachten? Hier ist rechtlich noch vieles ungeklärt, aber einige Probleme sollten in jedem Fall berücksichtigt werden. Dabei stellt sich als Erstes die Frage, was am Beispiel von ChatGPT im beruflichen Kontext zu beachten ist.

12.3.1 Datenschutz bei der geschäftlichen Nutzung der KI

Grundsätzlich ist bei der Nutzung von ChatGPT der Datenschutz dann zu beachten, wenn dabei personenbezogenen Daten verwendet werden. Das kann schnell der Fall sein, z. B. bei der Anmeldung unter der Verwendung von Username und Password. Zudem wird bei der Nutzung des Angebots auch die IP-Adresse des Nutzers übermittelt.

Und spätestens dann, wenn Namen oder sonstige persönliche Informationen im Rahmen eines Prompts eingegeben werden, ist in jedem Fall die DSGVO anwendbar. Insgesamt ist also davon auszugehen, dass die Nutzung unter die strengen Regeln des Datenschutzes fällt.

Dies bedeutet, dass weitere Anforderungen bestehen: Es muss eine valide Vereinbarung mit OpenAI als Betreiber von ChatGPT bestehen, es braucht eine Rechtsgrundlage und möglicherweise sogar eine Datenschutz-Folgenabschätzung.

12.3.2 Vertragliche Beziehung und Datenexport

Für eine nicht nur gelegentliche Nutzung des Angebots schließt man einen Vertrag mit OpenAI. Dieser enthält in der Version von Anfang 2023 zumindest für die Nutzung via API auch eine Auftragsverarbeitungsvereinbarung (AVV).

Ob die Einordnung der eigenen Dienste mit OpenAI als weisungsgebundener Auftragsverarbeiter rechtlich zutreffend ist, ist noch nicht geprüft. Dagegen spricht allerdings, dass ChatGPT die eingegebenen Inhalte nach eigenen Angaben auch zum weiteren Training der KI nutzt – und damit zu eigenen Zwecken. Diese Konstellation würde eher für eine gemeinsame Verantwortlichkeit sprechen. Trotzdem ist es in jedem Fall empfehlenswert, einen Auftragsverarbeitungsvertrag abzuschließen, soweit dies möglich ist. Faktisch bietet dieser eine größere Rechtssicherheit als nur eine abgeschlossene Nutzungsvereinbarung.

Bei der Nutzung von ChatGPT stellt sich zudem das Problem einer Datenübermittlung in die USA. Hier sollte idealerweise eine entsprechende Vereinbarung über Standarddatenschutzklauseln geschlossen werden (siehe dazu auch die Ausführungen in Kapitel 8).

12.3.3 Rechtsgrundlagen für die geschäftliche Nutzung

Nutzt man ChatGPT auch für die Verarbeitung von personenbezogenen Daten, ist dafür nach den allgemeinen Vorgaben der DSGVO eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO erforderlich. Denkbar ist hier z. B. die Vertragserfüllung oder ein dafür eingeholtes Einverständnis.

Der Regelfall wird aber das berechtigte Interesse sein. Im Rahmen der erforderlichen Interessenabwägung zwischen dem Verantwortlichen und dem Betroffenen dürfte es in der Praxis schwierig zu bewerten sein, wie die eingegebenen Daten durch OpenAI verarbeitet und genutzt werden. Das Unternehmen ist hier wenig transparent und wirkt weitgehend wie die sprichwörtliche Blackbox.

Spätestens dann, wenn besondere Kategorien von personenbezogenen Daten nach Art. 9 DSGVO oder ansonsten besonders sensible Daten wie beispielsweise Kontonummern oder Informationen über Kinder verarbeitet werden, dürfte die Interessenabwägung eindeutig zugunsten des Betroffenen ausfallen, sodass diese Rechtsgrundlage nicht infrage kommt.

Bei der Verarbeitung dieser Daten oder auch einer großen Anzahl von Datensätzen mit vielen Betroffenen kann die Erstellung einer Datenschutz-Folgenabschätzung erforderlich sein. Angesichts der fehlenden Einsicht in die Details der Datenverarbeitung und auch die Quelle der Daten bei OpenAI wird dieses Gutachten sicherlich nicht einfach zu erstellen sein.

Schließlich muss die Nutzung der KI auch Eingang in das Verzeichnis der Verarbeitungstätigkeiten und die Datenschutzerklärung finden.

12.3.4 Datenschutzanforderungen an die Betreiber der KI

Aus den Reihen der institutionellen Datenschützer gibt es einige Kritik an ChatGPT und dessen Anbieter OpenAI. So hat Ende März 2023 die italienische Datenschutzbehörde die Verarbeitung von Daten italienischer Nutzer durch OpenAI vorübergehend eingeschränkt.[7] Grund dafür sind angebliche Verstöße gegen Datenschutzgesetze, darunter die unrechtmäßige Sammlung von persönlichen Daten.

7 Siehe dazu beispielsweise die Pressemeldung der italienischen Behörde vom 31. März 2023, online verfügbar unter www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847#english_version (zuletzt aufgerufen am 15. Juni 2023).

Die italienische Behörde stellte fest, dass OpenAI den Nutzern keine Informationen zur Verfügung stellt und möglicherweise keine gesetzliche Grundlage für die massive Sammlung und Verarbeitung persönlicher Daten besteht, um die ChatGPT-Algorithmen zu trainieren. Sie betonte auch, dass die bereitgestellten Informationen nicht immer korrekt sind und somit ungenaue persönliche Daten verarbeitet werden. Zudem kritisierte die Behörde das Fehlen einer Altersüberprüfung, die Kinder vor ungeeigneten Inhalten schützen soll.

Obwohl das KI-Unternehmen nicht in der EU ansässig ist, hat das Unternehmen einen Vertreter im Europäischen Wirtschaftsraum (EWR) ernannt. OpenAI wurde zunächst aufgefordert, innerhalb von 20 Tagen mitzuteilen, welche Maßnahmen zur Einhaltung der Anordnung ergriffen wurden. Andernfalls droht eine Geldstrafe von bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes. Allerdings hat die Behörde zwischenzeitlich mitgeteilt, dass sie mit dem US-Unternehmen in einen Dialog eingetreten sei und die rechtliche Situation weiter untersuchen wolle.

Auch weitere Behörden haben im Frühjahr 2023 Verfahren gegen OpenAI angestoßen, darunter diejenigen in Kanada, Frankreich und Irland. Die deutschen Behörden haben angekündigt, im Rahmen eines Arbeitskreises die datenschutzrechtlichen Probleme und Auswirkungen von ChatGPT untersuchen zu wollen. Welche Auswirkungen diese Verfahren haben werden, ist derzeit noch völlig unklar.

12.3.5 Besonderheiten bei Bild-KI

Bei Bild-KI wie Midjourney, Stabel Diffusion oder DALL-E gibt es eine datenschutzrechtliche Besonderheit: Dort besteht die Möglichkeit, Bilder auf den Server des Anbieters hochzuladen, die dann erfasst und bearbeitet werden. Dies ist datenschutzrechtlich – aber auch urheberrechtlich – äußerst fragwürdig, da nicht im Detail bekannt ist, wie die Anbieter mit den hochgeladenen Bildern umgehen.

Daher sollten Unternehmen ein solches Hochladen grundsätzlich unterbinden. Dies darf allenfalls nur im Einzelfall und dann mit Vorliegen einer eindeutigen Einwilligung der Abgebildeten geschehen. Zudem muss eine entsprechende Lizenz des Fotografen vorliegen, die eine solche Nutzung erlaubt.

12.4 Geschäftsgeheimnisschutz und KI

Bei der Nutzung von KI-Angeboten ist auch zwingend der Geheimnisschutz zu beachten. Verpflichtungen, bestimmte Informationen geheim zu halten, ergeben sich u. a. aus dem Geschäftsgeheimnisgesetz, aber auch aus dem Berufsrecht (z. B. bei Anwälten, Ärzten oder Steuerberatern) oder vertraglichen Vereinbarungen wie Non Disclosure Agreements (NDA). Dies gilt für eigene wie für fremde Geschäftsgeheim-

nisse. Derartige Informationen dürfen unter keinen Umständen ihren Weg in die Eingabemaskenvon KI-Angeboten finden.

Fallbeispiel: Ein Mitarbeiter macht einen Fehler

Im Frühjahr 2023 wurde der Fall eines großen IT-Konzernsbekannt, dessen Mitarbeiter versehentlich streng geheime Daten während der Nutzung von ChatGPTpreisgegeben hatten.[8] Infolgedessen sind vertrauliche Informationen wie Quellcode für neue Programme und interne Besprechungsnotizennun offen verfügbar.

Hintergrund: Das Unternehmen erlaubte den Ingenieuren seiner Halbleiterabteilung, ChatGPTzur Lösung von Problemen in ihrem Quellcode zu verwenden. Dabei gaben die Mitarbeiter jedoch vertrauliche Daten ein. Innerhalb eines Monats kam es zu drei dokumentierten Vorfällen, bei denen Mitarbeiter über die Software sensible Informationen weitergaben. Da die KI Benutzereingaben speichert, um sich selbst weiter zu trainieren, sind diese Geschäftsgeheimnisse nun effektiv im Besitz von OpenAI.

Konkret bat ein Mitarbeiter in einem der bekannten Fälleder KI, Testabläufe zur Fehlererkennung in Chipszu optimieren – ein vertraulicher Vorgang, der jedoch erhebliche Zeit- und Kosteneinsparungen für Halbleiterunternehmen bedeuten kann. In einem anderen Fall verwendete ein Mitarbeiter ChatGPT,um Besprechungsnotizen in eine Präsentation umzuwandeln, deren Inhalte nicht für Dritte bestimmt waren.

Als Ergebnis warnte der Konzern seine Mitarbeiter vor den möglichen Gefahren der Preisgabevertraulicher Informationen, da solche Daten auf den Servern von OpenAI gespeichertsind und nicht mehr zurückgeholt werden können.

12.5 Richtlinien für die Nutzung von KI-Generatoren

Wer KI-Generatoren häufiger im betrieblichen Umfeld einsetzt, sollte die Vorgaben für die eigenen Mitarbeiter im Rahmen einer KI-Richtlinie festhalten. Bei der Erstellung dieses Papiersist es wichtig, alle relevanten Bereiche des Unternehmens einzubeziehen. Zugleich sollte die Richtlinie von den Mitarbeitern nicht als Verbot wahrgenommen werden. Vielmehr sollte – soweit möglich – die Nutzung von ChatGPT& Co.ausdrücklich gefördert und unterstützt werden, z. B.durch das Bereitstellen von kostenpflichtigen Zugängen zum Experimentieren. Zugleich sollten die Mitarbeiter aber auch auf drohende Risiken hingewiesen werden – bis hin zu Verboten bestimmter Arten der Nutzung.

8 Weitere Infos dazu sind beispielsweisezu finden unter www.golem.de/news/kuenstliche-intelligenz-samsung-ingenieure-leaken-interne-daten-an-chatgpt-2304-173220.html (zuletzt aufgerufen am 15.Juni 2023).

Was genau in eine solche Richtlinie gehört, ist stark von den Anforderungen des jeweiligen Unternehmens abhängig. Regelungen bieten sich z. B. in den folgenden Bereichen an:

- Beschränkung der Nutzung auf bestimmte Anbieter, deren Lizenz geprüft und für die jeweilige Nutzung freigegeben ist: Vermieden werden sollte ein Wildwuchs, bei dem von diversen Mitarbeitern unterschiedlichste Software genutzt wird.
- Klare Grenzen: In definierten Unternehmensbereichen darf keine KI eingesetzt werden.
- Kennzeichnungspflichten für KI-generierte Inhalte
- Umgang mit Externen: Dürfen Ergebnisse der KI an Dritte weitergegeben werden, oder ist es Dienstleistern umgekehrt erlaubt, KI-Inhalte an das eigene Unternehmen weiterzugeben?
- Regeln für die Verwendung von KI-Bildgeneratoren: Nutzungsmöglichkeiten und Grenzen. Beispielsweise keine Verwendung von eigenen Fotos, keine KI-Bilder von lebendigen Personen, keine herabwürdigenden Bilder.
- Verwendung von KI im Bereich der Programmierung
- Umgang mit dem Geschäftsgeheimnisschutz
- Datenschutzrechtliche Vorgaben, insbesondere im Hinblick auf sensible Daten
- Ansprechpartner für Fragen und Unklarheiten
- Überwachung der Vorgaben und Sanktionen bei Verstößen

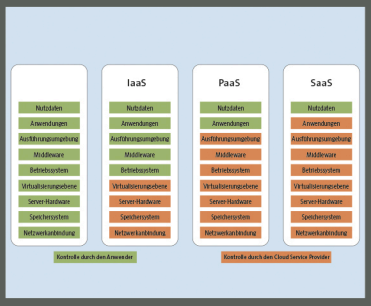
Bei der Gestaltung einer solchen Vereinbarung bietet es sich an, ChatGPT einen ersten Entwurf schreiben zu lassen, das hier bereits brauchbare Ergebnisse liefert.

Datenschutz und IT-Compliance

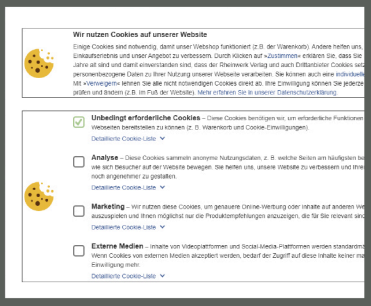
IT-Recht für Admins

Grundlagenwissen, Entscheidungshilfen und Praxis

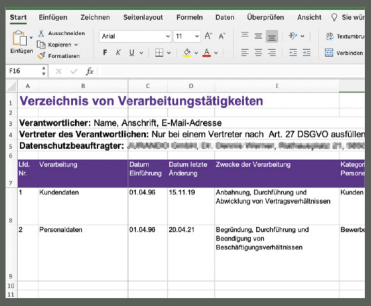
Was ist beim technischen Datenschutz zu beachten? Und was müssen Sie über DSGVO, TTDSG und Co. als Admin oder IT-Leiter wissen? Das interdisziplinäre Autorenteam aus Juristen und einem IT Professional gibt Ihnen mit diesem Leitfaden kompetent Auskunft zu allen Fragestellungen, damit Sie die Firmen-IT rechtssicher betreiben können.



Grundlagen Datenschutz



Anforderungen der DSGVO



Praktische Lösungen

DSGVO-Grundlagen, die Sie kennen sollten

Alles, was Sie über Datenschutz wissen müssen: Grundsätze und Prinzipien, Anforderungen der DSGVO an den IT-Betrieb, die IT-Sicherheit und an die Administration von Websites.

Wie Sie richtig mit Daten umgehen

Lernen Sie, wie Sie Datenschutzverpflichtungen als Unternehmen umsetzen, mit Datenschutzvorfällen umgehen, Daten richtig exportieren und Mitarbeiterdaten korrekt handhaben.

Compliance, Sanktionen, Haftung

Erfahren Sie, wie Sie sich gegen Compliance-Verletzungen schützen können und bei Regelverstößen reagieren. Außerdem: Welche Sanktionen haben Sie bei Datenschutzvergehen als IT-Admin zu befürchten?

Aus dem Inhalt

Joerg Heidrich ist Justiziar und Datenschutzbeauftragter von Heise Medien und zudem als Rechtsanwalt in Hannover tätig. **Christoph Wegener** ist seit 1999 freiberuflicher Berater mit der wecon.it-consulting in den Bereichen Informationssicherheit, Datenschutz und Open Source. **Dennis Werner** ist Fachanwalt für IT-Recht in der Kanzlei Bergfeld & Partner.

Rheinwerk Computing

Gedruckt in Deutschland
Papier aus nachhaltiger Waldwirtschaft
Mineralölfreie Druckfarben

€ 59,90 [D] € 61,60 [A]

Netzwerke & Datenbanken
ISBN 978-3-8362-8674-9