

RECHTSFALLEN BEI KI VERMEIDEN

DIE 5 HÄUFIGSTEN FEHLER UND WIE MAN SIE UMGEHT

DIGITALBEAT.
BESSER MIT KI

INHALTSVERZEICHNIS

01 Vom Spaß mit generativer KI bis zu Persönlichkeitsrechtsverletzungen & Deepfakes 1

02 Urheberrecht und Generative KI: So bleibst du im Marketing rechtssicher 2

03 DSGVO-Konformität & Künstliche Intelligenz 3

04 AI Act - Regulation oder Beschränkung Künstlicher Intelligenz? 4

05 KI, Datenschutz, Richtlinien & Rechtliche Themen: Wer haftet? 5

VOM SPASS MIT GENERATIVER KI BIS ZU PERSÖNLICHKEITSRECHTSVERLETZUNGEN & DEEPFAKES

Deepfakes sind täuschend echt wirkende, manipulierte Medieninhalte, die durch den Einsatz tiefenneuronaler Netze erzeugt werden. Ein bekanntes Beispiel für Deepfakes ist ein Video, in dem das Gesicht einer berühmten Person, wie etwa eines Politikers oder Schauspielers, digital in ein anderes Video eingefügt wird, sodass es aussieht, als würde diese Person etwas sagen oder tun, was sie in Wirklichkeit nie gesagt oder getan hat. Diese Technologie birgt erhebliche rechtliche Risiken, insbesondere wenn sie verwendet wird, um Fake News zu verbreiten oder um Einzelpersonen zu schaden. Die Erstellung von Deepfakes ohne die ausdrückliche Einwilligung der betroffenen Person kann als schwerwiegende Verletzung des Persönlichkeitsrechts angesehen werden und erhebliche strafrechtliche Konsequenzen nach sich ziehen.

Die Identifizierung des Erstellers eines Deepfakes stellt eine erhebliche Herausforderung dar und erschwert die rechtliche Verfolgung von Missbrauchsfällen. Daher ist es für Unternehmen, die Deepfakes im Marketing einsetzen möchten, unerlässlich, die rechtlichen Rahmenbedingungen genau zu kennen und zu verstehen.

Die Bundesregierung warnt eindringlich vor den Risiken, die mit Deepfakes verbunden sind, und hebt hervor, dass ihre täuschend echte Natur durch fortschrittliche künstliche Intelligenz ermöglicht wird. Es ist von größter Bedeutung, die rechtlichen Konsequenzen von Deepfakes im Blick zu behalten, um potenzielle Haftungsrisiken zu minimieren und verantwortungsbewusst mit dieser Technologie umzugehen. Nur durch eine umfassende Auseinandersetzung mit den rechtlichen Aspekten können die Chancen und Risiken von Deepfakes angemessen bewertet werden.

FALSCHES VORGEHEN

Beispiel 1 - Verbreitung von Fake News: Ein Unternehmen erstellt einen Deepfake, der einen prominenten Politiker zeigt, der eine kontroverse Aussage trifft. Dieser Clip wird ohne jegliche Kennzeichnung in den sozialen Medien geteilt, um die öffentliche Meinung zu manipulieren. Dies führt nicht nur zu einem Vertrauensverlust in den Medien, sondern kann auch rechtliche Konsequenzen für das Unternehmen nach sich ziehen.

Beispiel 2 - Verwendung ohne Einwilligung: Eine Marketingagentur nutzt ein Deepfake-Video, das das Gesicht einer bekannten Influencerin zeigt, um ein Produkt zu bewerben, ohne ihre Zustimmung eingeholt zu haben. Dies verletzt nicht nur das Persönlichkeitsrecht der Influencerin, sondern könnte auch zu einer Klage und hohen Schadensersatzforderungen führen.

RICHTIGES VORGEHEN

Beispiel 1 - Ethische Nutzung im Marketing: Ein Unternehmen möchte Deepfake-Technologie nutzen, um ein Werbevideo zu erstellen, das einen Schauspieler in verschiedenen Rollen zeigt. Vor der Produktion wird die Zustimmung des Schauspielers eingeholt, und im Video wird klar gekennzeichnet, dass es sich um eine digitale Manipulation handelt. Dadurch wird Transparenz geschaffen und rechtlichen Problemen vorgebeugt.

Beispiel 2 - Aufklärung und Sensibilisierung: Eine Organisation, die sich mit Medienkompetenz beschäftigt, nutzt Deepfakes in einem Bildungsprojekt, um die Öffentlichkeit über die Risiken und die Funktionsweise dieser Technologie aufzuklären. Die Inhalte werden mit dem Hinweis versehen, dass es sich um Deepfakes handelt, und die Zuschauer werden ermutigt, kritisch mit Medieninhalten umzugehen. Dies fördert ein verantwortungsbewusstes Verständnis von Deepfakes und deren Auswirkungen.

URHEBERRECHT UND GENERATIVE KI: SO BLEIBST DU IM MARKETING RECHTSSICHER

Generative KI bezieht sich auf Technologien, die in der Lage sind, neue Inhalte zu erstellen, sei es in Form von Text, Bildern, Musik oder Videos. Diese Technologien bieten Unternehmen im Marketingbereich spannende Möglichkeiten, bergen jedoch auch erhebliche rechtliche Risiken, insbesondere im Hinblick auf das Urheberrecht. Ein zentrales Anliegen ist die Frage, wie generierte Inhalte rechtlich korrekt eingesetzt werden können, ohne bestehende Urheberrechte zu verletzen.

Die Verwendung von generativer KI zur Erstellung von Marketinginhalten kann problematisch werden, wenn geschützte Werke ohne die erforderlichen Lizenzen oder Genehmigungen genutzt werden. Beispielsweise kann die Erstellung von Bildern oder Texten, die auf bestehenden urheberrechtlich geschützten Materialien basieren, zu Verletzungen des Urheberrechts führen. Unternehmen müssen sich der rechtlichen Rahmenbedingungen bewusst sein, um Haftungsrisiken zu minimieren und rechtliche Konsequenzen zu vermeiden.

Es ist wichtig zu beachten, dass leichte Veränderungen an einem Originalwerk nicht automatisch zu einem neuen Urheberrecht führen. Generierte Inhalte wie Bilder oder Texte sollten sich deutlich vom Original unterscheiden, um nicht als Urheberrechtsverletzung angesehen zu werden. Unternehmen sollten daher sicherstellen, dass die von ihnen erstellten Inhalte originell sind und genügend Eigenständigkeit aufweisen, um rechtliche Probleme zu vermeiden.

Neu mit KI erzeugte Inhalte können die Urheberrechte der Ursprungswerke verletzen, insbesondere wenn Teile fremder Werke ohne Einwilligung des Urhebers übernommen werden. Eine Ausnahme besteht, wenn ein hinreichender Abstand zum Original gewahrt bleibt. Es ist wichtig zu beachten, dass der Stil eines Künstlers nicht geschützt ist, jedoch dürfen Samples nur verwendet werden, wenn eine kreative Auseinandersetzung mit dem Werk erfolgt.

FALSCHES VORGEHEN

Beispiel 1 - Verwendung geschützter Inhalte ohne Erlaubnis: Ein Unternehmen nutzt generative KI, um ein Werbevideo zu erstellen, das Musik enthält, die urheberrechtlich geschützt ist, ohne die erforderlichen Lizenzen zu erwerben. Dies führt zu rechtlichen Konsequenzen, einschließlich möglicher Klagen und Schadensersatzforderungen.

Beispiel 2 - Plagiat von Inhalten: Eine Marketingagentur generiert Blogartikel mithilfe von KI, die stark an bestehenden Artikeln angelehnt sind, ohne die Quellen korrekt zu kennzeichnen. Dies kann als Plagiat angesehen werden und rechtliche Schritte nach sich ziehen.

RICHTIGES VORGEHEN

Beispiel 1 - Lizenzierung und Genehmigung: Ein Unternehmen, das generative KI zur Erstellung von Inhalten nutzt, stellt sicher, dass alle verwendeten Materialien lizenziert sind. Vor der Erstellung eines Werbevideos wird die Erlaubnis für die Nutzung von Musik und Bildern eingeholt, um rechtlichen Problemen vorzubeugen.

Beispiel 2 - Transparente Nutzung von KI-generierten Inhalten: Eine Organisation, die generative KI für Marketingzwecke einsetzt, kennzeichnet klar, welche Inhalte von KI erstellt wurden. Dies fördert Transparenz und hilft, das Vertrauen der Verbraucher zu gewinnen, während gleichzeitig die rechtlichen Risiken minimiert werden.

DSGVO-KONFORMITÄT & KÜNSTLICHE INTELLIGENZ

Künstliche Intelligenz (KI) ermöglicht die Erstellung neuer Inhalte und die Automatisierung von Entscheidungen, sei es in Form von Text, Bildern, Musik oder Datenanalysen. Diese Entwicklungen bieten Unternehmen und Organisationen spannende Möglichkeiten, bringen jedoch auch erhebliche rechtliche Risiken mit sich, insbesondere im Hinblick auf den Datenschutz und die Einhaltung der Datenschutz-Grundverordnung (DSGVO). Ein zentrales Anliegen ist, wie KI-generierte Inhalte und -Entscheidungen rechtlich korrekt eingesetzt werden können, ohne gegen Datenschutzbestimmungen zu verstoßen.

Die DSGVO schützt vor allem die Verarbeitung personenbezogener Daten. Personenbezogene Daten sind „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“. Identifiziert werden kann eine Person durch klare Informationen wie Name, Wohnort, Fingerabdruck oder Foto. Identifizierbar ist jedoch ein viel umfassenderer Begriff; dazu gehören auch Daten wie IP-Adressen oder Fotos, die eine Person an einem bestimmten Ort und zu einer bestimmten Zeit zeigen, selbst wenn das Gesicht nicht sichtbar ist. Die Verarbeitung dieser Daten umfasst alle Aktivitäten, die mit den Daten durchgeführt werden, wie Ändern, Speichern, Löschen oder das Füttern von Daten in KI-Systeme. Unternehmen müssen sich der rechtlichen Rahmenbedingungen bewusst sein, um Haftungsrisiken zu minimieren und rechtliche Konsequenzen zu vermeiden.

Trotz des Ziels, mit KI umfassende Daten zu sammeln und optimale Ergebnisse zu erzielen, verlangt die DSGVO eine selektive Vorgehensweise. Der Einsatz von KI ist zulässig, wenn die Datenverarbeitung verhältnismäßig und gut begründet ist. Interne Datenschutzrichtlinien und eine klare Datenschutzerklärung sind besonders wichtig, vor allem bei KI-Anwendungen wie dem Chatbot-Support. Zudem sollte eine Datenschutz-Folgenabschätzung erfolgen, um Risiken zu identifizieren und geeignete Maßnahmen zur Minimierung zu implementieren.

DATENSCHUTZ IN DER SCHWEIZ UND ÖSTERREICH

In der Schweiz regelt das Bundesgesetz über den Datenschutz (DSG) den Datenschutz, das weitgehend mit der DSGVO kompatibel ist, aber weniger strenge Einwilligungsanforderungen hat. Unternehmen müssen die Rechte der Betroffenen respektieren.

In Österreich ist die DSGVO direkt anwendbar, und das Datenschutzgesetz (DSG) legt strenge Anforderungen an Einwilligungen und Transparenz fest.

FALSCHES VORGEHEN

Beispiel 1 - Verarbeitung persönlicher Daten ohne Einwilligung: Eine Organisation nutzt KI, um Daten von Nutzern zu analysieren und personalisierte Empfehlungen zu erstellen, ohne die ausdrückliche Zustimmung der Nutzer einzuholen. Dies kann zu hohen Bußgeldern und rechtlichen Konsequenzen führen.

Beispiel 2 - Unzureichende Transparenz: Eine Institution generiert automatisierte Entscheidungen auf Basis von Nutzerdaten, ohne die betroffenen Personen über die Verwendung ihrer Daten zu informieren. Dies verstößt gegen die Transparenzanforderungen der DSGVO und kann das Vertrauen der Nutzer beeinträchtigen.

RICHTIGES VORGEHEN

Beispiel 1 - Einholung von Einwilligungen: Eine Organisation, die KI zur Verarbeitung von Daten nutzt, stellt sicher, dass alle verwendeten persönlichen Daten mit der ausdrücklichen Zustimmung der Nutzer verarbeitet werden. Vor der Analyse von Daten wird die Zustimmung eingeholt, um rechtlichen Problemen vorzubeugen.

Beispiel 2 - Transparente Nutzung von Daten: Eine Institution, die KI für Entscheidungsfindungen einsetzt, informiert klar und deutlich über die Verwendung von Nutzerdaten. Dies fördert Transparenz und hilft, das Vertrauen der Nutzer zu gewinnen, während gleichzeitig die rechtlichen Risiken minimiert werden.

AI ACT - REGULATION ODER BESCHRÄNKUNG KÜNSTLICHER INTELLIGENZ?

Der AI Act der Europäischen Union, der am 12. Juli 2024 im Amtsblatt veröffentlicht wurde und am 1. August 2024 in Kraft trat, zielt darauf ab, den Einsatz von Künstlicher Intelligenz (KI) umfassend zu regulieren. Dieser Gesetzesentwurf kategorisiert KI-Systeme nach ihrem Risiko und legt strenge Anforderungen für hochriskante Anwendungen fest, während bestimmte inakzeptable Anwendungen gänzlich verboten werden.
Um den rechtlichen Vorgaben gerecht zu werden und das Vertrauen der Nutzer zu gewinnen, müssen Unternehmen eine Vielzahl von Maßnahmen ergreifen. Diese Maßnahmen sind entscheidend, um die Compliance sicherzustellen und ethische Standards im Umgang mit KI zu wahren. Im Folgenden werden einige zentrale Anforderungen und deren korrekte Umsetzung dargestellt:

RISIKOKATEGORISIERUNG

Falsch: Ein Unternehmen klassifiziert ein KI-System zur Gesichtserkennung als unbedenklich, ohne die potenziellen Risiken und Auswirkungen auf die Privatsphäre zu prüfen.
Richtig: Das Unternehmen führt eine gründliche Risikobewertung durch und klassifiziert das System als hochriskant, um die erforderlichen Sicherheitsmaßnahmen zu implementieren.

TRANSPARENZPFLICHT

Falsch: Nutzer werden nicht darüber informiert, dass sie mit einem KI-System interagieren, z.B. bei einem Chatbot-Support.
Richtig: Das Unternehmen kennzeichnet klar, dass es sich um einen KI-gestützten Chatbot handelt, und erklärt, wie ihre Daten verarbeitet werden.

DOKUMENTATION UND BERICHTERSTATTUNG

Falsch: Ein Unternehmen führt keine Aufzeichnungen über die Verwendung seiner KI-Systeme.
Richtig: Das Unternehmen dokumentiert alle KI-Anwendungen und erstellt Berichte über deren Leistung und Compliance.

TECHNISCHE MASSNAHMEN

Falsch: Ein Unternehmen implementiert keine Sicherheitsprotokolle für seine KI-Systeme.
Richtig: Das Unternehmen setzt technische Maßnahmen wie Verschlüsselung und Zugriffskontrollen ein, um die Sicherheit der Systeme zu gewährleisten.

ANFORDERUNGEN AN HOHE RISIKEN

Falsch: Ein Unternehmen ignoriert die Dokumentationspflichten für ein KI-System zur Entscheidungsfindung im Personalwesen.
Richtig: Das Unternehmen erstellt umfassende Dokumentationen, die die Algorithmen, Datenquellen und Entscheidungsprozesse des KI-Systems detailliert beschreiben.

DATENSCHUTZ UND MENSCHENRECHTE

Falsch: Ein KI-System speichert personenbezogene Daten ohne Einwilligung der Nutzer.
Richtig: Das Unternehmen holt die ausdrückliche Zustimmung der Nutzer ein und implementiert Datenschutzmaßnahmen gemäß der DSGVO.

ZUSAMMENARBEIT MIT AUFSICHTSBEHÖRDEN

Falsch: Das Unternehmen ignoriert Anfragen von Aufsichtsbehörden zur Überprüfung seiner KI-Systeme.
Richtig: Das Unternehmen arbeitet aktiv mit den Aufsichtsbehörden zusammen und stellt alle erforderlichen Informationen bereit, um die Compliance nachzuweisen

SCHULUNG UND SENSIBILISIERUNG

Falsch: Mitarbeiter erhalten keine Schulungen zu den Anforderungen des AI Acts.
Richtig: Das Unternehmen bietet regelmäßige Schulungen an, um das Bewusstsein für die gesetzlichen Anforderungen und ethischen Standards zu schärfen.

KI, DATENSCHUTZ, RICHTLINIEN & RECHTLICHE THEMEN: WER HAFTET?

Die Haftungsfrage im Zusammenhang mit Künstlicher Intelligenz (KI) ist komplex und derzeit noch nicht abschließend geklärt. Der AI Act der Europäischen Union sieht zwar Strafen in Form von Bußgeldern vor, doch auf nationaler Ebene bleibt die Situation oft unklar. Solange die Haftungsprozesse für KI im AI Act nicht konkretisiert sind, müssen Unternehmen auf nationale Rechtsprechung und Gesetze zurückgreifen.

WER HAFTET AKTUELL FÜR KI?

Die Haftung kann verschiedene Akteure betreffen, darunter:

- Hersteller: Die Produzenten von KI-Systemen tragen eine wesentliche Verantwortung.
- KI-Tool-Anbieter: Unternehmen, die KI-Tools entwickeln und vertreiben.
- Betreiber: Diejenigen, die die KI-Systeme in ihrem Betrieb einsetzen.
- Programmierer: Entwickler, die die Algorithmen und Software erstellen.

In Deutschland wird oft auf die Produzentenhaftung verwiesen, die für Produkte auf dem Markt gilt. Dies bedeutet, dass ein Hersteller für Schäden haftet, die durch eine Verletzung der Sorgfaltspflicht entstehen.

SORGFALTSPFLICHT IM KONTEXT VON KI

Die Sorgfaltspflicht bezieht sich darauf, dass Unternehmen sicherstellen müssen, dass ihre KI-Systeme angemessen auf Risiken geprüft werden. Wenn eine KI nicht so risikolos ist, wie ursprünglich dargestellt, könnte dies zu einer Haftung führen. Beispielsweise könnte ein Nutzer in der Haftung stehen, wenn er KI-Prozesse integriert, ohne die damit verbundenen Risiken zu berücksichtigen.

ARBEITSRECHTLICHE ASPEKTE

Im Unternehmenskontext spielt das Arbeitsrecht eine entscheidende Rolle, insbesondere bei Bewerbungsprozessen und der Integration von KI. Die Haftung für Diskriminierung ist hierbei von großer Bedeutung. Differenzierungen, die auf personenbezogenen Daten basieren, können diskriminierend sein.

Es bedeutet jedoch nicht, dass KI nicht in diesen Prozessen eingesetzt werden kann. Vielmehr ist es wichtig, dass KI-Tools als Hilfsmittel genutzt werden, um beispielsweise Bewerberdaten auszuwerten. Die KI darf nicht gegen das Allgemeine Gleichbehandlungsgesetz (AGG) verstoßen. Richtiges Prompting und Training der KI sind entscheidend, um Diskriminierung im Personalmanagement zu vermeiden.

ZUKÜNFTIGE ENTWICKLUNGEN IN DER EU ZUR HAFTUNG

Die EU plant, die Produkthaftungsrichtlinien zu überarbeiten und spezifische Richtlinien zur Haftung im Zusammenhang mit KI zu entwickeln. Diese neuen Regelungen sollen Klarheit schaffen und die Verantwortlichkeiten im Umgang mit KI-Systemen besser definieren.

DIGITALBEAT.
BESSER MIT KI



www.digitalbeat.de
team@digitalbeat.de
Digital Beat GmbH, Hansaring 97, 50670 Köln
+49 (0) 221 8282 91 01