Mittelstand-Digital
Zentrum
Chemnitz

NACHGELESEN

KI im Marketing
Risiko richtig einschätzen

STEPHAN KUNITZ

Mittelstand-
Digital

Gefördert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Impressum

HERAUSGEBER
Mittelstand-Digital Zentrum Chemnitz
Tel: 0371 531 19935
Fax: 0371 531 819935
info@digitalzentrum-chemnitz.de
www.digitalzentrum-chemnitz.de

REDAKTION Anikó Lessi

GESTALTUNG
PUNKT191 – Marketing und Design
www.punkt191.de

BILDNACHWEIS
Titel: Diloka107 - Freepik.com

VERÖFFENTLICHUNG November 2023

© Storyset - Freepik.com

Risiko Marketing?

In diesem Nachgelesen erfahren Sie:

- Wie KI im Marketing vermehrt eingesetzt wird.
- Welche rechtlichen Rahmenbedingungen zu beachten sind.
- Wie das Zusammenspiel aus Risikoabsicherung und Verwendung von KI aussehen kann.

Marketing und KI

Die Implementierung künstlicher Intelligenz (KI) im Marketing eröffnet kleinen und mittleren Unternehmen faszinierende Möglichkeiten zur Optimierung ihrer Werbestrategien. Die Nutzung von KI in Werbekampagnen ermöglicht nicht nur eine präzisere Ausrichtung, sondern auch die Vorhersage des Verbraucherverhaltens aus umfangreichen Datenmengen. Diese innovative Technologie kann bis zu 80 % der physischen Arbeiten und 70 % der Datenverarbeitung automatisieren, was insbesondere für ressourcenknappe Unternehmen einen signifikanten Vorteil darstellt.[1]

Ein entscheidender Aspekt, der kleine Unternehmen aufhorchen lässt, ist die personalisierte Werbung durch den Einsatz von Machine Learning und KI-Algorithmen. Dies steigert nicht nur die Conversion-Rate, sondern ermöglicht auch eine stärkere Kundenbindung. Doch die Anwendung von KI im Marketing geht darüber hinaus. Die effiziente Auswertung von Daten der Nutzenden in Echtzeit ermöglicht es Unternehmen genau zu analysieren wann, wo und wie Verbraucherinnen und Verbraucher über ihre Marke sprechen. Dies erlaubt nicht nur die Anpassung von Inhalten an die Bedürfnisse der Zielgruppe, sondern auch eine gezielte Steigerung der Reichweite.

Ein weiterer spannender Aspekt ist die automatisierte Preisgestaltung durch KI. Unternehmen können mithilfe von Algorithmen schnell und präzise auf Markttrends reagieren und ihre Preisstrategien entsprechend optimieren. Was nicht nur Zeit, sondern auch Geld spart und Unternehmen wettbewerbsfähig macht.

Trotz dieser vielversprechenden Vorteile sollten sich Personen mit Entscheidungsbefugnis in kleinen und mittelständischen Unternehmen bewusst sein, dass die Nutzung von KI im Marketing auch Herausforderungen mit sich bringt. Diese reichen von möglichen Ungenauigkeiten in den Daten bis zur Notwendigkeit, sensible Verbraucherdaten zu schützen. Wir werden diese Aspekte vertieft betrachten und insbesondere den rechtlichen Rahmen für den Einsatz von KI im Marketing beleuchten.

Der rechtliche Rahmen

Der effiziente Einsatz selbstlernender Chatbots und digitaler Assistenten eröffnet mittelständischen Unternehmen vielfältige Chancen zur Umsatzsteigerung und individuellen Kundenansprache. Der Schlüssel dazu liegt in der umfassenden Erstellung von Nutzungsprofilen durch KI-gestützte Profiling-Maßnahmen. Hierbei werden nicht nur personenbezogene Daten gesammelt, sondern auch Stimmungsbilder und Präferenzen der Webseitenbesucher und -besucherinnen analysiert. Durch den Einsatz von Voice-Recognition-Systemen und Sentiment-Analysen können sogar Persönlichkeitsmerkmale und Emotionen erfasst werden, was eine gezielte Beeinflussung des Kundenstimmungsbilds ermöglicht. Durch die Verwendung personenbezogener Daten sind auch die jeweiligen datenschutzrechtlichen Vorgaben zu beachten. Nachfolgend stellen wir daher das datenschutzrechtliche Risiko, dessen Identifikation und die jeweiligen Eintrittswahrscheinlichkeiten vor, die notwendig sind um eine Risikoklassifikation vorzunehmen.

Die Anwendungsbereiche dieser Profile sind vielfältig. Unternehmen können mithilfe von Algorithmen abwanderungsgefährdete Kunden frühzeitig identifizieren und präventive Maßnahmen ergreifen. Recommendation Engines nutzen die gesammelten Daten, um personalisierte Produktempfehlungen auszuspielen, während auch die Preisbildung individualisiert erfolgen kann, basierend auf Merkmalen zur Zahlungsbereitschaft bestimmter Zielgruppen.

Allerdings ist beim Einsatz von KI-basierten Profiling-Maßnahmen im Marketing der Datenschutz zu beachten. Die Verbindung von Cookies und Algorithmen mit Persönlichkeitsprofilen fällt unter den Anwendungsbereich der DSGVO. Daher ist eine wirksame Rechtsgrundlage erforderlich, insbesondere unter Berücksichtigung der Voraussetzungen der Art. 6 Abs. 1, 22 Abs. 1 und 35 Abs. 1 DSGVO.[2]

So müssen neben einer wirksamen Einwilligung in das Setzen und Auslesen von Cookies nach § 26 TTDSG in Verbindung mit Art. 6 Abs. 1 DSGVO auch Erwägungen angestellt werden, ob eine automatisierte Entscheidung im Sinne des Art. 22 DSGVO vorliegt. Und auch, ob im Sinne des Art. 35 DSGVO ein besonderes Risiko durch die Form der Verarbeitung gegeben sein könnte:

„Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.“[3]

Entsprechend muss vor der Verwendung eines KI-Systems für derartige Profiling-Maßnahmen das Risiko einer solchen ermittelt werden.

Risiko im Sinne der DSGVO

Im Kontext der Datenschutzgrundverordnung (DSGVO) wird das Risiko als potenzieller Schaden für natürliche Personen definiert, der sich aus der Verarbeitung personenbezogener Daten ergeben kann. Dieser Schaden kann physischer, materieller oder immaterieller Natur sein, wobei insbesondere ungerechtfertigte Beeinträchtigungen der Rechte und Freiheiten von Einzelpersonen als immaterielle Schäden betrachtet werden. Ein Schadensereignis kann durch unrechtmäßige oder nicht den Grundsätzen der DSGVO entsprechende Verarbeitungstätigkeiten entstehen und zusätzliche Risiken wie Diskriminierung mit sich bringen.[4]

Die DSGVO unterscheidet zwischen verschiedenen Risikoniveaus: geringes Risiko, Risiko und hohes Risiko. Das Ziel der Risikobeurteilung besteht darin, die Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten zu bewerten. Dies ist insbesondere relevant in Bezug auf die Verantwortung des für die Verarbeitung Verantwortlichen, die Datenschutztechnikgestaltung, die Sicherheit der Verarbeitung, den Umgang mit Verletzungen des Datenschutzes sowie Datenschutz-Folgenabschätzungen und vorherige Konsultationen.[5]

Risikoidentifikation

Die Risikoidentifikation im Kontext der DSGVO erfordert eine systematische Durchführung in mehreren Phasen. Zunächst steht die genaue Beschreibung des zugrunde liegenden Sachverhalts im Fokus, für den das Risiko bewertet werden soll. Hierbei spielen Fragen nach den möglichen Schäden für natürliche Personen, den Ereignissen, die diese Schäden auslösen könnten, und den Risikoquellen eine entscheidende Rolle.

Die Identifikation von Ereignissen konzentriert sich auf die Nichteinhaltung der Datenschutzgrundsätze und die Nichtgewährung von Betroffenenrechten. Hierbei werden unbefugte oder unrechtmäßige Verarbeitungen, Verstöße gegen die Grundsätze von Treu und Glauben, intransparente Verarbeitungen und weitere Verstöße berücksichtigt.

Die Risikoquellen können vielfältig sein, von Verantwortlichen und Auftragsverarbeitern über unbefugte Angreifende bis hin zu staatlichen Stellen oder technischen Fehlfunktionen. Eine umfassende Identifikation dieser Quellen ist entscheidend, um die Risikobeurteilung gemäß den Anforderungen der DSGVO durchzuführen.

Eintrittswahrscheinlichkeit und Schwere der Schäden

Die Abschätzung der Eintrittswahrscheinlichkeit im Kontext der DSGVO erfordert eine differenzierte Betrachtung möglicher Schäden und ihrer Wahrscheinlichkeit. Gemäß den Vorgaben der DSGVO sollen objektive Kriterien zur Bewertung herangezogen werden, insbesondere bei immateriellen Schäden wie Rufschädigung. Eine mögliche Methode zur Bemessung besteht darin, die Schwere und Eintrittswahrscheinlichkeit auf einer Skala mit klaren Ausprägungen zu veranschaulichen, beispielsweise geringfügig, überschaubar, substanziell und groß.

Die Eintrittswahrscheinlichkeit wird anhand verschiedener Wege analysiert, die zu einem bestimmten Schadensereignis führen können. Dabei werden Faktoren wie unzureichende Sicherheitsvorkehrungen, fahrlässiges Verhalten von Mitarbeitenden, technische Fehlfunktionen oder externe Ausspähung berücksichtigt. Die Summierung dieser Wahrscheinlichkeiten ermöglicht eine umfassende Einschätzung.

Die Schwere eines möglichen Schadens wird anhand verschiedener Faktoren beurteilt. Dazu zählen beispielsweise die Art der verarbeiteten Daten, der Schutzstatus bestimmter Personengruppen, die Reversibilität des Schadens, die Möglichkeit der Selbstprüfung oder gerichtlichen Prüfung durch die betroffene Person, sowie die potenzielle systematische Überwachung. Eine sorgfältige Bewertung dieser Elemente ist entscheidend, um ein umfassendes Bild des Risikos im Kontext der DSGVO zu zeichnen.

Zuordnung zu Risikostufen

Die Zuordnung zu den Risikostufen „geringes Risiko“, „Risiko“ und „hohes Risiko“ gemäß der DSGVO erfordert die Berücksichtigung der Eintrittswahrscheinlichkeit und Schwere möglicher Schäden. Die DSGVO selbst gibt hierbei aber keinen detaillierten Leitfaden vor, was Raum für verschiedene Modelle lässt. Grundsätzlich wird das Risiko der Gesamtverarbeitung durch die höchste Risikoklasse der Einzelrisiken bestimmt. Wenn viele Einzelrisiken in dieser Klasse vorliegen, könnte in bestimmten Fällen eine höhere Risikoklasse angenommen werden.

Eine Risikomatrix, die die Eintrittswahrscheinlichkeit und Schwere des möglichen Schadens berücksichtigt, kann als Instrument zur Abschätzung dienen. Die Matrix ermöglicht es, Fälle zu identifizieren, in denen der Schadenseintritt wahrscheinlich ist oder der potenzielle Schaden besonders schwerwiegend wäre. In Grenzbereichen zwischen den Risikostufen kann eine Einzelfallbetrachtung notwendig sein, um trotz generischer Abschätzung zu bestimmen, ob ein hohes Risiko vorliegt. Der Fokus liegt darauf, die spezifischen Umstände der Datenverarbeitung zu berücksichtigen und das Ausgangsrisiko fundiert zu bestimmen.

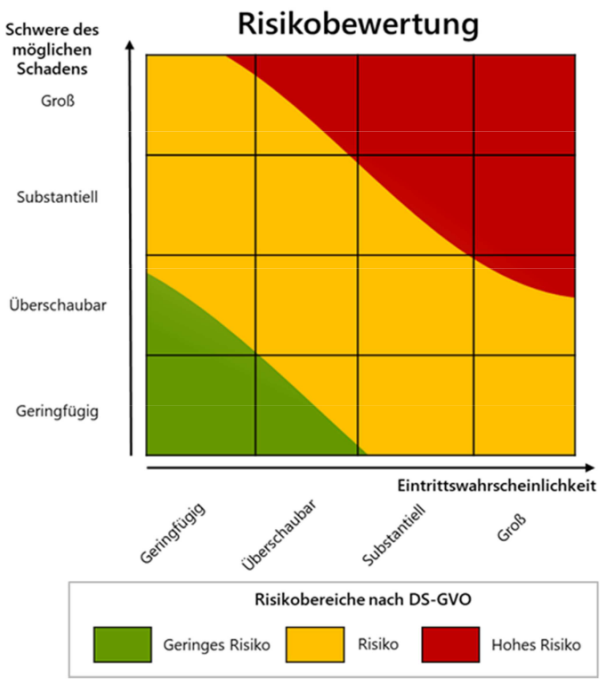

Abbildung 1: Beispiel einer Risikomatrix (DSK, 2019)

Fazit

Die Risikoermittlung stellt eine Schlüsselrolle im Zusammenhang mit KI-Anwendungen dar und ist unentbehrlich für eine an sie anschließende Datenschutzfolgeabschätzung. Identifikation von Risiken, Abschätzung von Eintrittswahrscheinlichkeiten und Schwere möglicher Schäden sowie die Zuordnung zu Risikostufen sind entscheidende Schritte. Beim Einsatz von künstlicher Intelligenz im Marketing, insbesondere bei die Auswertung von Nutzendendaten und automatisierter Preisgestaltung, sind präzise Risikobeurteilungen erforderlich. Klare Definitionen und Richtlinien für die Risikobeurteilung, einschließlich einer flexiblen Risikomatrix sind bereits vorhanden und gut zu nutzen. Diese Instrumente ermöglichen Unternehmen proaktive Maßnahmen, um Datenschutzverletzungen zu minimieren und den gesetzlichen Anforderungen gerecht zu werden.

Die differenzierte Herangehensweise an die Risikoermittlung bei KI-Anwendungen, besonders in kleinen und mittleren Unternehmen, ist von großer Bedeutung. Eine systematische Beurteilung der Risiken trägt nicht nur zur Einhaltung rechtlicher Verpflichtungen bei, sondern sichert auch langfristig die Integrität und Akzeptanz von KI-basierten Systemen.

Referenzen

1 A. Holl und B. Baer, KI in der Werbung: Maximale Personalisierung & Reichweite, 121WATT | School for Digital Marketing & Innovation. Zugegriffen: 2. November 2023. [Online]. Verfügbar unter: https://www.121watt.de/ki/ki-basierte-werbung/

2 T. Gausling, Künstliche Intelligenz im digitalen Marketing, ZD, Nr. 8, S. 335–341, 2019.

3 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Zugegriffen: 2. November 2023. [Online]. Verfügbar unter: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=de

4 M. Schröder, Schröder: Der risikobasierte Ansatz in der DSGVO, ZD, Nr. 11, S. 503–506, 2019.

5 DSK, DKS-Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürlicher Personen. Zugegriffen: 30. Oktober 2023. [Online]. Verfügbar unter: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf

Autor

STEPHAN KUNITZ ist wissenschaftlicher Mitarbeiter an der Professur für Privatrecht und Recht des geistigen Eigentums an der Technischen Universität Chemnitz. Im Mittelstand-Digital Zentrum Chemnitz beschäftigt er sich mit den Themen KI & Recht sowie Datenschutzrecht.
stephan.kunitz@digitalzentrum-chemnitz.de

Weitere Informationen

Das Mittelstand-Digital Zentrum Chemnitz gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Klimaschutz die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

WAS IST MITTELSTAND-DIGITAL?

Das Mittelstand-Digital Netzwerk bietet mit den Mittelstand-Digital Zentren und der Initiative IT-Sicherheit in der Wirtschaft umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Klimaschutz ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.mittelstand-digital.de.

Mittelstand-Digital
Zentrum
Chemnitz

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages