HAUFE. AKADEMIE

WHITEPAPER

KÜNSTLICHE INTELLIGENZ IM DATENSCHUTZRECHT

Neue Aufgaben für Datenschutzbeauftragte?

Management Summary

Tools wie ChatGPT, Dall-E, Midjourney, Stable Diffusion & Co. sind noch nicht perfekt – sie können aber schon eine ganze Menge. Künstliche Intelligenz (KI) hat in den letzten Jahren erhebliche Fortschritte gemacht. KI-Tools erobern immer mehr Einsatzfelder, vom Gesundheitsbereich über die Kreativbranche bis hin zur Unterhaltungsindustrie. Richtig eingesetzt können KI-Werkzeuge sehr nützlich sein und sogar Zeit und Geld sparen. Wer einen Blogbeitrag erstellen, einen fremdsprachigen Text ins Deutsche übersetzen oder Bilder für Vortragsfolien kreieren lassen will, sollte jedenfalls im geschäftlichen Umfeld die verschiedenen datenschutzrechtlichen Stolperfallen kennen. Der Datenschutz ist beim Einsatz von KI von zentraler Bedeutung, denn derartige Systeme erfordern regelmäßig umfangreiche Daten. Wir zeigen Ihnen die wichtigsten Aspekte, die hierbei zu beachten sind.

Inhaltsverzeichnis

Klicken Sie auf das Kapitel, um zur **Seite** zu gelangen

Wie intelligent ist die Künstliche Intelligenz?

Die Technik hinter ChatGPT, Dall-E, Midjourney, Stable Diffusion & Co. ist nicht neu. Forschungen an solchen Large Language Models (LLM), also an Sprachmodellen zur Auswertung einer riesigen Anzahl von Daten, gibt es schon seit etlichen Jahren. Allerdings wurde diese Art von KI erst mit der für alle verfügbaren Version von ChatGPT massentauglich und auch der Allgemeinheit bekannt. Dennoch sind nahezu alle derzeit auf dem Markt verfügbaren KI-Tools immer noch „Black Boxes", sodass mit Ausnahme der herstellenden Unternehmen niemand mit Sicherheit sagen kann, wie sie genau funktionieren. Klar ist, dass eine KI aus Computerprogrammen (Algorithmen) besteht, die mit einer Unmenge von Trainingsdaten gefüttert werden. Dadurch sollen sie an möglichst vielen Beispielen lernen (sog. maschinelles Lernen, engl.: machine learning, kurz: ML) und so ihre jeweilige Aufgabe erfüllen. Ein KI-System ist also nicht wirklich intelligent, sondern lediglich sehr gut im Erkennen von Mustern und in der Neuzusammensetzung von Erlerntem. Denn es hat letztlich mit Hilfe von unzähligen Daten trainiert und gelernt, Muster zu erkennen und auf Anforderung neu zusammenzusetzen. Wenn Sie Text-zu-Bild-Generatoren, wie z.B. Dall-E oder Midjourney, dazu auffordern, das Bild eines vor dem Kölner Dom stehenden Teddybären zu erstellen, dann ist das Tool dazu in der Lage, weil es zuvor Unmengen an Bildern von Teddybären und dem Kölner Dom ausgewertet hat. Aber die KI „versteht" dennoch nicht im menschlichen Sinne, was ein Teddybär ist – sie weiß nur genau, an welchen Merkmalen man ihn erkennt.

Beispiele

Heutzutage werden beispielsweise in folgenden Bereichen KI-Anwendungen genutzt:

- Diktierfunktion in Office-Anwendungen
- Spracherkennung im Smartphone oder anderen Geräten (Siri, Alexa & Co.)
- Navigationssysteme mit Echtzeitdaten im Firmenfahrzeug
- Übersetzungs-Tools wie Google Translator oder DeepL
- Gestaltung von geschäftlichen Inhalten wie Verträge, E-Mails, Werbetexte etc.
- Chatbots auf Websites für Kundensupport etc.

Was regelt das Datenschutzrecht?

Das Datenschutzrecht regelt den Umgang von Daten mit Bezug zu einer natürlichen Person, also zu einem Menschen. Es ist immer dann zu berücksichtigen, wenn personenbezogene Daten verarbeitet werden (z.B. Name, Anschrift, Kontaktdaten, Geburtsdaten, ärztliche Diagnosen, allgemeine äußerliche Merkmale, Kfz-Kennzeichen oder IP-Adressen). Da der Begriff des Personenbezugs in der Datenschutzgrundverordnung (DSGVO) grundsätzlich sehr weitgehend zu verstehen ist, sollten Sie im Zweifel davon ausgehen, dass das Datenschutzrecht in aller Regel anwendbar ist.

Achtung

Aber auch dann, wenn im Einzelfall kein Personenbezug anzunehmen sein sollte, kann es sich um sensible Daten handeln, z.B. um Geschäftsgeheimnisse. Diese unterliegen eigenen gesetzlichen Regelungen, insbesondere dem Geschäftsgeheimnisgesetz (GeschGehG).

Wenn beispielsweise der Text, den Sie in eine KI eingeben (der sog. Prompt), um das gewünschte Ergebnis zu erhalten, auch personenbezogene Daten enthält, dann ist das eine Verarbeitung im Sinne der DSGVO, sodass hier stets alle entsprechenden Vorgaben einzuhalten sind. Verwenden Sie daher so weit wie möglich Platzhalter- oder Fantasie- und keine echten Klardaten.

Ein absolutes Muss: die Rechtsgrundlage

Personenbezogene Daten dürfen immer nur auf Basis einer Rechtsgrundlage verarbeitet werden. Diese finden sich in Art. 6 Abs. 1 DSGVO. Für den nicht-öffentlichen Bereich, also für Unternehmen, sind insbesondere die folgenden Rechtsgrundlagen wichtig:

- Einwilligung
- Erfüllung einer (vor-) vertraglichen Maßnahme
- Erfüllung einer rechtlichen Verpflichtung
- überwiegende berechtigte Interessen

Zumindest eine Variante muss gegeben sein, es können bisweilen aber auch mehrere Rechtsgrundlagen bestehen.

Abbildung: Mögliche Rechtsgrundlagen finden sich nicht nur in der DSGVO.

Speziell für Bundes- bzw. Landesbehörden bieten das Bundesdatenschutzgesetz (BDSG) sowie die jeweiligen Landesdatenschutzgesetze weitere Rechtsgrundlagen. Außerdem existieren verschiedene Spezialregelungen, wie etwa im Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) für die Datenverarbeitung per Cookies & Co. Zusätzlich können sich auch noch in Satzungen oder Tarifverträgen Datenschutz-Rechtsgrundlagen finden.

Sie werden in aller Regel eine Einwilligung der Personen einholen müssen, deren Daten Sie im Rahmen des Einsatzes von KI-Tools nutzen wollen. Grundsätzlich ist aber auch der Abschluss eines Vertrages und die Erfüllung der entsprechenden Verpflichtung daraus denkbar. Das setzt jedoch eine transparente und faire vertragliche Regelung voraus. Als taugliche Rechtsgrundlage ausscheiden dürften hingegen die Erfüllung einer rechtlichen Verpflichtung sowie die berechtigten Interessen.

Transparenzgrundsatz beachten – Pflichtinformationen bereitstellen

Apropos Transparenz – ein sehr wichtiges Prinzip im Datenschutzrecht, was im Zusammenhang mit dem Einsatz von KI noch viel wichtiger ist. Nach Maßgabe von Art. 13 DSGVO müssen Sie gegenüber betroffenen Personen proaktiv bestimmte Informationspflichten erfüllen. Dazu zählen u.a. die folgenden Angaben:

- Namen und Kontaktdaten des verantwortlichen Unternehmens
- Kontaktdaten des:der Datenschutzbeauftragten
- Zweck(e) der Datenverarbeitung
- Rechtsgrundlage(n) der Datenverarbeitung
- Dauer der Datenspeicherung

Wichtig:

Diese Pflichten sind zu unterscheiden von der Auskunftspflicht nach Art. 15 DSGVO. Hier sind ähnliche Informationen gefordert, allerdings nur auf Verlangen von Betroffenen bereitzustellen.

Diese Informationspflicht ist etwa von der Online-Datenschutzerklärung bekannt, Art. 13 DSGVO gilt aber auch für analoge bzw. Offline-Datenverarbeitungen. Viele Angaben, die in Art. 13 DGSVO gefordert werden, kennen Sie in Bezug auf die meisten derzeit am Markt existierenden KI-Anwendungen jedoch gar nicht. Denn oftmals ist nicht klar, ob das Unternehmen, das die KI bereitstellt, die in die KI eingegebenen Inhalte zu Trainings-, zu Werbe- oder zu anderen Zwecken weiternutzt, wo genau die Daten verarbeitet werden, wie lange sie gespeichert bleiben oder wer sonst noch alles Zugriff darauf erhält.

Daher sollten Sie möglichst nur solche KI-Tools einsetzen, die ihrerseits ein ausreichendes Maß an Transparenz mitbringen und Sie dementsprechend in der Lage sind, Ihre Informationspflichten aus Art. 13 DSGVO zu erfüllen. Ideal ist ein KI-System, welches die eingegebenen Daten nur im Rahmen der Anfrage, aber nicht für weitere Zwecke (z.B. zum Training der KI) nutzt und diese so bald wie möglich wieder löscht.

Beispiel

Wenn Sie etwa Daten von Beschäftigten mittels KI verarbeiten wollen (z.B. zwecks Gestaltung eines Textes über das Firmenjubiläum im Intranet), dann müssen Sie genauso die passenden Art.-13-Informationen zur Verfügung stellen wie bei der Verwendung von Kund:innen- oder Bewerber:innendaten. In jedem Fall müssen den Betroffenen vorab die Pflichtinformationen bereitgestellt werden, z.B. als gedruckter Flyer oder als PDF-Anhang einer E-Mail.

Die drei wichtigsten Datenschutzgrundsätze: dokumentieren, dokumentieren, dokumentieren

Unternehmen müssen aufgrund des Nachweisprinzips belegen können, dass sie datenschutzkonform handeln (Art. 5 Abs. 2 DSGVO). Insbesondere die Dokumentationspflichten sind dadurch mit Einführung der DSGVO immens gestiegen. Zentrales Instrument ist hierbei das Verzeichnis von Verarbeitungstätigkeiten (VVT) gemäß Art. 30 DSGVO. Darin sind generell alle Verarbeitungstätigkeiten zu erfassen, in deren Zusammenhang auch personenbezogene Daten verarbeitet werden. Mit Ausnahme von rein anonymen oder Statistikdaten ist das im Grunde bei nahezu allen Datenverarbeitungen in Unternehmen der Fall. Folglich sind hier auch die Prozesse zu dokumentieren, bei denen KI zum Einsatz kommt. Für jede einzelne Verarbeitungstätigkeit sind u.a. anzugeben:

- Zwecke der Verarbeitung
- Kategorien betroffener Personen
- Kategorien personenbezogener Daten
- Kategorien von etwaigen Empfänger:innen der Daten
- Speicherdauer / Löschfristen
- technische und organisatorische Maßnahmen (TOMs) zum Schutz der verarbeiteten Daten (vgl. Art. 32 DSGVO)

In puncto Datenschutzdokumentation bestehen die gleichen Probleme wie bei den Informationspflichten (s.o.). Denn auch im Rahmen des VVT müssen Sie ggf. Informationen erfassen, die Sie nicht kennen und auch nicht von Seiten der KI-Unternehmen erhalten. Auch hier ist der Einsatz von KI-Tools aus solchen Unternehmen empfehlenswert, die alle erforderlichen Informationen bereitstellen.

Praxistipp

Beim Einsatz von KI kommen als geeignete TOMs u.a. die Verschlüsselung der Daten, eine Beschränkung der Zugriffsberechtigung auf wenige Personen oder eine Pseudonymisierung in Betracht.

Aufgepasst beim Datentransfer in außereuropäische Staaten

Mit ganz wenigen Ausnahmen sitzen diejenigen Unternehmen, die KI-Anwendungen entwickeln, im Nicht-EU-Ausland, zumeist in den USA, manche auch in Asien. Sofern Daten mit Personenbezug in solche Länder übermittelt werden sollen, muss sichergestellt werden, dass dort ein mit der Europäischen Union vergleichbares Datenschutzniveau besteht. Im Falle der USA existiert seit dem 10. Juli 2023 ein so genannter Angemessenheitsbeschluss, das **Data Privacy Framework (DPF).** US-Unternehmen können sich seitdem beim amerikanischen Handelsministerium in eine entsprechende Liste eintragen, wodurch sie datenschutzrechtlich wie ein Unternehmen mit Sitz in der EU behandelt werden. Abgesehen vom Datenschutzniveau müssen aber auch die vertraglichen Grundlagen stimmen. Daher ist beim Einsatz von KI-Technologie aus den USA der Abschluss der von der EU entwickelten Standardvertragsklauseln (engl.: standard contractual clauses, kurz: SCC) zu empfehlen. Die meisten großen KI-Unternehmen akzeptieren dies.

Aber auch dann, wenn die Daten innerhalb der EU bzw. des Europäischen Wirtschaftsraums (EWR) bleiben, ist bei der Übermittlung an Dritte ein spezieller Datenschutzvertrag abzuschließen, nämlich in aller Regel ein sog. Auftragsverarbeitungsvertrag.

Abschätzung möglicher Folgen des KI-Einsatzes

Da bei den meisten KI-Tools der Blick „unter die Motorhaube“ nicht möglich und somit nicht exakt nachvollziehbar ist, wie genau die eingegebenen Daten verarbeitet werden, besteht potenziell ein hohes Risiko für die betreffenden Daten. Somit ist regelmäßig vor der Nutzung von KI im Unternehmen eine so genannte Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO durchzuführen. Dabei handelt es sich um ein besonderes Verfahren zur Prüfung geplanter Datenverarbeitungen und Prüfung von existierenden Risiken. Im Zuge dieser DSFA sollen dann u.a. geeignete TOMs ermittelt werden, um die erkannten Risiken so weit wie möglich zu reduzieren. Ist dies nicht möglich, muss die zuständige Datenschutzaufsichtsbehörde kontaktiert und um Rat gefragt werden.

Hinweis

Eine DSFA ist in jedem Fall gut nachvollziehbar zu dokumentieren, selbst wenn keine Konsultation der Aufsichtsbehörde erfolgen muss.

Neue Aufgaben für Datenschutzbeauftragte?

Die Tätigkeit von Datenschutzbeauftragten (DSB) besteht insbesondere in der Überwachung der Einhaltung des Datenschutzes im Unternehmen sowie in der diesbezüglichen Beratung der Geschäftsleitung. Sollen zukünftig KI-Tools zum Einsatz kommen, muss der:die DSB in der Lage sein, die Verarbeitungstätigkeit sowohl technisch als auch juristisch zu beurteilen. Das wiederum bedeutet, dass das Unternehmen dem:der DSB die Möglichkeit zur Weiterbildung Bereich geben muss, indem ausreichende finanzielle und zeitliche Ressourcen bereitgestellt werden.

Fazit: KI ist gekommen, um zu bleiben

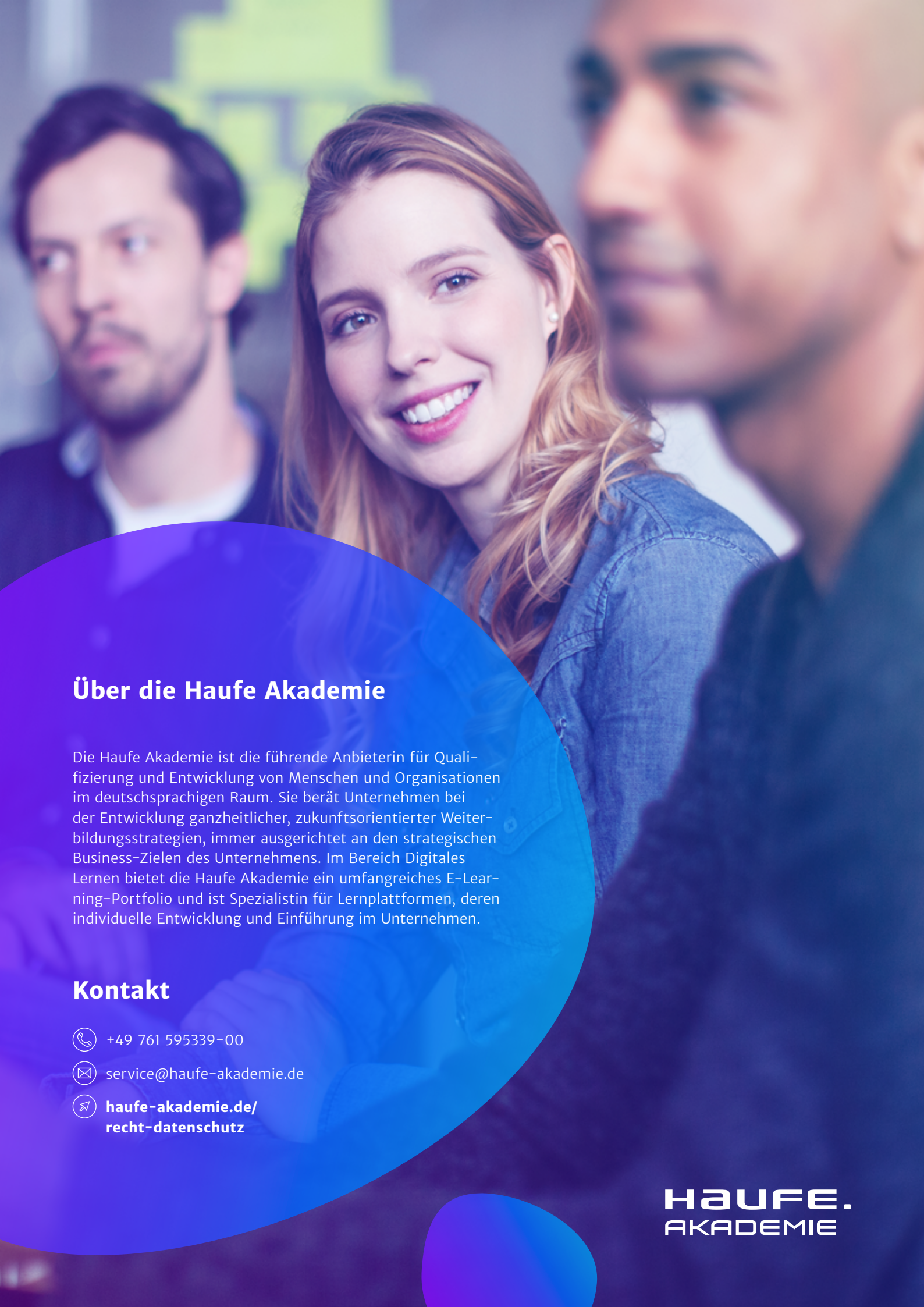
KI ist kein Trend, der irgendwann wieder verschwindet. Gerade im geschäftlichen Bereich wird der KI-Einsatz mehr und mehr zum Alltag werden. Beschäftigen Sie sich so bald wie möglich mit der Materie und auch mit den Problemen im Datenschutzkontext. Denn je eher Sie die bestehenden juristischen Probleme erkannt haben, desto schneller können Sie Lösungen entwickeln und KI rechtskonform nutzen. Dafür müssen Sie ggf. erst einmal Investitionen tätigen, langfristig wird sich der umsichtige Einsatz von KI jedoch auszahlen.

Um die im Bereich Datenschutz drohenden Bußgelder und Schadensersatzforderungen zu vermeiden, ist insbesondere eine datenschutzkonforme Gestaltung der KI-Nutzung zwingend erforderlich – bietet aber auch hervorragende Chancen für eine effiziente und gewinnbringende Einbindung moderner Technologien in den Unternehmensalltag.

Über den Autor

Michael Rohrlich
Rechtsanwalt

Michael Rohrlich ist Rechtsanwalt, Fachautor, Dozent und Video-Trainer (www.ra-rohrlich.de). Er hat seinen Kanzleisitz in Würselen (Nähe Aachen). Seine beruflichen Schwerpunkte liegen auf den Gebieten IT-, E-Commerce- und Datenschutzrecht. Seit 1997 publiziert er regelmäßig, sowohl im Print- als auch im Online-Bereich. Darüber hinaus ist er Autor mehrerer Bücher & E-Books. Als Video-Trainer ist er seit 2012 für LinkedIn Learning tätig.



Über die Haufe Akademie

Die Haufe Akademie ist die führende Anbieterin für Qualifizierung und Entwicklung von Menschen und Organisationen im deutschsprachigen Raum. Sie berät Unternehmen bei der Entwicklung ganzheitlicher, zukunftsorientierter Weiterbildungsstrategien, immer ausgerichtet an den strategischen Business-Zielen des Unternehmens. Im Bereich Digitales Lernen bietet die Haufe Akademie ein umfangreiches E-Learning-Portfolio und ist Spezialistin für Lernplattformen, deren individuelle Entwicklung und Einführung im Unternehmen.

Kontakt

+49 761 595339-00

service@haufe-akademie.de

haufe-akademie.de/recht-datenschutz

HAUFE. AKADEMIE