Blogartikel vom 06.12.2024
Rechtsgebiet: IT-Recht
Autor: Rechtsanwalt Norbert Geyer

Einsatz von Künstlicher Intelligenz in kleinen bis mittelständischen Unternehmen

Rechtliche Rahmenbedingungen und praktische Empfehlungen

Der Einsatz von Künstlicher Intelligenz (KI) birgt enorme Chancen für viele Unternehmen. Durch neue Technologien erhoffen sich insbesondere auch kleine und mittelständische Unternehmen eine Effizienzsteigerung. Die Künstliche Intelligenz stellt aber auch eine erhebliche Herausforderung dar. Neben den technischen Themen gibt es auch einige rechtliche Herausforderungen anzugehen.

Im Vergleich zu großen Konzernen mit eigenen Rechts- und IT-Abteilungen fehlen kleinen und mittelständischen Unternehmen oft die finanziellen und personellen Ressourcen, um den Einsatz von KI rechtskonform zu gestalten. Dennoch ist es auch für diese Unternehmen essenziell, ein Mindestmaß an Maßnahmen zu ergreifen, um rechtliche Risiken, insbesondere in Bezug auf den Datenschutz und die DSGVO, zu minimieren. Nachfolgend werden zentrale Punkte zur Vorbereitung und Implementierung des KI-Einsatzes erläutert.

1. Nutzung kostenpflichtiger KI-Accounts

Anbieter von Künstlicher Intelligenz, insbesondere von leistungsstarken Sprachmodellen (LLMs), bieten oft „kostenlose" Accounts an.

Hauptmerkmal dieser kostenlosen Accounts ist zumeist, dass die eingegebenen Daten fast komplett frei wieder zum Training verwendet werden. Der Nutzer bezahlt damit mit seinen Daten. Diese werden sowohl hinsichtlich der Eingaben z.B. in Form von Prompts als auch des generierten Outputs zum Lernen genutzt und finden sich mathematisch abgebildet im Sprachmodell wieder.

Um dies so gut wie möglich zu vermeiden, sollten kostenpflichtige Accounts für die Beschäftigten eingerichtet werden. Diese Accounts bieten entscheidende Vorteile, wie erweiterte Konfigurationsmöglichkeiten bezüglich der Verwendung der eingegebenen Daten und zusätzliche Sicherheitsfunktionen.

Eine Nutzung insbesondere der kostenlosen Modelle ist für den Unternehmenseinsatz sowohl aus Gesichtspunkten des Datenschutzes als auch hinsichtlich der Geschäfts- und Betriebsgeheimnisse nicht zu empfehlen.

2. Auswahl des Anbieters von KI-Modellen / Abschluss von datenschutzrechtlichen Vereinbarungen

Durch die Wahl des KI-Anbieters kann ebenfalls ein Zugewinn an Datenschutz erfolgen. So bieten zahlreiche Unternehmen Large Language Modelle an, die auf den bekannten Anbietern wie GPT basieren, aber auf eigenen Servern des Anbieters laufen.
Oftmals bieten diese Unternehmen den Abschluss von datenschutzrechtlichen Vereinbarungen (AVV; Auftragsverarbeitungsvereinbarung; DPA) an. Von dieser Möglichkeit sollte dringend Gebrauch gemacht werden. Ebenfalls sollten immer Anbieter favorisiert werden, die die Datenverarbeitung auf Servern innerhalb der EU beschränken.

Nach der DSGVO ist die Übermittlung personenbezogener Daten in Drittländer nur zulässig, wenn ein angemessenes Schutzniveau garantiert ist. Unternehmen sollten daher stets Anbieter bevorzugen, die ihre Daten ausschließlich auf Servern innerhalb der EU verarbeiten oder durch zusätzliche Maßnahmen, wie Standardvertragsklauseln, den Schutz gewährleisten können.

3. Datenschutzeinstellungen innerhalb des KI-Accounts

In den Einstellungen der KI-Anwendung sind oft zahlreiche Wahlmöglichkeiten bezüglich der Verwendung der eingegebenen Daten zu finden.
Bei der Nutzung von KI-Diensten ist es essenziell, alle möglichen Datenschutzoptionen zu aktivieren und die Einstellungen so datenschutzfreundlich wie möglich zu gestalten. Dazu gehören insbesondere:

- **Deaktivierung der Nutzung zu Trainingszwecken:** Viele Anbieter nutzen Kundendaten, um ihre KI-Modelle weiterzuentwickeln. Dies sollte, sofern möglich, deaktiviert werden.
- **Verhinderung der Weitergabe an Dritte:** Insbesondere im Hinblick auf Geschäftsgeheimnisse sollte die Weitergabe von Daten vollständig ausgeschlossen werden.

4. KI-Schulungen der Mitarbeiter

Ein zentraler Punkt beim Einsatz von Künstlicher Intelligenz ist die Sensibilisierung der Mitarbeiter für potenzielle Risiken. Nur durch regelmäßige Schulungen kann gewährleistet werden, dass Mitarbeiter die Künstliche Intelligenz verantwortungsvoll nutzen und mögliche Fehlerquellen erkennen.
Hierbei sollten insbesondere folgende Themen behandelt werden:

- Grundzüge der DSGVO, insbesondere im Umgang mit personenbezogenen Daten.
- Risiken durch unsachgemäße Nutzung von KI, wie Datenschutzverletzungen, Urheberrechtsverletzungen oder fehlerhafte Entscheidungen.
- Praktische Hinweise zur sicheren Nutzung der eingesetzten KI-Systeme.

Schulungen tragen dazu bei, dass alle Beteiligten ein Grundverständnis für die rechtlichen Anforderungen entwickeln. Hierdurch werden aber auch die Haftungsrisiken des Unternehmens reduziert. Zudem erhöhen Schulungen die Bereitschaft von Mitarbeitern, sich mit dem für alle Unternehmen wichtigen Thema Datenschutz und KI auseinanderzusetzen.

5. Erstellung von KI-Richtlinien

Eine klare unternehmensinterne Richtlinie zum Einsatz von Künstlicher Intelligenz führt weiter zu einem sicheren Umgang mit KI-Anwendungen. Solche Richtlinien sollten dabei insbesondere folgende Punkte regeln:

- Verbot der Nutzung kostenloser / privater Accounts
- Allgemeine Nutzungsprinzipien der KI-Systeme
- Zulässige und unzulässige Anwendungsbereiche / Nutzungen
- Umgang mit sensiblen Daten, insbesondere im Hinblick auf DSGVO-Vorgaben und Geschäftsgeheimnisse

Fazit: Künstliche Intelligenz in Unternehmen rechtssicher nutzen

Der Einsatz von Künstlicher Intelligenz ist auch für kleine und mittelständische Unternehmen mit überschaubaren Ressourcen möglich, wenn grundlegende rechtliche und organisatorische Maßnahmen beachtet werden. Die EU-KI-Verordnung und die DSGVO setzen Rahmenbedingungen, deren Einhaltung nicht nur Pflicht ist, sondern auch das Vertrauen von Kunden und Geschäftspartnern stärkt. Mit einer gezielten Vorbereitung, der Nutzung von kostenpflichtigen Accounts, abgeschlossenen Instanzen und datenschutzkonformen Einstellungen sowie durch Schulungen und Richtlinien können kleine und mittelständische Unternehmen bereits einiges unternehmen, um die Chancen der Künstlichen Intelligenz zu nutzen und dennoch rechtliche Risiken zu minimieren.