LEGAL UPDATE KÜNSTLICHE INTELLIGENZ

Frankfurt am Main, 14.03.2025

KI-Richtlinien als Teil der KI-Governance

Dr. Valentin Zipfel

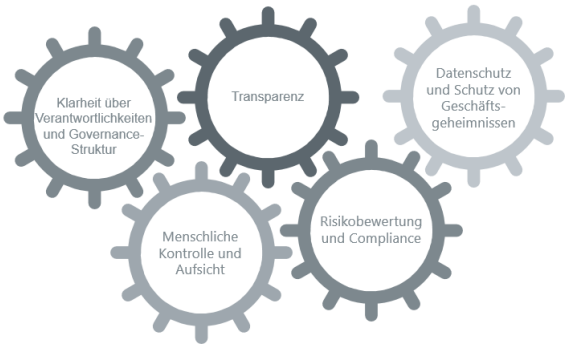
Der Einsatz Künstlicher Intelligenz (KI) in Unternehmen nimmt rasant zu. Ob in der Automatisierung von Geschäftsprozessen, der Analyse großer Datenmengen oder im Kundenservice – KI-Technologien bieten erhebliche Effizienzgewinne und neue Möglichkeiten der Wertschöpfung. Doch mit diesen Chancen gehen auch Risiken einher: Fehlerhafte Ergebnisse der KI, Verstöße gegen Datenschutzvorgaben oder mangelnde Transparenz in Entscheidungsprozessen können rechtliche Herausforderungen mit sich bringen.

Angesichts dieser Dynamik ist es für Unternehmen essenziell, eine klare und durchdachte Richtlinie zum Einsatz von KI (KI-Richtlinie) zu etablieren. Derartige Richtlinien schaffen nicht nur Rechtssicherheit und minimieren Haftungsrisiken. Vielmehr sorgen sie auch für einheitliche Standards im Umgang mit KI-Technologien. Übergeordnet tragen sie dazu bei, das Vertrauen von Geschäftspartnern und Kunden, aber auch von Mitarbeitenden in die mithilfe von KI erzielten Ergebnisse zu stärken.

Doch welche Inhalte sollte eine KI-Richtlinie umfassen? Welche rechtlichen Rahmenbedingungen sind zu beachten? Und wie kann eine KI-Richtlinie wirksam in die Unternehmenspraxis integriert werden? Dieses Legal Update gibt einen Überblick über die wesentlichen Bestandteile einer KI-Richtlinie und zeigt ihre Bedeutung für eine erfolgreiche KI-Governance auf.

Zielsetzung und Anwendungsbereich einer KI-Richtlinie

Eine KI-Richtlinie hat das Ziel, die Grenzen der rechtlich zulässigen Nutzung von KI-Technologien unter gleichzeitiger Berücksichtigung der Unternehmensziele und -strategie zu regeln. Ihrem Zweck entsprechend sollte eine KI-Richtlinie für alle Mitarbeitenden und Abteilungen gelten, die in irgendeiner Weise mit KI-Systemen arbeiten oder deren Ergebnisse nutzen. Es sollten klare Angaben getroffen werden, welche KI-Anwendungen (un-)zulässig sind und in welcher Form diese genutzt werden dürfen (z.B. nur über freigegebene Unternehmensaccounts). Außerdem sollte sich eine KI-Richtlinie auf den gesamten „KI-Lebenszyklus“ erstrecken (von der Planung über die Entwicklung, die Implementierung sowie Nutzung von KI einschließlich ihrer Deaktivierung) und sämtliche Nutzungsformen erfassen.



Verantwortlichkeiten und Governance-Struktur

Ein effektives KI-Management erfordert eine klare Zuordnung von Zuständigkeiten. In der KI-Richtlinie sollten deshalb die Verantwortlichkeiten im Zusammenhang mit dem Einsatz von KI geregelt werden. Die Unternehmensführung (Vorstand, Geschäftsführung, ggfs. auch einzelne Ressorts) trägt die Gesamtverantwortung für die Nutzung von KI. Sie muss sicherstellen, dass KI in Einklang mit den strategischen und operativen Unternehmenszielen eingesetzt wird. Außerdem ist sie für die Einhaltung der rechtlichen Anforderungen verantwortlich.

Daneben sollte – abhängig von der jeweiligen Unternehmensgröße – ein KI-Verantwortlicher bzw. ein entsprechendes Expertenteam benannt werden, der / das für die Implementierung, Überwachung und Bewertung von KI-Systemen zuständig ist. Diese Person sollte idealerweise über Schnittstellenkompetenzen in den Bereichen Datenschutz und Compliance, IT-Sicherheit sowie den insofern maßgeblichen Bestimmungen verfügen bzw. aus Mitgliedern besetzt sein, die diese Disziplinen abdecken.

Auch die Mitarbeitenden spielen eine wesentliche Rolle. Sie sollten zur Einhaltung der KI-Richtlinie verpflichtet werden. Sensibilisierung und Schulungen tragen zudem dazu bei, das Bewusstsein für die Chancen und Herausforderungen von KI geschärft werden.

Grundsätze für den verantwortungsvollen Einsatz von KI

Um eine verantwortungsvolle Nutzung von KI sicherzustellen, sollten Unternehmen einige grundlegende Prinzipien in ihrer KI-Richtlinie regeln. Transparenz ist ein entscheidender Faktor: Mitarbeitende und betroffene Stakeholder müssen nachvollziehen können, wie KI-gestützte Entscheidungen zustande kommen. Daher ist eine umfassende Dokumentation dieser Prozesse erforderlich.

Ein weiterer zentraler Grundsatz ist die menschliche Kontrolle. Relevante Entscheidungen dürfen nicht ausschließlich von / durch KI getroffen werden. Dies gilt insbesondere in den Konstellationen, in denen die Entscheidung für die betroffene Person weitreichende Auswirkungen hat oder besonders sensible Bereiche betroffen sein können (z.B. Kreditvergabe). Insofern ist erforderlich, dass stets eine menschliche Instanz in den Entscheidungsprozess eingebunden bleibt, um mögliche Fehler, Verzerrungen sowie Halluzinationen der KI zu identifizieren und zu korrigieren.

In einer KI-Richtlinie sollte ebenfalls geregelt werden, wie KI-Tools gegen Missbrauch und unbefugte Zugriffe Dritter geschützt sind bzw. welche Maßnahmen Mitarbeitende insofern ergreifen können.

Wesentlicher Bestandteil einer KI-Richtlinie ist außerdem der Umgang mit teilweise in den KI-Systemen angelegten und möglichen durch KI erzeugten Diskriminierungen. Datensätze müssen deshalb auf Verzerrungen („Bias“) geprüft und etwaige Fehler beseitigt werden, um sicherzustellen, dass keine (un-)bewussten Vorurteile die KI-Ergebnisse beeinflussen. Im laufenden Betrieb sollten KI-Tools regelmäßig auf mögliche Bias überprüft und ggfs. angepasst werden, um eine faire und unvoreingenommene Entscheidungsfindung zu gewährleisten.

Datenschutz und Schutz von Geschäftsgeheimnissen

Im Mittelpunkt einer KI-Richtlinie sollte außerdem die Sicherstellung von Datenschutz sowie der Schutz von Geschäftsgeheimnissen sein.

Unternehmen müssen klare Regeln für den Umgang mit sensiblen Daten definieren. Dazu gehört, dass KI-Systeme ausschließlich mit genehmigten und datenschutzkonformen Technologien betrieben werden dürfen. Mitarbeitende sollten verpflichtet werden, keine personenbezogenen Daten in externe KI-Tools einzugeben. Zusätzlich sollte eine KI-Richtlinie Maßnahmen zur Datenminimierung enthalten. Wo immer möglich, sollten personenbezogene Daten pseudonymisiert oder anonymisiert werden, um das Risiko von Datenschutzverletzungen zu minimieren.

Ebenfalls ist zu regeln, ob und, falls ja, in welchen Fällen Mitarbeitende unternehmens- und kundenbezogene Daten in die KI-Systeme eingeben dürfen. Um Geschäftsgeheimnisse des Unternehmens zu schützen, sollten insoweit klare Anforderungen formuliert werden.

Risikobewertung und Compliance

Vor der Einführung von KI-Systemen sollte eine umfassende Risikobewertung durchgeführt werden. Unternehmen sollten dabei insbesondere prüfen, ob durch den Einsatz der KI potenzielle rechtliche, ethische oder sicherheitsrechtliche Risiken entstehen könnten. Eine detaillierte Analyse möglicher Rechtsverletzungen sowie eine Bewertung der eingesetzten KI-Systeme mit Blick auf Verzerrungen, Halluzinationen oder fehlerhafte Annahmen sind essenziell.

Die Zuverlässigkeit und Genauigkeit der von den KI-Systemen erzeugten Ergebnisse sollte kontinuierlich überwacht werden, um Fehlinformationen oder Fehlentscheidungen zu vermeiden. Zudem ist es ratsam, interne und externe Compliance-Anforderungen regelmäßig zu überprüfen und sicherzustellen, dass sämtliche KI-Anwendungen den jeweils relevanten gesetzlichen Anforderungen (KI-VO, DS-GVO, IT-Sicherheitsrecht, UrhG usw.) entsprechen.

Empfehlung

Die Implementierung einer KI-Richtlinie ist für Unternehmen unerlässlich, um die Vorteile von KI effektiv und verantwortungsvoll zu nutzen. Eine strukturierte KI-Richtlinie stellt sicher, dass KI im Einklang mit rechtlichen Anforderungen eingesetzt wird und langfristig einen positiven Beitrag zur Unternehmensentwicklung leistet.

Abhängig von der Unternehmensgröße und den Strukturen ist eine Beteiligung / Einbindung des Betriebsrats bei der Einführung entsprechender Richtlinien ggfs. erforderlich. Das sollten Unternehmen im Einzelfall prüfen.

Darüber hinaus stellt eine KI-Richtlinie gewissermaßen nur einen Baustein einer erfolgreichen KI-Governance dar. Aufbauend auf den in der KI-Richtlinie festgehaltenen Anforderungen an die Nutzung von KI sollten die Mitarbeitenden regelmäßig geschult werden. Es sollten grundlegende Kenntnisse über die Funktionsweise von KI, ihre Chancen und Risiken, aber auch die relevanten rechtlichen Vorgaben vermittelt werden. Ziel ist es, Mitarbeitende in die Lage zu versetzen, KI-gestützte Prozesse kritisch zu hinterfragen und verantwortungsbewusst mit diesen umzugehen.

Um den sicheren Einsatz von KI langfristig zu gewährleisten, empfehlen wir Unternehmen außerdem, die Zuständigkeiten und Verantwortlichkeiten innerhalb des Unternehmens klar zu definieren. Wie bereits angeklungen, sollten Unternehmen des Weiteren als Teil der KI-Governance ein KI-Register einführen, in dem die eingesetzten KI-Tools einer Risikobewertung unterzogen und mögliche Gefahren klassifiziert werden. Gerne unterstützen wir Sie bei der Implementierung entsprechender KI-Governance-Strukturen.

Hinweis
Dieser Überblick dient ausschließlich der allgemeinen Information und kann konkreten Rechtsrat im einzelnen Fall nicht ersetzen. Sprechen Sie bei Fragen bitte Ihren gewohnten Ansprechpartner bei GÖRG bzw. die Autoren Dilan Mienert unter +49 30 884503-146 oder dmienert@goerg.de oder Viktoria von Pfeil unter +49 30 884503-224 oder vvonpfeil@goerg.de an. Informationen zum Autor finden Sie auf unserer Homepage www.goerg.de.

Wir verwenden das generische Maskulinum und sehen von einer Nennung aller Geschlechtsidentitäten ab, damit dieser Text besser lesbar ist, und meinen damit ausdrücklich jeden in jeder Geschlechtsidentität.

Unsere Standorte

GÖRG Partnerschaft von Rechtsanwälten mbB

BERLIN
Kantstr. 164, 10623 Berlin
Tel. +49 30 884503-0
Fax +49 30 882715-0

HAMBURG
Alter Wall 20 - 22, 20457 Hamburg
Tel. +49 40 500360-0
Fax +49 40 500360-99

FRANKFURT AM MAIN
Ulmenstr. 30, 60325 Frankfurt am Main
Tel. +49 69 170000-17
Fax +49 69 170000-27

KÖLN
Kennedyplatz 2, 50679 Köln
Tel. +49 221 33660-0
Fax +49 221 33660-80

MÜNCHEN
Prinzregentenstr. 22, 80538 München
Tel. +49 89 3090667-0
Fax +49 89 3090667-90