In vielen kleinen und mittelständischen Unternehmen (KMU) wird Künstliche Intelligenz (KI) bereits eingesetzt – häufig ohne ausdrückliche Entscheidung der Geschäftsführung. Mitarbeitende nutzen KI-Anwendungen, insbesondere Sprachmodelle – sog. Large Language Models – etwa für E-Mails, Präsentationen, Übersetzungen, Recherchen, Auswertungen oder schlimmstenfalls Kundenunterlagen. Nicht selten geschieht dies über frei verfügbare Tools, private Accounts oder ohne klare Vorgaben dazu, wie sich das Unternehmen zum Umgang und Einsatz von KI positioniert.

Für Geschäftsführer oder Unternehmer entsteht daraus konkreter Handlungsbedarf. Der Einsatz von KI kann erhebliche Effizienzgewinne ermöglichen, berührt aber zugleich zentrale rechtliche Verantwortungsbereiche und Compliance-Themen der Geschäftsleitung: Datenschutz, Schutz von Geschäftsgeheimnissen, IT-Sicherheit, Urheberrecht, Arbeitsrecht, Haftung und die Vorgaben des „EU AI Act“ der Europäischen Union. Unternehmen, die KI nutzen oder deren Nutzung dulden, sollten daher verbindliche interne Regeln schaffen.

1. KI-Nutzung ist eine Organisationsaufgabe der Geschäftsleitung

Die Einführung von KI ist nicht lediglich eine technische Frage. Sie betrifft die ordnungsgemäße Organisation des Unternehmens. Die Geschäftsleitung muss sicherstellen, dass rechtliche Risiken erkannt, bewertet und durch geeignete interne Maßnahmen begrenzt werden.

Dies gilt insbesondere dann, wenn Mitarbeitende KI für berufliche Zwecke nutzen und dabei Daten oder vertrauliche Informationen in die „Blackbox“ der Sprachmodelle spülen. Ohne verbindliche Vorgaben besteht das Risiko einer unkontrollierten Schattennutzung, die zu empfindlichen Konsequenzen für das Unternehmen führen kann.

Aus Sicht der Geschäftsleitung sollte daher zunächst geklärt werden: welche KI-Tools bereits genutzt werden, welche Daten verarbeitet werden, ob hierfür Unternehmens- und/oder Privataccounts verwendet werden bzw. welche Nutzungen künftig erlaubt,

eingeschränkt oder ausgeschlossen werden sollen.

2. Datenschutz als ein zentraler Prüfungspunkt

Ein wesentlicher rechtlicher Schwerpunkt liegt im Datenschutz. Sobald personenbezogene Daten in KI-Systeme eingegeben oder dort verarbeitet werden, ist die Datenschutzgrundverordnung (DSGVO) zu beachten.

Zu prüfen sind insbesondere die Rechtsgrundlage der Datenvereinbarung und ob ein Auftragsverarbeitungsvertrag mit Anbieter der Software geschlossen wurde. Bereits vorab lohnt sich der Blick auf möglicherweise kritische Speicherorte und ggf. verbotene Drittlandübermittlungen von Daten. Denn eine zentrale Schwäche der gängigen Sprachmodelle ist die Intransparenz bei der Nutzung, Speicherung und Verarbeitung von Daten und die nahezu nicht vorhandene Möglichkeit, Dateneingaben langfristig nachzuvollziehen oder sie gar rückgängig zu machen.

Besondere Vorsicht ist bei Beschäftigtendaten, Bewerberdaten, Kundendaten sowie sensiblen bzw. vertraulichen Daten geboten. In vielen Fällen wird es nicht ausreichen, Mitarbeitenden allgemein „sorgfältige Nutzung“ vorzugeben. Erforderlich sind viel mehr konkrete Verbote und Freigabeprozesse.

3. Schutz von Geschäftsgeheimnissen und vertraulichen Informationen

Neben personenbezogenen Daten sind vertrauliche Informationen wie Geschäftsgeheimnisse besonders relevant. Angebote, Kalkulationen, Preislisten, Vertragsentwürfe, Strategiepapiere, technische Unterlagen, Quellcode oder Kundenlisten sollten keinesfalls unkontrolliert in KI-Tools eingegeben werden.

Unternehmen müssen angemessene Geheimhaltungsmaßnahmen treffen, wenn sie den Schutz vertraulicher Informationen erhalten wollen. Unternehmensinterne Vorgaben sollten daher ausdrücklich regeln, welche Informationen niemals in nicht freigegebene KI-Systeme

eingegeben werden dürfen.

4. Arbeitsrecht und Mitbestimmung

Besondere rechtliche Anforderungen bestehen beim Einsatz von KI im Beschäftigtenkontext. Das betrifft etwa Bewerberauswahl, Leistungsbewertung, Schichtplanung, Zielkontrolle oder die Analyse von Kommunikationsdaten.

Hier sind Datenschutzrecht, Arbeitsrecht und gegebenenfalls Informations- oder gar Mitbestimmungsrechte eines Betriebsrats zu beachten.

5. Anforderungen des EU AI Act

Der EU AI Act verpflichtet Unternehmen unter anderem dazu, für ein ausreichendes Maß an Kompetenz im Umgang mit KI bei Mitarbeitenden zu sorgen, die zu beruflichen Zwecken mit KI umgehen. Geschäftsführer sollten daher nicht nur eine Richtlinie einführen, sondern im Anschluss entsprechende Kompetenzschulungen vorsehen und diese dokumentieren.

Je nach Einsatzbereich können weitere Pflichten hinzukommen, insbesondere bei Hochrisiko-KI-Systemen. Deshalb sollte vor Einführung neuer KI-Anwendungen geprüft werden, ob der konkrete Anwendungsfall besondere regulatorische Anforderungen auslöst.

6. KI-Richtlinie als zentrales Steuerungsinstrument

Kernstück einer rechtssicheren Einführung sollte ein Code of Conduct oder eine verbindliche KI-Richtlinie sein. Sie sollte kurz, verständlich und praktisch anwendbar sein, zugleich aber die wesentlichen rechtlichen Risiken regeln und gesetzliche Anforderungen erfüllen.

Eine solche Richtlinie sollte insbesondere regeln: welche KI-Tools freigegeben sind, welche Daten dort eingegeben werden dürfen, wann Datenschutzbeauftragter, IT oder

Geschäftsleitung einzubinden sind, wer Ergebnisse prüfen und freigeben muss oder wie Vorfälle zu melden bzw. welche Schulungen verpflichtend sind.

Sinnvoll ist zudem eine fortlaufend gepflegte Tool-Liste mit freigegebenen KI-Anwendungen und zulässigen Nutzungszwecken.

Mitarbeitende sollten durch klare Vorgaben und gezielte Schulungen auf den rechtssicheren Umgang mit KI-Tools angemessen vorbereitet werden.

7. **Praktisches Vorgehen für die Geschäftsleitung**

Für Unternehmen, die bislang keine verbindlichen Vorgaben haben, bietet sich folgendes Vorgehen an:

- bestehende KI-Nutzung erfassen;
- Datenarten und Anwendungsfälle rechtlich bewerten;
- nicht zulässige Nutzungen sofort untersagen;
- freigegebene Tools und zulässige Zwecke definieren;
- KI-Richtlinie erstellen;
- Mitarbeitende schulen;
- Freigabeprozess für neue KI-Anwendungen einführen;
- Umsetzung regelmäßig überprüfen.

Dabei sollte nie der Maßstab sein, den Einsatz von KI bewusst und auf alle Ewigkeit zu verhindern. Ziel ist vielmehr, eine rechtssichere und kontrollierte Nutzung zu ermöglichen und den rechtlichen Pflichten nachzukommen.

Fazit

KI bietet kleinen und mittelständischen Unternehmen erhebliche Chancen. Ohne klare rechtliche Leitplanken entstehen vermeidbare Risiken – insbesondere im Datenschutz, beim Schutz von Geschäftsgeheimnissen, im Arbeitsrecht, im Urheberrecht und im Hinblick auf den EU AI Act.

Geschäftsführer sollten die Nutzung von KI deshalb frühzeitig und proaktiv steuern.

Wir unterstützen KMU bei der rechtssicheren Implementierung von KI-Anwendungen, insbesondere bei der Ausgestaltung unternehmensinterner und verbindlicher Nutzungsrichtlinien.

Wer KI im Unternehmen einsetzen möchte, sollte frühzeitig klare rechtliche Leitplanken schaffen – bevor sensible Daten unkontrolliert verarbeitet werden oder Haftungs-, Datenschutz- und Compliance-Fragen erst im Nachhinein geklärt werden müssen.