
**NEUE SPIELREGELN.** Die EU und der Gesetzgeber in Österreich haben Regelwerke geschaffen, die den Einsatz von KI-Tools in Unternehmen genauestens regulieren – bei Nichtbeachtung drohen harte Strafen.

# Künstliche Intelligenz, reale Gefahren

**Der Einsatz von KI in Unternehmen wird zum Milliardengeschäft. Die Umsetzung muss jedoch strenge rechtliche Vorgaben erfüllen. Wenn diese verletzt werden, drohen ab dem Sommer Millionenstrafen.**

VON **ANDRÉ EXNER**

Künstliche Intelligenz (KI) hat ein enormes Potenzial. Und nicht nur im Backoffice, wie von vielen ursprünglich gedacht: Allein im Handel schätzt das Beratungsunternehmen Strategy& in einer aktuellen Studie das Potenzial für autonome Einkäufe auf ein Volumen von über 100 Milliarden Euro und damit auf 15 Prozent des gesamten E-Commerce-Umsatzes in Europa. Im Bereich Immobilien kommt Morgan Stanley auf 34 Milliarden US-Dollar an KI-bedingten Effizienzeinsparungen allein in den USA. Warum auch nicht? Jenseits des Atlantiks wird laut Complexity Science Hub bereits ein Drittel der Software von KI-Tools geschrieben – vor drei Jahren waren es erst fünf Prozent, und in zwei Jahren sollen es 50 Prozent sein.

Der Boom ist damit schneller und branchenumfassender, als selbst von den optimistischen KI-Befürwortern erhofft wurde. Denn der digitale Kollege ist niemals krank, rund um die Uhr im Einsatz und kann, so zumindest die Versprechen der Anbieter, selbstständig sowie fehlerfrei arbeiten und dank Machine Learning immer besser werden.

**UMFASSENDE REGELUNG.** Die Revolution findet jedoch nicht im rechtsfreien Raum statt. Im Gegenteil: Unternehmen müssen sich vor dem Einsatz von KI genau informieren, was sie dürfen, was sie müssen und was unter keinen Umständen erlaubt ist. Mit EU-Vorgaben wie NIS2 oder AI Act und deren in nationales Recht gegossenen Varianten wie die KI-Verordnung haben die Gesetzgeber ein umfassendes Regelwerk geschaffen, das die Spielregeln für den Einsatz von KI-Tools in Unternehmen vorgibt. Ganz klar ist es jedoch nicht: Bereits bestehendes Recht gilt auch für KI, und manche neuen Regeln überschneiden sich mit bestehenden. Dazu kommt, dass die strenge und für Millionenstrafen berüchtigte Datenschutzgrundverordnung (DSGVO) auch die meisten Bereiche betrifft, wo KI im Einsatz kommt.

„KI-Compliance ist Legal Compliance“, sagt Rechtsanwalt Martin Schiefer, Schiefer Rechtsanwälte: Jeder Schritt auf dem Weg in die KI-Zukunft muss rechtlich genauestens geplant und mit entsprechender Rechtsbegleitung umgesetzt werden. „Wer KI im Unternehmen einsetzt, ist nach dem AI Act Betreiber und hat konkrete Pflichten: Dokumentation, Transparenz, Risikobewertung und nachweisliche Schulung aller Beteiligten“, so Schiefer, der beim renommierten Symposium Lech Impact Ende Juni zum Thema „Wem gehören meine Daten?“ referieren wird. „Gleichzeitig bleibt die DSGVO vollständig anwendbar. Beide Regelwerke müssen bereits seit Monaten parallel erfüllt werden. Das ist kein Zukunftsthema mehr“, sagt der Anwalt.

Die Zeit drängt, sagt auch Andreas Lichtenberger, auf Datenschutzrecht spezialisierter Rechtsanwalt bei CMS ▶

FOTO: GETTY IMAGES

Reich-Rohrwig Hainz Rechtsanwälte: Sobald bei der Nutzung eines KI-Systems personenbezogene Daten verarbeitet werden, sind neben den neuen Regelwerken auch die bestehende DSGVO und das österreichische Datenschutzgesetz anwendbar. Die neue KI-Verordnung gilt parallel, lässt bestehende datenschutzrechtlichen Pflichten aber unberührt. „Ausgangspunkt jeder Prüfung ist daher, ob überhaupt personenbezogene Daten verarbeitet werden", sagt er. „Das ist in der Praxis häufig der Fall. Liegt eine Verarbeitung personenbezogener Daten vor, gelten die allgemeinen Grundsätze des DSGVO uneingeschränkt. Die zentrale Frage lautet daher nicht, ob KI eingesetzt werden darf, sondern welches System zu welchem Zweck mit welchen Daten eingesetzt wird – und auf welcher Rechtsgrundlage." Die KI-Verordnung schreibt zudem neu vor, ein ausreichendes Maß an KI-Kompetenz sicherzustellen – und dafür brauchen Unternehmen Zeit. Die Pflicht gilt bereits seit dem Vorjahr, ihre Überwachung und Durchsetzung wird aber im August „scharf gestellt" – inklusive möglicher Strafen.

„KI-Kompetenz ist dabei nicht auf technische Schulung zu reduzieren", so Lichtenberger. „Erforderlich ist vielmehr ein Mindestverständnis der Funktionsweise und Grenzen der eingesetzten Systeme, der zulässigen und unzulässigen Eingaben, der Risiken fehlerhafter Outputs, der Anforderungen an menschliche Aufsicht sowie der datenschutz-, geheimnis-, arbeits- und gegebenenfalls sektorspezifischen Vorgaben. Sinnvoll ist daher ein gestuftes Schulungsmodell mit vertieften Modulen für Fachbereiche."

**KLARE STRUKTUREN SCHAFFEN.** Unternehmen brauchen bei der KI-Einführung zunächst eine klare Zuständigkeitsstruktur: Der Vorstand muss Grundsatzentscheidungen, Freigabekriterien so-wie Risikotoleranzen festlegen. Dazu braucht es ein operatives Governancemodell mit klaren Prozessen von Toolfreigaben bis zu Datenschutzfolgenabschätzungen und der Dokumentation. Eine verbindliche KI-Richtlinie, eine Positivliste freigegebener Tools, Prompt- und Uploadregeln, ein Eskalationsprozess für sensible Anwendungsfälle, standardisierte Beschaffungs- und Prüffragen für Anbieter, Trainings: Die To-Do-Liste ist lang – und mit Kosten verbunden, die durch den Effizienzgewinn der KI erst einmal verdient werden müssen. Und Punkte von der Liste zu streichen, geht nicht: „Die Verpflichtung zur Erstellung einer technischen Dokumentation besteht zwar nur für Anbieter von Hochrisiko-KI-Systemen und nicht für Betreiber", nennt Lichtenberger ein Beispiel. „Eine interne Dokumentation ist dennoch sehr empfehlenswert, insbesondere zur Nachvollziehbarkeit von Entscheidungen und als Grundlage für einen allfälligen Austausch mit den Behörden."

Die enormen Mengen – meist hochsensibler personenbezogener – Daten müssen dabei mit Vorsicht angefasst werden, so Axel Anderl, Managing Partner bei Dorda, der das IT/IP- Team und die Digital Industries Group der Kanzlei leitet: „Der Einsatz von KI ist kein reines IT- oder Innovations-, sondern stets auch ein Datenschutzprojekt", so Anderl: „Rechtliche Beratung spielt eine zentrale Rolle." Denn KI-Systeme können tief in bestehende Datenverarbeitungen eingreifen – oft ohne dass dies den Verantwortlichen sofort bewusst ist.

Beispiele aus der Praxis sind die Einführung neuer Assistenzsysteme, die eine neue Verarbeitung einführen, die Einbindung von Large-Language-Modellen, und damit ein erweiterter Datenzugriff, oder das Training von KI-Modellen zur Optimierung des Outputs. „Auch bei der Lizenzierung von Dritt-KI-Systemen sind Unternehmen gut beraten, klare vertragliche Leitplanken zu setzen", so Anderl.

> KI-Compliance ist Geschäftsführerpflicht: Fehlt die Governance, fehlen Schulungen und Dokumentation, steht persönliche Haftung im Raum."
>
> **Martin Schiefer, Schiefer Rechtsanwälte**

**VOR DEM NUTZEN RISIKEN KLÄREN.** Auch Schiefer warnt, dass neben dem möglichen Nutzen der KI-Tools stets auch Risiken beachtet werden müssen, um rechtliche Fettnäpfchen zu vermeiden: „AI Act, KI-Verordnung, DSGVO, NIS2 und vertragliche Pflichten erzeugen ein regulatorisches Geflecht, das nur mit rechtlicher Strukturierung beherrschbar ist", so der Anwalt. „KI-Compliance ist Geschäftsführerpflicht: Fehlt Governance, fehlen Schulungen und Dokumentation, steht persönliche Haftung im Raum. Dazu kommt ein praktisches Problem: Wenn Daten einmal bei einem KI-Anbieter in einem Drittland gelandet sind, ist tatsächliche Kontrolle kaum mehr durchsetzbar, Löschungsansprüche laufen ins Leere, Nachverfolgbarkeit bleibt eine zahnlose vertragliche Pflicht am Papier." Vorausschauende rechtliche Strukturierung kann diese Vollstreckungshindernisse zumindest abmildern, etwa durch vertragliche Absicherung der Datenflüsse, klare Löschungsregimes und bewusste Auswahl von Anbietern mit Serverstandort in der EU. Auch wenn das zunächst Geld kostet: Die nachträgliche Bereinigung kommt deutlich teurer.

Lichtenberger nennt eine potenzielle Gefahrenquelle für Unternehmen: Ein KI-Provider gilt nur dann als reiner Auftragsverarbeiter, wenn er Daten ausschließlich auf Weisung des Unternehmens verarbeitet. Verwendet er diese hingegen auch intern, etwa für Produktverbesserung, ist gesondert zu prüfen, ob der Anbieter selbst Verantwortlicher ▶

FOTO: LUKAS ILGNER

oder allenfalls gemeinsam Verantwortlicher ist. „Die Rollenfrage darf daher nicht allein anhand der Vertragsbezeichnung, sondern muss anhand der tatsächlichen Verarbeitung und der Einflussmöglichkeiten auf Zwecke und Mittel beurteilt werden“, so der Anwalt.

**EINDEUTIGE DOS UND DON’TS.** Zu den wesentlichen Dos zählen daher insbesondere die vorgelagerte Dokumentation des konkreten Anwendungsfalls, die Prüfung der datenschutzrechtlichen Rollenverteilung, der Abschluss eines DSGVO-konformen Vertrags, die Deaktivierung eines etwaigen Anbietertrainings mit eingegebenen Daten, die Festlegung klarer Lösch- und Aufbewahrungsfristen sowie die Prüfung, ob eine Datenschutz-Folgenabschätzung erforderlich ist. Ebenso wesentlich ist die Prüfung allfälliger Drittlandtransfers.

Zu den klaren Don’ts zählen der ungeprüfte Einsatz von Gratis- oder Standardversionen generativer KI mit echten Kunden-, Mitarbeiter- oder Bewerberdaten – ChatGPT & Co. mögen zwar gratis sein, Unternehmen können die mit ihrer Verwendung eingesparten Kosten aber teuer zu stehen kommen. Weitere No-Gos betreffen das Einspeisen sensibler Informationen ohne Rechtsgrundlage und ohne technische Schutzmaßnahmen, die Nutzung eines Tools, dessen Anbieter Daten intern weiterverarbeitet, und der Einsatz von KI in der HR zur Entscheidung über Personen mit rechtlicher Wirkung. „Die DSGVO zieht hier enge Grenzen“, so der CMS-Experte. „Maßgeblich ist dabei nicht, ob formal noch ein Mensch eingebunden ist, sondern ob tatsächlich eine eigenständige menschliche Prüfung und Korrekturmöglichkeit besteht.“ Verboten sind zudem bestimmte KI-Praktiken laut der im Sommer scharf gestellten KI-Verordnung wie Social Scoring oder Emotionserkennung am Arbeitsplatz.

Grauzonen gibt es aber auch hier, vor allem in drei Bereichen. Erstens bei der Frage, wann Prompts sensible Daten enthalten. Zweitens bei der datenschutzrechtlichen Rollenverteilung mit externen KI-Anbietern. Drittens bei KI-gestützten Empfehlungen, bei denen in der Praxis oft unklar ist, ob eine bloße Entscheidungshilfe oder eine faktische automatisierte Letztentscheidung vorliegt. KI definiert damit auch die Grenzen des Datenschutzrechts neu: Ein System, das Standortdaten mit dem Kaufverhalten in der Apotheke kombiniert, leitet auch Gesundheitsprognosen ab, ohne dass diese je eingegeben wurden, nennt Schiefer ein Beispiel aus der Praxis. „Legal Compliance heißt deshalb: Nicht nur klassifizieren, was man eingibt, sondern bewerten, welche Erkenntnisse die KI daraus ableiten kann. Mitarbeitende müssen verstehen, dass scheinbar harmlose Daten in den Händen eines KI-Systems zu hochsensiblen Ergebnissen werden.“

> „Bei sensiblen Daten ist ein größerer Fokus darauf zu legen, ob durch den KI-Einsatz eine neue Rechtsgrundlage erforderlich ist.“
>
> **Alexandra Ciarnau, Dorda**

Zu den besonderen Kategorien personenbezogener Daten zählen Angaben zur Gesundheit, zu ethnischer Herkunft, politischen Meinungen, religiösen Überzeugungen, Gewerkschaftszugehörigkeit sowie genetische und biometrische Daten zur eindeutigen Identifizierung, zählt Alexandra Ciarnau, Partnerin und Co-Leiterin der Digital Industries Group bei Dorda, auf. „Deren Verarbeitung unterliegt erhöhten Schutzanforderungen und beschränkt auch mögliche Rechtfertigungen“, so Ciarnau. „Insofern ist bei sensiblen Daten ein größerer Fokus darauf zu legen, ob sich durch den KI-Einsatz die Datenverarbeitung verändert und daher eine neue Rechtsgrundlage erforderlich ist. Hier werden Verantwortliche oft mit einer Einwilligung arbeiten müssen.“

**ENORME STRAFEN DROHEN.** Die Sanktionsrisiken sind erheblich: Bei Verstößen drohen Megastrafen. Nach der DSGVO können schwere Verstöße, insbesondere gegen die Grundsätze der Verarbeitung, die Betroffenenrechte oder behördliche Anordnungen, mit Geldbußen von bis zu 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes geahndet werden, je nachdem, welcher Betrag höher ist. Die KI-Verordnung sieht zum Teil sogar noch härtere Sanktionen vor, die bis zu 35 Millionen Euro oder sieben Prozent des globalen Jahresumsatzes betragen.

Dazu kommt weiterer möglicher Ärger für Unternehmen wie behördliche Untersagungen, Anpassungsanordnungen, Abschaltungen von Systemen, Reputationsschäden und zivilrechtliche Folgen. Selbst Doppelstrafen sind möglich, warnt Anderl, etwa wenn Unternehmen verbotene KI-Praktiken einsetzen, mit denen regelmäßig auch die Verarbeitung personenbezogener Daten einhergeht. „Außerdem sind aus potenziellen Verstößen gegen Urheberrecht, Konsumentenschutz oder Gesetz gegen unlauteren Wettbewerb weitere Sanktionen wie Unterlassungsansprüche, Urteilsveröffentlichungen und doppeltes angemessenes Entgelt denkbar“, sagt er.

„Das österreichische Verwaltungsstrafrecht bestraft jeden Verstoß gesondert und jeden Geschäftsführer persönlich“, weist auch Schiefer hin. Selbst mit einer Strafe ist ein Verstoß also nicht immer abgetan, denn es gibt noch zivilrechtliche Ansprüche auf Schadenersatz und Unterlassung, etwa aufgrund nicht überprüfter KI-generierter Inhalte oder der Verletzung vertraglicher Compliance-Zusiche-

FOTOS: CAIO KAUFFMANN

> Der ‚digitale Omnibus' befindet sich noch im Gesetzgebungsprozess. Unternehmen können sich daher nicht auf diese Erleichterungen berufen."
>
> **Andreas Lichtenberger, CMS Reich-Rohrwig Hainz**

rungen. Der härteste Hebel ist oft gar nicht die Strafe: Ohne dokumentierte KI-Compliance verlieren Unternehmen Zugang zu Großkunden und öffentlichen Aufträgen.

**WARTEN AUF ERLEICHTERUNGEN.** Verständlich, dass viele Unternehmen mit den neuen Rahmenbedingungen gar nicht glücklich sind und Verbände wie IV und WKO laute Kritik äußern. Die EU scheint zuzuhören: Mit dem Entlastungsregelwerk „digitaler Omnibus" hat sie Vereinfachungen versprochen. Bei der KI-Verordnung zielt der „Omnibus" vor allem auf Umsetzungsvereinfachungen. So sollen die Umsetzungspflichten zeitlich entzerrt und stärker an die Verfügbarkeit von Standards, Spezifikationen und unterstützenden Compliance-Instrumenten gekoppelt werden. Zusätzlich werden für KMU Erleichterungen bei Dokumentation, Monitoring und Unterstützung diskutiert. Ein Hoffnungsschimmer am Horizont für die geplagten Unternehmen. Doch der „digitale Omnibus" ist noch kein Recht, wie Lichtenberger hinweist: „Das Verfahren befindet sich noch im Gesetzgebungsprozess. Unternehmen können sich daher nicht auf diese Erleichterungen berufen." Sprich: Wer heute KI einführt, muss auf Basis des bestehenden Rechts agieren, das auch Unklarheiten und Doppelgleisigkeiten enthält.

„Der ‚digitale Omnibus' ist im Bereich des AI Act höchst fragwürdig", resümiert daher Ciarnau: „Der Gesetzesakt wurde gerade erst erlassen und soll schon reformiert werden. Das spricht nicht für die Qualität des initialen Wurfs und stärkt nicht das Vertrauen der Unternehmen." Die KI ist offenbar schneller, als der Gesetzgeber erlaubt – das kann Unternehmen im Ernstfall teuer kommen. T