KI-Tools im Unternehmen einsetzen

Special Dossier

WEKA

Autor

RA Marco S. Meier, MLaw, CIPP/E, Informatiker EFZ, Partner bei Binder Legal KLG und ist spezialisiert auf Informations- und Kommunikationstechnologierecht (ICT). Er berät und vertritt nationale und internationale Mandanten in sämtlichen Bereichen des IT-, Technologie-, Datenschutz-, Cyber-Security- und Immaterialgüterrechts sowie in technologiebezogenen Compliance-Fragen, wie beispielsweise dem Einsatz oder der Entwicklung von künstlicher Intelligenz (KI). Als ausgebildeter Informatiker und Certified International Privacy Professional Europe (CIPP/E) bringt er fundiertes technisches Wissen und praktische Erfahrung in Projekte ein. Er hat umfangreiche Erfahrung in der Umsetzung von Datenschutz-Compliance-Projekten nach Schweizer Recht und der EU-Datenschutz-Grundverordnung. Zudem ist er versiert in Software- und Lizenzfragen sowie Technologie- und Outsourcing-Projekten in diversen Branchen. Die Beilegung von Streitigkeiten im ICT-Bereich sowie die Beratung bezüglich digitaler Marketingaktivitäten sind weitere Schwerpunkte seiner Tätigkeit.

Impressum

KI-Tools im Unternehmen einsetzen
Special Dossier

Autor Marco S. Meier

Projektleitung Ina Görke **Layout/Satz** Sarah Rutschmann **Korrektorat** Margit Bachfischer M.A., Bobingen

WEKA Business Media AG, Hermetschloostrasse 77, 8048 Zürich, Tel. 044 434 88 34
info@weka.ch, www.weka.ch, www.weka-library.ch

Zürich • Kissing • Paris • Wien

SD8128-2162-202508

Inhaltsverzeichnis

1

Einführung

Künstliche Intelligenz (KI) ist seit längerer Zeit das Thema der Stunde. Das ist nachvollziehbar, bietet KI doch unzählige Chancen. Neben den Chancen bestehen selbstredend auch verschiedene Risiken beim Einsatz von KI. Gerade für Unternehmen, welche den Einsatz von KI-Tools planen, ist das Bewusstsein zu den Chancen und Risiken zentral – nicht zuletzt, weil bestimmte Tools gerade «en vogue» sind oder aktuell fast als unverzichtbar wahrgenommen werden. Dadurch kann der Druck im Unternehmen, ein bestimmtes KI-Tool zu beschaffen, rasch hoch werden. Dieser Druck kann die Entscheidungsträger dazu bewegen, die Risikoabwägung zu vernachlässigen, obwohl der Umgang, die Bewertung und das Treffen von risikomindernden Massnahmen bei der Beschaffung von KI-Tools von immanenter Bedeutung sind. Dabei geht es nicht nur um rechtliche Risiken, auf welche sich dieses Dossier fokussiert, sondern auch um andere Risiken wie bespielsweise Reputationsrisiken, Risiken in Bezug auf ethische Fragen, Risiken der Diskriminierung oder das Risiko, von einem Anbieter abhängig zu sein.

«Der Erfolg bei der Schaffung effektiver KI könnte das grösste Ereignis in der Geschichte unserer Zivilisation sein. Oder das letzte, es sei denn, wir lernen, wie man die Risiken vermeidet.» **Stephen Hawking**

Eindrücklich zeigt dies Stephen Hawking mit seiner provokanten Aussage zum Thema KI auf. Die Aussage mag zwar überspitzt sein, sie zeigt aber deutlich auf, dass der verantwortungsvolle Umgang mit Risiken, welche beim Einsatz von KI vorhanden sind, zentral ist und bleibt.

Dieses Dossier befasst sich vorrangig mit den rechtlichen Risiken im Zusammenhang mit der Beschaffung und Nutzung von KI-Tools. Ziel ist es, Unternehmen bei der Identifikation und Minimierung der häufigsten rechtlichen Risiken zu unterstützen und ihnen dabei als praxisorientierter Leitfaden zu dienen. Darüber hinaus bietet das Dossier einen Überblick über verschiedene rechtlich relevante Themenbereiche.

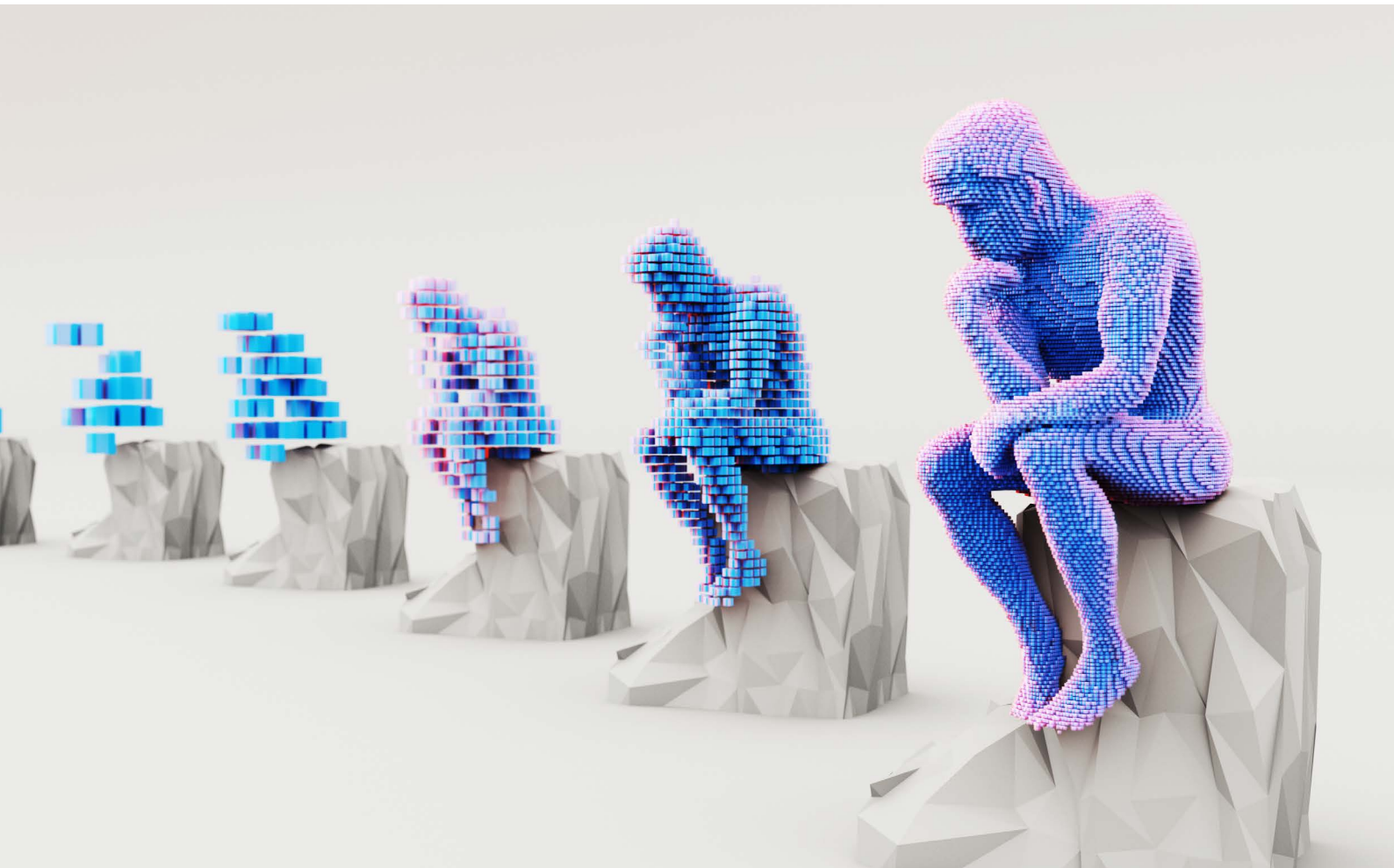
2

Hintergrund

2.1 Kurze Geschichte zu KI

Das Thema der künstlichen Intelligenz beschäftigt die Menschheit schon seit Urzeiten. Seit jeher waren Menschen davon fasziniert, eine nicht menschliche Intelligenz zu erschaffen, welche dem Menschen ähnelt. Beispiele dafür finden sich in den Geschichtsbüchern unzählige. Kreta wurde beispielsweise von Talos, einem Riesen aus Bronze, bewacht, der die Insel jeweils mehrmals täglich umkreiste und Steine auf sich nähernde Schiffe geworfen haben soll. Auch die Literatur oder Filme befassen sich immer wieder mit dem Thema der künstlichen Intelligenz, und das nicht erst, seit KI-Tools im Jahr 2022/2023 im Mainstream angekommen sind.

Obwohl man meinen könnte, dass das Thema KI erst seit Kurzem aktiv erforscht wird, beschäftigt sich die Wissenschaft schon seit den 1950er-Jahren damit, als sich künstliche Intelligenz als eigenständiges Forschungsgebiet der Wissenschaft etablierte. Seit dieser Zeit entwickelte sich die Forschung rund um die künstliche Intelligenz rasant weiter. Nachdem auf KI basierende Systeme den besten Schachspielern der Welt überlegen waren und Quizshows gewannen, zogen später KI-basierte Assistenten wie Alexa in die Wohnungen vieler ein. Der Durchbruch war damit nur noch eine Frage der Zeit, insbesondere deshalb, weil die Weiterentwicklung von KI nicht linear, sondern exponentiell erfolgt. Dank ChatGPT war KI 2022 bzw. 2023 plötzlich in aller Munde, sodass heute ein sich stetig erweiterndes Anwendungsfeld besteht.



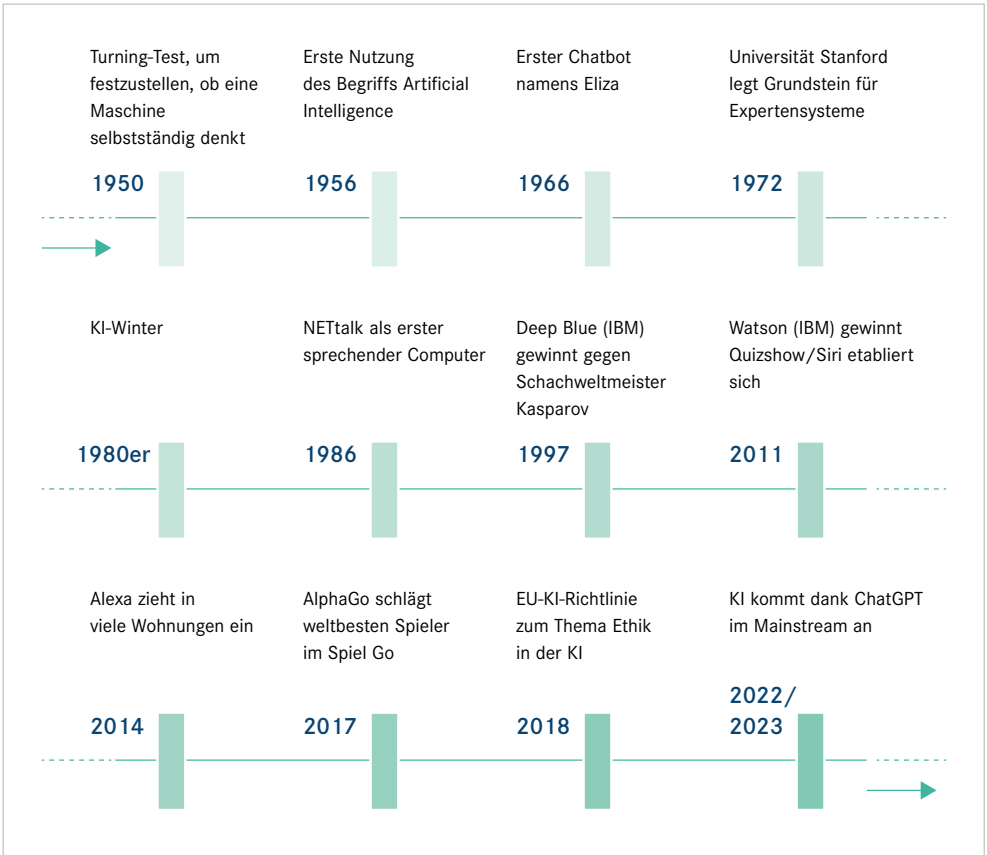


Abbildung 1: Geschichte zu KI

2.2 Der Begriff künstliche Intelligenz

KI ist ein Forschungsteilgebiet, das der Informatik zugeordnet wird, wobei sich zum Begriff KI aus rechtlicher Sicht noch keine einheitliche Definition etabliert hat. In der Wissenschaft enthalten jedoch die meisten Definitionen die klassischen Aspekte, welche im Jahr 1956 durch John McCarthy und einer Gruppe von Wissenschaftlern geprägt wurden. So lässt sich KI als System beschreiben, das Probleme lösen kann, welche üblicherweise menschenähnliche Intelligenz erfordern. Beispiele hierfür sind Fähigkeiten wie Sprachverständnis, logisches Denken, Planen oder Kreativität. Diese Ansichtsweise und der Begriff KI werden teilweise auch als unpassend und reisserisch empfunden, da die «natürliche Intelligenz» der Menschen nicht mit einer maschinellen bzw. mathematisch herbeigeführten Intelligenz verglichen werden sollte (vgl. neuronale Netzwerke). So stellt an dieser Stelle die Definition im EU AI Act (vgl. Kapitel 7) eine wesentlich technischere Umschreibung von KI dar, welche ein umfassenderes Bild vermitteln mag.

Der EU AI Act definiert ein KI-System als *«ein maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie betrieben werden kann und nach seiner Einführung Anpassungsfähigkeit zeigt, und das für explizite oder implizite Ziele aus den Eingaben, die es erhält, ableitet, wie es Ausgaben wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen generieren kann, die physische oder virtuelle Umgebungen beeinflussen können».*

Damit wird KI deutlich breiter beschrieben, als es die übliche wissenschaftliche Definition tut. Der Fokus liegt mithin weniger auf dem Vergleich mit Fähigkeiten der menschlichen Intelligenz. So können bereits einfache statistische Modelle, welche keinerlei menschenähnliche Fähigkeiten aufweisen, unter den KI-Begriff fallen. Dadurch soll sichergestellt werden, dass sämtliche automatisierten «Ableitungssysteme» mit Wirkung auf den Menschen einem Risiko- und Compliance-Rahmen unterliegen. Es bleibt allerdings hervorzuheben, dass diese Definition lediglich im EU-Recht verankert ist. In der Schweiz (sowie in anderen Ländern) besteht noch keine etablierte Definition des Begriffs KI.

2.3 Methoden künstlicher Intelligenz

Um KI besser verständlich zu machen, können die verschiedenen Methoden, inwiefern Wissen in einem Modell repräsentiert wird, beschrieben werden. Nach klassischer wissenschaftlicher Auffassung bezeichnet der Begriff KI alle Technologien, die Maschinen dazu befähigen, Aufgaben zu übernehmen, die normalerweise menschliche Intelligenz erfordern. KI verfolgt dabei nicht das Ziel, den Menschen zu ersetzen, sondern ihn in Entscheidungs-, Analyse- oder Automatisierungsprozessen zu unterstützen – oft schneller, konsistenter und datenbasierter. Die Einteilung bzw. Abstufung erfolgt üblicherweise in vier verschiedene «Schichten», welche jeweils eine Teilmenge der anderen sein können:

- künstliche Intelligenz
- Machine Learning
- Deep Learning
- neuronale Netzwerke

Begriffe Input- und Output-Daten

In diesem Dossier wird der Begriff «Input» dort verwendet, wo eine getrennte Betrachtung wenig sinnvoll und inhaltlich nicht erforderlich ist. Ansonsten wird unterschieden zwischen Promptdaten (Eingabeaufforderung bei der Nutzung eines KI-Tools) und Trainingsdaten (Datenbasis zur Modellentwicklung), welche beide Teile des Inputs sind. Der Begriff «Output» bezeichnet jeweils die vom Modell berechnete Vorhersage bzw. Antwort.