Digitalisierung

FAQ zur Künstlichen Intelligenz (KI)

04.10.2024

Auf einen Blick

- Künstliche Intelligenz verändert Wirtschaft und Gesellschaft grundlegend – mit ihr entstehen aber auch komplexe Fragen.
- Das neue economiesuisse-FAQ liefert Antworten und Orientierung in diesem wichtigen Thema.

Die Bedeutung von Künstlicher Intelligenz (KI) für Wirtschaft und Gesellschaft nimmt stetig zu. Mit ihrem Einsatz entstehen jedoch zahlreiche rechtliche und praktische Fragestellungen. Gemeinsam mit der Anwältin Cornelia Stengel sowie den Anwälten Luca Stäuble und Jonas Tresch hat economiesuisse ein FAQ erstellt. Dieses bietet einen Überblick über zentrale regulatorische und anwendungsbezogene Aspekte der KI.

Rechtlicher Hinweis: Diese Zusammenstellung dient ausschliesslich Informations- und Sensibilisierungszwecken und ersetzt keine Rechtsberatung. economiesuisse übernimmt keine Haftung für Handlungen oder Unterlassungen im Zusammenhang mit der Nutzung dieser Informationen.

Als Ergänzung und Fortführung des nachfolgenden FAQ finden Sie weitere Tools und Informationen unter dem KI-Selbsteinschätzungs-Tool und dem Blog von Kellerhals Carrard.

1. Wie definieren wir KI?

Der Begriff «KI» ist nicht einfach zu definieren, weshalb sich bis heute noch keine einheitliche Umschreibung vollends durchgesetzt hat. Eine mögliche Definition liefert das Europäische Parlament mit der folgenden Formulierung:

«Künstliche Intelligenz ist die Fähigkeit einer Maschine, menschliche Fähigkeiten wie logisches Denken, Lernen, Planen und Kreativität zu imitieren.»

Bei Anwendungsfällen von KI handelt es sich, im Gegensatz zu herkömmlich automatisierten Prozessen, nicht um vorprogrammierte «Wenn-Dann-Schemata», sondern um «lernende» Algorithmen. Entsprechend verlangen auch die meisten Definitionen einen gewissen Grad an Selbstständigkeit und eine Art des Nachempfindens menschlicher Fähigkeiten.

2. Was sind die Chancen von KI?

KI-gestützte Anwendungen bringen zahlreiche Chancen mit sich. Mit ihnen lassen sich insbesondere Effizienz, Produktivität, Verfügbarkeit und Qualität erheblich steigern (z.B. im Rahmen des Marketings, der Kundenbetreuung oder der Compliance). Aufgrund der zahlreichen – und stets neuen – Anwendungsbereiche, ergeben sich mit der technischen Weiterentwicklung von KI ständig neue Vorteile.

3. Was sind die Herausforderungen von KI?

Im Zusammenhang mit KI ergeben sich Herausforderungen, die nicht nur technischer Natur sind, sondern auch ethische, wirtschaftliche und rechtliche Dimensionen berühren. Konkret sind das nicht zuletzt datenschutzrechtliche Risiken, die Gefahr der Diskriminierung, die Verwendung KI-basierter Anwendungen für widerrechtliche Tätigkeiten oder die oftmals fehlende Transparenz. Diesen Herausforderungen ist angesichts einer geplanten Verwendung KI-basierter Technologie stets Rechnung zu tragen.

4. Wie steht es um die Regulierung von KI in der Schweiz?

Die Schweiz sieht aktuell (noch) keine spezifischen Regelungen für die Entwicklung, den Vertrieb oder den Einsatz von KI-gestützten Anwendungen vor. Allerdings hat der Bundesrat das UVEK beauftragt, bis Ende 2024 einen Bericht vorzulegen, der mögliche Ansätze für die Regulierung von KI aufzeigen soll. Es ist also damit zu rechnen, dass die Regulierung von KI auch in der Schweiz Einzug halten wird. Offen ist, in welcher Form diese Regulierung erfolgen wird. Denkbar ist zunächst ein «horizontaler» bzw. branchenübergreifender Ansatz, wie ihn die EU mit der am 1. August 2024 in Kraft getretenen KI-Verordnung («AI Act») kennt. Dieser Ansatz trägt jedoch branchenspezifischen Besonderheiten nicht angemessen Rechnung und ist daher nach Auffassung der Autoren abzulehnen. Vielmehr sollte ein ergebnisorientierter Ansatz verfolgt werden, der nur dort reguliert, wo dies aufgrund einer vorgängigen Risikobeurteilung angezeigt ist.

5. Heisst das, der Einsatz von KI findet aktuell im rechtsfreien Raum statt?

Nein. Die Schweizer Rechtsnormen sind typischerweise so ausgestaltet, dass sie unabhängig von der eingesetzten Technologie Anwendung finden (sog. «Technologieneutralität»). Ein Unternehmen, das beispielsweise Anlageberatungen anbietet, hat die entsprechenden Gesetze (z.B. FIDLEG) auch dann einzuhalten, wenn es die Finanzanalyse KI-gestützt durchführt. Zusätzlich spielen Querschnittsmaterien wie das Datenschutzrecht auch bei KI-Anwendungen eine grosse Rolle.

Ausserdem veröffentlichen die Schweizer Behörden (z.B. die FINMA oder der EDÖB) bereits heute regelmässig Praxishinweise und Auslegungshilfen, um für die Unternehmen die Rechtssicherheit zu erhöhen.

6. Welchen geltenden Bestimmungen ist beim Einsatz von KI besondere Beachtung zu schenken?

In Fällen, wo der Einsatz von generativer KI (z.B. ChatGPT) geplant ist, stellen sich diverse Fragen in Bezug auf das Urheberrecht. So ist etwa für den Entwickler solcher Anwendungen von Bedeutung, welche Daten er als Trainingsdaten verwenden darf. Diese Frage beschäftigt derzeit in vielen Ländern die Justiz und es wird sich zeigen, ob und inwiefern eine einheitliche Lösung zustande kommt. Für den Betreiber der Anwendung stellt sich die Frage, welche Daten er als Inputdaten, d.h. für das «Prompten», verwenden darf. Handelt es sich bei den Inputdaten um urheberrechtlich geschützte Werke (z.B. Texte oder Bilder), so bedarf es hierfür grundsätzlich einer Lizenz. Weiter gilt es zu beachten, dass auch der KI-generierte Output das Urheberrecht Dritter verletzen kann. Diese Frage ist insbesondere dann relevant, wenn der Output Dritten zugänglich gemacht werden soll. Schliesslich stellt sich die Frage, ob bzw. unter welchen Voraussetzungen der KI-generierte Output selbst urheberrechtlichen Schutz geniesst. Für einen urheberrechtlichen Schutz bedarf es einer «geistigen Schöpfung», woran es bei durch KI-generierten Werken regelmässig fehlt. Ausnahmen sind denkbar, wenn der Output die geistige Schöpfung des Betreibers widerspiegelt bzw. lediglich zur geistigen Schöpfung eines Menschen hinzutritt (z.B. bei Übersetzungen). Andere Meinungen sprechen sich unter gewissen Bedingungen für die Anwendung des Urheberrechts auf KI-Anwendungen aus. Sie argumentieren, dass die geistige Schöpfung auch bei KI-generiertem Output vorhanden ist (z.B. durch das Festlegen von Parametern). Aufgrund der dargelegten Unsicherheiten sind Fragen im Einzelfall unter Berücksichtigung der konkreten Umstände zu beurteilen und weitere Entwicklungen zu beobachten.

Weil im Zusammenhang mit dem Einsatz von KI-gestützten Anwendungen regelmässig auch Personendaten bearbeitet werden, ist der Einhaltung des Datenschutzrechts besondere Aufmerksamkeit zu schenken – auch weil die Verletzung gewisser Regelungen des Datenschutzgesetzes (neu) sanktionsbedroht ist (z.B. Informationspflicht).

In Fällen, wo KI-gestützte Anwendungen von einem Dienstleister erbracht werden (z.B. Software as a Service [SaaS]), dieser Dienstleister Zugang zu Personendaten erhält und diese Daten im Auftrag seines Kunden bearbeitet, ist zudem sicherzustellen, dass die erforderlichen Abklärungen in Bezug auf die Gewährleistung der Datensicherheit durchgeführt und die erforderlichen vertraglichen Regelungen mit dem Dienstleister getroffen werden (z.B. Abschluss eines Auftragsbearbeitungsvertrags).

Falls KI-gestützte Anwendungen dazu eingesetzt werden, um (Geschäfts-)Entscheidungen zu treffen, ist jeweils zu prüfen, ob es sich dabei um eine «automatisierte Einzelentscheidung» im Sinne des Datenschutzgesetzes handelt. Eine solche liegt vor, wenn die Entscheidung ausschliesslich auf einer automatisierten Bearbeitung von Personendaten beruht und eine gewisse Komplexität aufweist (z.B. Selektion von Stellenbewerbern oder Kreditentscheid). Das Vorliegen einer solchen Entscheidung kann besondere Informationspflichten mit sich bringen.

Darüber hinaus sind in der Praxis oft weitere sektoriell geltende Bestimmungen zu beachten, welche anhand der Umstände, in der die KI-Anwendung stattfindet, zunächst identifiziert werden müssen.

7. Wie gehe ich vor, wenn ich eine KI-Anwendung einsetzen möchte?

Der Einsatz von KI-Anwendungen kann rasch rechtliche Konsequenzen nach sich ziehen. Dies zeigte auch der Prozess zwischen SVP-Nationalrat Andreas Glarner und Nationalrätin Sibel Arslan (Grüne). Andreas Glarner veröffentlichte ein mithilfe von KI modifiziertes Video der Nationalrätin, wie sie u.a. dazu aufruft, den SVP-Nationalrat zu wählen. Nationalrätin Sibel Arslan hat im Anschluss rechtliche Schritte eingeleitet und Recht erhalten.

Um negativen Folgen vorzubeugen, sollte vor dem Einsatz einer KI-Anwendung stets eine Risikoanalyse erfolgen. Dabei ist unter anderem zu prüfen, ob die Anwendung zuverlässige, nicht-diskriminierende Resultate liefert, ob der Anbieter der fraglichen Anwendung die Datensicherheit gewährleisten kann und ob die Nutzungsrechte an den allfälligen Input- und Output-Daten geregelt sind. Weitere Punkte, die mit dem Anbieter zu regeln sind, betreffen insbesondere die Geheimhaltung in Bezug auf Geschäftsgeheimnisse sowie Haftungsfragen.

Es empfiehlt sich, ein Verzeichnis über die KI-Anwendungen zu führen, die im Unternehmen im Einsatz sind. Darin können etwa die internen Zuständigkeiten und die getroffenen (vertraglichen) Massnahmen (z.B. in Bezug auf die Datensicherheit) festgehalten werden. Ein solches Verzeichnis lässt sich ggfs. auch in ein allfälliges vorbestehendes Verzeichnis über die Bearbeitung von Personendaten («Bearbeitungsverzeichnis») integrieren.

Schliesslich sollte geprüft werden, ob der Einsatz der KI-Anwendung vom Geltungsbereich des AI Act erfasst ist. Sollte Unsicherheit betreffend die Rolle ihres Unternehmens unter dem AI Act bestehen, besuchen Sie das KI-Selbsteinschätzungs-Tool. Unter Umständen – insbesondere beim Einsatz von «Hochrisiko-KI-Systemen» – unterliegt Ihr Unternehmen strengen Compliance-Anforderungen.

8. Wie ist die Rechtslage in der EU und inwiefern sind Schweizer Unternehmen betroffen?

a. Was ist der Zweck und der Regelungsinhalt des EU AI Act?

Mit dem AI Act (in Kraft seit 1. August 2024) beabsichtigt die EU, die Entwicklung und den Einsatz von KI-Systemen zu fördern und gleichzeitig die Risiken für die Gesundheit, Sicherheit und Grundrechte zu minimieren.

Der AI Act verfolgt einen risikobasierten Ansatz zur Regulierung von KI-Systemen. Wie hoch das Risiko im Einzelfall ist und welche Verpflichtungen entsprechend eingehalten werden müssen, gilt es im Detail abzuklären.

Der AI Act unterscheidet grundsätzlich zwischen den folgenden Risikokategorien:

- Verbotene KI-Praktiken (z.B. Social Scoring): Solche KI-Systeme dürften nicht eingesetzt werden.
- Hochrisiko-KI-Systeme: Solche KI-Systeme unterliegen spezifischen Anforderungen im Rahmen eines Risikomanagementsystems. Die entsprechenden Pflichten treffen primär die Anbieter des KI-Systems. Einige Pflichten adressieren hingegen auch die Betreiber des Systems.
- KI-Systeme mit begrenztem Risiko: Insbesondere KI-Systeme, die mit betroffenen Personen interagieren (z.B. Chatbots) sowie generative KI-Systeme unterliegen gewissen Transparenzpflichten.

— KI-Systeme mit minimalem Risiko: Sie sind vom Geltungsbereich des AI Act ausgenommen.

Der AI Act ist am 1. August 2024 in Kraft getreten, sieht für die Umsetzung der Vorgaben jedoch verschieden Übergangsfristen vor: Für die Regelung zu den verbotenen KI-Praktiken gilt eine kurze Übergangsfrist von sechs Monaten. Die Umsetzung der Anforderungen an Hochrisiko-KI-Systeme hat innerhalb von 36 Monaten zu erfolgen. Für die übrigen Vorgaben gilt eine Frist von 24 Monaten.

b. Für wen gilt der AI Act grundsätzlich?

Der AI Act erfasst primär Anbieter und Betreiber von KI-Systemen. Als Anbieter gelten Personen bzw. Unternehmen, die AI-Systeme entwickeln und auf den EU-Markt bringen; als Betreiber gelten Personen bzw. Unternehmen, welche solche Systeme in eigener Verantwortung verwenden. Der persönliche, nicht-berufliche Bereich ist hingegen nicht erfasst.

c. Gilt der AI Act auch für Personen bzw. Unternehmen in der Schweiz?

Der AI Act hat – wie die DSGVO – einen extraterritorialen Geltungsbereich. Das bedeutet, dass auch Anbieter und Betreiber von KI-Systemen in Drittstaaten wie der Schweiz von der Verordnung erfasst werden können, wenn das betreffende KI-System innerhalb der EU genutzt wird oder das vom KI-System erzeugte Ergebnis («Output») innerhalb der EU verwendet wird.

Unternehmen in der Schweiz werden mit Blick auf die von ihnen eingesetzten KI-Systeme im Einzelfall prüfen müssen, ob ein solcher «Link» zum EU-Raum gegeben ist. Besuchen Sie hierzu das KI-Selbsteinschätzungs-Tool.

9. Fallbeispiel I: Werbekampagne durch KI

Ich bin für die Werbekampagne eines neuen Produkts verantwortlich und möchte durch die Verwendung einer generativen KI-Anwendung ein Plakat mit Bild und Werbeslogan erstellen. Was muss ich dabei beachten?

Zunächst sollte betriebsintern abgeklärt werden, ob spezifische Richtlinien für die Beschaffung und/oder den Einsatz von KI-Anwendungen existieren. Falls nicht, sollte das Projekt als Anlass genommen werden, eine zweckmässige AI Governance im Unternehmen zu implementieren, wozu insbesondere das Festlegen von Verantwortlichkeiten und Prozessen gehört (Stichwort «Weisungswesen»).

Bei der Auswahl des Dienstleisters der KI-Anwendung sollten unter anderem folgende Punkte zwingend beachtet werden:

- Räumt der Dienstleister unserem Unternehmen die notwendigen Immaterialgüterrechte bzw. das Recht zur kommerziellen Nutzung des von der KI-Anwendung generierten Outputs (Plakat-Design, Slogan etc.) ein?
- Falls im Rahmen der Nutzung der KI-Anwendung Personendaten (z.B. von unseren Kunden oder Mitarbeitenden) als Inputdaten erforderlich sind: Gewährleistet der Dienstleister die Datensicherheit (Vertraulichkeit, Integrität und Verfügbarkeit der betroffenen Personendaten) und besteht ein schriftlicher Auftragsbearbeitungsvertrag (sog. «ADV») nach Massgabe des anwendbaren Datenschutzrechts (DSG und ggfs. DSGVO)?
- Falls unsere Geschäftsdaten (z.B. Know-how) als Inputdaten erforderlich sind: Gewährleistet der Dienstleister die Geheimhaltung in Bezug auf unsere Geschäftsgeheimnisse?

Falls in Bezug auf den Einsatz der KI-Anwendung der AI Act zur Anwendung gelangen sollte (vgl. oben Frage 8; z.B. weil die Kampagne auch in der EU durchgeführt wird und somit der Output in der EU verwendet wird), gilt Folgendes: Falls es sich beim Plakat um einen Bildinhalt handelt, der einen sog. «Deepfake» (d.h. täuschend echt wirkendes Bildmaterial) darstellt, ist offenzulegen, dass dieser Inhalt künstlich erzeugt oder manipuliert wurde. Diese Information muss den betroffenen natürlichen Personen (d.h. im Falle der Werbekampagne der Öffentlichkeit) spätestens im Zeitpunkt der ersten Darstellung in klarer und erkennbarer Weise zur Kenntnis gebracht werden.

Für Unternehmen in der Schweiz, die nicht unter den AI Act fallen, sieht das geltende schweizerische Recht keine explizite Pflicht vor, einen entsprechenden Hinweis anzubringen. Falls also die Werbekampagne ausschliesslich an Personen in der Schweiz gerichtet ist, dürfte der AI Act nicht anwendbar sein. Allerdings verlangt der EDÖB von den Unternehmen, dass der Einsatz von Systemen, die Deepfakes ermöglichen, den betroffenen Personen gegenüber stets deutlich erkennbar gemacht wird. Zudem können auch lauterkeitsrechtliche Vorgaben eine Kennzeichnung erforderlich machen.

10. Fallbeispiel II: Automatisierte Entscheidungen im Rekrutierungsprozess

Ich bin für die Beschaffung und Einführung eines betriebseigenen KI-Systems verantwortlich, welches im Rahmen unseres Rekrutierungsprozesses eine KI-unterstützte Vorauswahl der eingereichten Bewerbungen aus Deutschland, Liechtenstein und der Schweiz vornimmt, uns passende Profile vorschlägt und die Bewerber und Bewerberinnen über den weiteren Rekrutierungsprozess informiert. Die übrigen Bewerbungen erhalten automatisch einen negativen Bescheid. Obliegen uns besondere Pflichten?

Um allfällige Pflichten mit Blick auf den allenfalls anwendbaren AI Act zu eruieren, bedarf es anfänglich folgender Prüfung: (1) Die Rolle Ihres Unternehmens im Rahmen der KI-Anwendung, (2) Das Vorhandensein des erforderlichen EU-Bezugs und (3) Die Risikokategorie der KI-Anwendung. Da es sich beim AI Act um ein komplexes Regelwerk handelt, ist der Beizug von Rechtsexperten zur Beurteilung dieser Fragen empfehlenswert.

- 1. Als Anbieter gilt und dadurch dem AI Act unterstellt ist insbesondere, wer ein KI-System entwickelt oder entwickeln lässt und es unter eigenem Namen oder eigener Handelsmarke (in der EU) in Verkehr setzt oder in Betrieb nimmt. Falls die KI-Anwendung nach den spezifischen Bedürfnissen und den Instruktionen Ihres Unternehmens von einem Dritten entwickelt wird, dürfte die Entwicklertätigkeit Ihrem Unternehmen zugerechnet werden. Andererseits kann, falls Ihr Unternehmen ein bestehendes KI-System «einkauft» bzw. nur in Bezug auf dessen Darstellung an das Corporate Design anpasst, der Standpunkt vertreten werden, dass damit keine Entwicklertätigkeit vorliegt. Obwohl die Rolle als Anbieter ohne eine Inverkehrsetzung oder Inbetriebnahme in der EU gemäss AI Act streng genommen nicht vorgesehen ist, widerspricht dieser Wortlaut dem klaren Willen des europäischen Gesetzgebers, auch «Anbieter und Betreiber» aus Drittstaaten dem AI Act zu unterstellen, «wenn die vom KI-System hervorgebrachte Ausgabe in der Union verwendet wird». Aufgrund der Differenz zwischen Wortlaut und Wille des Gesetzgebers, sollte vorsichtshalber davon ausgegangen werden, dass auch Unternehmen, die ein KI-System ausserhalb der EU unter eigenem Namen bzw. eigener Handelsmarke in Verkehr setzen oder in Betrieb nehmen, als Anbieter gelten, solange die Ausgabe bzw. der Output des KI-Systems in der EU verwendet wird.
- 2. Im vorliegenden Fall soll das KI-System gemäss seinen Zweckbestimmungen eingegangene Bewerbungen prüfen, geeignete Bewerbungen vorschlagen und ohne weiteres menschliches Zutun Bewerberinnen und Bewerber über einen positiven oder negativen Bescheid informieren. Es ist davon auszugehen, dass mit der erfolgreichen Kommunikation des Bescheids ein «Verwenden» der Ausgabe bzw. des Outputs des KI-Systems in der EU gegeben ist und ein ausreichender EU-Bezug vorliegt. Durch die dargelegte Verwendung der Ausgabe bzw. des Outputs des KI-Systems in der EU sind die Voraussetzungen für die Rolle als Anbieter gegeben und entsprechende Pflichten sind zu beachten.

— 3. Wie umfassend die Pflichten Ihres Unternehmens als Anbieter eines KI-Systems letztendlich sind, hängt nicht zuletzt von der einschlägigen Risikokategorie ab. Den Anbietern von Hochrisiko-KI-Systemen obliegen die umfassendsten Pflichten. Als Fallgruppe von Hochrisiko-KI-Systemen nennt der AI Act unter anderem Systeme, die für die Einstellung oder Auswahl natürlicher Personen verwendet werden sollen und dabei Bewerbungen sichten und filtern. Vorliegend ist genau das die vorgesehene Aufgabe des KI-Systems. Folglich handelt es sich beim geplanten KI-System um ein Hochrisiko-KI-System, womit Ihr Unternehmen umfassende Vorgaben und Pflichten (z.B. Risikomanagement, Data Governance, technische Dokumentation, menschliche Aufsicht, Cybersicherheit, Konformitätsbewertung) einzuhalten hat. Für die Sicherstellung der Compliance bleibt aufgrund der Übergangsfristen zwar noch Zeit, jedoch sollte für die Umsetzung der entsprechenden Massnahmen (Festlegen von Verantwortlichkeiten und Prozessen) ausreichend Zeit eingeplant werden.

Darüber hinaus findet im Rahmen der KI-Anwendung eine DSG- bzw. DSGVO-relevante Datenbearbeitung statt. Das KI-System analysiert eingereichte Bewerbungen – und damit Personendaten – und entscheidet ohne weiteres menschliches Zutun, ob die Bewerbung an Sie weitergeleitet oder ein negativer Bescheid an den Bewerber bzw. die Bewerberin versendet wird. Bei Datenbearbeitungen, die automatisierte Einzelentscheidungen beinhalten, sind unter Umständen besondere Vorgaben zu beachten (z.B. Information über das Recht auf «menschliches Gehör» und das Recht zur Stellungnahme). Weitere Pflichten bleiben vorbehalten.

11. Fallbeispiel III: Chatbot

Ich bin für die Beschaffung und Einführung eines Chatbots auf unserer Webseite verantwortlich. Der Chatbot soll den Nutzerinnen und Nutzern aus der Schweiz und dem Ausland Auskünfte zu unseren Produkten und Dienstleistungen erteilen und einfache Fragen dazu beantworten. Was muss ich hierbei aus regulatorischer Sicht beachten? Die Implementierung des Chatbots auf der Webseite, die (auch) auf Nutzerinnen und Nutzer im EU-Ausland ausgerichtet ist, dürfte vorliegend wohl zur Anwendung des AI Act führen (vgl. zu den Voraussetzungen ***Fallbeispiel II***).

Ein Chatbot stellt per se kein Hochrisiko-KI-System dar, weshalb die entsprechenden Anbieter und Betreiber nicht umfassenden Vorgaben und Pflichten unterstehen. Allerdings haben auch sie gewisse Anforderungen, insbesondere in Bezug auf die Transparenz, zu erfüllen. Der AI Act schreibt vor, dass Personen über die Tatsache, dass sie mit einem KI-Systemen interagieren, informiert werden müssen – sofern dies nicht aufgrund der Umstände offensichtlich ist. Diese Pflicht trifft jedoch lediglich Anbieter, nicht aber den Betreiber. Falls Ihr Unternehmen den Chatbot selbst entwickelt oder entwickeln lässt, müssen Sie im Rahmen der Konzipierung und Entwicklung eine entsprechende Information vorsehen. Kaufen Sie den Chatbot hingegen als «Standardlösung» bei einem Dritten ein, dürfte Ihr Unternehmen unter gewissen Bedingungen lediglich als Betreiber des KI-Systems qualifiziert werde und entsprechend nicht der Transparenzpflicht unterliegen.

Ab wann genau eine Entwicklungstätigkeit und damit eine Anbietereigenschaft im Sinne des AI Act vorliegt, ist (noch) nicht abschliessend klar. Der Frage, inwiefern ein «Standard-Chatbot» eines Anbieters auf die individuellen Bedürfnisse eines Unternehmens angepasst werden kann, ohne dass das Unternehmen infolge dieser Anpassungen selbst zum Anbieter wird, dürfte jedoch eine erhebliche praktische Bedeutung zukommen. Es bestehen zahlreiche Möglichkeiten, ein KI-System auf die individuellen Bedürfnisse eines Unternehmens anzupassen (z.B. Vorgabe von «Prompts», Training auf spezialisierte Daten [sog. «Finetuning»] oder Einsatz von abfragebasierten Modellen [sog. «Retrieval-Augmented Generation»]). Entscheidend dürfte sein, ob durch die Anpassungen das KI-System als solches (weiter-)entwickelt wird. Das könnte beim Finetuning der Fall sein, weil diesfalls in das dem System zugrundliegende Modell eingegriffen wird. Anders könnte hingegen beim RAG argumentiert werden, weil hierbei nicht das KI-System selbst, sondern lediglich die Daten, auf welche im Rahmen der KI-Anwendung zurückgegriffen werden kann, angepasst werden.

Vor der Beschaffung und Einführung des Chatbots sollte – gegebenenfalls gemeinsam mit dem Anbieter – die Frage nach der Anbietereigenschaft und der Wahrnehmung entsprechender Pflichten geklärt werden. Der Chatbot sollte nach seiner Implementierung nicht ohne vorgängige Absprache mit dem Rechtsdienst angepasst werden, weil solche Anpassungen unter Umständen zu einer Änderung der Rolle des Unternehmens (Betreiber wird zum Anbieter) und damit zu zusätzlichen Pflichten führen können. Um in Bezug auf die im Unternehmen eingesetzten KI-Anwendungen und die jeweilige Rolle des

Unternehmens Klarheit zu schaffen, ist das Führen eines Verzeichnisses empfehlenswert. Dieses kann nebst Use Case und Rolle bzw. Pflichten unter dem AI Act auch Angaben zum jeweiligen System-Eigner, Verträgen mit Dritten, Datenbearbeitungen und Risikobeurteilungen enthalten.

Schliesslich ist auch hier der Erlass von Weisungen und/oder Nutzungshinweisen in Bezug auf die Verwendung von KI-Systemen bzw. des Chatbots hilfreich, um Compliance sicherzustellen und die Mitarbeitenden zu sensibilisieren.

Erich Herzog
Bereichsleiter Wettbewerb & Regulatorisches, General Counsel, Mitglied der erweiterten Geschäftsleitung

© economiesuisse | www.economiesuisse.ch