haufe akademie

Whitepaper

Den AI Act verstehen

Rechte und Pflichten kennen

Management Summary

Die KI-Verordnung, auch bekannt als AI Act, legt seit dem 1. August 2024 den rechtlichen Rahmen für Künstliche Intelligenz auf EU-Ebene fest. Ziel ist ein sicherer und ethischer Umgang mit KI. Der AI Act gilt für KI-Systeme, die entwickelt, vertrieben oder genutzt werden. Je nach Risikoklasse (unannehmbar, hoch, begrenzt oder minimal) bestehen unterschiedliche Pflichten für Anbieter, Betreiber und Händler. Bei hohem Risiko ist ein umfangreicher Pflichtenkatalog zu erfüllen, u.a. ein Risikomanagementsystem, eine CE-Kennzeichnung, Transparenzpflichten, Daten-Governance oder auch Meldung von Sicherheitsvorfällen nötig. Das klingt komplex? Wir bringen Licht ins Dunkel und klären was sich hinter dem AI Act verbirgt und welche Pflichten, Anforderungen, aber auch Chancen die Verordnung mit sich bringt.

Inhalt

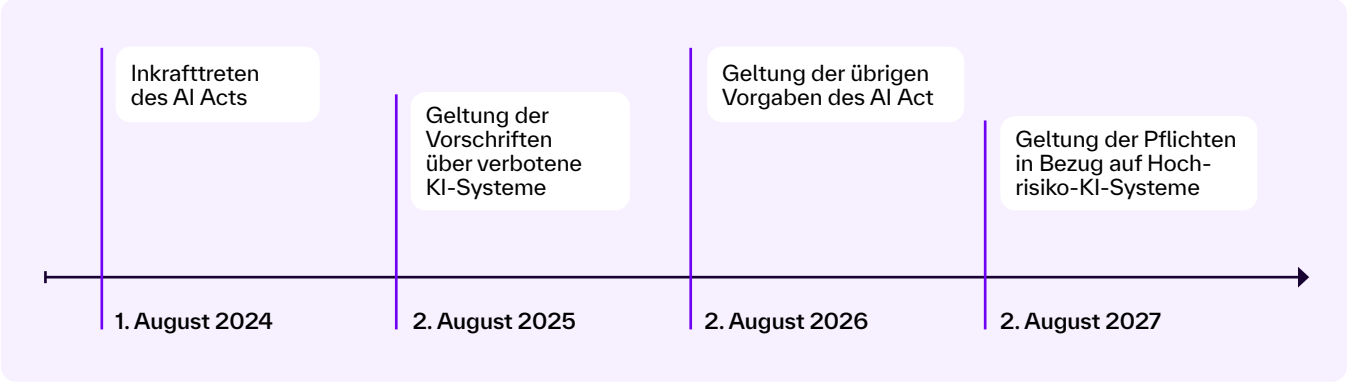
Das ABC des AI Acts

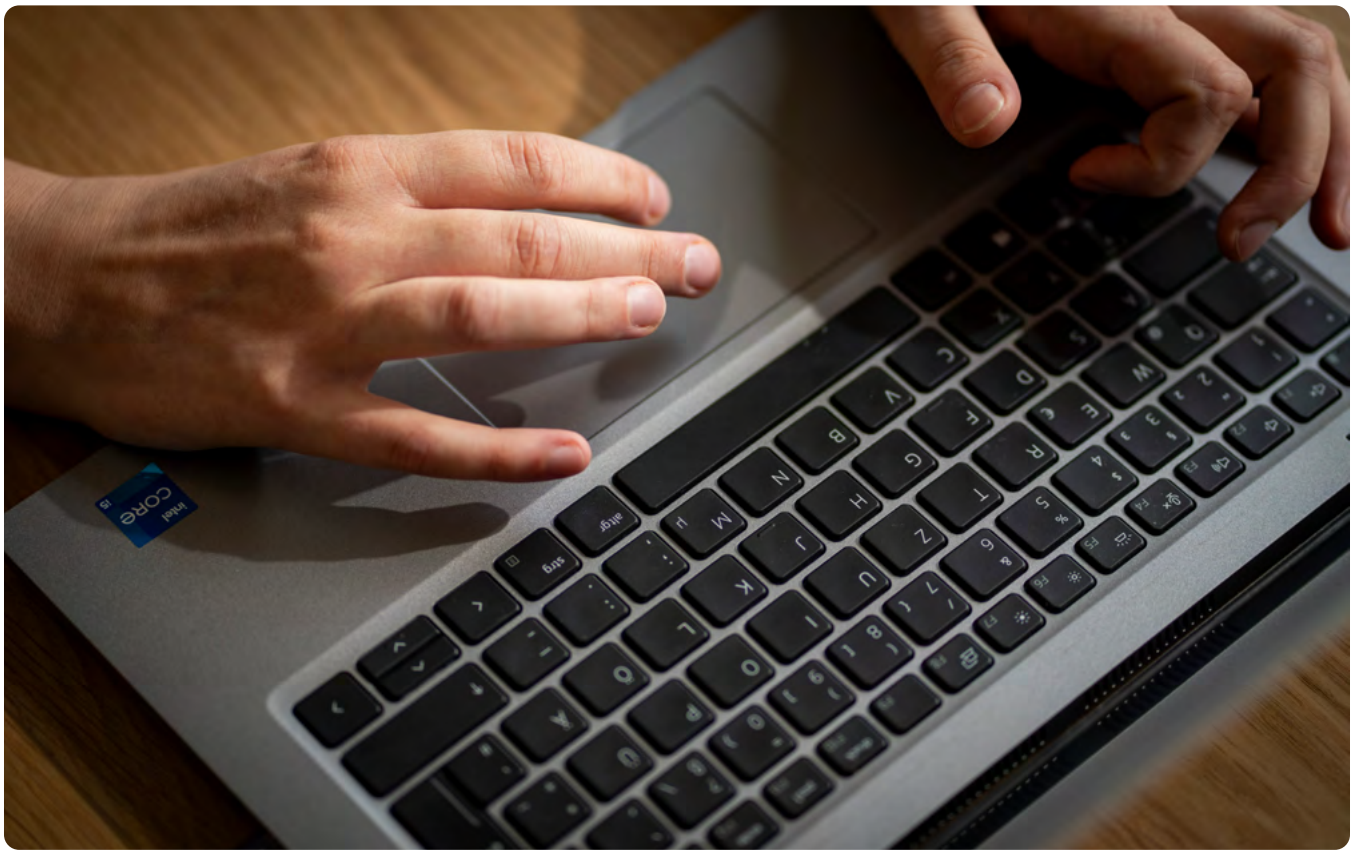
Die Verordnung (EU) 2024/1689 vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz, kurz: KI-Verordnung oder AI Act legt den rechtlichen Rahmen für die Herstellung, den Vertrieb und die Anwendung von Künstlicher Intelligenz (KI) auf EU-Ebene fest. Ziele dieser Verordnung, die als solche unmittelbar in den einzelnen EU-Mitgliedstaaten anwendbar ist, sind insbesondere der sichere und ethische Umgang mit KI. Daher liegen dem AI Act folgende Prinzipien zugrunde:

- menschliches Handeln und menschliche Aufsicht
- technische Robustheit und Sicherheit
- Privatsphäre und Daten-Governance
- Transparenz
- Vielfalt, Nichtdiskriminierung und Fairness
- soziales und ökologisches Wohlergehen
- Rechenschaftspflicht

Im Kern handelt es sich hierbei also um Vorgaben zur Produktregulierung, wie sie auch aus anderen Bereichen bekannt sind (z. B. bei Lebensmitteln oder Kinderspielzeug). Allerdings geht es im AI Act nicht um physische Produkte, sondern um Compliance in Bezug auf Softwareanwendungen, die zumeist als Software-as-a-Service-Angebot oder Cloud-Software verfügbar sind. Zudem sind KI-Systeme, wie ChatGPT, Midjourney, Microsoft Copilot, Stable Diffusion etc. erst seit Herbst 2022 auf dem Markt verfügbar, so dass es sich insoweit noch um eine brandneue Technologie handelt. Inzwischen finden sich solche Anwendungen nahezu in allen Bereichen sowohl im privaten als auch im beruflichen Alltag wieder. Der KI-Siegeszug scheint jedoch gerade erst begonnen zu haben, die Flut an ständig neuen KI-Modell-Versionen, neuen KI-Systemen, neuen Fähigkeiten, neuen Einsatzzwecken sowie verbesserten Ergebnissen ist schier unüberschaubar. Daher ist es also nicht nur sinnvoll, sondern zumindest im geschäftlichen Kontext unerlässlich, sich mit diesem Phänomen unserer Zeit zu befassen.

Es ist aber natürlich nicht verboten, sich jetzt bereits an alle Regelungen des AI Act zu halten. Im Gegenteil: **Je eher man sich mit den gesetzlichen Vorgaben auseinandersetzt und sich auf sie vorbereitet, desto besser.**





Wann ist der AI Act anwendbar?

Allerdings gilt der AI Act nicht automatisch in jedem Fall. Es müssen vielmehr bestimmte Voraussetzungen vorliegen, damit man die sich aus dem AI Act ergebenden Pflichten erfüllen muss. Die Antworten auf die folgenden Fragen geben Auskunft darüber, wer den AI Act in welchem Umfang beachten muss:

1. **Geht es um ein KI-System im Sinne des AI Act?**
2. **Wird dieses KI-System entwickelt, vertrieben oder genutzt?**
3. **In welche Risikoklasse ist das KI-System einzuordnen?**

Nur dann, wenn ein KI-System sowie ein Akteur im Sinne des AI Act gegeben ist, müssen die gesetzlichen Vorgaben beachtet werden. Je höher das dabei bestehende Risiko, desto umfangreicher ist der Pflichtenkatalog, der zu beachten ist.

Hinweis

Für manche Konstellationen ist die Anwendbarkeit des AI Act ausgeschlossen, z. B. für Open-Source-KI oder bei KI-Systemen für militärische Zwecke.

Was ist ein KI-System im Sinne des AI Act?

Um zu verstehen, was genau sich hinter einem solchen KI-System verbirgt, hilft ein Blick auf die Definition nach Art. 3 Abs. 1 AI Act:

„ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können".

Systeme generativer KI, wie ChatGPT & Co., sind daher von einfacheren herkömmlichen Softwaresystemen und Programmierungsansätzen abzugrenzen. Der AI Act sollte sich nicht auf Systeme beziehen, die auf ausschließlich von natürlichen Personen definierten Regeln für das automatische Ausführen von Operationen beruhen.

Die im AI Act enthaltene Definition von „KI-System" ist alles andere als simpel, zudem gibt es dazu weder ausreichend Praxiserfahrung noch einschlägige Rechtsprechung. Daher ist es derzeit sehr umstritten, was genau unter den Anwendungsbereich des AI Act fällt – die Zielrichtung dürfte jedoch klar auf generative KI-System zeigen. Wer also beispielsweise ChatGPT, Midjourney oder Microsoft Copilot in irgendeiner Form nutzen möchte, sollte von der Anwendbarkeit des AI Act ausgehen.

KI-Modell vs. KI-System

In der Verordnung wird zwischen KI-Modellen und KI-Systemen differenziert. Als sog. großes Sprachmodell (engl.: large language model, kurz: LLM) stellt z. B. OpenAI GPT 4 bereit. Darauf basieren dann verschiedene KI-System, wie z. B. ChatGPT oder der Microsoft Copilot. Die Regulierung im AI Act bezieht sich regelmäßig auf KI-Systeme.

Regeln kennen und die Umsetzung meistern

Der AI Act nennt verschiedene Akteure, die die gesetzlichen Anforderungen einhalten müssen:

Anbieter (Art. 3 Nr. 3 AI Act)

Eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich. Es geht hier primär also um Hersteller (z. B. OpenAI, Google, Meta, Anthropic), aber auch um solche Unternehmen, die ein KI-System eines Anbieters einkaufen und es unter einer eigenen Bezeichnung Dritten anbieten. Auch derjenige, der eine KI-Lösung maßgeblich verändert und dann in Verkehr bringt, kann als Anbieter in diesem Sinne gelten.

Betreiber (Art. 3 Nr. 4 AI Act)

Eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet. Es geht also im weitesten Sinne um KI-Nutzer, wie z. B. Unternehmen, die ihren Beschäftigten oder ihrer Kundschaft ein (ggf. individuell angepasstes) KI-System bereitstellen.

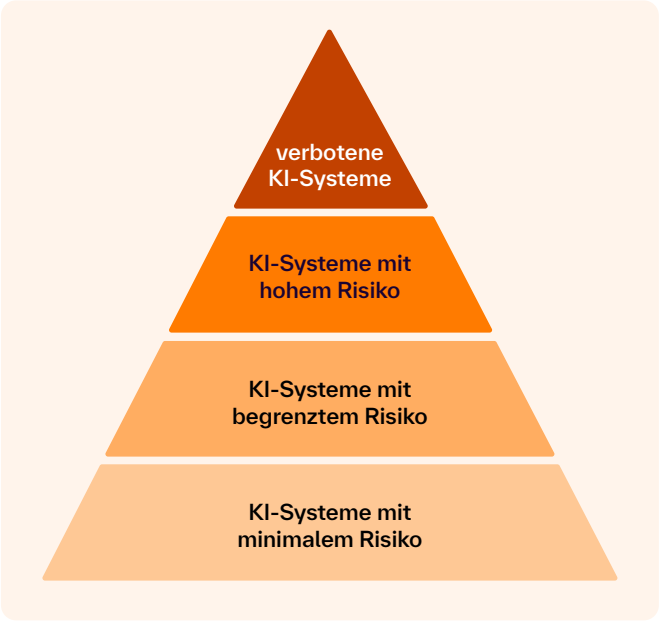
Händler (Art. 3 Nr. 7 AI Act)

Eine natürliche oder juristische Person in der Lieferkette, die ein KI-System auf dem Unionsmarkt bereitstellt, mit Ausnahme des Anbieters oder des Einführers. Dazu zählen etwa KI-Zwischen- oder -Großhändler.

Außerdem tauchen in manchen Vorschriften des AI Act auch „Nutzer“ oder „Produkthersteller“ auf. Als Produkthersteller in diesem Sinne gilt z. B. derjenige, der ein KI-System in ein eigenes Produkt einbindet und dieses Dritten gegenüber anbietet. Nutzer sind alle diejenigen, die KI einsetzen, die also beispielsweise mit Hilfe von ChatGPT Marketingtexte erstellen oder in Midjourney Bilder erzeugen lassen. Darüber hinaus benennt der AI Act auch noch „Bevollmächtigte“, die auf dem Gebiet der EU bestimmte Pflichten für KI-Anbieter erfüllen, sowie „Einführer“, also KI-Importeure.

Risikoklassen kennen

Je nach KI-Risikoklasse und Rolle des Akteurs gelten unterschiedliche Pflichten, hier muss genau in die einzelnen Normen hineingeschaut werden. Der AI Act verfolgt dabei einen risikobasierten Ansatz, d.h. mit steigendem Risiko steigen auch die gesetzlichen Pflichten. Es sind insgesamt vier Risikoklassen vorgesehen, von unannehmbaren über hohe und begrenzte bis hin zu minimalen Risiken. Bei einem unannehmbaren Risiko sieht der AI Act ein Verbot des entsprechenden KI-Systems vor.



Als KI-Systeme mit unannehmbarem Risiko werden insbesondere die folgenden eingestuft:

- unterschwellige Beeinflussung
- Ausnutzung der Schwäche oder Schutzbedürftigkeit von Personen
- biometrische Kategorisierung
- Bewertung des sozialen Verhaltens
- biometrische Echtzeit-Fernidentifizierungssysteme
- Risikobeurteilung von natürlichen Personen
- Datenbanken zur Gesichtserkennung
- Ableitung von Emotionen natürlicher Personen
- Analyse von aufgezeichnetem Bildmaterial

Als Hochrisiko-KI-System zählen hingegen u.a.:

- Biometrische Identifizierung
- Verwaltung und Betrieb kritischer Infrastrukturen (KRITIS)
- Allgemeine und berufliche Bildung
- Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit
- Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen (z. B. Wohnen, Strom, Heizung, Internet, Ärzte)
- Strafverfolgung
- Migration, Asyl und Grenzkontrolle
- Rechtspflege und demokratische Prozesse

Beispiele für KI-Systeme mit begrenztem Risiko sind etwa Chatbots, in die Stufe „minimales Risiko“ fallen hingegen etwa Suchalgorithmen, Computerspiele oder Spam-Filter.

Zusätzlich werden im AI Act auch noch KI-Modelle mit allgemeinem Verwendungszweck (engl.: general purpose AI, kurz: GPAI) adressiert. Damit sind große Sprachmodelle, wie etwa GPT von OpenAI, gemeint. Denn damit wird nicht ein bestimmter Einsatzzweck verfolgt, sie können vielmehr von Kochrezepten über Schulaufsätze bis hin zu Programmcode vielen verschiedenen Zwecken dienen. Aber auch bei GPAI richten sich die gesetzlichen Pflichten nach dem Risikopotential des jeweiligen konkreten Einsatzzwecks.

Pflichten des AI Act

Die meisten Pflichten müssen bei KI-Systemen der Hochrisikoklasse erfüllt werden. Dazu gehören insbesondere:

- Beachtung des Stands der Technik
- Betrieb eines Risikomanagement- bzw. Qualitäts-managementsystems
- Umsetzung von Maßnahmen zur Resilienz / Cyber-Security
- Betrieb eines Testverfahrens bzw. regelmäßige Durchführung von Tests
- EU-Konformitätserklärung und CE-Kennzeichnung
- Zusammenarbeit mit den zuständigen Behörden
- Durchführung von Korrekturmaßnahmen
- Bereitstellung von Pflichtinformationen
- Erstellung einer technischen Dokumentation
- Erfüllung von Transparenzvorgaben
- Protokollierung von Funktionsmerkmalen
- Beobachtung nach Markteinführung
- Meldung von „schwerwiegenden Vorfällen“
- Durchführung einer Grundrechte-Folgenabschätzung
- Durchführung einer Datenschutz-Folgenabschätzung
- Entwicklung mit Trainingsdaten, die eine bestimmte Qualität aufweisen (sog. Daten-Governance)
- Einhaltung der Registrierungspflicht
- Bereitstellung menschlicher Aufsicht
- Ergreifen von Maßnahmen zur Barrierefreiheit

Im Wesentlichen werden hier Anbieter von Hochrisiko-KI-Systemen in die Pflicht genommen, teilweise aber auch deren Betreiber. Manche Pflichten gelten zudem in Bezug auf GPAI.

Beim Einsatz von KI-Systemen mit begrenztem oder minimalem Risiko bestehen im Wesentlichen Transparenzpflichten. So sieht Art. 50 AI Act beispielsweise vor, dass über den Einsatz von KI-Chatbots oder Deepfakes informiert werden muss.

Welche Strafen drohen bei Nichteinhaltung des AI Acts?

Mit den Pflichten geht auch Verantwortung einher und so sind auch Strafen möglich. Bei Verstößen gegen die Regelungen des AI Act drohen zum Teil schwere Sanktionen. Diese müssen „wirksam, verhältnismäßig und abschreckend“ sein (Art. 99 Abs. 1 S. 2 AI Act). Die Interessen von Unternehmen im KMU-Bereich sowie von Startups müssen dabei jedoch berücksichtigt werden. Je nach Verstoß drohen Geldbußen bis zu 35 Mio. Euro oder bis zu 7 Prozent des weltweit erzielten Vorjahresumsatzes – je nachdem, welcher der beiden Beträge höher ist.

Verantwortung übernehmen

Anders als die in der DSGVO vorgeschriebene Benennung eines:einer Datenschutzbeauftragten sieht der AI Act keine Pflicht vor, einen „KI-Beauftragten“ bzw. einen „KI-Manager“ oder gar ein „KI-Kompetenz-Team“ zu benennen. Gleichwohl ist dies in den meisten Fällen sinnvoll. Denn jedenfalls muss ein ausreichendes Maß an KI-Kompetenz vorhanden sein. Dies schreibt Art. 4 AI Act für alle Risikoklassen und Akteure vor. Insbesondere Anbieter und Betreiber von KI-Systemen müssen Maßnahmen ergreifen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen. Dabei sind vor allem technische Kenntnisse, Erfahrungen, Ausbildung und Schulung sowie der Kontext, in dem die KI-Systeme eingesetzt werden sollen, relevant. Zudem sind die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen. KI-Kompetenz umfasst die Fähigkeiten, Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen ermöglichen, KI-Systeme einzusetzen und sich über die Chancen und Risiken von KI bewusst zu werden. Insofern wird im AI Act zwar keine „KI-Manager“-Pflicht, sehr wohl aber eine Fortbildungspflicht geregelt. KI-Richtlinien, entsprechenden Arbeitsanweisungen, Fortbildungsangeboten sowie ggf. Betriebsvereinbarungen sind Wege, um dies möglich zu machen.

Datenschutzrechtliche Anforderungen

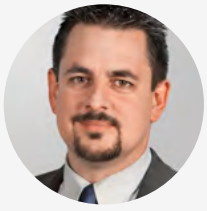
Werden in einem KI-System Daten mit Personenbezug verarbeitet kommt die Datenschutzgrundverordnung (DSGVO) zum Tragen. Diese bleibt von den Regelungen des AI Act unberührt (Art. 2 Abs. 7 AI Act). Es sind dann alle datenschutzrechtlichen Pflichten zu erfüllen, wie sie auch für andere „Werkzeuge“ zur Datenverarbeitung gelten. Dabei sind insbesondere folgende Aspekte zu berücksichtigen:

- **Verantwortlichkeit** (insbesondere die Frage, ob der Anbieter eines KI-Systems als Auftragsverarbeiter oder als gemeinsam Verantwortlicher einzustufen ist)
- **Rechtsgrundlage** (in Frage kommen etwa die Einwilligung, ein Vertrag oder berechtigte Interessen)
- **Dokumentation** (Aufnahme des KI-Systems in das Verzeichnis von Verarbeitungstätigkeiten bzw. in die List der technischen und organisatorischen Maßnahmen)
- **Informationspflichten** (z. B. im Rahmen der Datenschutzerklärung beim Einsatz eine KI-Chatbots auf der eigenen Website)
- **Reaktion auf Betroffenenrechte** (z. B. auf Auskunft oder Löschung)
- **Umgang mit Datenpanne** (z. B. wenn das KI-System personenbezogene Daten ungeplant „verrät“)
- **Durchführung einer Datenschutz-Folgenabschätzung** (beim Einsatz von KI-Systemen regelmäßig erforderlich)
- **Datenübermittlung an Dritte** (insbesondere an den KI-Anbieter, der ggf. im Nicht-EU-Ausland sitzt)

Fazit

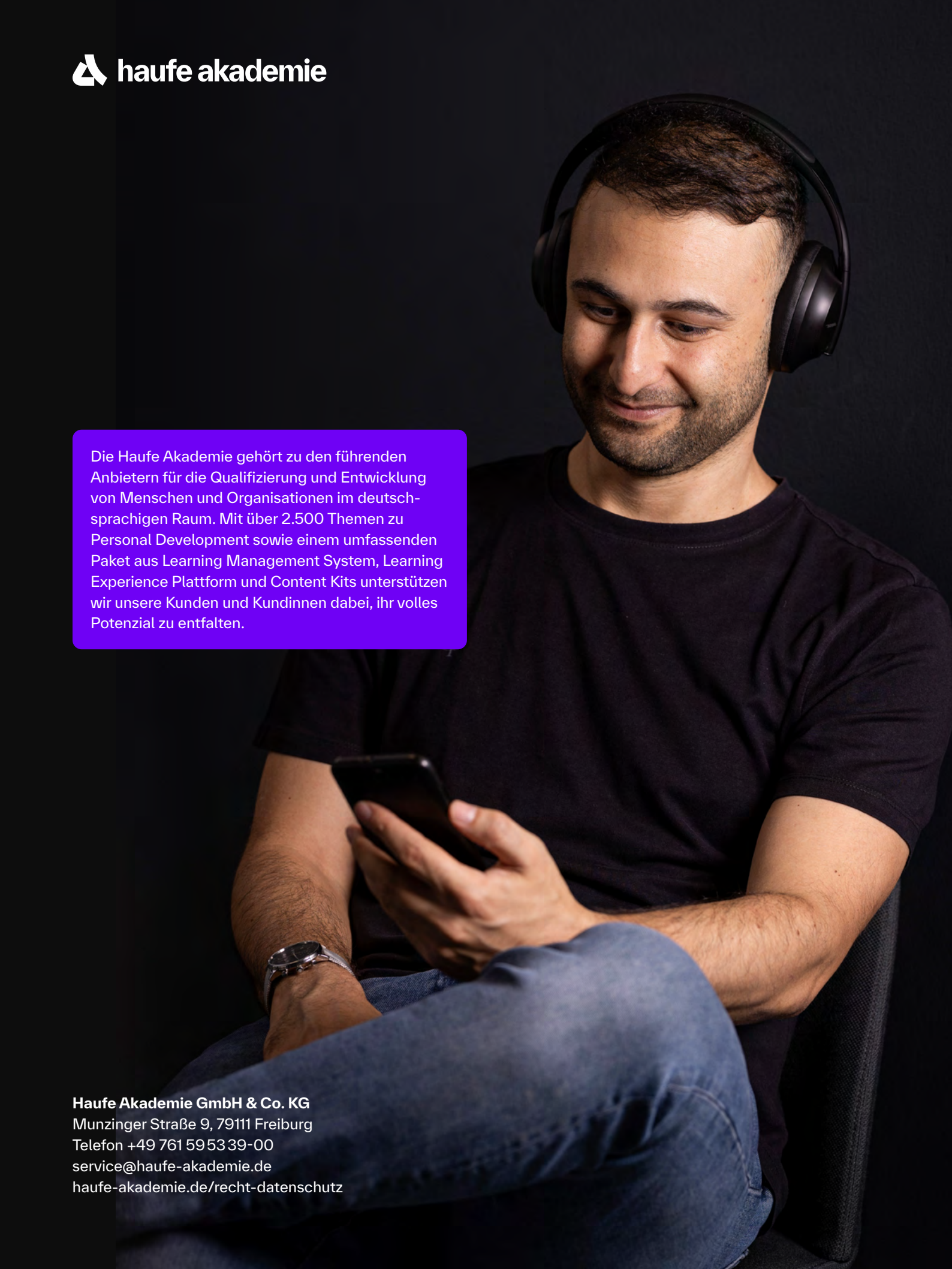
Der AI Act enthält Pflichten, bietet aber auch Chancen

Der AI Act bringt umfangreiche Pflichten für Unternehmen mit sich, die KI entwickeln, anbieten oder nutzen. Eine frühzeitige Auseinandersetzung mit den Anforderungen ist ratsam, insbesondere mit Blick auf die Pflicht zur Gewährleistung ausreichender KI-Kompetenz. Unternehmen sollten prüfen, ob sie KI-Systeme im Sinne des AI Act einsetzen und welcher Risikoklasse diese zuzuordnen sind. Je höher das Risiko, desto mehr Pflichten sind zu erfüllen. Auch wenn ein „KI-Beauftragter“ gesetzlich nicht vorgeschrieben ist, empfiehlt es sich, KI-Expertise im Unternehmen aufzubauen. Insbesondere der Datenschutz darf beim KI-Einsatz nicht vernachlässigt werden. Mit einer strategischen Herangehensweise lässt sich der AI Act bewältigen. Er sollte als Chance begriffen werden, KI verantwortungsvoll und rechtssicher zu nutzen.



Michael Rohrlich ist Rechtsanwalt, Fachautor, Dozent und Video-Trainer (www.ra-rohrlich.de). Er hat seinen Kanzleisitz in Würselen (Nähe Aachen). Seine beruflichen Schwerpunkte liegen auf den Gebieten IT-, E-Commerce- und Datenschutzrecht. Seit 1997 publiziert er regelmäßig, sowohl im Print- als auch im Online-Bereich. Darüber hinaus ist er Autor mehrerer Bücher und E-Books. Als Video-Trainer ist er seit 2012 für LinkedIn Learning tätig.

haufe akademie



Die Haufe Akademie gehört zu den führenden Anbietern für die Qualifizierung und Entwicklung von Menschen und Organisationen im deutschsprachigen Raum. Mit über 2.500 Themen zu Personal Development sowie einem umfassenden Paket aus Learning Management System, Learning Experience Plattform und Content Kits unterstützen wir unsere Kunden und Kundinnen dabei, ihr volles Potenzial zu entfalten.

Haufe Akademie GmbH & Co. KG
Munzinger Straße 9, 79111 Freiburg
Telefon +49 761 59 53 39-00
service@haufe-akademie.de
haufe-akademie.de/recht-datenschutz