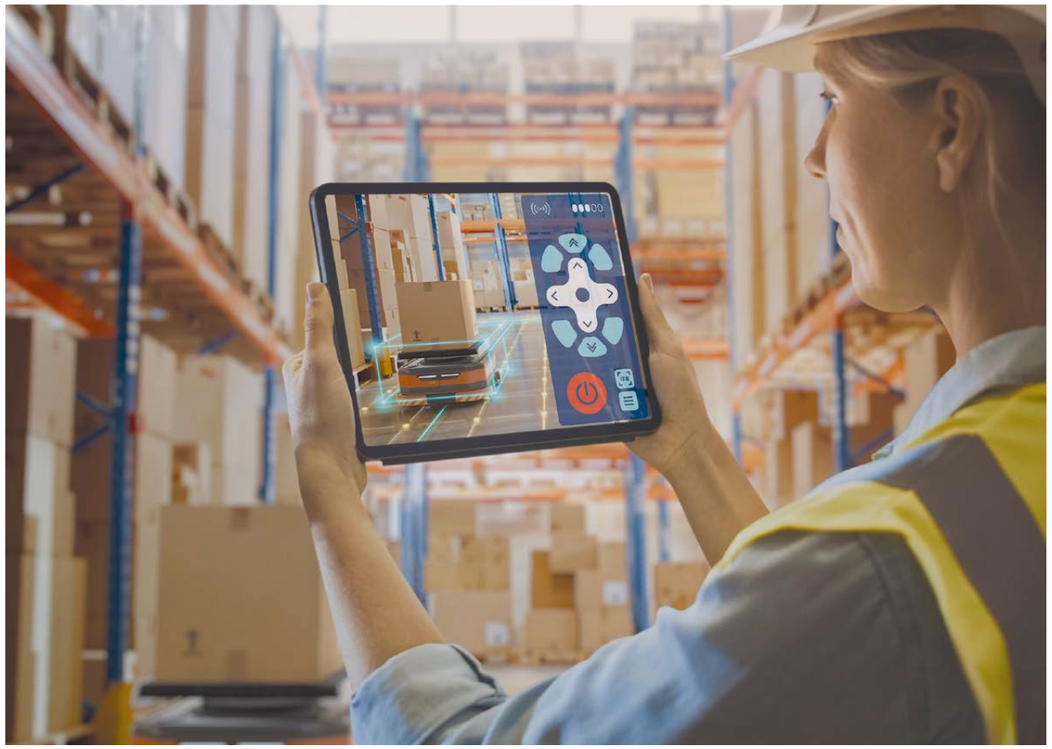

Der AI Act: Compliance-Anforderungen für Anbieter und Betreiber von KI-Systemen

Am 13.03.2024 hat das EU-Parlament dem AI Act zugestimmt. Mit Beschluss des Rates der Europäischen Union kann der Rechtsakt in Kraft treten. Anschließend finden die Vorgaben des AI Acts nach einem vierstufigen System Anwendung. Damit werden auch neue Pflichten für Anbieter und Betreiber von KI-Systemen verbindlich. Die Kataloge sind lang, und bei Verstößen drohen empfindliche Sanktionen, die von einem neuen Aufsichtssystem durchgesetzt werden können.

Prof. Dr. Domenik H. Wendt, LL.M.

Selten hat ein Rechtsakt der Europäischen Union (EU) in jüngerer Zeit solch intensive rechtspolitische Diskussionen ausgelöst wie der AI Act. Das liegt zum einen am Regelungsgegenstand, denn Künstliche Intelligenz (KI) ist alles andere als eine einfach zu greifende Materie. Zum anderen liegt es an der Zielsetzung der Verordnung, die Ansätze des Produktsicherheitsrechts mit Elementen des Grundrechtsschutzes kombiniert, wie Art. 1 Abs. 1 AI Act ausdrücklich klarstellt.

Um dieser komplexen regulatorischen Aufgabe Rechnung zu tragen, setzt der Gesetzgeber unter anderem auf einen ausdifferenzierten Pflichtenkatalog insbesondere für Anbieter und Betreiber von KI-Systemen sowie auf ein neues Aufsichtssystem, das bei Verstößen empfindliche Sanktionen durchsetzen kann.

Anbieter und Betreiber von KI-Systemen

Als Anbieter gelten natürliche oder juristische Personen, Behörden, Einrichtungen oder sonstige Stellen, die ein System bzw. Modell entwickeln oder entwickeln lassen und es unter eigenen Namen oder ihrer Handelsmarke in Verkehr bringen oder in Betrieb nehmen, sei es entgeltlich oder unentgeltlich. Als Betreiber gelten dagegen natürliche oder juristische Personen, Behörden, Einrichtungen oder sonstige Stellen, die ein KI-System in eigener Verantwortung für ihre berufliche Tätigkeit verwenden.

Für die Einordnung als Anbieter ist eine Nähe zum KI-System erforderlich, weil eine Mitwirkung am Entwicklungsprozess vorausgesetzt wird. Hierfür reicht es allerdings bereits aus, wenn Personen, Behörden, Einrichtungen oder sonstige Stellen ein KI-System für sich entwickeln lassen und es anschließend unter eigenem Namen in Verkehr bringen oder in Betrieb nehmen. Wer nicht am Entwicklungsprozess beteiligt ist und ein KI-System zu beruflichen Zwecken nutzt, gilt als Betreiber.

Viele Pflichten für Anbieter von Hochrisiko-KI

Ausgehend vom bekannten mehrstufigen risikobasierten Regulierungsansatz (verbotene KI-Systeme, Hochrisiko-KI-Systeme, KI-Systeme mit Transparenzrisiken und KI-Systeme mit minimalen oder ohne Risiken, s. dazu auch *unternehmensjurist* 1/2024, S. 44) setzen die Pflichten insbesondere bei Hochrisiko-KI-Systemen an. Der Pflichtenkatalog für Anbieter dieser KI-Systeme ist umfangreich.

Einige der Regelungen fordern ausdrücklich, dass Hochrisiko-KI-Systeme auf eine bestimmte Art und Weise konzipiert und entwickelt werden müssen (vgl. insbesondere Art. 13 bis 15 AI Act). Damit adressiert der AI Act den bekannten Compliance-by-Design-Ansatz. Das Produkt – in diesem Fall das Hochrisiko-KI-System – ist also so zu konzipieren bzw. zu entwickeln, dass Compliance-Verstöße nicht oder nur mit reduzierter Wahrscheinlichkeit auftreten.

Die meisten Anforderungen müssen die Anbieter erfüllen, bevor sie das System in Verkehr bringen oder in Betrieb nehmen.

Anbieterpflichten vor der Markteinführung von Hochrisiko-KI (Art. 16 AI Act)

Anbieter müssen:

- sicherstellen, dass ihre KI-Systeme die in Art. 8 bis 15 AI Act festgelegten Anforderungen erfüllen, insbesondere durch
  - Einrichtung eines Risikomanagementsystems, das angewandt, dokumentiert und aufrechtzuerhalten ist (Art. 9 AI Act),
  - Einhaltung einer Daten-Governance (Art. 10 AI Act),
  - Erstellen einer technischen Dokumentation (Art. 11 AI Act),
  - Ermöglichung der automatischen Aufzeichnung von Ereignissen (Art. 12 AI Act),
  - Einhaltung von Transparenzanforderungen und Erstellung von Gebrauchsanweisungen (Art. 13 AI Act),
  - Ermöglichung einer wirksamen menschlichen Aufsicht (Art. 14 AI Act) sowie durch ein
  - angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit (Art. 15 AI Act)
- den eingetragenen Handelsnamen bzw. die eingetragene Handelsmarke und ihre Kontaktanschrift angeben;
- über ein Qualitätsmanagementsystem verfügen (Art. 17 AI Act);
- die Dokumentation (Art. 18 AI Act) und
- die automatisch erzeugten Protokolle aufbewahren (Art. 19 AI Act);
- sicherstellen, dass das KI-System einem Konformitätsbewertungsverfahren unterzogen wird (Art. 43 AI Act);
- eine EU-Konformitätserklärung ausstellen (Art. 47 AI Act);
- die CE-Kennzeichnung anbringen (Art. 48 AI Act) und
- den Registrierungspflichten nachkommen (Art. 49 AI Act).

Einige Pflichten treffen die Anbieter aber auch nach Inverkehrbringen des Hochrisiko-KI-Systems.

Anbieterpflichten nach der Markteinführung von Hochrisiko-KI

Anbieter müssen:

- erforderliche Korrekturmaßnahmen ergreifen und Informationen bereitstellen (Art. 20 AI Act);
- auf begründete Anfrage einer nationalen Aufsichtsbehörde nachweisen, dass das KI-System insbesondere die in Art. 8 bis 15 AI Act genannten Anforderungen erfüllt und
- ein System zur Beobachtung nach dem Inverkehrbringen einrichten sowie dokumentieren (Art. 71 AI Act).

Schwerpunkt

„Der AI Act adressiert ausdrücklich den Compliance-by-Design-Ansatz."

Die Pflichten der Betreiber von Hochrisiko-KI-Systemen sind weniger umfangreich.

Pflichten für Betreiber von Hochrisiko-KI
Betreiber haben:

- durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass sie diese Systeme entsprechend den Gebrauchsanweisungen verwenden;
- besonders geschulten Personen die menschliche Aufsicht über die KI-Systeme zu übertragen;
- den Betrieb des KI-Systems anhand der Gebrauchsanweisung zu überwachen und unter besonderen Umständen Anbieter oder Händler und die zuständige Marktüberwachungsbehörde zu informieren;
- die vom KI-System automatisch erzeugten Protokolle mindestens sechs Monate datenschutzkonform aufzubewahren;
- vor Inbetriebnahme oder Verwendung eines Hochrisiko-KI-Systems am Arbeitsplatz die Arbeitnehmervertreter und die betroffenen Arbeitnehmer darüber zu informieren, dass sie Gegenstand des Einsatzes des Hochrisiko-KI-Systems sein werden.

Besondere Pflichten sieht der Gesetzgeber unter anderem für Betreiber vor, die als Finanzmarktakteure Hochrisiko-KI-Systeme verwenden. Diese Banken und Versicherungen müssen vor Inbetriebnahme eines solchen Systems eine Grundrechte-Folgenabschätzung nach Art. 27 AI Act vornehmen.

Daneben gelten Registrierungs- und Informationspflichten für Betreiber, die Organe, Einrichtungen und sonstige Stellen der EU sind, und spezifische Vorgaben für Betreiber, die ein Hochrisiko-KI-Systems zur nachträglichen biometrischen Fernidentifizierung verwenden.

Besondere Pflichten: Transparenzrisiken und GPAI
Weitere Anforderungen normiert der AI Act für KI-Systeme mit Transparenzrisiken. Solche Risiken erkennt der Gesetzgeber vor allem bei KI-Systemen, die für die direkte Interaktion mit natürlichen Personen bestimmt sind. Und auch hier adressiert der Gesetzgeber den Compliance-by-Design-Ansatz: Die Systeme sind grundsätzlich so zu konzipieren und zu entwickeln, dass natürliche Personen informiert werden, sobald sie mit dem KI-System interagieren.

Besondere Regelungen gibt der AI Act auch für KI mit allgemeinem Verwendungszweck (General Purpose AI – GPAI) vor. GPAI hat die Fähigkeit, in einer Vielzahl von Anwendungen genutzt zu werden. Der AI Act unterscheidet zwischen GPAI-Modellen mit geringerem und solchen mit einem größeren Risiko (systemisches Risiko). Der Differenzierung zugrunde gelegt werden die sog. Floating Point Operations per Second (Flop-Werte), also eine Maßeinheit, mit deren Hilfe die Leistungsfähigkeit des KI-Systems gemessen wird. Anbieter dieser KI-Modelle sind mit weiteren Pflichten belegt (Art. 53 und Art. 55 AI Act).

Harmonisierte Standards
Der AI Act steht nicht für sich alleine. Er ist Teil eines neuen Regelsystems für KI in der EU. Der Rechtsakt wird durch Anhänge, die als delegierte Rechtsakte erlassen werden, und durch Leitlinien der EU-Kommission ergänzt.

Von großer praktischer Bedeutung sind die harmonisierten Normen (*harmonised standards*) im Sinne des Art. 40 AI Act. Sie flankieren die weitestgehend technologieneutralen Bestimmungen des AI Acts durch technologiebezogene Vorgaben. Diese Standards werden aktuell in den zuständigen Gremien von den Komitees für Normung (CEN) und für elektrotechnische Normung (CENELEC) auf EU-Ebene erarbeitet. Ihre große praktische Bedeutung erhalten die harmonisierten Normen auch durch das vom Gesetzgeber im AI Act verankerte Anreizsystem: Stimmen Hochrisiko-KI-Systeme mit harmonisierten Normen überein, wird insoweit eine Konformität mit den Anforderungen aus Art. 8 bis 15 AI Act vermutet.

Neues Aufsichtsregime
Über die Einhaltung des Regelsystems wacht zukünftig ein neues Aufsichtsregime. Hier setzt der Gesetzgeber auf ein Zusammenspiel zwischen Behörden auf EU-Ebene und in den Mitgliedstaaten.

Die EU-Kommission übernimmt mit dem angegliederten AI Office die Kontrolle für GPAI. Die übrigen KI-Systeme werden von nationalen Aufsichtsbehörden beaufsichtigt. Ein Europäischer Ausschuss für Künstliche Intelligenz, der sich aus Vertretern und Vertreterinnen der zuständigen nationalen Aufsichtsbehörden sowie dem Europäischen Datenschutzbeauftragten und der Kommission zusammensetzt, soll eine reibungslose, wirksame und vor allem einheitliche Umsetzung der Verordnung sicherstellen. Der Ausschuss wird zudem Normungstätigkeiten unterstützen. Für zusätzliches Fachwissen wird ein Beratungsforum eingerichtet, das aus Interessenträgern aus Industrie, Start-ups, KMU, Zivilgesellschaft und Wissenschaft besteht.

Teure Verstöße
Bei Verstößen gegen die Vorgaben des AI Acts können die zuständigen Stellen gem. Art. 99 AI Act empfindliche Sanktionen erlassen: Wird ein verbotenes KI-System in Verkehr gebracht oder betrieben, drohen Geldbußen von bis zu 35 Mio. Euro bzw. 7 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres (je nachdem, welcher Betrag höher ist). Bei Verstößen gegen die zuvor skizzieren Pflichtenkataloge können Anbieter und Betreiber mit Geldbußen von bis zu 15 Mio. Euro bzw. 3 % des Jahresumsatzes sanktioniert werden; entsprechendes gilt bei Verstößen gegen die Transparenzpflichten gem. Art. 50 AI Act und gegen Pflichten für Anbieter von GPAI-Modellen. Bei falschen, unvollständigen oder irreführenden Informationen können Geldbußen von bis zu 7,5 Mio. Euro bzw. 1 % Jahresumsatz verhängt werden.

Eine Erleichterung gilt für KMU einschließlich Start-up-Unternehmen. Hier wird der jeweils niedrigere Betrag der genannten Prozentsätze oder Summen in Ansatz gebracht.

Gestufte zeitliche Anwendbarkeit
Die zeitliche Anwendbarkeit des AI Acts vollzieht sich in Stufen:

- Die Regelungen für verbotene KI-Praktiken gelten bereits sechs Monate nach dem Inkrafttreten der Verordnung;
- die Verpflichtungen für KI-Modelle mit allgemeinem Verwendungszweck sind nach zwölf Monaten anwendbar;
- für den Hauptteil der Verordnung einschließlich der Hochrisiko-KI-Systeme, die in Anhang III als Liste der Anwendungsfälle mit hohem Risiko geführt sind, ist eine Übergangsfrist von 24 Monaten vorgesehen und
- nach 36 Monaten werden abschließend auch die Verpflichtungen für Hochrisiko-KI-Systeme nach Anhang II anwendbar.

Fazit
Der AI Act enthält für Anbieter und Betreiber von Hochrisiko-KI-Systemen Pflichtenkataloge, die beeindrucken. Der Gesetzgeber adressiert hierbei zum Teil ausdrücklich den Compliance-by-Design-Ansatz. Betreiber, die Banken und Versicherungen sind, müssen zudem eine Grundrechte-Folgenabschätzung vornehmen. Daneben bestehen Pflichten bei KI-Systemen mit Transparenzrisiken und bei GPAI-Modellen. Im Zusammenhang mit der Einhaltung der neuen Compliance-Anforderungen spielen neue harmonisierte Standards eine erhebliche Rolle.

Bei Nichteinhaltung der Vorgaben sind empfindliche Sanktionen möglich, deren Durchsetzung durch ein neues Aufsichtssystem sichergestellt wird. Die meisten Vorgaben des AI Acts, einschließlich der neuen Compliance-Anforderungen für Anbieter und Betreiber von Hochrisiko-KI-Systemen, greifen 24 Monate nach Inkrafttreten der Verordnung. Eine frühzeitige Befassung mit den neuen Vorgaben ist dennoch sinnvoll, auch um Verstöße gegen die bereits in sechs Monaten geltenden Verbote oder die für Anbieter von GPAI-Modellen bereits nach zwölf Monaten geltenden Pflichten zu vermeiden.

Prof. Dr. Domenik H. Wendt, LL.M.
Professor für Bürgerliches Recht, Europäisches Wirtschaftsrecht und Europarecht

Prof. Dr. Domenik H. Wendt, LL.M. ist Professor für Bürgerliches Recht, Europäisches Wirtschaftsrecht und Europarecht an der Frankfurt University of Applied Sciences und Direktor des Reseach Lab for Law and applied Technologies (ReLLaTe) in Frankfurt a.M. Seine Forschungsschwerpunkte sind das Finanzmarktrecht, das neue Recht der Künstlichen Intelligenz, das Recht neuer Mobilitäts- und Logistiklösungen sowie die Digitalisierung des Rechtsmarktes.