

Tim Wybitul, RA/FAArbR/CIPP/E*

Welche Pflichten haben Betreiber von Hochrisiko-KI-Systemen nach der EU-KI-Verordnung?

Überblick, Handlungsempfehlungen und Checkliste

Die neue EU-KI-Verordnung (KI-VO) regelt die Entwicklung und den Einsatz von KI-Systemen risikobasiert. Hochrisiko-KI-Systeme, z. B. zur Beobachtung und Bewertung von Beschäftigten, sind besonders geregelt. Dieser Beitrag soll Unternehmen helfen, ihre Pflichten beim Einsatz solcher Systeme zu identifizieren und umzusetzen. Er erläutert die Kriterien zur Einordnung als Betreiber eines Hochrisiko-KI-Systems, beschreibt deren Pflichten, gibt Handlungsempfehlungen und enthält eine Checkliste, die die wichtigsten Pflichten zusammenfasst.

I. Einleitung

Die Leistungsfähigkeit von KI-Systemen hat in den letzten Jahren sprunghaft zugenommen. Unternehmen setzen KI immer öfter und immer gezielter ein. Die EU hat mit der KI-VO am 12.7.2024 das weltweit erste umfassende Gesetzeswerk zur Regelung von KI veröffentlicht.¹ Die KI-VO² trat am 2.8.2024 in Kraft. Die einzelnen Regelungen gelten nach den jeweiligen Umsetzungsfristen zwischen sechs und 36 Monaten ab dem Inkrafttreten. Das erste Kapitel der KI-VO mit den grundlegenden Regelungen gilt ab dem 2.2.2025, die letzten Regelungen sind ab dem 2.8.2027 verbindlich. Bereits jetzt kann man absehen, dass diese Fristen in Anbetracht der enormen Komplexität der Neuregelung und ihrer weitreichenden Anforderungen eher knapp bemessen sind.

1. Rechtsrahmen

Als EU-Verordnung wirkt die KI-VO unmittelbar und direkt (Art. 288 Abs. 2 AEUV). Die Mitgliedstaaten müssen die KI-VO daher nicht mehr in nationales Recht umsetzen, sondern lediglich flankierende Begleitgesetze schaffen, um die in der Verordnung vorgegebenen Strukturen auf nationaler Ebene umzusetzen, etwa durch die Einrichtung entsprechender Marktaufsichtsbehörden. Auch die Sanktionierung von Verstößen erfolgt weitgehend nach nationalem Recht (vgl. Art. 99 Abs. 1 KI-VO), soweit die KI-VO keine vorrangigen Regelungen trifft (etwa in Art. 99, Art. 70 oder Art. 74 ff. KI-VO).

2. Anwendungsbereich

Die KI-VO hat einen weiten räumlichen Anwendungsbereich.³ Sie gilt zunächst weltweit für Anbieter, die in der EU KI-Systeme in Verkehr bringen oder in Betrieb nehmen (Marktortprinzip). Dies gilt ebenso für das Inverkehrbringen von KI-Modellen mit allgemeinem Verwendungszweck (Art. 2 Abs. 1 lit. a KI-VO). Sie gilt ferner auch für Betreiber von KI-Systemen, die ihren Sitz in der Union haben oder sich dort befinden (Sitz- oder Aufenthaltsprinzip; Art. 2 Abs. 1 lit. b KI-VO). Zudem gilt die KI-VO auch, sofern das von einem KI-System hervorgebrachte Ergebnis in der EU verwendet wird (Ergebnisprinzip; Art. 2 Abs. 1 lit. c KI-VO). Daneben gilt sie noch für sonstige Akteure nach Art. 3 Nr. 8 KI-VO (Art. 2 Abs. 1 lit. d bis lit. f KI-VO) und für

betroffene Personen (vgl. zur Definition Art. 3 Nr. 50 KI-VO) im Sinne von Art. 4 Nr. 1 DSGVO (Art. 2 Abs. 2 lit. g KI-VO).

II. Einordnung als Betreiber von Hochrisiko-KI-Systemen

Dieser Überblick zeigt, unter welchen Voraussetzungen Unternehmen Betreiber von Hochrisiko-KI-Systemen sind.

1. Hochrisiko-KI-Systeme

Die Definition von KI-Systemen ist ausgesprochen weit (Art. 3 Nr. 1 KI-VO). Sie gilt nur für maschinengestützte Systeme. Diese Systeme müssen für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt sein. Zudem müssen sie nach ihrer Betriebsaufnahme anpassungsfähig sein. Vor allem müssen sie aus den erhaltenen Eingaben für explizite oder implizite Ziele Ableitungen treffen können. Diese Fähigkeit zum Ableiten muss das Hervorbringen von Ergebnissen betreffen, wie etwa von Vorhersagen, Inhalten, Empfehlungen oder Entscheidungen, die physische oder virtuelle Umgebungen beeinflussen können. Diese Definition kann man ohne Übertreibung als sprachlich und damit auch inhaltlich missglückt einordnen. Letztlich sind damit für die Einordnung eines Systems als KI-System im Sinne von Art. 3 Abs. 1 KI-VO wohl folgende Kriterien relevant:

- Maschinengestütztes System,
- ausgelegt für autonomen Betrieb,
- kann (aber muss nicht) anpassungsfähig sein und
- trifft Ableitungen (englisch: „*infers ... how to generate outputs*“⁴) aus erhaltenen Eingaben, wie Ergebnisse hervorgebracht werden können.

Für die Frage, ob ein KI-System als Hochrisiko-KI-System einzuordnen ist, gibt es keine allgemeingültige Definition. Vielmehr arbeitet die KI-VO mit abschließenden Aufzählungen. Sie nennt eine ganze Reihe von Systemtypen, die in die Kategorie der Hochrisiko-KI-Systeme fallen. Die in der Praxis für die meisten Unternehmen voraussichtlich wichtigsten Anwendungsfälle sind in Anhang III KI-VO aufgezählt. Dies betrifft etwa Systeme zur Auswahl, Beobachtung oder Bewertung von Bewerbern oder Arbeitnehmern (Anhang III Nr. 4 KI-VO), zur beruflichen Bildung (Anhang III Nr. 3 KI-VO), für kritische Infrastrukturen (Anhang III Nr. 2 KI-VO) oder zur Prüfung der Kreditwürdigkeit (Anhang III Nr. 5 lit. b KI-VO). Es gibt zudem eine Reihe von Ausnahmen und Rückausnahmen (vgl. Art. 6 Abs. 2 KI-VO).

* Der Verfasser dankt Rechtsreferendar Cenk Nickel, Ass. iur. Hannah Jürges und RAin Dr. Isabelle Brams für wertvolle Anregungen und Vorarbeiten.

1 Vgl. hierzu umfassend Ashkar/Schröder, BB 2024, 771.

2 VO (EU) 2024/1689 vom 13.6.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der VO (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der RL 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz).

3 Vgl. Ashkar/Schröder, BB 2024, 771, 772.

2. Betreiber

Betreiber ist eine juristische Person oder sonstige Stelle, die ein KI-System in eigener Verantwortung im Rahmen einer beruflichen Tätigkeit verwendet (vgl. Art. 3 Nr. 4 KI-VO).⁴ Aus Unternehmenssicht ist also entscheidend, ob man ein KI-System für betriebliche oder betriebsbezogene Zwecke einsetzt.

Praxistipp: In der Praxis müssen Betreiber bei jedem relevanten KI-System im Einzelnen anhand der Zweckbestimmung des Systems und unter Berücksichtigung der Gesamtumstände seiner Nutzung prüfen, ob es sich um ein Hochrisiko-KI-System handelt. Sofern Unternehmen nicht über entsprechende Aufstellungen verfügen, müssen sie sich also zunächst einen Überblick darüber verschaffen, welche KI-Systeme sie im Rahmen ihrer beruflichen beziehungsweise betrieblichen Tätigkeit verwenden. In einem zweiten Schritt sind diese KI-Systeme in die unterschiedlichen Risikoklassen der KI-VO einzuordnen.⁵

Praxistipp: Besonderes Augenmerk sollten Betreiber von Hochrisiko-KI-Systemen (vgl. Art. 6 KI-VO) auch auf Art. 25 KI-VO legen. Nach dieser Vorschrift werden Betreiber zu Anbietern von Hochrisiko-KI-Systemen, wenn sie wesentliche Änderungen an dem System vornehmen (Art. 26 Abs. 1 lit. b KI-VO) oder dieses mit ihrem Namen oder ihrer Handelsmarke versehen (Art. 26 Abs. 1 lit. a KI-VO). In diesem Fall muss das betroffene Unternehmen die deutlich umfassenderen Pflichten eines Anbieters eines Hochrisiko-KI-Systems umsetzen (Art. 8 bis 22 KI-VO).

III. Pflichten für Betreiber von Hochrisiko-KI-Systemen

Der folgende Überblick zeigt die in der Praxis relevantesten Rechtspflichten für Unternehmen, die Betreiber von Hochrisiko-KI-Systemen nach Art. 6 KI-VO sind.⁶

1. Schulungspflichten

Der rechtskonforme Betrieb von Hochrisiko-KI-Systemen setzt umfassende Schulungen von Mitarbeitern und sonstigem, beim Einsatz dieser Systeme beschäftigtem Personal voraus.

a) Training KI-Kompetenz

Betreiber von KI-Systemen müssen sicherstellen, dass nur Personen mit dem Betrieb oder der Nutzung von KI-Systemen befasst sind, die über ein ausreichendes Maß an KI-Kompetenz verfügen (Art. 4 KI-VO). Diese Rechtspflicht gilt neben den anderen grundlegenden Vorschriften des ersten Kapitels der KI-VO bereits sechs Monate nach Inkrafttreten der KI-VO, also ab dem 2.2.2025 (Art. 113 Abs. 1 lit. a KI-VO).

b) Training von Aufsichtspersonen

Betreiber müssen sicherstellen, dass natürliche Personen die menschliche Aufsicht über den Einsatz des Hochrisiko-KI-Systems ausüben. Der Betreiber muss zudem dafür sorgen, dass diese Personen über die erforderliche Ausbildung verfügen (Art. 26 Abs. 2 KI-VO, vgl. auch Art. 14 KI-VO), etwa durch entsprechende Trainings.

2. Operative Pflichten

a) Technische und organisatorische Maßnahmen

Betreiber von Hochrisiko-KI-Systemen müssen sicherstellen, dass die von ihnen eingesetzten KI-Systeme entsprechend den vom Anbieter dieser KI-Systeme beizufügenden Betriebsanleitungen und gemäß

Art. 26 Abs. 3 bis Abs. 6 KI-VO verwendet werden (Art. 26 Abs. 1 KI-VO). Dies betrifft konkret folgende Maßnahmen:

aa) Umsetzung von Betriebsanleitungen

Betreiber müssen technische und organisatorische Maßnahmen treffen, die sicherstellen, dass das Hochrisiko-KI-System ausschließlich entsprechend der vom Anbieter beizufügenden Betriebsanleitungen (vgl. Art. 13 Abs. 2 und Abs. 3 KI-VO) verwendet wird.

bb) Erfüllung sonstiger Rechtspflichten

Es sind technische und organisatorische Maßnahmen zur Erfüllung sonstiger Pflichten der Betreiber nach Unionsrecht oder nationalem Recht zu treffen.

cc) Kontrolle von Eingabedaten

Betreiber müssen durch entsprechende technische und organisatorische Maßnahmen sicherstellen, dass die Eingabedaten der Zweckbestimmung des Hochrisiko-KI-Systems entsprechen und ausreichend repräsentativ sind.

dd) Informationspflichten

Es sind technische und organisatorische Maßnahmen zur Erfüllung von Informationspflichten zu ergreifen. Diese Maßnahmen betreffen Informationen gegenüber Anbietern, Händlern und der zuständigen Marktüberwachungsbehörde sowie Maßnahmen zur Aufbewahrung der von dem Hochrisiko-KI-System automatisch erzeugten Protokolle.

b) Qualitätsmanagement Eingabedaten

Betreiber müssen kontrollieren, dass in ihrem Einflussbereich stehende Eingabedaten der Zweckbestimmung des Hochrisiko-KI-Systems entsprechen und ausreichend repräsentativ sind (Art. 26 Abs. 4 KI-VO).

c) Befugnisse für Aufsichtspersonen

Wie bereits angesprochen, müssen Betreiber sicherstellen, dass natürliche Personen die menschliche Aufsicht über den Einsatz des Hochrisiko-KI-Systems ausüben. In operativer Hinsicht müssen Betreiber gewährleisten, dass diese Personen auch über die nötigen Befugnisse im Unternehmen verfügen (Art. 26 Abs. 2 KI-VO, vgl. auch Art. 14 KI-VO).

d) Aussetzung des Betriebs

Hat ein Betreiber Grund zur Annahme, dass die Verwendung gemäß der Betriebsanleitung dazu führen kann, dass ein Hochrisiko-KI-System ein Risiko im Sinne von Art. 79 Abs. 1 KI-VO birgt, so setzt der Betreiber die Verwendung des Systems aus (Art. 26 Abs. 5 S. 2 KI-VO).

3. Kontrollpflichten

a) Vorprüfung verbotene Praktiken

Betreiber müssen prüfen, dass der Einsatz eines Hochrisiko-KI-Systems nicht unter die nach Art. 5 KI-VO verbotenen KI-Praktiken fällt. Andernfalls sollte man den Einsatz des Systems unterbinden. Diese

⁴ Es gelten Ausnahmen für rein persönliche Tätigkeiten, vgl. auch *Ashkar/Schröder*, BB 2024, 771, 777.

⁵ Vgl. auch *Ashkar/Schröder*, BB 2024, 771, 779.

⁶ Pflichten für Behörden oder sonstige Stellen sind hierbei bewusst ausgeklammert.

Rechtspflicht gilt bereits sechs Monate nach Inkrafttreten der KI-VO, also zum 2.2.2025 (Art. 113 Abs. 1 lit. a KI-VO).

b) Aufsicht durch natürliche Personen

Betreiber müssen dafür sorgen, dass natürliche Personen die menschliche Aufsicht bzw. Kontrolle über den Einsatz des Hochrisiko-KI-Systems ausüben. Der Betreiber muss zudem sicherstellen, dass diese Personen über die erforderliche Kompetenz, Ausbildung und Befugnisse verfügen. Ferner muss der Betreiber diesen natürlichen Personen die erforderliche Unterstützung zukommen lassen (Art. 26 Abs. 2 KI-VO, vgl. auch Art. 14 KI-VO).

c) Kontrolle von Eingabedaten

Betreiber müssen dafür sorgen, dass Eingabedaten, die ihrer Kontrolle unterliegen, der Zweckbestimmung des Hochrisiko-KI-Systems entsprechen und ausreichend repräsentativ sind (Art. 26 Abs. 4 KI-VO).

d) Kontinuierliche Überwachung

Betreiber sind verpflichtet, den Betrieb des Hochrisiko-KI-Systems anhand der vom Anbieter des Systems bereitgestellten Betriebsanleitung kontinuierlich zu überwachen (Art. 26 Abs. 5 S. 1 KI-VO). Einzelheiten in Bezug auf die im Rahmen solcher Betriebsanleitungen vom Anbieter zur Verfügung zu stellenden Mindestinformationen sind in Art. 13 Abs. 3 KI-VO geregelt. Die entsprechenden Kontrollmaßnahmen umfassen insbesondere eine durchgehende Risikoprüfung, um festzustellen, ob die Verwendung gemäß der Betriebsanleitung dazu führen kann, dass das Hochrisiko-KI-System Risiken im Sinne von Art. 79 Abs. 1 KI-VO birgt (vgl. Art. 26 Abs. 5 S. 2 KI-VO).

e) Prüfung der Voraussetzungen von zusätzlichen Pflichten als Anbieter

Betreiber von Hochrisiko-KI-Systemen müssen kontinuierlich prüfen, ob sie wesentliche Veränderungen an dem Hochrisiko-KI-System vornehmen oder ob sonstige Voraussetzungen vorliegen, unter denen sie den Pflichten von Anbietern unterliegen, vgl. oben Abschnitt II. 1 (vgl. Art. 25 KI-VO).

Praxistipp: Beim Betrieb von Hochrisiko-KI-Systemen wird sich häufig die Frage stellen, inwiefern bereits ein umfassendes Trainieren eines solchen Systems oder die Vornahme relevanter Voreinstellungen eine wesentliche Veränderung darstellt. Unternehmen sind gut beraten, vorgenommene Veränderungen ebenso zu dokumentieren wie die Gründe, warum diese nicht als wesentlich zu bewerten sind.

f) Prüfung der Notwendigkeit einer Grundrechte-Folgenabschätzung

Betreiber, bei denen es sich um Einrichtungen des öffentlichen Rechts handelt oder private Einrichtungen, die öffentliche Dienste erbringen, müssen unter den in Art. 27 Abs. 1 Alt. 1 KI-VO genannten Voraussetzungen Grundrechte-Folgenabschätzungen durchführen. Dies gilt auch für Betreiber, die ein KI-System zur Kreditwürdigkeits- und Bonitätsprüfung natürlicher Personen oder zur Risikobewertung und Preisbildung im Fall von Lebens- und Krankenversicherungen für natürliche Personen einsetzen (Art. 27 Abs. 1 S. 1 Alt. 2 KI-VO i.V.m. Anhang III Nr. 5 lit. b und c). Daher sollten Betreiber von Hochrisiko-KI-Systemen prüfen, ob sie dieser Rechtspflicht unterliegen beziehungsweise ob eine der Ausnahmen des Anhangs III Nr. 2 KI-VO

(Verwendung des Systems zum Betrieb oder zur Verwaltung kritischer Infrastruktur) eingreift.

4. Dokumentationspflichten

a) Aufbewahrung von KI-Protokollen

Die Technik eines Hochrisiko-KI-Systems muss die automatische Aufzeichnung von Ereignissen während des gesamten Lebenszyklus ermöglichen (Art. 12 Abs. 1 KI-VO). Diese Protokollierungsfunktionen müssen unter anderem die Überwachung des Betriebs des Hochrisiko-KI-Systems zur Erfüllung von Betreiberpflichten ermöglichen (vgl. Art. 12 Abs. 2 lit. c KI-VO, der auf die Pflicht zur Aufbewahrung von Protokollen durch Betreiber nach Art. 26 Abs. 6 KI-VO verweist). Soweit diese automatisch erzeugten Protokolle der Kontrolle des Betreibers unterliegen, gelten Aufbewahrungspflichten. Der Betreiber muss diese Protokolle für einen der Zweckbestimmung des Hochrisiko-KI-Systems angemessenen Zeitraum aufbewahren (Art. 26 Abs. 6 KI-VO). Dieser Zeitraum darf sechs Monate nicht unterschreiten, sofern im geltenden Unionsrecht oder im nationalen Recht nichts anderes bestimmt ist. Eine solche Ausnahme kann sich insbesondere aus den Rechtsvorschriften über den Schutz personenbezogener Daten (DSGVO), beispielsweise dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO), dem Zweckbindungsgrundsatz (Art. 5 Abs. 1 lit. b DSGVO) oder dem Recht auf Löschung (Art. 17 DSGVO), ergeben.

b) Dokumentations- und Aufbewahrungspflichten nach sonstigen Vorschriften

Betreiber sind gut beraten, beim Einsatz von KI-Systemen neben den Vorgaben der KI-VO auch Rechtspflichten aus anderen Rechtsakten der EU oder nach nationalen Vorschriften zu berücksichtigen. Dies betrifft bei der (oft unausweichlichen) Verarbeitung personenbezogener Daten etwa auch Vorgaben nach dem datenschutzrechtlichen Rechenschaftsprinzip oder weiterer datenschutzrechtlicher Vorschriften (vgl. Art. 30 DSGVO).

5. Informationspflichten

a) Informationspflichten gegenüber Anbietern

Die Anbieter von Hochrisiko-KI-Systemen sind dazu verpflichtet, das System auch nach dem Inverkehrbringen systematisch zu beobachten (Art. 26 Abs. 5 S. 1 KI-VO). Stellen Betreiber Umstände fest, die für eine solche systematische Beobachtung relevant sind, informieren sie gegebenenfalls die Anbieter (vgl. Art. 72 KI-VO).

b) Informationspflichten bei Risiken

Hat ein Betreiber Grund zur Annahme, dass die Verwendung gemäß der Betriebsanleitung dazu führen kann, dass ein Hochrisiko-KI-System ein Risiko im Sinne von Art. 79 Abs. 1 KI-VO birgt, so informiert er unverzüglich den Anbieter oder den Händler des Hochrisiko-KI-Systems und die zuständige Marktüberwachungsbehörde (Art. 26 Abs. 5 S. 2 KI-VO).

c) Informationspflichten bei schwerwiegenden Vorfällen

Stellt ein Betreiber beim Betrieb eines Hochrisiko-KI-Systems einen schwerwiegenden Vorfall fest, so informiert er unverzüglich zuerst den Anbieter, dann den Einführer oder den Händler und die zuständigen Marktüberwachungsbehörden über den Vorfall (Art. 26 Abs. 5 S. 3 KI-VO). Kann der Betreiber den Anbieter nicht erreichen, treffen

ihn zusätzlich die Meldepflichten bei schwerwiegenden Vorfällen nach Art. 73 KI-VO.

d) Informationspflichten gegenüber Arbeitnehmern und ihren Vertretern

Vor der Inbetriebnahme oder Verwendung eines Hochrisiko-KI-Systems, das am Arbeitsplatz eingesetzt wird, gelten Informationspflichten (Art. 26 Abs. 7 S. 1 KI-VO). In diesem Fall informiert der Betreiber, der ein Arbeitgeber ist, die Arbeitnehmervertreter und die betroffenen Arbeitnehmer entsprechen. Diese Informationspflicht ist darauf gerichtet, die Arbeitnehmervertreter und betroffenen Arbeitnehmer darüber zu unterrichten, dass sie Gegenstand des Einsatzes des Hochrisiko-KI-Systems sein werden. Diese Informationen werden gegebenenfalls im Einklang mit den Vorschriften und Gepflogenheiten auf Unionsebene und auf nationaler Ebene in Bezug auf die Unterrichtung der Arbeitnehmer und ihrer Vertreter bereitgestellt. In Deutschland sind dabei insbesondere die Vorgaben des Betriebsverfassungsrechts zu beachten (Art. 26 Abs. 7 S. 2 KI-VO).

e) Informationspflicht bei Entscheidungen gegenüber natürlichen Personen

Betreiber von im Anhang III der KI-VO aufgeführten Hochrisiko-KI-Systemen (also etwa auch von derartigen Systemen, die am Arbeitsplatz eingesetzt werden) treffen Informationspflichten gegenüber natürlichen Personen. Der Betreiber informiert natürliche Personen darüber, dass ein Hochrisiko-KI-System sie betreffende Entscheidungen trifft oder bei solchen Entscheidungen Unterstützung leistet. Diese Information ist darauf gerichtet, dass diese natürlichen Personen unterrichtet werden, dass sie Gegenstand des Einsatzes des Hochrisiko-KI-Systems sind.

f) Sonstige Informationspflichten

Neben den Informationspflichten, die spezifisch die Betreiber von Hochrisiko-KI-Systemen betreffen, können noch weitere Transparenzpflichten für Betreiber gelten, die unabhängig von der Einordnung als Hochrisiko-KI-System bestehen. Dies betrifft etwa den Betrieb von Systemen zur Emotionserkennung oder Systemen zur biometrischen Kategorisierung (Art. 50 Abs. 3 KI-VO), KI-Systeme, die sogenannte Deepfakes in Bild-, Ton- oder Videoinhalten erzeugen oder manipulieren (Art. 50 Abs. 4 S. 1 KI-VO) oder den Betrieb von KI-Systemen, die Text erzeugen oder manipulieren, der veröffentlicht wird, um die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren (Art. 50 Abs. 4 S. 3 KI-VO).

6. Weitere Pflichten nach sonstigen Rechtsakten

a) Umsetzung sonstiger Rechtspflichten

Betreiber müssen neben der KI-VO sämtliche sonstigen einschlägigen Rechtspflichten nach dem Unionsrecht oder dem für sie geltenden nationalen Recht umsetzen (Art. 26 Abs. 3 KI-VO). Die KI-VO tritt neben solche sonstigen Rechtspflichten und ersetzt diese nicht.

b) Insbesondere: DSGVO-Pflichten

Bei Verarbeitung personenbezogener Daten mittels KI-Systemen muss der Betreiber zusätzlich sämtliche Pflichten nach der DSGVO erfüllen (vgl. Art. 26 Abs. 3 KI-VO), insbesondere Erlaubnistatbestände, Grundsätze, Erfüllung Betroffenenrechte, Dokumentationspflichten, Datensicherheit sowie Rechenschafts- und Kooperationspflicht.

c) Sonderregelung zur Datenschutz-Folgenabschätzung

Die Anbieter von Hochrisiko-KI-Systemen müssen den Betreibern in transparenter Weise Informationen bereitstellen. Dies betrifft insbesondere die gesetzlich vorgeschriebenen Betriebsanleitungen für Hochrisiko-KI-Systeme. Die Betreiber dieser Systeme verwenden die vom Anbieter bereitzustellenden transparenten Informationen, sofern sie verpflichtet sind, eine Datenschutz-Folgenabschätzung durchzuführen (Art. 26 Abs. 9 KI-VO). Bei dem Einsatz von Hochrisiko-KI-Systemen dürfte eine solche Rechtspflicht zur Durchführung einer Datenschutz-Folgenabschätzung in aller Regel vorliegen. Eine Besonderheit ergibt sich im Rahmen der Grundrechte-Folgenabschätzung (Art. 27 KI-VO). Hat der Betreiber des Hochrisiko-KI-Systems bereits eine Datenschutz-Folgeabschätzung gemäß Art. 35 DSGVO oder Art. 27 der Richtlinie (EU) 2016/680 durchgeführt und erfüllt diese teilweise die Anforderung der Grundrechte-Folgenabschätzung nach Art. 27 KI-VO, muss die Datenschutz-Folgeabschätzung nur noch gemäß Art. 27 Abs. 4 KI-VO ergänzt werden.

7. Kooperationspflichten

Betreiber arbeiten mit den zuständigen nationalen Behörden bei allen Maßnahmen zusammen, die diese Behörden im Zusammenhang mit dem vom Betreiber eingesetzten Hochrisiko-KI-System zur Umsetzung der KI-VO ergreifen (Art. 26 Abs. 12 KI-VO). Diese Kooperationspflichten betreffen oftmals vor allem die auf nationaler Ebene eingerichteten Marktüberwachungsbehörden. Sie gelten zudem unabhängig von sonstigen Rechtspflichten zur Kooperation mit anderen Behörden, etwa mit Datenschutzbehörden im Rahmen von Art. 31 DSGVO bei der Verarbeitung personenbezogener Daten.

IV. Handlungsempfehlungen für Betreiber von Hochrisiko-KI-Systemen

Unternehmen sind gut beraten, die auf sie zukommenden Anforderungen nach der KI-VO zeitnah zu identifizieren und in ihrer weiteren Planung zu berücksichtigen. Angesichts der Komplexität der anstehenden Aufgaben bleibt dafür nicht allzu viel Zeit. Die Fristen für die Umsetzung der Vorgaben der KI-VO sind gestaffelt. Einige dieser Vorgaben gelten bereits nach sechs Monaten (Art. 113 lit. a KI-VO verweist auf die Kapitel I und II der KI-VO, also auf Art. 1 bis Art. 5 KI-VO). Dies betrifft etwa das Verbot unzulässiger KI-Praktiken (Art. 5 KI-VO). Auch die Verpflichtung, Personen, die mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, ein ausreichendes Maß an KI-Kompetenz zu vermitteln, gilt bereits nach sechs Monaten. Andere Verpflichtungen gelten zwölf, 24 oder 36 Monate nach dem Datum des Inkrafttretens der KI-VO. Auch wenn die Pflichten für Betreiber von Hochrisiko-KI-Systemen erst ab dem 2.8.2027 gelten, ist dieser Zeitraum für die Anpassung der KI-Strategie vieler Unternehmen und die Umsetzung erforderlicher Maßnahmen nicht zu lang bemessen.

Diese Zeit sollten Unternehmen nutzen, um ihre KI-Strategie möglichst zeitnah an die bald geltenden Vorgaben anzupassen. Hierfür sollte man künftig geltende Verpflichtungen anhand des vorstehenden Überblicks identifizieren und Maßnahmen zu deren Umsetzung planen. Nach Möglichkeit sollte man dabei auf bereits im Unternehmen bestehende Prozesse aufsetzen. So eignen sich etwa besonders die Prozesse und Strukturen zur Erfüllung der sogenannten Betroffenenrechte nach Art. 12 ff. DSGVO auch zur Umsetzung entsprechender Vorgaben der KI-VO.

V. Checkliste: Pflichten für Betreiber von Hochrisiko-KI-Systemen

BB-Checkliste

Schulungspflicht

- Training KI-Kompetenz? Training von Aufsichtspersonen

Operative Pflichten

- Technische und organisatorische KI-Maßnahmen

Befugnisse für Aufsichtspersonen

- Qualitätsmanagement Eingabedaten
- Aussetzung des Betriebs bei Risiko nach 79 Abs. 1 KI-VO

Kontrollpflichten

- Vorprüfung verbotener Praktiken im Sinne von Art. 5 KI-VO
- Aufsicht durch natürliche Personen
- Kontrolle von Eingabedaten
- Kontinuierliche Überwachung
- Prüfung der Voraussetzungen von zusätzlichen Pflichten als Anbieter
- Prüfung der Notwendigkeit einer Grundrechte-Folgenabschätzung

Dokumentationspflichten

- Aufbewahrung von Protokollen
- Dokumentations- und Aufbewahrungspflichten nach anderen Rechtsvorschriften, z. B. DSGVO

Informationspflichten

- Informationspflichten gegenüber Anbietern

- Informationspflichten bei Risiken
- Informationspflichten bei schwerwiegenden Vorfällen
- Informationspflichten gegenüber Arbeitnehmern und ihren Vertretern
- Informationspflicht bei Entscheidungen gegenüber natürlichen Personen
- Sonstige Informationspflichten, etwa nach Art. 13, 14 DSGVO

Pflichten nach sonstigen Rechtsakten

- Umsetzung sonstiger Rechtspflichten
- DSGVO-Pflichten
- Datenschutz-Folgenabschätzung

Kooperationspflichten

- Kooperation mit nationalen Behörden nach der KI-VO
- Kooperation mit Behörden nach anderen Rechtsvorschriften, z. B. DSGVO

Tim Wybitul, RA/FAArbR und CIPP/E, ist Partner der Sozietät Latham & Watkins LLP in Frankfurt a.M. Er berät umfassend im Digital- und Datenrecht, z. B. zur DSGVO und zur KI-Verordnung. Insbesondere verteidigt er Unternehmen in Bußgeldverfahren und sonstigen gerichtlichen oder verwaltungsrechtlichen Verfahren im Datenschutz.



Dr. Thomas Bloch und Marcel Krause*

Pension Buy-out im M&A-Kontext

Pensionsverpflichtungen sind regelmäßig Thema in M&A-Transaktionen. In den meisten Transaktionen sind sie „nur“ ein Bewertungsthema, sie können aber auch ein Transaktionshindernis darstellen. Die Auslagerung von Pensionsverpflichtungen auf eine (externe) Rentnergesellschaft – analog zum Pension Buy-out in angelsächsischen Märkten – kann dann eine Lösung bieten. Der Beitrag erläutert die Funktionsweise dieses Pension Buy-outs und dessen Integration in einen M&A-Prozess.

I. Einleitung

Pensionsverpflichtungen der betrieblichen Altersversorgung (bAV) sind immer wieder Thema in M&A-Transaktionen.

In den meisten Transaktionen sind Pensionsverpflichtungen „nur“ ein Bewertungsthema: In der Unternehmensbewertung hat es sich seit vielen Jahren etabliert, dass Pensionsverpflichtungen wie Finanzverbindlichkeiten behandelt und entsprechend bei der Bestimmung des Wertes für das Eigenkapital bzw. den Kaufpreis vom Unternehmenswert abgezogen werden. Die Diskussion begrenzt sich in vielen Fällen auf den anzuwendenden Rechnungszins, also die Wahl des marktnahen IFRS-Rechnungszinses, versus dem durchschnittlichen Marktzins der vergangenen zehn Geschäftsjahre gemäß HGB. Teilweise und insbesondere in Folge der zwischenzeitlich hohen Inflation werden auch ein etwaiger Anpassungsstau hinsichtlich anstehender Rentenerhö-

hungen oder auch entstandene Deckungslücken, z. B. bei Rückdeckungsversicherungen oder Durchführungswegen wie der Pensionskasse, berücksichtigt. Weitere Ergebnisse einer Pension Due Diligence, die sich aktuell zu einem festen Bestandteil der Due Diligence etabliert hat, werden durch eher pauschale Bewertungsanpassungen oder Garantien adressiert. Wesentliche Pensionsrisiken wie Langlebigkeit oder bei bestehenden Deckungsvermögen inhärente Kapitalanlagerisiken werden teilweise gar nicht detailliert betrachtet. Das ist meist damit zu begründen, dass Pensionsverpflichtungen im Gesamtkontext einer M&A-Transaktion eine untergeordnete Rolle spielen, das Eintauchen in eine zu hohe Komplexität den Ausgang des M&A-Prozesses gefährden könnte bzw. manche Risiken noch nicht standardmäßig in der eigentlich notwendigen Tiefe beleuchtet werden.

In einigen M&A-Transaktionen haben Pensionsverpflichtungen dann aber sehr wohl das Potential, das Ergebnis eines Transaktionsprozesses zu beeinflussen oder sogar zu gefährden.

Dies ist meist dann der Fall, wenn im Verhältnis zum Unternehmenswert oder der Bilanzsumme die Pensionsverpflichtungen sehr hoch sind. Entsprechend der Größe stellen sich Fragen hinsichtlich der Bilanzstruktur, Auswirkungen zukünftiger Bilanzschwankungen und

* Dieser Beitrag basiert auf einem Vortrag, den der Verfasser Bloch am 23.1.2024 auf der M&A-Konferenz des Betriebs-Berater in Düsseldorf gehalten hat.