Neue KI-Gesetze und wie man sich bereits jetzt vertraglich absichern kann

Seit wenigen Wochen steht nun fest: das europäische Gesetz über Künstliche Intelligenz, der *AI Act*"(„KI-VO"), kommt. Seit der Verkündung einer Einigung am 8. Dezember 2023 in den Trilogverhandlungen scheint eine Verabschiedung der KI-VO noch vor dem Ende der Legislaturperiode und den Europawahlen im Juni 2024 realistisch. Noch ist der genaue Inhalt der KI-VO zwar nicht bekannt - vielmehr wird auf die Entwürfe von Kommission und Rat sowie über Parlamentarier bekanntgewordene Informationen bzgl. der getroffenen Einigung zurückgegriffen -, aber schon jetzt besteht großer Handlungsbedarf.

Der EU-Gesetzgeber hat es sich zum Ziel gemacht, in einer umfassenden Abwägung der Chancen und Risiken des Einsatzes von KI in verschiedensten Feldern neue regulatorische Standards für den Umgang von KI-Systemen zu setzen. Neben der allgemeineren KI-VO soll eine speziellere KI-Haftungs-Richtlinie verabschiedet werden. Mit diesen beiden zentralen Gesetzgebungsvorhaben ändern sich die rechtlichen Rahmenbedingungen für Hersteller, Händler und Nutzer von KI-Systemen weitgehend – in den folgenden Ausführungen soll daher dargestellt werden, welche Erfahrungen wir bisher bei Verträgen über die Entwicklung sowie der Lizenzierung von KI-Systemen gemacht haben. Schon jetzt wirkt sich die zu erwartenden KI-Regulierung im (IT-)Vertragsrecht aus.

Der allgemeine Rahmen: Die KI-Verordnung

Die KI-VO setzt grundlegende Rahmenbedingungen für den Betrieb von KI-Systemen in verschiedenen Wirtschaftssektoren und unter verschiedenen Nutzungsbedingungen und wird den weltweit ersten Regulierungsansatz mit explizitem KI-Bezug darstellen. Dabei verfolgt die EU einen risikobasierten Ansatz. Während der Einsatz von KI-Systemen unter gewissen Umständen aufgrund von Risikoerwägungen mit Bezug auf Sicherheits- und Grundrechtsgefährdungen von vornherein verboten werden soll, werden die zulässigen KI-Systeme je nach Risikopotenzial Ihrer konkreten Anwendung kategorisiert. Dies hat zur Folge, dass diejenigen KI-Anwendungen, die aufgrund Ihrer Anwendung in hochsensiblen bzw. kritischen Anwendungsgebieten als sog. Hochrisiko-Systeme (Art. 6 ff. KI-VO-Entwurf („KI-VO-E")) eingestuft werden, der umfassendsten Regulierung ausgesetzt sind. Hochrisiko-Systeme unterfallen weitgreifenden Pflichten in punkto Compliance und Risikomanagement, die sich aus der KI-VO-E ergeben.

In Titel III, Kapitel 2 KI-VO-E werden Anforderungen an Hochrisiko-Systeme aufgelistet, die von Herstellern und Entwicklern dieser Systeme eingehalten werden müssen.

Hochrisiko-Systeme müssen demnach bereits so konzipiert sein, dass bereits mit Beginn ihrer Entwicklung ein Risikomanagement-System eingerichtet wird. Es müssen konkrete Maßnahmen festgelegt werden zu: (i) Ermittlung der Risiken, (ii) Bewertung der Risiken, (iii) Beseitigung, Verringerung der Risiken. Zudem müssen die Systeme so konzipiert sein, dass sie von Menschen hinreichend beaufsichtigt werden können, dass sie transparent betrieben werden können und ihr Betrieb dokumentiert werden kann. Weiterhin existieren strenge Anforderungen an die verwendeten Trainingsdaten sowie daran, dass die Systeme robust, genau und (cyber-)sicher konzipiert sein müssen.

Diese o.g. Anforderungen betreffen das Hochrisiko-System als solches. Erst Titel III, Kapitel 3 legt fest, inwieweit der Anbieter, also das letzte Glied in der Wertschöpfungskette vor dem Nutzer der KI, für diese Anforderungen einzustehen hat. Als Anbieter einer KI, welcher nicht selbst Hersteller dieser ist, scheint es hier ratsam, vertraglich eine unbeschränkte Haftung des KI-Auftragnehmers für den Fall, dass die KI die in Titel III, Kapitel 2 des KI-VO-E genannten Anforderungen nicht erfüllt, zu vereinbaren.

Derartige vertragliche Regelungen könnten sich an der branchenüblichen unbeschränkten Haftung für die Verletzung von "Datenschutzgesetzen" orientieren. Damit Hand in Hand könnte etwa eine vertraglich vereinbarte Freistellung und Schadloshaltung durch den Auftragnehmer bei Verstößen gegen die o.g. Anforderungen an die KI selbst gehen. Lässt der Anbieter eine KI-Lösung extern entwickeln, sollte die Erfüllung der gesetzlichen Anforderungen an das Hochrisiko-System bereits in die Produktbeschreibung aufgenommen werden und so zu einer Hauptvertragspflicht gemacht werden. Ohne vertragliche Verpflichtung des Herstellers könnte man dem Anbieter, der die KI-Lösung in Auftrag gibt schon einen Verstoß gegen Art. 16 KI-VO-E vorwerfen („*Anbieter von Hochrisiko-KI-Systemen müssen sicherstellen, dass ihre Hochrisiko-KI-Systeme die Anforderungen in Kapitel 2 dieses Titels erfüllen*.“).

Zu beachten ist jedoch stets, dass der Anbieter eines Hochrisiko-Systems der Adressat von Verpflichtungen des Titel III Kapitels 3 des KI-VO-E bleibt. Durch die vertragliche Verlagerung der Pflichten an den Hersteller/Auftragnehmer kann sich der Anbieter hiervon nicht befreien, das „*enforcement*“-Risiko bleibt also beim Anbieter. Ein Grund mehr, dafür zu sorgen, dass nur das kontrollierbare Risiko eines Verstoßes gegen die KI-VO-E auch von diesem getragen werden muss. Nimmt man bspw. die Pflicht des Art. 20 KI-VO-E, zur Aufbewahrung der Protokolle, welche die KI automatisch erstellt, liegt auf der Hand, dass ein Anbieter dieser Pflicht nicht nachkommen kann, wenn das KI-System nicht so konzipiert ist, dass es den Aufzeichnungspflichten gem. Art. 10 KI-VO-E nachkommen kann. Nach außen bleibt zwar auch hier der Anbieter verantwortlich, im Innenverhältnis hat er jedoch regelmäßig keinen Einfluss darauf, ob diese Anforderungen erfüllt werden können und sollte sich vertraglich absichern.

Dies kann an folgendem Beispiel veranschaulicht werden: Ein Unternehmen erweitert seine an Ärzte und Krankenhäuser vertriebenen Softwarelösung um ein KI-System zur Unterstützung von Diagnosevorgängen. Dieses System lässt er von einem KI-Start-Up entwickeln und trainieren. Der Entwicklungsvertrag mit dem KI-Entwickler sollte neben Regelungen zur KI-VO-Konformität Regelungen dazu enthalten, wer für die Einhaltung der Anforderung an Medizinprodukte verantwortlich ist. Aus der Einordnung als ein Medizinprodukt im Sinne der Verordnung (EU) 2017/745 über Medizinprodukte ergibt sich überhaupt erst die Einstufung als Hochrisiko-System gem. Art. 6 Abs. 1 lit. a KI-VO-E.

Das Vertragswerk mit dem KI-Entwickler sollte zudem explizit festhalten, dass der Hersteller für die Einhaltung der Verpflichtungen der Art. 6 ff. KI-VO-E für Hochrisiko-Systeme im Innenverhältnis allein verantwortlich ist: zum einen um zu dokumentieren, dass der Anbieter sicherstellt, dass die KI-Lösung mit Titel III, Kapitel 2 konform ist und darüber hinaus, damit der Anbieter für nicht in seiner Kontrolle liegende (Folge-)Pflichtverstöße kein finanzielles Risiko übernimmt.

Darüber hinaus können auch die Nutzer einer künstlichen Intelligenz Pflichten nach der KI-VO treffen. Daher ist es ratsam, diese Haftungsstruktur auch im Rahmen der vertraglichen Vereinbarungen mit dem Nutzer des KI-Systems festzuhalten. Hier sollte darauf verwiesen werden, dass der Anbieter im Verhältnis zum Endnutzer nicht für die von dem Hersteller zu leistende Komponenten zuständig ist. Es muss jedoch sorgfältig geprüft werden, inwieweit hier überhaupt eine Abschichtung möglich ist. Dies gilt, insbesondere wenn es sich bei den Endnutzern um Verbraucher und nicht wie vorliegend um Unternehmer handelt.

Noch wichtiger dürfte es sein, gegenüber den Endnutzern klar und transparent festzulegen, dass sämtliche Verstöße gegen die in Art. 29 KI-VO-E vorgeschriebenen Pflichten des Nutzers eines Hochrisiko-Systems, nicht zu Lasten des Anbieters /Unternehmens geht.

Wenn es ernst wird: Die KI-Haftungs-RL und die Neufassung der Produkthaftungs-RL

Weitere Gesetzesvorhaben, welche für die Vertragsgestaltung im Zusammenhang mit der Lizensierung und dem Vertrieb von KI-Systemen zu berücksichtigen sein werden, sind die KI-Haftungs-RL (zum Entwurf) und die Novelle der Produkthaftungs-RL (zum Entwurf). Die Ungewissheit über Haftungsfragen im Zusammenhang mit KI-Systemen zählt laut einer repräsentativen Umfrage aus dem Jahre 2020 zu den drei wichtigsten externen Hindernissen für eine betriebliche Anwendung von KI-Systemen in europäischen Unternehmen. Alles Wissenswerte zu den neuen (KI-) Haftungsregeln haben wir im Detail bereits hier für Sie zusammengefasst.

Der derzeitige Richtlinienvorschlag enthält zwei wesentliche Elemente: Zum einen sollen Geschädigte aufgrund der Kausalitätsvermutung von der Pflicht entbunden werden, die Ursächlichkeit des Schadens darzulegen, der aus der Anwendung einer fehlerhaften KI entstanden ist. Zudem soll bei Schäden durch Hochrisiko-KI-Systeme, im Sinne der KI-VO-E der Zugang zu Beweismitteln erleichtert werden, die sich im Besitz von Unternehmen oder KI-Anbietern befinden. So wird einem Anspruchsteller unter der Voraussetzung, dass der gestellte Anspruch als „plausibel“ bewertet werden kann, ein Auskunftsrecht über die Arbeitsweise des Hochrisiko-KI-Systems zugesprochen, um dem Betroffenen eine Darlegung des tatsächlichen Bestehens dieses Anspruches zu ermöglichen. Zuvor muss der Anspruchsteller jedoch nachweisen, alle angemessenen Anstrengungen unternommen zu haben, um die begehrten Informationen vom Beklagten/Unternehmen zu erhalten. Kommt der KI-Anbieter dieser, aufgrund der Plausibilität des Anspruchs entstandenen Auskunftspflicht nicht nach, führt dies zu einer Beweislastverlagerung auf den KI-Anbieter, der in der Folge beweisen muss, dass der entstandene Schaden nicht innerhalb seines Verantwortungsbereiches seinen Ursprung hat.

Diese, im Fall eines Schadensersatzprozesses anwendbaren Sonderregelungen sollten bereits bei der Entwicklung/Beauftragung von KI-Lösungen mitgedacht werden. Ein Unternehmen, welches eine extern entwickelte KI-Lösung in seine (Software-) Produkte einbaut, unterliegt gegenüber seinen Endkunden den o.g. Regelungen der Beweiserleichterung und Informationspflichten. Zwar hilft dem Anbieter hier bereits die KI-VO, welche vorschreibt, dass die KI Dokumentation und Proto-kolle erstellen können muss. Gerade bei einer fehlerhaften KI, die nicht den Anforderungen der KI-VO-E entspricht, ist jedoch nicht sichergestellt, dass der Anbieter den Informationsansprüchen aus der Produkt/-KI-Haftungs-RL selbstständig und ohne Mithilfe des KI-Entwicklers nachkommen kann. Hier sollten daher z.B. Vereinbarungen dahingehend getroffen werden, dass der Entwickler bei sämtlichen Ansprüchen unterstützt und im Zweifel dafür haftet, wenn sich aus der durch ihn verursachten Nicht-erfüllung als Konsequenz eine Beweislastumkehr zu Lasten des Anbieters ergibt. Es sollten daher Regelungen dazu aufgenommen werden, welche Informationen der Anbieter vom Entwickler im konkreten Fall mindestens verlangen kann und welche Informationen im Hinblick auf mögliche „Black-Box-Situation“ technisch gar nicht heraus-gegeben werden können. Da solche Informationen teils Geschäftsgeheimnisse des die KI entwickelnden Unternehmens enthalten können, ist mit Widerstand von KI-Entwicklern in Vertragsverhandlungen zu rechnen. Das Auftraggeber-Unternehmen wird hier versuchen, dem Entwickler die Übernahme von Garantien (also verschuldensunabhängige Haftungs-verpflichtungen) für die Unterstützung und Hilfe bei der Beantwortung von Anfragen gemäß der AI-Haftungsrichtlinie, abzuringen. Die KI-Unternehmen dürften an möglichst konkret formulierten Aus-nahmen von ihrer Auskunfts- und Mitwirkungspflicht interessiert sein. Im Ergebnis liegt es jedoch im gemeinsamen Interesse beider Parteien eine Kompromiss-Lösung zu finden, um Rechtssicherheit zu schaffen um Schadensansprüchen von potenziellen Geschädigten möglichst effektiv und nachhaltig begegnen zu können.

Where the money lies… Rechte an Input und Output

Bisher enthalten die EU-Gesetzesvorhaben keine Regelungen zu den Rechten an Input und Output von KI-Lösungen. Auch das geltende Immaterialgüterrecht, insbesondere das Urheberrecht, schützt den In- und Output nicht umfassend und interessengerecht. Dabei liegt gerade hier der, vor allem kommerzielle, Wert vieler KI-Lösungen. Aus diesem Grund ist es maßgeblich in Verträgen über die Lizenzierung oder Entwicklung von KI-Lösungen schuldrechtliche Regelungen zu den Rechten an den durch die KI erzeugten Ergebnissen zu treffen. Zu regelnde Fragen sind etwa: Wer trägt die Verantwortung für die Vollständigkeit und die Richtigkeit des Outputs? Wer trägt – im Verhältnis zwischen den Vertragsparteien – die Verantwortung für die Diskriminierungsfreiheit des Outputs? Wer darf den Output wie weiter verwerten?

Ebenso relevant sind die Nutzungsrechte an den Daten, mit denen die KI trainiert wird. Der Auftragnehmer, welche eine KI-Lösung für ein Unternehmen als Kunden entwickelt wird regelmäßig ein großes Interesse daran haben, mit den (anonymisierten) Daten auch weitere KI-Lösungen, die er (als Standardsoftware) entwickelt, trainieren zu können. Für den Auftraggeber stellen sich dabei die Fragen, ob die (personenbezogenen) Daten und Geschäftsgeheimisse, welche er der Entwicklung beisteuert, hinreichend geschützt sind und auch, ob er an der Weiternutzung und Kommerzialisierung dieser Daten ausreichend finanziell beteiligt wird.

Neben Regelungen zu Input und Output sollte auch ein besonderer Wert auf Geheimhaltungsklauseln gelegt werden, die explizit die Bestandteile erfassen, die urheberrechtlich nicht geschützt werden, wie beispielsweise das KI-Modell, sowie den Verlauf und die Ergebnisse einer Anlernphase.

Wie geht man vor?

Bereits jetzt können aber durch die Berücksichtigung der einschlägigen Regulierungen zahlreiche Pflichten, die innerhalb der Wertschöpfungskette unter verantwortungsbewussten Akteuren eine Rolle spielen, identifiziert und angemessen zugeteilt werden. Eine Orientierung an den in den Regulierungen festgesetzten Pflichten ist hier dringend zu empfehlen. Es bleibt jedoch weiter abzuwarten, wie die konkreten Gesetzestexte der KI-Regulierungen letztendlich ausgestaltet werden und inwiefern wirksam von der gesetzgeberisch vorgesehenen Risikoverteilung abgewichen werden kann. Unter Umständen können für langfristige Projekte Vertragsanpassungen erforderlich sein, welche bereits jetzt durch Öffnungsklauseln gesichert werden können. Aus Kundensicht ist es ist zudem zu empfehlen, auf allgemeine Garantie über die Einhaltung der einschlägigen Gesetzesvorschriften (u.U. mit Nennung dieser Vorschriften) in den Vertrag aufzunehmen. Zudem sollten Unternehmen, welche KI-Lösungen in ihre Produkte integrieren, unbedingt urheberrechtliche und geheimnisschutzrechtliche Fragen identifizieren und diese vertraglich beantworten, sowie gegebenenfalls mit Vertragsstrafen und Freistellungsverpflichtungen bei Verstößen zu verbinden.

Kontaktieren Sie uns

Frauke Tepe
Associate

T +49 221 5108 4007
frauke.tepe@osborneclarke.com

Lucas Mayr
Associate

T +49 221 5108 4168
lucas.mayr@osborneclarke.com