Sara Dokmanac, Joana Günther

III. Künstliche Intelligenz in der radiologischen Diagnostik: Rechtliche Aspekte

1. Allgemeine regulatorische Einbettung

Künstliche Intelligenz (KI) birgt im Gesundheitswesen ein enormes Innovationspotenzial. Sie kann wesentlich dazu beitragen, diagnostische und therapeutische Verfahren zu verbessern, Abläufe effizienter zu gestalten und damit die Versorgungsqualität insgesamt zu erhöhen. Sowohl bei der Auswertung medizinischer Bilddaten, der Analyse großer Datenmengen zur Krankheitsfrüherkennung oder in der Entwicklung personalisierter Behandlungsansätze, etwa personalisierter Therapiekonzepte, kann KI medizinische Prozesse nicht nur beschleunigen, sondern auch qualitativ aufwerten. Gleichzeitig wirft der Einsatz von KI-Systemen grundlegende rechtliche und regulatorische Fragestellungen auf, die sowohl Entwickelnde als auch Anwendende vor erhebliche Herausforderungen stellen. In Deutschland fehlt es bislang an einem einheitlichen, speziell auf den Einsatz von KI im Gesundheitswesen zugeschnittenen Regelwerk. Stattdessen besteht ein komplexes Zusammenspiel unterschiedlicher Normen, darunter insbesondere zivilrechtliche, datenschutzrechtliche und haftungsrechtliche Vorschriften. Relevante Rechtsgrundlagen sind unter anderem die Bundesdatenschutzgesetz (BDSG), das Medizinprodukterecht (MPG), das Produkthaftungsgesetz (ProdHaftG) sowie berufsrechtliche Regelungen. Diese fragmentierte Rechtslage führt in der Praxis häufig zu Unsicherheiten und Auslegungsproblemen.

KI-basierte Anwendungen, die als Medizinprodukte einzuordnen sind, unterliegen bislang der europäischen Medizinprodukteverord-

nung[1] (im Folgenden: MP-VO). Diese definiert grundlegende Anforderungen an Sicherheit, Leistungsfähigkeit und klinische Bewertung, berücksichtigt jedoch nicht die spezifischen Charakteristika von KI-Systemen – etwa ihre Komplexität, den autonomen Entscheidungscharakter oder die fehlende Nachvollziehbarkeit von Entscheidungswegen (Black-Box-Problematik).

Vor diesem Hintergrund legte die Europäische Kommission bereits im April 2021 den Entwurf für eine Verordnung zur Regulierung Künstlicher Intelligenz vor. Die am 13. Juni 2024 verabschiedete Verordnung zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz[2] (KI-Verordnung, im Folgenden: KI-VO) ergänzt das bestehende europäische Rechtsgefüge sowohl sektorübergreifend als auch sektorspezifisch. Ihr Ziel ist es, den rechtlichen Rahmen für den Einsatz von KI in der Europäischen Union zu harmonisieren und insbesondere in sensiblen Bereichen – wie dem Gesundheitswesen – ein hohes Maß an Sicherheit, Transparenz und Grundrechtskonformität zu gewährleisten.

2. KI-Verordnung

2.1 Vorab: Forschungsprivileg

Im gesundheitsbezogenen Kontext, in dem Forschung und Entwicklung eng miteinander verzahnt sind, spielt das sog. Forschungsprivileg eine Rolle. Bevor auf die konkreten Regelungen der Verordnung eingegangen wird, soll dieser Ausnahmebereich daher zunächst grob skizziert werden. Unter einem Forschungsprivileg versteht

1 Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates, (ABl. L 117 S. 1, 2019 L 117 S. 9, L 334 S. 165; 2021 ABl. L 241 S. 7).

2 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), (ABl. L 2024/1689, 12.7.2024).

man eine gesetzlich verankerte Ausnahme oder Sonderregelung, die wissenschaftliche Forschungstätigkeiten ganz oder teilweise von bestimmten rechtlichen Anforderungen ausnimmt (Martini & Wendehorst/*Wendehorst*, 2024, Art. 2 Rn. 83 f.). Ziel solcher Regelungen ist es, die wissenschaftliche Freiheit zu wahren und Innovationen nicht durch übermäßige regulatorische Hürden zu hemmen. Auch die KI-VO enthält entsprechende Ausnahmen zugunsten der wissenschaftlichen Forschung. Nach Art. 2 Abs. 6 KI-VO findet die Verordnung keine Anwendung auf KI-Systeme, die ausschließlich zum Zweck der wissenschaftlichen Forschung und Entwicklung in Betrieb genommen werden. Sobald ein KI-System für andere – insbesondere kommerzielle oder operative – Zwecke eingesetzt wird, greift das Privileg nicht mehr, und das System unterfällt in vollem Umfang den Anforderungen der KI-VO. Darüber hinaus stellt Art. 2 Abs. 8 KI-VO klar, dass Forschungs-, Test- und Entwicklungstätigkeiten zu KI-Systemen oder KI-Modellen vor Inverkehrbringen oder Inbetriebnahme grundsätzlich nicht unter die Verordnung fallen, vorausgesetzt es handelt sich um Tests unter Realbedingungen. Ziel ist es, frühe Entwicklungsphasen von KI-Systemen nicht durch die umfangreichen Vorgaben der Verordnung zu erschweren.

Die Privilegierung wissenschaftlicher Forschung ist weder im europäischen noch im nationalen Recht ein neues Konzept. So sieht etwa § 2 Abs. 2 Nr. 1 Gendiagnostikgesetz (im Folgenden: GenDG) vor, dass das Gesetz nicht für genetische Untersuchungen und Analysen sowie den Umgang mit genetischen Proben und Daten zu Forschungszwecken gilt. Auch das Datenschutzrecht enthält entsprechende Öffnungsklauseln: Art. 89 DSGVO eröffnet den Mitgliedstaaten die Möglichkeit, für wissenschaftliche, historische oder statistische Zwecke besondere Regelungen vorzusehen. Von dieser Öffnungsklausel hat der deutsche Gesetzgeber mit § 27 BDSG Gebrauch gemacht. Die Norm konkretisiert damit die Anforderungen und Voraussetzungen für die Verarbeitung insbesondere besonderer Kategorien personenbezogener Daten im Rahmen wissenschaftlicher Forschung und ergänzt so den unionsrechtlichen Rahmen durch spezifische nationale Vorgaben. Abweichend von Art. 9 Abs. 1 DSGVO kann eine solche Verarbeitung auch ohne Einwilligung der betroffenen Person zulässig sein, soweit sie erforderlich ist und das Interesse der verantwortlichen Stelle an der Verarbeitung das schutzwürdige Interesse der betroffenen Person erheblich überwiegt.

Gemäß Erwägungsgrund Nr. 159 DSGVO ist der Forschungsbegriff dabei weit auszulegen, um dem großen Erkenntnispotential der Auswertung und Erforschung gesundheitsbezogener Daten im Hinblick auf Krankheitsverläufe, Therapien und die Versorgungspraxis Rechnung zu tragen (Spitz, et. al, 2021). Zwar enthält die KI-VO – anders als die DSGVO in Erwägungsgrund Nr. 159 – keinen ausdrücklichen Verweis auf die in Art. 179 AEUV (Vertrag über die Arbeitsweise der Europäischen Union) formulierte Idee eines europäischen Forschungsraums, dennoch ist Art. 2 Abs. 6 KI-VO gleichermaßen in diesem Sinne auszulegen (Spitz, 2025).

Die Privilegierung der Forschung im Rahmen der KI-VO zielt darauf ab, die wissenschaftliche Freiheit zu schützen und Europa als innovationsfreundlichen Standort für digitale Technologien zu stärken (Martini & Wendehorst/*Wendehorst*, 2024, Art. 2 Rn. 73).

2.2 Ziele der Verordnung

Ausgangspunkt der folgenden Betrachtung ist die Zielsetzung der Verordnung. Bereits in Erwägungsgrund Nr. 1 KI-VO heißt es:

> »Zweck dieser Verordnung ist es, das Funktionieren des Binnenmarkts zu verbessern, indem ein einheitlicher Rechtsrahmen insbesondere für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen künstlicher Intelligenz (KI-Systeme) in der Union im Einklang mit den Werten der Union festgelegt wird […]«.

Zwar existieren für die verschiedenen rechtlichen Teilbereiche – etwa das Medizinprodukterecht, das Berufsrecht oder das Haftungsrecht – bereits einschlägige Rechtsnormen. Diese enthalten jedoch bislang keine spezifischen Regelungen für den Einsatz von KI. Mit der KI-VO wird nun erstmals eine sektorübergreifende und zugleich horizontal wirkende Regulierung für Künstliche Intelligenz in Europa angestrebt. Zu diesem Zweck legt die Verordnung einheitliche harmonisierende Anforderungen, insbesondere im Hinblick auf das Inverkehrbringen und die Inbetriebnahme von KI-Systemen, für alle Sektoren fest. Ein zentrales Leitmotiv ist hierbei die Stärkung des Binnenmarktes, der sowohl Rechtssicherheit als auch fairen Wettbewerb fördern soll.

Darüber hinaus verfolgt die KI-VO gemäß Art. 1 KI-VO das Ziel, das Vertrauen in KI zu stärken und gleichzeitig ein hohes Schutzni-

veau in Bezug auf Gesundheit, Sicherheit und die in der Charta verankerten Grundrechte – einschließlich Demokratie, Rechtsstaatlichkeit und Umweltschutz – vor schädlichen Auswirkungen von KI-Systemen in der Union zu gewährleisten. Dabei sollen Innovationen gezielt gefördert werden, während zugleich betont wird, dass KI stets im Dienste des Menschen eingesetzt werden soll und diesen weder ersetzen noch kontrollieren darf, sog. menschenzentrierte KI (Erwägungsgrund Nr. 1, 6, 8 und 27 KI-VO).

Der Begriff des KI-Systems wird in Art. 3 Nr. 1 KI-VO legal definiert als:

> »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.«

Angesichts der wachsenden Bedeutung von KI soll sichergestellt werden, dass KI-Systeme verantwortungsvoll, sicher und grundrechtskonform entwickelt und eingesetzt werden. Ein besonderes Augenmerk liegt dabei auf der Vermeidung von Verzerrungen durch fehlerhafte oder einseitige Trainingsdaten (sog. Bias) und daraus resultierenden Diskriminierungspotenzialen. Die menschliche Kontrolle bleibt darüber hinaus auch bei KI-gestützten Entscheidungen substanziell. Insgesamt verfolgt die KI-VO einen Regulierungsansatz, der darauf abzielt, harmonisierende Vorgaben für die Verwendung von KI in der europäischen Union zu schaffen und Europa als zentralen Standort für KI zu etablieren.

2.3 Risikobasierter Ansatz

2.3.1 Grundkonzept

Das zentrale Regelungskonzept der KI-VO ist der risikobasierte Ansatz. Die KI-VO bestimmt die regulatorischen Anforderungen in Abhängigkeit des jeweiligen Gefährdungspotenzials eines KI-Systems. Art und Inhalt der Vorschriften richten sich dabei nach Intensität und Umfang der Risiken, die von dem KI-System ausgehen: Je höher das Risiko für die Gesundheit, Sicherheit oder die Grundrechte von

Personen, desto strenger die Anforderungen. Zu diesem Zweck unterteilt die Verordnung KI-Systeme in vier Risikokategorien: unannehmbares Risiko, hohes Risiko, beschränktes Risiko und minimales Risiko.

KI-Systeme, die nach Einschätzung des europäischen Gesetzgebers ein unannehmbares Risiko für die Sicherheit oder die Grundrechte von Personen darstellen, sind gemäß Art. 5 KI-VO grundsätzlich verboten. Davon werden KI-Systeme umfasst, die Techniken der unterschwelligen Beeinflussung oder manipulative, täuschende Techniken einsetzen, um das Verhalten einer Person wesentlich zu ändern und ihr erheblichen Schaden zuzufügen (Art. 5 Abs. 1 lit. a). Darüber hinaus sind KI-Systeme umfasst, die Schutzbedürftige ausnutzen (Art. 5 Abs. 1 lit. b) sowie soziale Bewertungen durchführen (Art. 5 Abs. 1 lit. c). Hierzu zählen insbesondere Systeme, die auf manipulative Weise Einfluss auf das Verhalten oder die Entscheidungsfreiheit von Personen nehmen und dadurch mit hinreichender Wahrscheinlichkeit erheblichen Schaden verursachen können, beispielsweise das »Social Scoring«. Im medizinischen Bereich finden derartige Systeme in der Regel keine Anwendung. Den normativen Kern der Verordnung bilden die Hochrisiko-KI-Systeme im Sinne von Art. 6 KI-VO, die auch den Großteil der medizinischen KI-Anwendungen ausmachen. Diese Kategorie umfasst Systeme, deren Einsatz in sicherheitskritischen oder grundrechtsrelevanten Kontexten erfolgt – darunter insbesondere kritische Infrastrukturen, der Bildungsbereich, das Personalwesen und das Gesundheitswesen. Für Hochrisiko-KI-Systeme gelten umfangreiche Anforderungen, etwa hinsichtlich Risikomanagement, Sicherheit, Nachvollziehbarkeit, Datenqualität und Überwachung (Abschnitt 2.3.2 [»Anforderungen an Hochrisiko-KI-Systeme«]).

Unter KI-Systeme mit beschränktem Risiko fallen solche, von denen zwar keine unmittelbare Gefährdung ausgeht, die aber dennoch Auswirkungen auf das Verhalten oder die Wahrnehmung von Nutzer*innen haben können. Dazu zählen etwa KI-gestützte Chatbots oder automatisierte Assistenzsysteme. Diese Systeme müssen bestimmten Informations- und Transparenzanforderungen genügen. Im Gesundheitswesen wären hier etwa KI-gestützte Systeme zur Terminvergabe einzuordnen. Die KI-VO verlangt in diesen Fällen, dass für Nutzende klar erkennbar ist, dass sie mittels eines automatisierten Systems interagieren und nicht mit medizinischem Fachper-

sonal. Zudem sollen die bereitgestellten Informationen in einfacher und verständlicher Weise kommuniziert werden.

Schließlich gibt es KI-Systeme mit minimalem Risiko, von denen kein besonderes Gefährdungspotenzial ausgeht. Hierzu zählen etwa rein unterstützende oder administrative KI-Systeme ohne sicherheitsrelevante Wirkung. Sie sind daher von regulatorischen Pflichten, die über das allgemeine EU-Recht hinausgehen, weitgehend ausgenommen.

Im Anschluss soll dargestellt werden, welche konkreten Anforderungen sich aus der Verordnung für die jeweiligen Systeme ergeben (siehe dazu sogleich unter Abschnitt 2.3.2 [»Anforderungen an Hochrisiko-KI-Systeme«]). Dabei ist hervorzuheben, dass sich die Regelungen der KI-VO auf den gesamten Lebenszyklus eines KI-Systems erstrecken – von der Entwicklung und Konzeption über das Inverkehrbringen und den Betrieb bis hin zur Marktüberwachung und Sanktionierung von Verstößen. Sie erfassen dabei sowohl technische Anforderungen als auch organisatorische Pflichten und flankierende Durchsetzungsmechanismen.

2.3.2 Anforderungen an Hochrisiko-KI-Systeme

Ob es sich bei einem KI-System um ein regulierungsbedürftiges Hochrisiko-KI-System handelt, hat die jeweils verpflichtete Person grundsätzlich eigenverantwortlich zu beurteilen. Der objektive Maßstab für die Einschätzung ergibt sich aus Art. 6 KI-VO (Klawonn, 2025, Art. 6 Rn. 1). Gemäß Art. 6 Abs. 1 KI-VO liegt ein Hochrisiko-KI-System vor, wenn zwei kumulative Voraussetzungen erfüllt sind:

1. es handelt sich um ein Sicherheitsbauteil oder Produkt im Sinne einer der in Anhang I genannten Harmonisierungsrechtsvorschriften (lit. a), und
2. das Produkt oder Sicherheitsbauteil unterliegt im Rahmen des Inverkehrbringens oder der Inbetriebnahme einer Konformitätsbewertung durch Dritte nach Maßgabe der jeweiligen sektorspezifischen Vorschriften (lit b).

Zu den in Anhang I Abschnitt A aufgeführten Harmonisierungsrechtsvorschriften zählen unter anderem die Medizinprodukteverordnung sowie die Verordnung (EU) 2017/746 über In-vitro-Diagnostika (ABl. L 117 vom 5.5.2017, S. 176). Daraus folgt, dass KI-

basierte Medizinprodukte regelmäßig als Hochrisiko-KI-Systeme einzustufen sind und den spezifischen Anforderungen der KI-VO unterliegen (siehe dazu unter Abschnitt 2.4 [»Beteiligte und Verantwortliche«]).

Darüber hinaus gelten gemäß Art. 6 Abs. 2 KI-VO auch solche KI-Systeme als hochriskant, die in Anhang III ausdrücklich benannt sind. Dabei handelt es sich um Systeme, bei denen aufgrund ihres Einsatzbereichs eine erhebliche Beeinträchtigung der Gesundheit, Sicherheit oder Grundrechte natürlicher Personen zu befürchten ist. Beispiele hierfür sind KI-Systeme zur biometrischen Identifikation (Nr. 1) sowie Anwendungen im Bereich der Bereitstellung grundlegender privater und öffentlicher Dienste und Leistungen (Nr. 5) – etwa zur Bewertung eines Anspruchs auf Sozialleistungen oder zur Risikobewertung und Preisbildung im Rahmen von Lebens- und Krankenversicherungen. Ein in Art. 6 Abs. 2 i. V. m. Anhang III genanntes System kann gemäß Art. 6 Abs. 3 KI-VO ausnahmsweise nicht als hochriskant eingestuft werden, wenn es im konkreten Fall nachweislich kein erhebliches Risiko für die genannten Rechtsgüter birgt. Soweit weder der Ausnahmetatbestand des Art. 6 Abs. 3 KI-VO greift noch ein Ausschluss nach sonstigen Vorschriften gegeben ist, sind für die Hochrisiko-Systeme die Anforderungen aus Art. 8 ff. KI-VO einzuhalten. Dazu zählen insbesondere die Einrichtung eines Risikomanagementsystems (Art. 9 KI-VO), die Qualitätssicherung von Trainingsdaten (Art. 10 KI-VO), Dokumentations- und Aufzeichnungspflichten (Art. 11 und 12 KI-VO) und die Sicherstellung einer menschlichen Aufsicht (Art. 14 KI-VO). Ergänzt werden diese Pflichten durch Vorgaben zur Durchführung eines Konformitätsbewertungsverfahren (Art. 43 KI-VO) sowie zur Anbindung einer dazugehörigen CE-Kennzeichnung (Art. 48 KI-VO). Eine vertiefte Auseinandersetzung mit den Pflichten der einzelnen Beteiligten erfolgt sogleich unter Abschnitt 2.4.1 (»Pflichten gemäß KI-VO«).

2.4 Beteiligte und Verantwortliche

Der Einsatz von KI-Systemen im medizinischen Bereich wirft eine Vielzahl regulatorischer Fragen auf. Die in diesem Zusammenhang relevanten Wirtschaftsbeteiligten, die im Folgenden näher beleuchtet werden, treffen teils unterschiedliche und teils sich überschneidende

Pflichten. Wie bereits in Abschnitt 2.2 (»Ziele der Verordnung«) erwähnt, ist die KI-VO der bislang einzige KI-spezifische Normtext und insbesondere auch auf KI-Systeme im Gesundheitssektor anwendbar (Abschnitt 2.3.2 [»Anforderungen an Hochrisiko-KI-Systeme«]). Erfüllt KI-basierte Software jedoch eine medizinische Zweckbestimmung, gilt sie gemäß Art. 2 Abs. 1 MP-VO auch als Medizinprodukt:

> »›Medizinprodukt‹ bezeichnet ein Instrument, einen Apparat, ein Gerät, eine Software, ein Implantat, ein Reagenz, ein Material oder einen anderen Gegenstand, das dem Hersteller zufolge für Menschen bestimmt ist und allein oder in Kombination einen oder mehrere der folgenden spezifischen medizinischen Zwecke erfüllen soll:
> – Diagnose, Verhütung, Überwachung, Vorhersage, Prognose, Behandlung oder Linderung von Krankheiten,
> – Diagnose, Überwachung, Behandlung, Linderung von oder Kompensierung von Verletzungen oder Behinderungen,
> – Untersuchung, Ersatz oder Veränderung der Anatomie oder eines physiologischen oder pathologischen Vorgangs oder Zustands,
> – Gewinnung von Informationen durch die In-vitro-Untersuchung von aus dem menschlichen Körper – auch aus Organ-, Blut- und Gewebespenden – stammenden Proben, und dessen bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologische oder immunologische Mittel noch metabolisch erreicht wird, dessen Wirkungsweise aber durch solche Mittel unterstützt werden kann.
> Die folgenden Produkte gelten ebenfalls als Medizinprodukte:
> – Produkte zur Empfängnisverhütung oder -förderung,
> – Produkte, die speziell für die Reinigung, Desinfektion oder Sterilisation der in Artikel 1 Absatz 4 genannten Produkte und der in Absatz 1 dieses Spiegelstrichs genannten Produkte bestimmt sind.«

Die Klassifizierung der KI-Software als eigenständiges Medizinprodukt der verschiedenen Klassen erfolgt gemäß Anhang VIII Regel 11 MP-VO allerdings abhängig vom potenziellen Risiko, das von ihrer Nutzung ausgeht. Dies ähnelt der Vorgehensweise bei der KI-VO (Abschnitt 2.3.1 [»Grundkonzept«]). Die umfangreiche Aufzählung der spezifischen medizinischen Zwecke für die Einordnung als Medizinprodukt verdeutlicht zudem, dass die MP-VO in den meisten Fällen von medizinischer KI parallel zur KI-VO anwendbar sein wird. Ein möglicher Anwendungsfall ist der Einsatz einer KI-gestütz-

ten Software zur automatischen Erkennung von Brustkrebs.[3] In diesem Fall unterliegt die medizinische KI sowohl dem Anwendungsbereich der KI-VO als auch der MP-VO. Dies hat eine komplexe und unübersichtliche Rechtslage zur Folge, die zu Unsicherheiten bei den verantwortlichen Personen führen kann. Der folgende Abschnitt verschafft einen Überblick über die relevanten Wirtschaftsbeteiligten und beleuchtet die Abgrenzungsproblematik im Kontext medizinischer KI-Systeme.

Wie in Abschnitt 2.3.2 (»Anforderungen an Hochrisiko-KI-Systeme«) festgestellt, sind medizinische KI-Systeme als Hochrisiko-KI-Systeme einzustufen, sodass die KI-VO uneingeschränkt Anwendung findet. »Anbieter«[4] wird gemäß Art. 3 Nr. 3 KI-VO definiert als »natürliche oder juristische Person […], die ein KI-System […] entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder […] in Betrieb nimmt, sei es entgeltlich oder unentgeltlich«. »Betreiber« sind gemäß Art. 3 Nr. 4 KI-VO natürliche oder juristische Personen oder Organisationen, die ein KI-System in eigener Verantwortung verwenden, wobei die ausschließlich private Nutzung explizit ausgenommen ist. Exemplarisch können an dieser Stelle Gesundheitseinrichtungen sowie medizinisches Fachpersonal angeführt werden. Eine besondere Herausforderung besteht auch in der Abgrenzung der Rolle des Anbieters von der des Betreibers. Dies ist insbesondere in Konstellationen relevant, in denen Beteiligte – etwa Gesundheitseinrichtungen – beide Rollen gleichzeitig ausüben, beispielsweise wenn ein eigenständig entwickeltes medizinisches KI-System im Rahmen derselben Gesundheitseinrichtung zum Einsatz kommt. Darüber hinaus können auch die in Art. 3 Nr. 8 KI-VO aufgeführten Beteiligten – wie »Einführer« (Art. 3 Nr. 6 KI-VO), »Händler« (Art. 3 Nr. 7 KI-VO) oder »Produkthersteller« (Art. 3 Nr. 8 KI-VO) – von Relevanz sein. Im Folgenden soll der Fokus jedoch auf die in

3 Siehe PRAIM-Studie, in der mehr als 460.000 Frauen im Rahmen des nationalen Mammographie-Screening-Programms (MSP) untersucht wurden. Der Einsatz einer KI-gestützten Doppelbefundung führte dabei zu einer 17,6 % höheren Brustkrebs-Erkennungsrate im Vergleich zur herkömmlichen Befundung (Eisemann et al., 2025).

4 Gesetzlich festgelegte Begriffe (z. B. »Anbieter«, »Betreiber«) werden in der im Gesetz verwendeten Form wiedergegeben. Im Übrigen erfolgt eine genderneutrale Formulierung.

diesem Zusammenhang wichtigsten Anbieter und Betreiber gelegt werden.

In der MP-VO kommen die Begriffe »Anbieter« oder »Betreiber« nicht vor. Stattdessen sollen die in der MP-VO verwendeten Definitionen zu »Hersteller« und »Anwender«, sowie die in der am 14.02.2025 ausgefertigten Verordnung über das Betreiben und Benutzen von Medizinprodukten[5] (Medizinprodukte-Betreiberverordnung, im Folgenden: MPBetreibV) vorkommenden »Betreiber« und »Benutzer« näher beleuchtet werden.

In Art. 2 Nr. 30 MP-VO ist der Begriff des Herstellers definiert als »natürliche oder juristische Person, die ein Produkt herstellt oder als neu aufbereitet bzw. entwickeln, herstellen oder als neu aufbereiten lässt und dieses Produkt unter ihrem eigenen Namen oder ihrer Marke vermarktet«. Der Begriff ähnelt im Wesentlichen dem Begriff des Anbieters i. S. d. KI-VO (Martini & Wendehorst/ *Wendehorst*, 2024, Art. 3 Rn. 64). Als Anwender sind gemäß Art. 2 Nr. 37 MP-VO hingegen alle »Angehörigen der Gesundheitsberufe oder Laien, [die] ein Medizinprodukt anwende[n]« qualifiziert. In diesem Kontext nennt das nationale Recht gemäß § 2 Abs. 3 MPBetreibV den Begriff des Benutzers und definiert ihn als eine Person, die »ein Produkt […] am Patienten einsetzt«. Beide Definitionen beziehen sich dabei auf Personen, die ein Produkt tatsächlich anwenden. Sie sehen dabei die Möglichkeit vor, dass auch weisungsgebundene Personen wie Pflegekräfte in den Kreis der Betroffenen fallen. Das nationale Recht fasst den Begriff lediglich enger, indem es den Einsatz gezielt zur Wirkung bei Patient*innen fordert und damit typischerweise medizinisches Personal betrifft (Rehmann & Wagner/*Rehmann*, 2023, Art. 2 Rn. 52). Die MP-VO hingegen umfasst darüber hinaus auch fachfremde Personen.

In der MP-VO wird der Begriff des Betreibers nicht verwendet. Gemäß § 2 Abs. 2 S. 1 MPBetreibV ist damit »jede natürliche oder juristische Person, die für den Betrieb der Gesundheitseinrichtung verantwortlich ist, in der das Produkt durch dessen Beschäftigte betrieben oder benutzt wird«, gemeint. Darüber hinaus wird das medizinische Personal selbst zum Betreiber, sofern ein eigenes Pro-

5 Medizinprodukte-Betreiberverordnung vom 14. Februar 2025 (BGBl. 2025 I Nr. 38), die durch Artikel 1 der Verordnung vom 14. Februar 2025 (BGBl. 2025 I Nr. 39) geändert worden ist.

dukt in die Gesundheitseinrichtung mitgebracht und dort verwendet oder auch außerhalb der Einrichtung zur Nutzung bereitgestellt wird (§ 2 Abs. 2 S. 2, 3 MPBetreibV). Als Gesundheitseinrichtung ist gemäß § 2 Abs. 4 MPBetreibV jeder Ort zu verstehen, an dem Medizinprodukte von medizinischem Fachpersonal, Pflegekräften oder anderen befugten Personen verwendet oder betrieben werden. Auch hier ist eine gewisse Ähnlichkeit zum Betreiberbegriff i. S. d. KI-VO erkennbar. Während die KI-VO jede Verwendung in eigener Verantwortung – außer ausschließlich private – erfasst, konzentriert sich die vorliegende Definition auf den Betrieb durch Beschäftigte innerhalb einer Gesundheitseinrichtung und legt den Fokus auf die Organisationsverantwortung. Eine private Nutzung ist damit nicht ausgeschlossen.

Medizinische KI-Systeme stellen einen Sonderfall dar, in dem die Regelungen der KI-VO und die der MP-VO in der Regel parallel anwendbar sind. Diese Doppelregulierung kann erweiterte Pflichten für die Betroffenen zur Folge haben und die eindeutige Zuweisung bestehender Pflichten erschweren. Die folgenden Abschnitte geben einen Überblick über die bestehenden Pflichten der wichtigsten beteiligten Personen im Gesundheitswesen.

2.4.1 Pflichten gemäß KI-VO

a) Pflichten der Anbieter

Der Begriff des Anbieters i. S. d. KI-VO wurde in Abschnitt 2.4 (»Beteiligte und Verantwortliche«) bereits definiert. Seine Relevanz zeigt sich insbesondere im Hinblick auf den umfassenden, aber nicht abschließenden Pflichtenkatalog des Art. 16 KI-VO. Gemäß Art. 16 lit. a) KI-VO muss der Anbieter zunächst sicherstellen, dass das infrage stehende Hochrisiko-KI-System den Anforderungen der Art. 8 bis 15 KI-VO genügt (Abschnitt 2.3.2 [»Anforderungen an Hochrisiko-KI-Systeme«]). Damit trägt er die größte Verantwortung für die Qualitätssicherung, die Gefahrenabwehr und auch die Risikovorsorge (Hilgendorf & Roth-Isigkeit/*Linardatos*, 2023, § 7 Rn. 1). Um die Kommunikation mit anderen beteiligten Personen zu erleichtern, ist der Anbieter gemäß Art. 16 lit. b) KI-VO dazu verpflichtet, seine Kontaktdaten so bereitzustellen, dass eine Kontaktaufnahme ohne Weiteres möglich ist, etwa auf dem KI-System, der Verpackung oder

der beigefügten Dokumentation (Martini & Wendehorst/*Eisenberger*, 2024, Art. 16 Rn. 19).

Art. 16 KI-VO verweist darüber hinaus auf verschiedene Pflichten, die sich aus anderen Bestimmungen der Verordnung ergeben. Dazu gehören insbesondere die folgenden Pflichten: die Pflicht zur Einrichtung eines Qualitätsmanagementsystems (Art. 17 KI-VO), die Pflicht zur Aufbewahrung von technischer Dokumentation und automatisch erzeugten Protokollen (Art. 18 und 19 KI-VO), die Registrierungspflicht in einer EU-Datenbank (Art. 49 Abs. 1 i. V. m. Art. 71 KI-VO), sowie die Pflicht, bei Verstößen oder Risiken geeignete Korrekturmaßnahmen zu ergreifen und, soweit notwendig, Betreiber, Bevollmächtigte oder Einführer zu informieren (Art. 20 KI-VO). Vor der Einführung oder Nutzung des Systems muss der Anbieter zudem auch ein Konformitätsbewertungsverfahren gemäß Art. 43 KI-VO durchführen. In diesem Zusammenhang wird die Übereinstimmung mit den gesetzlichen Vorgaben überprüft, sodass »KI-spezifische Risiken« möglichst im Vorhinein vermieden werden können (Gerdemann, 2024). Sobald dieses Verfahren erfolgreich abgeschlossen wurde, muss eine sogenannte EU-Konformitätserklärung gemäß Art. 47 KI-VO erstellt werden. Diese stellt verbindlich die Erfüllung der genannten Anforderungen fest (Art. 47 Abs. 2 S. 1 KI-VO) und ordnet eindeutig zu, für welches KI-System sie gilt (Art. 47 Abs. 1 S. 2 KI-VO).

Mit der Ausstellung übernimmt der Anbieter die volle Verantwortung für die Einhaltung der Anforderungen (Art. 47 Abs. 4 S. 1 KI-VO). Er muss die Erklärung gegebenenfalls aktualisieren (Art. 47 Abs. 4 S. 2 KI-VO) und sie mindestens zehn Jahre lang aufbewahren. Auf Anfrage muss er sie den nationalen Behörden bereitstellen (Art. 47 Abs. 1 S. 1 KI-VO). Daraufhin muss eine CE-Kennzeichnung gemäß Art. 48 KI-VO erfolgen. Sie sollte sich nach den Grundsätzen des Art. 30 der Verordnung (EU) Nr. 765/2008 über die Vorschriften für die Akkreditierung und die Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten richten. Mit ihr wird die Konformität mit den geltenden Anforderungen sowie die Übernahme der Verantwortung durch den Anbieter bescheinigt (Art. 47 Abs. 2, 3 KI-VO). Auf begründete Nachfrage der zuständigen Behörde treffen den Anbieter zudem gemäß Art. 16 lit. k) KI-VO Nachweispflichten im Hinblick auf die Einhaltung der Anforderungen aus Art. 8 bis 15 KI-VO. Er hat außerdem gemäß

Art. 16 lit. l) KI-VO sicherzustellen, dass die Barrierefreiheitsanforderungen[6] erfüllt sind. Die mit dem Einsatz von Hochrisiko-KI-Systemen – insbesondere im Gesundheitswesen – verbundenen Risiken begründen den Bedarf nach verstärkter Kontrolle und machen die Anbieter in hohem Maße zu Verantwortlichen.

b) Pflichten der Betreiber

Ungeachtet des bereits umfangreichen Pflichtenkatalogs des Anbieters, der in Abschnitt 2.4.1.1 (»Pflichten der Anbieter«) näher beleuchtet wurde, ergeben sich für Betreiber im Sinne der KI-VO – bislang im Produktrecht eher ungewöhnlich – darüber hinausgehende Pflichten. Dort stehen regelmäßig »Endnutzer« und »Anwender« im Fokus, für die regelmäßig Schutzmaßnahmen als Verpflichtungen vorgesehen sind (Martini & Wendehorst/*Eisenberger*, 2024, Art. 3 Rn. 80). Gerade im Zusammenhang mit Hochrisiko-KI-Systemen – besonders im Gesundheitswesen – ergibt aber ein gesonderter Pflichtenkatalog für Betreiber, die dem tatsächlichen Einsatz deutlich näher sind als die Anbieter, durchaus Sinn und kann zu einer Minimierung des Risikos führen (Schuh & Witt, 2025).

In diesem Zusammenhang kann die Frage aufgeworfen werden, ob Mitarbeitende als Betreiber qualifiziert werden können, wenn sie das KI-System im Rahmen ihrer beruflichen Tätigkeit nutzen. Ein Blick auf den Wortlaut »in eigener Verantwortung« (Art. 3 Nr. 4 KI-VO) lässt zunächst den Schluss zu, dass eine solche Einordnung nicht vorgesehen ist. Soweit Mitarbeitende im Rahmen von dienstlichen Weisungen innerhalb einer hierarchischen Struktur tätig sind – was in Gesundheitseinrichtungen regelmäßig der Fall sein sollte –, haben sie keine Entscheidungsbefugnisse inne und handeln auch nicht in eigener Verantwortung (Hilgendorf & Roth-Isigkeit/*Gless & Janal*, 2023, § 2 Rn. 45). Es sind allerdings auch Ausnahmefälle denkbar. So kann beispielsweise leitendes medizinisches Perso-

6 Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates vom 17. April 2019 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen, ABl. L 151 vom 07.6.2019; (EU) 2016/2102 des Europäischen Parlaments und des Rates vom 26. Oktober 2016 über den barrierefreien Zugang zu den Websites und mobilen Anwendungen öffentlicher Stellen, ABl. L 327 vom 02.12.2016.

nal, wie ein Chefarzt oder eine Chefärztin im Einzelfall als Betreiber i. S. d. KI-VO anzusehen sein. Dazu müsste z. B. eigenverantwortlich über die Auswahl, den Einsatz und den Zweck des KI-gestützten Systems entschieden oder die organisatorische und inhaltliche Kontrolle über die Anwendung ausgeübt werden. Entscheidend ist somit immer, ob tatsächlich Entscheidungsbefugnisse und eigene Verantwortung für den Einsatz des KI-Systems bestehen. Nur in diesem Fall sind Mitarbeitende – anders als im Regelfall – als Betreiber im Sinne der KI-VO zu qualifizieren.

Die Pflichten der Betreiber von Hochrisiko-KI-Systemen sind im Wesentlichen in Art. 26 ff. KI-VO geregelt. Betreiber müssen gemäß Art. 26 Abs. 1 i. V. m. Abs. 3 und 6 KI-VO sicherstellen, dass das KI-System nur gemäß Betriebsanleitung, Unionsrecht und nationalem Recht verwendet wird. Diese Pflicht darf die unternehmerische Freiheit allerdings nicht unangemessen beeinträchtigen. Protokolle, die vom KI-System automatisch erzeugt werden, müssen für mindestens sechs Monate aufbewahrt werden. Gemäß Art. 26 Abs. 2 i. V. m. Art. 14 KI-VO muss eine natürliche Person mit entsprechender Fachkompetenz das KI-System überwachen. Diese »menschliche Aufsicht« muss dabei dem Charakter des KI-Systems entsprechen (Martini & Wendehorst/*Eisenberger*, 2024, Art. 26 Rn. 27). Bei medizinischen KI-Systemen ist das in der Regel das medizinische Fachpersonal. Grund für diese Vorkehrung ist die »[…] Verhinderung oder Minimierung der Risiken für Gesundheit, Sicherheit oder Grundrechte […]« (Art. 14 Abs. 2 KI-VO).

Der Betreiber muss darüber hinaus sicherstellen, dass die verwendeten Eingabedaten dem vorgesehenen Zweck entsprechen und repräsentativ genug, d. h. nicht diskriminierend verzerrt sind (Art. 26 Abs. 4 KI-VO). Aus der Betriebsanleitung ergeben sich zudem Überwachungspflichten. Werden Risiken für Gesundheit, Sicherheit oder Grundrechte erkannt, müssen unverzüglich die anderen Beteiligten informiert und der Betrieb gegebenenfalls ausgesetzt werden, beispielsweise wenn eine Gefahr für Patientinnen und Patienten angenommen wird (Art. 26 Abs. 5 KI-VO, Art. 79 Abs. 1 KI-VO). Ist der Betreiber gleichzeitig arbeitgebende Person, muss er gemäß Art. 26 Abs. 7 KI-VO die Arbeitnehmervertretung und die Arbeitnehmenden über die Nutzung informieren und dabei alle einschlägigen arbeitsrechtlichen Vorschriften beachten. Zusätzlich zu den allgemeinen Transparenzpflichten i. S. d. Art. 50 KI-VO müssen vom

KI-System betroffene Personen – hier regelmäßig Patient*innen – informiert werden (Art. 26 Abs. 11 KI-VO). Sollte eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO erforderlich sein – was gemäß Art. 9 Abs. 1 DSGVO bei Gesundheitsdaten der Fall sein dürfte – muss das KI-System gemäß Art. 25 Abs. 8 KI-VO in einer EU-Datenbank registriert werden. Werden personenbezogene Daten, insbesondere sensible Gesundheitsdaten verarbeitet, ist zudem eine DSFA nach Art. 26 Abs. 9 KI-VO i. V. m. Art. 35 DSGVO oder Art. 27 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 (Datenschutzrichtlinie für den Bereich Strafverfolgung) erforderlich. Dafür dürfen nur die in Art. 13 KI-VO aufgeführten Informationen verwendet werden, beispielsweise der Name und die Kontaktdaten des Anbieters (Abs. 3 lit. a) oder die Merkmale, Fähigkeiten und Leistungsgrenzen des Hochrisiko-KI-Systems (Abs. 3 lit. b). Betreiber müssen außerdem aktiv mit den zuständigen Behörden – z. B. den Datenschutzbehörden – zusammenarbeiten (Art. 26 Abs. 12 KI-VO). Zusätzlich zur DSFA ist eine Grundrechte-Folgenabschätzung gemäß Art. 27 KI-VO durchzuführen. Ziel ist es, Risiken für Grundrechte zu identifizieren und vorbeugende Maßnahmen zu planen (Martini & Wendehorst/*Eisenberger*, 2024, Art. 27 Rn. 4). Der Inhalt wird durch Art. 27 Abs. 1 S. 2 KI-VO bestimmt.

Betreiber von Hochrisiko-KI-Systemen unterliegen insgesamt umfassenden Verpflichtungen, die die Pflichten in Abschnitt 2.4.1.1 (»Pflichten der Anbieter«) zum Teil ergänzen. Die Pflichten erstrecken sich auf ein breites Spektrum, das von der Sicherheit über den Datenschutz bis hin zu den Grundrechten reicht. Die Einbeziehung des dem Geschehen meist näheren Betreibers ist aufgrund der hohen Risiken, die insbesondere im Gesundheitssektor bestehen, von großer Bedeutung. Es obliegt seiner Verantwortung, die korrekte Verwendung, Überwachung und Dokumentation des medizinischen KI-Systems sicherzustellen, während der Anbieter die notwendige Unterstützung leistet.

c) Einbeziehung in den Pflichtenkreis des Anbieters

Denkbar sind auch Fallkonstellationen, in denen die Trennung zwischen der Betreiber- und Anbietereigenschaft mit erheblichen

Abgrenzungsschwierigkeiten einhergeht, so dass der jeweilige Pflichtenumfang nicht eindeutig bestimmt werden kann. Dieses Abgrenzungsdefizit dürfte in der praktischen Anwendung der KI-VO erheblich werden, wobei sich – ähnlich wie im Datenschutz – der Gedanke einer gemeinsamen Verantwortung aufdrängt (Art. 26 DSGVO).

Die »Verantwortlichkeiten entlang der Wertschöpfungskette« werden in Art. 25 KI-VO behandelt. Die sogenannte Anbieterfiktion lässt sich in Art. 25 Abs. 1 KI-VO beobachten. Diese Regelung bestimmt, dass auch Händler, Einführer, Betreiber oder sonstige Dritte unter bestimmten Umständen als Anbieter eines Hochrisiko-KI-Systems gelten und damit den entsprechenden in Art. 16 KI-VO aufgelisteten Pflichten (Abschnitt 2.4.1.1 [»Pflichten der Anbieter«]) unterliegen. Dies ist insbesondere dann der Fall, wenn sie das System unter eigenem Namen vertreiben, es wesentlich verändern oder dessen Zweck so anpassen, dass es als Hochrisiko-KI eingestuft wird. Der Anbieter des ursprünglichen KI-Systems wird nun von dem Anbieter des neuen spezifischen KI-Systems abgelöst (Art. 25 Abs. 2 S.1 KI-VO), muss diesen nach Art. 25 Abs. 2 S. 2 KI-VO allerdings angemessen unterstützen, indem er relevante Informationen bereitstellt, technischen Zugang ermöglicht und damit bei der Erfüllung der Pflichten bei der Konformitätsbewertung von Hochrisiko-KI-Systemen hilft. Ausgenommen sind dabei nur Fälle, in denen der Erstanbieter die Umwandlung ausdrücklich untersagt hat (Art. 25 Abs. 2 S. 3 KI-VO).

Im Gesundheitssektor lässt sich ein praxisnaher Anwendungsfall der sogenannten Anbieterfiktion beobachten, wenn z. B. ein zunächst rein kosmetisch eingesetztes KI-System durch einen Gesundheitsdienstleister zweckverändert und für die medizinische Diagnose verwendet wird, so dass dieses nachträglich als Hochrisiko-KI-System i. S. d. Art. 6 KI-VO eingestuft wird.

2.4.2 Exkurs: Pflichten gemäß MP-VO

a) Pflichten der Hersteller

Zusätzlich zu den in Abschnitt 2.4.1.1 (»Pflichten der Anbieter«) genannten Pflichten könnten im Falle eines Medizinprodukts die allgemeinen Herstellerpflichten gemäß Art. 10 MP-VO Anwendung finden. Nach Art. 10 Abs. 1 MP-VO dürfen Produkte nur in den

Verkehr gebracht werden, wenn sie den Anforderungen der MP-VO entsprechend ausgelegt und hergestellt worden sind. Die konkreten Anforderungen ergeben sich vor allem aus Anhang I Kapitel II MP-VO (Rehmann & Wagner/*Wagner*, 2023, Art. 10 Rn. 3).

Die zentralen Pflichten der Hersteller nach Art. 10 MP-VO lassen sich wie folgt zusammenfassen:

- Implementierung eines Risikomanagementsystems (Abs. 2),
- Durchführung einer klinischen Bewertung (Abs. 3),
- Erstellung und Pflege der technischen Dokumentation (Abs. 4),
- Ausstellung einer EU-Konformitätsbewertung gemäß Art. 19 MP-VO und Anbringung der CE-Kennzeichnung gemäß Art. 20 MP-VO (Abs. 6) und
- Aufbewahrung von Dokumentation und Konformitätserklärung für mindestens zehn Jahre (Abs. 8 S. 1, 2).

Darüber hinaus bestehen weitere Pflichten: Hersteller müssen ein Überwachungssystem gemäß Art. 10 Abs. 10 i. V. m. Art. 83 MP-VO sowie ein Qualitätsmanagementsystem gemäß Art. 10 Abs. 9 MP-VO implementieren. Zudem muss die eindeutige Kennzeichnung der Produkte über das UDI-System (Unique Device Identification) nach Art. 10 Abs. 7 i. V. m. Art. 27 MP-VO sowie die Registrierung des Produkts und des Herstellers in den vorgeschriebenen Datenbanken gemäß Art. 10 Abs. 7 MP-VO i. V. m. Art. 29 und Art. 31 MP-VO beachtet werden. Die europäische Datenbank für Medizinprodukte (engl.: European database for medical devices, EUDAMED) ist jedoch noch nicht vollständig betriebsbereit. Sie kann – soweit fertiggestellt – bereits freiwillig verwendet werden, eine verpflichtende Nutzung ist jedoch bis zur vollständigen Fertigstellung nicht vorgesehen (Europäische Kommission, o. D.). Für den Fall, dass EUDAMED nicht funktionsfähig ist, regelt § 97 MPDG entsprechende Übergangsregelungen. Die Bekanntmachungen des Bundesministeriums für Gesundheit konkretisieren diese (§ 97 Abs. 2 MPDG).

Weiterhin müssen Hersteller sicherstellen, dass alle Produktinformationen verständlich, dauerhaft und in der richtigen Amtssprache vorliegen (Art. 10 Abs. 11 MP-VO). Bei festgestellter Nichtkonformität sind unverzüglich Korrekturmaßnahmen zu ergreifen und sowohl die Behörden als auch die Händler, Bevollmächtigten und Importeure zu informieren (Art. 10 Abs. 12 MP-VO). Zudem besteht die Pflicht, ein System zur Aufzeichnung und Meldung schwerwiegen-

der Vorkommnisse zu betreiben (Art. 10 Abs. 13 MP-VO), auf Anfrage vollständige Unterlagen und Proben bereitzustellen sowie bei Risikomaßnahmen mit den Behörden zu kooperieren (Art. 10 Abs. 14 MP-VO). Es ist ein Bevollmächtigter gemäß Art. 11 MP-VO sowie eine verantwortliche Person für die Einhaltung der Regulierungsvorschriften gemäß Art. 15 MP-VO zu benennen. Schließlich müssen Hersteller auch für Produktschäden haften und eine angemessene finanzielle Absicherung garantieren (Art. 10 Abs. 16 MP-VO). Weniger relevant im vorliegenden Kontext sind die Sonderregelungen zu Sonderanfertigungen (Art. 10 Abs. 5 MP-VO) und Fremdentwicklungen (Art. 10 Abs. 15 MP-VO).

Die MP-VO formuliert einen umfangreichen Pflichtenkatalog. Dabei fällt auf, dass sich einige Pflichten mit denen aus Abschnitt 2.4.1 (»Pflichten gemäß KI-VO«) überschneiden. So werden beispielsweise ein systematisches Risikomanagement, eine Konformitätsbewertung, eine CE-Kennzeichnung und eine aktive Überwachung gefordert. Beide Verordnungen fordern zudem eine umfangreiche technische Dokumentation. Die KI-VO legt durch Anhang IV allerdings den Fokus auf KI-spezifischere Aspekte wie Trainings- oder Testdaten. Auch bei den Transparenzpflichten gibt es Übereinstimmungen, jedoch fordert die KI-VO eine spezifischere und umfangreichere Bereitstellung durch den Betreiber. Während die KI-VO Anforderungen an die Qualität der Daten und die Datengovernance stellt, enthält die MP-VO dazu keine detaillierte Regelung. Diese Aspekte werden indirekt über das Risikomanagementsystem und die klinische Bewertung abgedeckt. Auch die menschliche Aufsicht ist in der KI-VO spezifisch geregelt, während die MP-VO diese nicht explizit vorschreibt. Beide Verordnungen fordern zudem Aufzeichnungen, doch während sich die MP-VO auf die Meldung schwerwiegender Vorkommnisse fokussiert, erweitert die KI-VO die Aufzeichnungspflicht, um zu gewährleisten, dass »das Funktionieren des Hochrisiko-KI-Systems in einem der Zweckbestimmung des Systems angemessenen Maße rückverfolgt werden kann« (Art. 12 Abs. 2 S. 1 KI-VO). Sowohl die KI-VO als auch die MP-VO fordern eine Registrierung in einer Datenbank. Die KI-VO verlangt jedoch eine Registrierung in einer EU-Datenbank für Hochrisiko-KI-Systeme, während die MP-VO eine Registrierung bei EUDAMED vorsieht. Demnach müssten sich Anbieter bzw. Hersteller von medizinischen

Hochrisiko-KI-Systemen trotz derselben Zielsetzung derzeit noch in beiden Datenbanken registrieren.

Aufgrund der zahlreichen Überschneidungen könnte der Eindruck entstehen, die MP-VO sei durch die spezifischere KI-VO verdrängt worden. Es ist allerdings hervorzuheben, dass es keine Vorrangregelung gibt und somit beide Verordnungen nebeneinander anwendbar sind. So verbleiben Bereiche, die nach wie vor nur durch die MP-VO geregelt werden, wie z. B. die klinische Bewertung oder die Registrierung bei EUDAMED. Eine sorgfältige rechtliche Abstimmung ist in diesem Zusammenhang unerlässlich.

b) Pflichten der Betreiber

In Abschnitt 2.4.1.2 (»Pflichten der Betreiber«) wurden die Pflichten i. S. d. KI-VO bereits ausführlich behandelt. Die Pflichten des in der MP-VO legal definierten Anwenders sind jedoch nicht so umfangreich formuliert wie die des Herstellers und der anderen Beteiligten. Aus der MP-VO ergeben sich allerdings einige wenige indirekte Pflichten für Anwender. So wird gemäß Art. 16 Abs. 1 MP-VO »eine sonstige natürliche oder juristische Person« in den Pflichtenkreis des Herstellers einbezogen, soweit sie ein Produkt verändert oder unter eigenem Namen in Verkehr bringt. Auch praktische Pflichten wie die Einhaltung der Gebrauchsanweisung oder die Meldung schwerwiegender Vorkommnisse an den Hersteller sind denkbar, werden aber nicht konkret erwähnt. Der Anwender zählt in erster Linie zum geschützten Personenkreis, wohingegen der Betreiber nach der KI-VO spezifische Pflichten zu erfüllen hat (Martini & Wendehorst/ *Wendehorst*, 2024, Art. 26 Rn. 2).

In Deutschland gelten indes verbindliche Vorgaben gemäß der MPBetreibV, von denen die wichtigsten im Folgenden aufgeführt werden. Der Betreiber ist gemäß § 3 Abs. 1 MPBetreibV verpflichtet, die ihm zugewiesenen Pflichten zu erfüllen, um den sicheren und ordnungsgemäßen Einsatz der Produkte in der Gesundheitseinrichtung zu gewährleisten. Diese Pflichten werden allerdings nicht weiter konkretisiert. Vielmehr sollen alle Pflichten i. S. d. MPBetreibV Beachtung finden und deren Einhaltung dem Ziel Rechnung tragen, den Schutz und die Sicherheit von Patient*innen zu gewährleisten (Bundesrat, 2016). So sind Betreiber und Benutzer gemäß § 4 Abs. 1

MPBetreibV gleichermaßen dazu verpflichtet, die bestimmungsgemäße Anwendung des Produktes sicherzustellen. Das Produkt darf nur von Personen verwendet werden, die »die dafür erforderliche Ausbildung oder Kenntnis und Erfahrung besitzen« (§ 4 Abs. 2 MPBetreibV) und i. S. d. § 4 Abs. 3 S. 1 MPBetreibV ordnungsgemäß eingewiesen wurden. Für die Einhaltung der Anforderungen aus Abs. 1 und 2 ist der Betreiber verantwortlich (§ 4 Abs. 5 S. 1 MPBetreibV).

Der Benutzer muss sich dagegen vor Verwendung des Produkts vergewissern, dass es funktionsfähig und in einwandfreiem Zustand ist (§ 4 Abs. 6 S. 1 MPBetreibV). Die Gebrauchsanweisung mit allen mitgelieferten sicherheitsrelevanten Informationen und Wartungshinweisen ist gemäß § 4 Abs. 7 S. 1 MPBetreibV so aufzubewahren, dass sie dem Benutzer jederzeit zur Verfügung steht. Auch hier ist denkbar, dass dem Benutzer darüber hinaus praktische Pflichten obliegen, wie beispielsweise die Meldung von Fehlern oder schwerwiegenden Vorkommnissen an die nächsthöhere Person in der Verantwortungskette. Dies wäre insbesondere bei risikobehafteten Produkten im Gesundheitswesen sinnvoll, da Fehler so schneller erkannt und das Risiko für Patient*innen minimiert werden könnte. Der Betreiber hat zudem einen sachkundigen und zuverlässigen »Beauftragte[n]« für Medizinproduktesicherheit zu ernennen, soweit er eine Gesundheitseinrichtung mit mehr als 20 Beschäftigten führt (§ 6 Abs. 1 S. 1 MPBetreibV). Gemäß § 6 Abs. 4 MPBetreibV sollte dessen Funktions-E-Mail-Adresse auf der Internetseite bekannt gegeben werden, sodass er bei Bedarf erreicht werden kann. Nach § 7 Abs. 1 S. 1 MPBetreibV hat der Betreiber die Produkte instand zu halten. Davon umfasst sind insbesondere Wartungen und Inspektionen sowie Instandsetzungen zur Wiederherstellung der Funktionsfähigkeit (§ 7 Abs. 2 S. 1 MPBetreibV). Zuletzt muss der Betreiber bei Produkten aus Anlage 1 gemäß § 12 Abs.1 S. 1 i. V. m. S. 2, 3 MPBetreibV spätestens alle zwei Jahre sicherheitstechnische Kontrollen durchführen. Anlage 1 formuliert einen Katalog von Produkten, wobei KI in verschiedenen Bereichen zunehmend eine Rolle spielt.

Dieser Überblick zeigt in vielerlei Hinsicht Übereinstimmungen mit den Pflichten der Betreiber i. S. d. KI-VO. Letztere stellt jedoch umfangreichere Anforderungen an den Betrieb von KI-Systemen und definiert KI-spezifische Pflichten für Betreiber. Die MPBetreibV deckt die Basispflichten ab, die auch KI umfassen, während die KI-VO diese um spezifische Anforderungen an KI-Systeme ergänzt.

Beide Verordnungen sollten zwar parallel beachtet werden, die KI-VO wird aber in den meisten Aspekten umfangreicher sein.

2.5 Sanktionsmechanismen

Beim Einsatz von KI im Gesundheitswesen gibt es strenge Vorschriften, die in Abschnitt 2.4 (»Beteiligte und Verantwortliche«) näher beleuchtet wurden. So regelt die KI-VO den Einsatz von Hochrisiko-KI-Systemen, während die MP-VO die Anforderungen an Medizinprodukte festlegt. Die KI-VO sieht gemäß Erwägungsgrund Nr. 168 S. 1 KI-VO vor, »die Verhängung von Sanktionen und anderen Durchsetzungsmaßnahmen« zu ergreifen, um die Einhaltung der jeweiligen Anforderungen durchzusetzen. Durch sehr hohe Bußgelder – mit abschreckender Wirkung – soll der regelkonforme Einsatz von KI-Systemen sichergestellt werden (Erwägungsgrund Nr. 168 S. 2 KI-VO). Diese Sanktionen sind insbesondere im Gesundheitswesen von großer Bedeutung, da Patient*innen vor potenziell schwerwiegenden und lebensgefährlichen Fehlern geschützt werden müssen. Die Umsetzung wird dabei den Mitgliedstaaten überlassen. Das MPDG setzt im Hinblick auf Medizinprodukte die MP-VO in nationales Recht um und enthält dort konkrete Bußgeld- und Strafregelungen.

Die Sanktionsregelungen der KI-VO (Art. 99 bis 101 KI-VO) orientieren sich sodann systematisch an den Sanktionsvorschriften der DSGVO (Art. 83 ff. DSGVO). Art. 99 KI-VO regelt hierbei allgemeine Sanktionen bei Verstößen gegen die KI-VO durch die Beteiligten. Bei Verstößen gegen Art. 5 KI-VO (Abschnitt 2.3.1 [»Grundkonzept«]) belaufen sich die Bußgeldhöchstgrenzen auf 35 Millionen Euro oder 7 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem welcher Betrag höher ausfällt (Art. 99 Abs. 3 KI-VO).[7] Verstöße gegen die Pflichten der verschiedenen Beteiligten, wie beispielsweise von Anbietern gemäß Art. 16

7 Die Bemessung der Bußgeldhöhe als Prozentsatz des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres ist bereits aus anderen Regelwerken bekannt: Verordnung (EG) Nr. 1/2003 des Rates vom 16. Dezember 2002 zur Durchführung der in den Artikeln 81 und 82 EG-Vertrag niedergelegten Wettbewerbsregeln; (EU) 2016/679 vom 27. April 2016 (Datenschutz-Grundverordnung).

KI-VO oder Betreibern gemäß Art. 26 KI-VO, werden ebenfalls mit Bußgeldern geahndet. So formuliert Art. 99 Abs. 4 KI-VO:

> »Für Verstöße gegen folgende für Akteure oder notifizierte Stellen geltende Bestimmungen, mit Ausnahme der in Artikel 5 genannten, werden Geldbußen von bis zu 15 000 000 EUR oder – im Falle von Unternehmen – von bis zu 3 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist:
> a) Pflichten der Anbieter gemäß Artikel 16;
> b) Pflichten der Bevollmächtigten gemäß Artikel 22;
> c) Pflichten der Einführer gemäß Artikel 23;
> d) Pflichten der Händler gemäß Artikel 24;
> e) Pflichten der Betreiber gemäß Artikel 26;
> f) für notifizierte Stellen geltende Anforderungen und Pflichten gemäß Artikel 31, Artikel 33 Abs. 1, 3 und 4 bzw. Artikel 34;
> g) Transparenzpflichten für Anbieter und Betreiber gemäß Artikel 50.«

Diese können eine Höhe von bis zu 15 Millionen Euro oder im Falle von Unternehmen 3 % des Jahresumsatzes des vergangenen Jahres erreichen. Die Bemessung erfolgt gemäß Art. 99 Abs. 4 KI-VO unter Berücksichtigung des jeweils höheren Betrags. Nach Art. 99 Abs. 5 KI-VO werden im Falle einer unrichtigen Auskunftserteilung gegenüber Behörden Geldbußen in Höhe von 7,5 Millionen Euro oder ein Prozent des Jahresumsatzes verhängt. Art. 100 KI-VO behandelt spezifisch die Verhängung von Geldbußen gegen Organe, Einrichtungen und sonstige Stellen der Union durch den Europäischen Datenschutzbeauftragten, während Art. 101 KI-VO die Geldbußen gegenüber Anbietern von KI-Modellen mit allgemeinem Verwendungszweck (General Purpose AI, GPAI) regelt. Für KI-Systeme im Gesundheitswesen wird regelmäßig Art. 99 KI-VO die primäre Sanktionsnorm darstellen.

Die Umsetzung dieser Maßnahmen ist den Mitgliedstaaten – soweit sie wirksam, verhältnismäßig und abschreckend sind – selbst überlassen (Art. 99 Abs. 1 KI-VO).[8] Aufgrund dieser Umsetzung soll dann eine dezentrale Durchsetzung der Regelungen erfolgen (Scheffzig & Kilian/*Schefzig*, 2025, Art. 99 Rn. 19). Deutschland hat bislang keine nationalen Sanktionsvorschriften erlassen, die ausschließlich

8 Siehe zur Festlegung der Merkmale *wirksam*, *verhältnismäßig* und *abschreckend* auch EuGH, Urteil vom 21.09.1989 – Rs. 68/88, NJW 1990, 2245, sowie EuGH, Urteil vom 10.07.1990 – Rs. 326/88, BeckRS 2004, 70816.

Verstöße gegen die KI-VO betreffen. Der erste Referentenentwurf eines Gesetzes zur Durchführung der KI-Verordnung – bislang noch nicht offiziell veröffentlicht – sieht vor, Teile der Sanktionsregelungen über das Gesetz über Ordnungswidrigkeiten (OWiG) abzubilden. Nach diesem Entwurf soll die Bundesnetzagentur die Befugnis erhalten, Bußgelder bei Verstößen gegen die KI-VO zu verhängen (BMWK & BMJ, 2024). Mit diesem Entwurf liegt der erste konkrete Schritt zur nationalen Umsetzung der KI-VO vor. Er bietet eine Grundlage für die weitere politische Diskussion. Das geplante KI-Marktüberwachungsgesetz (KIMÜG) wird dabei als stabiles Fundament gesehen, stößt jedoch auch auf Kritik (Schreiber & Bronner, 2025). Die Umsetzungsfrist läuft bis August 2025. Bisher ist jedoch noch kein entsprechendes Gesetz verabschiedet worden. Eine Verabschiedung wird in naher Zukunft erwartet.

Daneben können bei Verstößen gegen die Anforderungen an Medizinprodukte auch Bußgelder nach §§ 92 ff. MPDG verhängt werden, sofern dieselbe Handlung nicht bereits durch die KI-VO sanktioniert wurde.

Das Verbot der Doppelbestrafung[9] (Art. 50 Charta der Grundrechte der Europäischen Union) steht der Anwendung des MPDG nicht entgegen, sofern unterschiedliche Schutzgüter betroffen sind oder unterschiedliche Rechtsgüter vorliegen.

2.6 Kritik und Herausforderungen

Der Zweck der KI-VO wurde bereits in Abschnitt 2.2 (»Ziele der Verordnung«) thematisiert. Mit anderen Worten soll die Verordnung dafür sorgen, dass in der gesamten EU einheitliche Regeln für die Entwicklung, den Verkauf, den Betrieb und die Nutzung von KI-Systemen geschaffen werden, um verantwortungsvolle KI zu ermöglichen, ohne den technischen Fortschritt zu behindern. Nichtsdestotrotz gibt die KI-VO durchaus Anlass zu Kritik, die im Folgenden näher beleuchtet werden soll.

9 EuGH, Urt. v. 14.9.2023 – C-27/22, EuZW 2023, 1045 zur Möglichkeit der Anwendung des Doppelbestrafungsverbots auf Verwaltungssanktionen; EuGH, Urt. v. 22.3.2022 – C-151/20, NZKart 2022, 203, Rn. 36 f. zum Grundsatz *ne bis in idem* und dem Erfordernis des Vorliegens derselben Tat.

In Abschnitt 2.3 (»Risikobasierter Ansatz«) wurde bereits darauf hingewiesen, dass die KI-VO keine einheitlichen Regeln für alle KI-Systeme festlegt, sondern die Anforderungen nach dem jeweiligen Risiko für Gesundheit, Sicherheit oder Grundrechte der Menschen ausrichtet. Insbesondere die Einordnung als »Hochrisiko-KI-System« ist nicht gelungen (Hacker, 2023), da nahezu jedes KI-System in diese Kategorie fällt, während nur besonders extreme Ausprägungen unter die in Art. 5 KI-VO genannten verbotenen Praktiken fallen. Dadurch verliert der risikobasierte Ansatz in vielen Fällen an Wirkung und führt dazu, dass KI-Systeme in der Regel den strengeren Vorgaben für Hochrisiko-KI-Systeme unterliegen (Spranger & Wenzel, 2023).

Die KI-VO stellt zahlreiche Anforderungen an die Beteiligten, die teilweise sehr abstrakt und offen formuliert sind. Bereits die Einordnung dessen, was genau unter ein »KI-System« fällt oder als »Hochrisiko-KI-System« zu qualifizieren ist, bereitet Probleme und führt in der Folge zu Rechtsunsicherheit (Bomhard & Siglmüller, 2024). Die bisher noch allgemeinen Regeln der KI-VO müssen nach Art. 96 KI-VO durch EU-Leitlinien konkretisiert werden. Diese Leitlinien sind jedoch noch nicht veröffentlicht. Da die Umsetzungsfristen unabhängig von der Ausarbeitung der Leitlinien gelten, wird sich der Erfolg der Maßnahmen erst im Zeitverlauf beurteilen lassen (Art. 113 KI-VO). Nicht zu unterschätzen ist dabei auch der bürokratische Aufwand, den die KI-VO für die jeweiligen Mitgliedstaaten mit sich bringt. Dieser Problematik wird nur teilweise mit den verlängerten Fristen begegnet (Becker & Feuerstack, 2024).

Die parallele Anwendung der KI-VO mit sektorspezifischen Regelungen, wie im medizinischen Bereich mit der MP-VO, kann zu einer sogenannten horizontalen Doppelregulierung führen (Abschnitt 2.5 [»Sanktionsmechanismen«]). Die teilweise überlappenden Pflichten schaffen eine undurchsichtige und komplexe Rechtslage für alle Beteiligten, die sich intensiv mit den ihnen obliegenden Pflichten auseinandersetzen müssen, um potenzielle Sanktionen zu vermeiden. Eine entsprechende Überregulierung könnte zulasten von technologischen Innovationen und Fortschritten im medizinischen Sektor entstehen. Es besteht mithin Bedarf nach einer Harmonisierung der Regulierungen (BVMed, 2021).

Die KI-VO differenziert zwar zwischen zahlreichen Beteiligten (Abschnitt 2.4 [»Akteure und Verantwortliche«]), berücksichtigt je-

doch die Unternehmensgröße weitgehend nicht. Dies kann insbesondere für kleine und mittlere Unternehmen (KMU) zu erheblichen Herausforderungen führen. Ihnen könnten die personellen und finanziellen Ressourcen fehlen, um die umfangreichen Anforderungen der KI-VO vollständig zu prüfen und umzusetzen. Gleichzeitig drohen bei Verstößen hohe Geldbußen (Abschnitt 2.5 [»Sanktionsmechanismen«]), was für KMU ein besonders hohes wirtschaftliches Risiko bedeuten kann (Hacker & Berz, 2023).

Nach Art. 2 der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 werden KMU wie folgt eingestuft:

> »Mitarbeiterzahlen und finanzielle Schwellenwerte zur Definition der Unternehmensklassen
> 1. Die Größenklasse der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (KMU) setzt sich aus Unternehmen zusammen, die weniger als 250 Personen beschäftigen und die entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf höchstens 43 Mio. EUR beläuft.
> 2. Innerhalb der Kategorie der KMU wird ein kleines Unternehmen als ein Unternehmen definiert, das weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 10 Mio. EUR nicht übersteigt.
> 3. Innerhalb der Kategorie der KMU wird ein Kleinstunternehmen als ein Unternehmen definiert, das weniger als 10 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 2 Mio. EUR nicht überschreitet.«

Als KMU gelten demnach Unternehmen mit weniger als 250 Beschäftigten und einem Jahresumsatz von höchstens 50 Millionen Euro. Diese Definition weicht von der in der Allgemeinheit oft vertretenen Vorstellung ab, wonach KMU überwiegend sehr kleine Betriebe sind. Folglich erscheint eine pauschale Privilegierung dieser Unternehmensgruppe gegenüber großen Unternehmen nicht uneingeschränkt gerechtfertigt. Eine Einzelfallbetrachtung wäre dabei differenzierter. Die KI-VO erkennt in Erwägungsgrund Nr. 143 S. 1 ausdrücklich die Bedeutung des Schutzes von KMU zur Förderung von Innovationen an. Dieses Prinzip wird unter anderem in Art. 99 Abs. 6 KI-VO durch die Wahl des jeweils niedrigeren Sanktionsbetrags umgesetzt. Zudem sieht Art. 11 Abs. 1 S. 4 KI-VO Erleichterungen für kleine und Kleinstunternehmen bei der technischen Dokumentation vor. Gleichwohl bleibt fraglich, ob diese punktuellen Entlastungen ausreichen, um die strukturellen Nachteile für KMU wirksam zu kompensieren.

Diese und weitere Aspekte werden von der KI-VO bislang unberücksichtigt gelassen. Sie lässt damit durchaus Raum für Kritik. Erst die zukünftige Entwicklung wird Aufschluss darüber geben, ob die Realisierung der Ziele ohne negative Auswirkungen auf die medizinische Forschung und Innovationsentwicklung im Gesundheitswesen möglich ist.

3. Haftungsrichtlinie und Produkthaftungsrecht

Die zunehmenden Einsatzmöglichkeiten von KI werfen darüber hinaus grundlegende haftungsrechtliche Fragen auf. Gerade in sicherheitsrelevanten Bereichen, wie etwa dem Gesundheitswesen, bedarf es einer umfassenden Betrachtung. Insbesondere stellt sich die Herausforderung, wie Schadensfälle zu behandeln sind, bei denen die Ursache in einem teilweise autonomen Verhalten eines KI-Systems liegt, das auf selbstlernenden oder datenbasierten Prozessen beruht. Ein wichtiger Baustein für die Schaffung eines kohärenten rechtlichen Rahmens für KI in der EU ist daher das Haftungsrecht. Das bisherige europäische Haftungsrecht, dabei insbesondere das Zivil- und Deliktsrecht, ist stark national geprägt. Die bestehenden zivilrechtlichen Regelwerke – insbesondere die verschuldensunabhängige Produkthaftung nach dem Produkthaftungsgesetz (ProdHaftG) – waren bislang auf klassische, deterministisch funktionierende Produkte zugeschnitten. Die derzeitig bestehenden nationalen Haftungsvorschriften umfassen demnach nicht ausdrücklich Schadensersatzansprüche infolge von durch KI-gestützte Produkte oder Dienstleistungen verursachte Schäden. Die sich daraus ergebenden Lücken und Unsicherheiten haben zu einer politischen Diskussion über eine Anpassung des Haftungsrahmens geführt, insbesondere auf europäischer Ebene im Zuge der Überarbeitung der Produkthaftungsrichtlinie (siehe dazu unter Abschnitt 3.2. [»Status quo«]) und einer geplanten Richtlinie über die Haftung für KI-Systeme (KI-HaftungsRL-E) (siehe dazu unter Abschnitt 3.1 [»Ursprünglicher Regulierungsansatz«]).

3.1 Ursprünglicher Regulierungsansatz

Um Rechtsunsicherheiten zu vermeiden und unter der Prämisse eines stets zu wahrenden hohen Schutzstandards plante die Kommission, Haftungsvorschriften für Schäden, die durch KI-Systeme verursacht werden, unionsrechtlich zu vereinheitlichen. Dazu veröffentlichte sie im Jahr 2022 den Vorschlag für eine Richtlinie zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (Richtlinie über KI-Haftung). Ziel war es, einen harmonisierten Rechtsrahmen in der EU zu schaffen, um der Gefahr der Fragmentierung des Binnenmarktes zu entgegnen. Gleichzeitig sollte sichergestellt werden, dass eine durch KI-Technologie geschädigte Person in gleicher Weise entschädigt wird, wie in vergleichbaren Fällen ohne KI-Beteiligung. Mit Zusammenkunft der neuen Kommission wurde der Vorschlag für die KI-Haftungsrichtlinie in ihrem Arbeitsprogramm für 2025 überraschend zurückgezogen. Stattdessen soll auf bereits bestehende Haftungsvorschriften zurückgegriffen werden.

De lege lata gib es verschiedene rechtliche Vorgaben, die einen etwaigen Schadensersatzanspruch beinhalten: Zunächst kommt eine verschuldensunabhängige Haftung des Herstellers eines KI-Systems in Betracht, wenn sein Produkt fehlerhaft ist und dadurch ein Schaden entsteht. Hierbei wird allerdings der Fall außer Acht gelassen, dass das KI-System selbst nicht fehlerhaft ist, sondern erst nach dem Inverkehrbringen durch maschinelles Lernen von geplantem Output »abweicht«, sodass in diesem Fall eine Regelungslücke besteht.

Im Deliktsrecht kommt eine Haftung des medizinischen Personals oder des Klinikträgers – etwa wegen Verletzung der ärztlichen Sorgfaltspflicht oder eines Organisationsverschuldens – in Betracht, wenn durch ein KI-System ein Schaden entsteht (z. B. eine fehlerhafte medizinische Diagnose). Auch im Rahmen eines vertraglichen Anspruchs (z. B. Behandlungsvertrag) – etwa auf Schadensersatz wegen Schlechterfüllung – muss das Verschulden nachgewiesen werden. Problematisch dabei ist, dass die bestehenden Regelungen ein Verschulden oder einen klaren Produktfehler voraussetzen. Beides ist bei KI-Systemen mit lernenden, teilweise intransparenten Entscheidungen häufig schwierig zu beweisen, wodurch echte Haftungslücken entstehen.

Ziel der geplanten Haftungsrichtlinie war es, solche Haftungslücken zu schließen, indem in Ergänzung zum Produkthaftungsrecht ein Schaden auch in den Konstellationen ersetzt werden sollte, in denen gerade kein Produktfehler vorliegt. Zur Umsetzung sah der Vorschlag einen vereinfachten Zugang zu Informationen vor und enthielt Vorschriften über die Offenlegung von Beweismitteln, um die Beweislast der geschädigten Person zu erleichtern. Neben dem Zugang zu Beweismitteln stellte die vorgesehene Kausalitätsvermutung eine wesentliche Maßnahme dar. Demnach sollte der für Schadensersatzansprüche üblicherweise erforderliche ursächliche Kausalzusammenhang zwischen dem Verschulden des Beklagten und dem Output des KI-Systems (widerlegbar) vermutet werden, wenn die in Art. 4 Abs. 1 KI-HaftungsRL-E benannten Voraussetzungen erfüllt sind: Zum einen muss ein Verschulden auf Seiten des Beklagten in der Weise vorliegen, dass gegen eine im Unionsrecht oder im nationalen Recht festgelegte Sorgfaltspflicht, deren unmittelbarer Zweck darin besteht, den eingetretenen Schaden zu verhindern, verstoßen wurde (Art. 4 lit. a KI-HaftungsRL-E). Darüber hinaus muss der Sorgfaltspflichtverstoß den vom KI-System hervorgebrachten Output auf Grundlage der Umstände des Falls nach vernünftigem Ermessen beeinflusst haben (Art. 4 lit. b KI-HaftungsRL-E). Schließlich muss das vom KI-System hervorgebrachte Ergebnis oder aber die Tatsache, dass das KI-System kein Ergebnis hervorgebracht hat, zu dem Schaden geführt haben.

Handelt es sich um einen Schadensersatzanspruch gegenüber einem »Nutzer« eines Hochrisiko-KI-Systems, beispielsweise einem Arzt oder einer Ärztin, konkretisiert Art. 4 Abs. 3 KI-HaftungsRL-E für den Nachweis einer Sorgfaltsverletzung, dass eine solche vorliegt, wenn das KI-System entgegen der beigefügten Gebrauchsanweisung verwendet oder überwacht wurde und die Eingabedaten der Zweckbestimmung des Systems widersprechen. Mit dem Vorschlag sollten die mit KI-Systemen einhergehenden neuen Fragen geklärt und etwaige Rechtsunsicherheiten behoben werden. Durch die Streichung der Richtlinie vom Arbeitsplan muss nun erneut auf die vorliegenden nationalen Haftungsvorschriften zurückgegriffen werden.

3.2 Status quo

Um dennoch den weiterhin bestehenden Gefahren der Fragmentierung des Binnenmarktes entgegenzuwirken und bestehende Haftungslücken zu schließen, wird in diesem Zuge nun auf Änderungen in der Produkthaftungsrichtlinie verwiesen. Bereits vor dem Rückzug der KI-Haftungsrichtlinie hat die EU-Kommission Ende 2024 die Produkthaftungsrichtlinie (ProdHaft-RL) novelliert und dabei die Haftung für Software, einschließlich KI, erweitert (Richtlinie 2024/2853). Sie wurde am 18.11.2024 im Amtsblatt der Europäischen Union veröffentlicht und muss von den Mitgliedstaaten bis zum Jahr 2026 in nationales Recht umgesetzt werden. Durch die Änderungen wurde der Produktbegriff auf Software und KI-Systeme ausgeweitet, sodass KI-Modelle nun ebenfalls haftungsrechtlich erfasst sind. Hersteller von KI-Anwendungen haften künftig auch für Ausfälle oder Schäden, die durch unzureichende Updates oder Sicherheitslücken entstehen (Art. 11 Abs. 2 ProdHaft-RL). Darüber hinaus gibt es Vorgaben bezüglich der Offenlegung von Beweismitteln und zugleich wurde die Anspruchsdurchsetzung zugunsten der Opfer durch Beweiserleichterungen und Vermutungsregeln für Geschädigte erleichtert.

4. European Health Data Space

Das politische Konzept der europäischen Datenräume überspannt im Bereich des Umgangs mit Gesundheitsdaten spezifische Vorschriften wie etwa die Datenschutz-Grundverordnung oder die KI-Verordnung. Die Kommission plant insoweit ein regelbasiertes Daten-Ökosystem, das unter anderem die Sekundärdatennutzung von Gesundheitsdaten maßgeblich erleichtern soll. Diese Einbettung birgt verschiedene rechtliche Folgen für die gesundheitsbezogene KI-Nutzung, die sich nur in der Gesamtschau zufriedenstellend einordnen und klären lassen.

Sowohl in Bezug auf Therapien als auch das Verständnis von Krankheiten und der Entwicklung von Medikamenten ist die Forschung mit medizinischen Daten essenziell für Innovation und Weiterentwicklung in der Medizin. Das Problem ist dabei häufig der Schutz solcher Daten. Dass die Signifikanz der Forschung grund-

sätzlich mitbedacht wird, sieht man bereits an der expliziten Privilegierung der Forschung sowohl in der KI-VO als auch der DSGVO. Durch die neuen Möglichkeiten, die aus der Anwendung von KI resultieren, eröffnen sich weitreichende neue Chancen. Der European Health Data Space (EHDS) ist dabei ein zentrales Vorhaben der EU zur digitalen Transformation des Gesundheitswesens. Es soll einen sicheren, einheitlichen Rahmen schaffen, um Gesundheitsdaten sowohl für die primäre Versorgung als auch für sekundäre Zwecke – insbesondere Forschung, Innovation und Politikgestaltung – grenzüberschreitend verfügbar zu machen. Konkret wurde im März 2025 die zugehörige Verordnung (EU) 2025/327 über den europäischen Gesundheitsdatenraum (Abl. L 2025/327 v. 05.03.2025) veröffentlicht (im Folgenden EHDS-VO).

Im Verhältnis zur DSGVO fungiert die EHDS-VO nicht als konkurrierendes Regelwerk. Vielmehr stellt sie eine Konkretisierung der datenschutzrechtlichen Anforderungen für den Gesundheitsbereich als sektorenspezifische Ausgestaltung dar. Gleichzeitig ergänzt die EHDS-VO die KI-VO, indem sie den Zugang zu qualitativ hochwertigen Gesundheitsdaten regelt, was von großer Bedeutung für das Training, die Prüfung und Validierung von KI-Systemen in der medizinischen Forschung und Versorgung ist. Im Grunde sollen alle personenbezogenen Gesundheitsdaten für die Sekundärnutzung verfügbar gemacht werden. Art. 51 EHDS-VO legt zu diesem Zweck einen Mindestkatalog elektronischer Gesundheitsdaten fest, die von den »Gesundheitsdateninhabern« für die Sekundärnutzung zur Verfügung gestellt werden müssen, soweit nicht ausdrücklich widersprochen wird (sog. »Opt-out-Modell«). Zu den benannten Gesundheitsdaten gehören beispielsweise elektronische Gesundheitsdaten aus Systemen für elektronische Gesundheitsaufzeichnungen (electronic health records, EHR) (lit. a), Daten zu Faktoren, die sich auf die Gesundheit auswirken, einschließlich sozioökonomischer, umweltbedingter und verhaltensbezogener Gesundheitsfaktoren (lit. b), menschliche genetische, epigenomische und genomische Daten (lit. f), Daten aus Wellness-Anwendungen (lit. i) und Gesundheitsdaten aus Biobanken und zugehörigen Datenbanken (lit. q). Darüber hinaus kann der Katalog nach Art. 51 Abs. 2 EHDS-VO durch die Mitgliedstaaten erweitert werden. Um Zugang zu den nach Art. 51 EHDS-VO erhobenen Sekundärdaten zu erlangen, muss die Verarbeitung der Daten für einen der in Art. 53 EHDS-VO gelisteten

Zwecke erforderlich sein. Dazu gehören etwa öffentliche Interessen im Bereich der öffentlichen Gesundheit oder der Gesundheit am Arbeitsplatz, Politikgestaltung und Regulierungstätigkeiten zur Unterstützung von öffentlichen Stellen oder Organen, Statistiken im Sinne von Art. 3 Nr. 1 der Verordnung (EG) Nr. 223/2009, Bildungs- oder Lehrtätigkeiten im Gesundheitswesen oder im Pflegesektor auf der Ebene der Berufs- oder Hochschulbildung, wissenschaftliche Forschung im Bereich des Gesundheitswesens oder des Pflegesektors und die Verbesserung der Pflege und Gesundheitsversorgung. Im Ergebnis ist nahezu jeder mit dem Gesundheits- oder Pflegesektor zusammenhängender Zweck ausreichend, um von der Zugangsstelle für Gesundheitsdaten (Art. 55 EHDS-VO) die entsprechenden Daten zu erhalten.

Obwohl der EHDS darauf abzielt, einen kohärenten und grenzüberschreitenden Rahmen für die Nutzung von Gesundheitsdaten in der EU zu schaffen, steht der Verordnung in der Fachliteratur und Praxis teils erheblicher Kritik gegenüber. Die Verpflichtung von Gesundheitseinrichtungen, sensible medizinische Informationen an neue staatliche Agenturen in jedem EU-Mitgliedstaat weiterzugeben, kann die Vertraulichkeit der »Arzt-Patienten-Beziehung« negativ beeinträchtigen. Dies könnte zur Folge haben, dass Patient*innen relevante Informationen gegenüber dem Behandlungspersonal zurückhalten (Konopik, 2025). Zudem wird beanstandet, dass ethisch-gesellschaftliche Aspekte, darunter insbesondere Transparenz gegenüber Betroffenen, informierte Einwilligung sowie Schutz vor Diskriminierung, bislang nicht hinreichend ausgearbeitet wurden.[10] Bereits in einer Pressemitteilung vom 05. April 2023 äußerte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) Bedenken hinsichtlich des ausreichenden Schutzes der Gesundheitsdaten und einer nicht angemessenen Berücksichtigung des Grundrechts auf Datenschutz bzw. des Rechts auf informationelle Selbstbestimmung. Besonders kontrovers diskutiert wird in diesem Zusammenhang das »Opt-out-Modell«, wonach Gesundheitsdaten grundsätzlich für Sekundärzwecke genutzt werden dürfen, solange die betroffene Person dem nicht ausdrücklich widerspricht. Dieses Vorgehen wird kritisch gesehen, da es die informatio-

10 Siehe zur informierten Einwilligung auch Lanzerath, 2025, Zeitschrift für medizinische Ethik, 71(1), 53–69.

nelle Selbstbestimmung der Betroffenen einschränken könnte und insbesondere vulnerable Gruppen, etwa Personen mit Sprachbarrieren oder eingeschränkter digitaler Kompetenz, trotz des in Art. 71 Abs. 2 EHDS-VO vorgesehenen »barrierefreien und leicht verständlichen Mechanismus zum Widerspruch«, faktisch von einer wirksamen Widerspruchsmöglichkeit ausgeschlossen sein könnten.

Ein weiterer Kritikpunkt betrifft die technische Realisierbarkeit der EHDS-Vorgaben. Teilweise wird in dem Zusammenhang eine gemeinsame europäische Auslegung und koordinierte Umsetzung gefordert, um Inkonsistenzen zwischen den nationalen Systemen der Mitgliedstaaten und daraus resultierende Sicherheitslücken zu vermeiden (Konopik, 2025). Die DSK fordert zudem die Streichung der vorgesehenen Regelung zur Bereitstellung von persönlichen Genomdaten, da dies in den intimsten Bereich der betroffenen Personen und ihrer Angehörigen eingreife (DSK, Pressemitteilung v. 05. April 2023). Schließlich wird darauf hingewiesen, dass die Verordnung strukturell eine Bevorteilung großer Technologieunternehmen begünstigen könnte. Diese verfügen über die notwendigen Ressourcen, um die komplexen Anforderungen an Datennutzung, Interoperabilität und Sicherheit zu erfüllen, während kleinere Akteure im Gesundheitswesen Gefahr laufen, abgehängt zu werden. Damit droht eine Machtkonzentration im digitalen Gesundheitssektor, die sowohl wettbewerbsrechtliche als auch innovationspolitische Implikationen hat.

Zusammenfassend lässt sich festhalten, dass der EHDS zwar das Potenzial hat, die Nutzung von Gesundheitsdaten in der EU erheblich zu erleichtern und innovative Forschungsansätze zu fördern, zugleich aber gewichtige Bedenken offenbart. Neben datenschutz- und ethisch-rechtlichen Herausforderungen, insbesondere im Hinblick auf Transparenz, informierte Einwilligung und das »Opt-out-Modell«, bestehen Zweifel an der technischen Umsetzbarkeit und der Wahrung der Vertraulichkeit der »Arzt-Patienten-Beziehung«. Maßgeblich ist, ob ein angemessener Schutz individueller Grundrechte sowie faire Wettbewerbsbedingungen gewährleistet werden können.

5. Schlussbetrachtung und Ausblick

Künstliche Intelligenz entwickelt sich rasant weiter und wird auch künftig – insbesondere im Gesundheitswesen – Fortschritte mit sich

bringen. Die Ausschöpfung dieses Potenzials hängt allerdings maßgeblich von der Klärung rechtlicher Rahmenbedingungen und der Sicherstellung von Datensicherheit ab. Die Privilegierung der Forschung im Rahmen der KI-VO macht die Relevanz von KI sowie die Bedeutung der Schaffung eines innovationsfreundlichen Standorts für digitale Technologien deutlich.

Mit der im Juni 2024 verabschiedeten KI-Verordnung wurde ein erster Versuch unternommen, einheitliche Vorschriften für KI zu schaffen. Sie regelt unter anderem die Risikoklassifizierung von Systemen, die Pflichten der Beteiligten sowie technische Anforderungen. Bei Verstößen drohen hohe Geldbußen. Gleichzeitig bestehen jedoch Überschneidungen mit der MP-VO, was mangels Vorrangregelung zu Rechtsunsicherheiten führt. Diese sogenannte horizontale Doppelregulierung bildet gemeinsam mit zahlreichen anderen Aspekten – wie der Offenheit der Begriffe, der mangelnden Konkretisierung und der angezweifelten Einordnung der Hochrisiko-KI-Systeme – den Grundstein für eine kritische Betrachtung.

Der von der Kommission entwickelte Entwurf einer KI-Haftungsrichtlinie sollte Schadensansprüche infolge von durch KI-gestützte Produkte oder Dienstleistungen verursachten Schäden regeln. Er wurde allerdings im aktuellen Arbeitsprogramm überraschend zurückgezogen und es wurde stattdessen auf bestehende Haftungsvorschriften verwiesen. Zudem sorgt der European Health Data Space mit der Zugangserleichterung zu personenbezogenen Gesundheitsdaten für die Sekundärnutzung im Gesundheitswesen für Kritik hinsichtlich des Datenschutzes.

Die Rechtslage bezüglich der Regulierung von KI-Systemen im Gesundheitswesen ist nach wie vor unsicher. Es gibt Unklarheiten und rechtliche Grauzonen im Hinblick auf die KI-VO, Haftungsfragen sowie bei der Unterscheidung zwischen echten und unechten Haftungsprivilegien. Wie sich dies auswirkt, wird sich in der Zukunft ergeben. Erwartete Änderungen in der KI-VO werden zeigen, ob die aktuellen Probleme gelöst werden können. Unternehmen und Institutionen sollten die bestehenden Vorgaben daher sorgfältig beachten und sich frühzeitig auf absehbare Änderungen einstellen.

Literaturverzeichnis

Becker, D., & Feuerstack, D. (2024). Die EU-KI-Verordnung: Überblick und Bewertung der finalen Fassung der KI-VO. *Künstliche Intelligenz und Recht,* (2), 62–69.

Bundesministerium für Wirtschaft und Klimaschutz & Bundesministerium der Justiz (BMJ). (2024, 4. Dezember). *Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024… (Verordnung über künstliche Intelligenz)* [Nicht offiziell veröffentlichter Referentenentwurf]. https://assets.ctfassets.net/jq1xw71av3v5/6AKrXoeiDtYvFgYjrEwLYI/774c67d2d73ccc94aee94f894a936a87/241204_BMWK-BMJ_RefE_AI-Act-Umsetzung.pdf

Bundesrat. (2016). *Zweite Verordnung zur Änderung medizinprodukterechtlicher Vorschriften* [Drucksache 397/16 v. 04.08.2016]. https://www.bundesrat.de/SharedDocs/drucksachen/2016/0301-0400/397-16.pdf

Bomhard, D., & Siglmüller, J. (2024). AI Act – das Trilogergebnis. *Recht Digital (RDi),* 45–52.

BVMed. (2021). BVMed-Positionen zum Entwurf des »Artificial Intelligence Act« (AIA). *Medizin Produkte Recht (MPR),* (5), 176–182.

Ebers, M., & Streitbörger, C. (2024). Die Regulierung von Hochrisiko-KI-Systemen in der KI-Verordnung. *Recht Digital (RDi), 2024,* 393–400.

Eisemann, N., Bunk, S., Mukama, T., Baltus, H., Elsner, S. A., Gomille, T., Hecht, G., Heywang-Köbrunner, S., Rathmann, R., Siegmann-Luz, K., Töllner, T., Vomweg, T. W., Leibig, C., & Katalinic, A. (2025). Nationwide real-world implementation of AI for cancer detection in population-based mammography screening. *Nature Medicine, 31*, 917–924. https://doi.org/10.1038/s41591-024-03408-6

Europäische Kommission. (o. D.). *Medical devices – EUDAMED: Überblick.* https://health.ec.europa.eu/medical-devices-eudamed/overview_de

Gerdemann, S. (2024). Konformitätsbewertung als Kernpflicht der KI-Verordnung. *Neue Juristische Wochenschrift (NJW),* 2209–2215.

Hacker, P. (2023). Die Regulierung von ChatGPT et al. – ein europäisches Trauerspiel. *Gewerblicher Rechtsschutz und Urheberrecht (GRUR),* (5), 289–290.

Hacker, P., & Berz, A. (2023). Der AI Act der Europäischen Union – Überblick, Kritik und Ausblick. *Zeitschrift für Rechtspolitik,* (8), 226–229.

Hilgendorf, E., & Roth-Isigkeit, D. (2023). *Die neue Verordnung der EU zur Künstlichen Intelligenz. Kommentar* (1. Aufl.). C. H. Beck.

Konopik, J. (2025). Der Europäische Raum für Gesundheitsdaten (EHDS) und seine Bedeutung für das deutsche Gesundheitswesen. *Prävention und Gesundheitsförderung.* https://doi.org/10.1007/s11553-025-01200-z

Lachenmann, M. (2024). EU-Rat stimmt KI-Verordnung zu – neue Pflichten für Unternehmen. *MMR-Aktuell*, (4), 01359.

Lanzerath, D. (2025). Access and Benefit-Sharing: Gesundheitsdaten in der medizinischen Forschung nutzen. *Zeitschrift für medizinische Ethik, 71*(1), 53–69. https://doi.org/10.30965/29498570-20250108.

Martini, M., & Wendehorst, C. (Hrsg.). (2024). *KI-VO: Verordnung über künstliche Intelligenz. Kommentar* (1. Aufl.) C. H. Beck.

Rehmann, W., & Wagner, S. (Hrsg.). (2023). *MP-VO. Verordnung (EU) 2017/745 über Medizinprodukte. Kommentar* (4. Aufl.). C. H. Beck.

Schefzig, J., & Kilian, R. (Hrsg.). (2025). *BeckOK KI-Recht (2. Edition)*. C. H. Beck.

Schreiber, M., & Bronner, P. (2025). Der Referentenentwurf für ein Gesetz zur Durchführung der KI-Verordnung. *jurisPR-ITR, 7,* Anm. 2.

Schuh, M., & Witt, H. (2025). KI-Systeme und ihre Betreiber nach der KI-VO: Pflichten und Abgrenzung zum Endnutzer. *Zeitschrift für Europäisches Daten- und Informationsrecht (EuDIR)*, 142–148.

Spitz, M., Cornelius, K., Jungkunz, M., & Schickhardt, C. (2021). Rechtlicher Rahmen für eine privilegierte Nutzung klinischer Daten zu Forschungszwecken. *Medizinrecht (MedR), 39*, 499–504. https://doi.org/10.1007/s00350-021-5898-7

Spitz, M. (2025). Die KI-Verordnung und die Privilegierung medizinischer Forschung. *Medizinrecht MedR), 43,* 601–604. https://doi.org/10.1007/s00350-025-7102-y

Spranger, T. M., & Wenzel, M. (2023). Künstliche Intelligenz in der Medizin: Anmerkungen zum aktuellen Verordnungsentwurf der Europäischen Kommission. In S. Bohnet-Joschko & K. Pilgrim (Hrsg.), *Handbuch Digitale Gesundheitswirtschaft* (S. 263–266). Springer Gabler. https://doi.org/10.1007/978-3-658-41781-9_55