BDPK
Bundesverband
Deutscher Privatkliniken e.V.

25.06.2026

Forderungen des BDPK zum sicheren Einsatz von Cloud-Computing-Diensten im deutschen Gesundheitswesen

Vorbemerkung

In der Praxis divergieren sowohl Aufsichtsbehörden als auch Marktakteure bei der Auslegung und Anwendung der einschlägigen Vorschriften des § 393 SGBV zur Verarbeitung von Sozial- und Gesundheitsdaten in Cloud-Computing-Diensten erheblich, da kein einheitliches Verständnis darüber besteht, unter welchen Voraussetzungen der Cloud-Einsatz rechtssicher möglich ist. Der § 393 SGB V ist in seiner aktuellen Fassung weder hinreichend klar noch konsistent mit den unionsrechtlichen Vorgaben der Verordnung (EU) 2016/679 (DSGVO) ausgestaltet. Vor diesem Hintergrund regen wir an, diese Unsicherheiten im Wege einer gesetzlichen Klarstellung, beispielsweise im Rahmen des aktuellen Gesetzgebungsverfahren zum Gesetz für Daten und digitale Innovation im Gesundheitswesen (GeDIG), zu beseitigen.

Konkrete Vorschläge zur Änderung des § 393 SGB V nebst Begründung

Aktuelle Regelung § 393 SGB V	**Vorschlag für Neuregelung § 393 SGB V (neu)**	**Begründung**
(1) Leistungserbringer im Sinne des Vierten Kapitels und Kranken- und Pflegekassen sowie ihre jeweiligen Auftrags-datenverarbeiter dürfen Sozialdaten und Gesundheitsdaten auch im Wege des Cloud-Computing-Dienstes verarbeiten, sofern die Voraussetzungen der Absätze 2 bis 4 erfüllt sind.	(1) Zur Verbesserung der Versorgung durch leistungsfähige, hochverfügbare, innovative und gleichzeitig sichere IT-Anwendungen dürfen Leistungserbringer im Sinne des Vierten Kapitels und Kranken- und Pflegekassen sowie ihre jeweili- gen Auftrags~~daten~~verarbeiter ~~dürfen~~ Sozialdaten und Gesundheitsdaten auch im Wege des Cloud-Computing-Dienstes verarbeiten, sofern die Voraussetzungen der Absätze 2 bis 4 erfüllt sind.	I. Einfügen der Formulierung: *„Zur Verbesserung der Versorgung durch leistungsfähige, hoch- verfügbare, innovative und gleichzeitig sichere IT-Anwendungen dürfen […]“.* Es soll klargestellt werden, dass § 393 SGB V den Cloud-Einsatz fördern und damit unter Einhaltung bestimmter Voraussetzungen ermöglichen soll. Die fortschreitende Digitalisierung des Gesundheitswesens ist eine unumgängliche Voraussetzung, um die medizinische Versorgung in Deutschland zukunftsfähig, effizient und sicher zu gestalten. Gleichzeitig stellen europäische Regulierungen im Rahmen der EU-Digitalstrategie, wie der European Health Data Space, hohe Anforderungen an die Interoperabilität, die Sicherheit und den grenzüberschreitenden Austausch von Gesundheitsdaten. Im Zentrum dieser Transformation steht die Fähigkeit, sensible Gesundheitsdaten in modernen IT-Infrastrukturen zu verarbeiten, die leistungsfähig, hochverfügbar und gleichzeitig sicher sind. Die Migration von traditionellen, lokal betriebenen Rechenzentren der einzelnen Gesundheitseinrichten in die Cloud ist dabei nicht nur eine Frage der Effizienz oder Kostenoptimierung, sondern eine strategische Notwendigkeit, um die Qualität und die Sicherheit der Patientenversorgung nachhaltig zu verbessern. Insbesondere fordern neue KI-

		basierte Softwareanwendungen eine besonders leistungsfähige und interoperable Infrastruktur, die derzeit und künftig nur durch Cloud-Infrastrukturen bereitgestellt werden kann. Ein eindeutiger gesetzlicher Rahmen soll daher die (rechts)sichere Nutzung der Cloud ausdrücklich ermöglichen. II. Ersetzung der Formulierung *„Auftragsdatenverarbeiter“* durch *„Auftragsverarbeiter“.* Redaktionelle Anpassungen in Einklang mit der Terminologie der DSGVO.
Keine	(1a) Im Sinne dieses Buches bezeichnet der Ausdruck 1. „Verarbeitung im Wege des Cloud-Computing-Dienstes“ eine Verarbeitung von Sozialdaten und Gesundheitsdaten, die selbst und unmittelbar durch einen Cloud-Computing- Dienst erfolgt. 2. „datenverarbeitende Stelle“ das Unternehmen oder die Stelle, die die für die Bereitstellung des Cloud-Computing- Dienstes	I. Einfügen einer neuen klarstellenden Definition in Abs. (1a) Nr. 1. Das Tatbestandsmerkmal „im Wege des Cloud-Computing-Dienstes“ (enthalten in Abs. 1 und 2) bedarf aus Gründen der Rechtssicherheit der Klarstellung. Bisher ist nur der Cloud-Computing-Dienst in § 384 Nr. 5 wie folgt legal definiert: „Cloud- Computing-Dienst einen digitalen Dienst, der auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht, auch wenn diese Ressourcen auf mehrere Standorte verteilt sind.“ Nach rechtsmethodischem Verständnis des Zusatzes „im Wege“ liegt dem gesamten Tatbestandsmerkmal „im Wege des Cloud-Computing-Dienstes“ ein technisches Verständnis zugrunde, das sich auf die Cloud-spezifischen Risiken bezieht. Unter Berücksichtigung des gesetzgeberischen Ziels (Förderung des Cloud-Einsatzes im Gesundheitswesen bei Schaffung einer

	erforderliche Infrastruktur technisch betreibt und unmittelbar kontrolliert.	hinrei- chenden Sicherheit) fallen demnach nur solche Datenverarbeitungen in den Anwendungsbereich von § 393 SGB V, die selbst und unmittelbar auf einem Cloud-Computing-Dienst beruhen, da nur insofern die Cloud-spezifischen Risiken entstehen und reguliert werden müssen. Daher sollen u.a. Support-Leistungen, die ihrerseits nicht auf Cloud-Computing-Diensten beruhen, sondern ausschließlich per remote-Zugriff erfolgen, nicht erfasst sein. Die neue klarstellende Definition schärft den Anwendungsbereich praxistauglich und entlang des gesetzgeberischen Willens sowie auf Ebene der auch grundrechtlich gerechtfertigten Regulierung, ohne das Cloud-bedingte Schutzniveau abzusenken. II. Einfügen einer neuen klarstellenden Definition in Abs. (1a) Nr. 2. Das Tatbestandsmerkmal der „datenverarbeitenden Stelle“ (enthalten in Abs. 2 und 3) ist weder im SGB V, noch der DSGVO oder dem BDSG legaldefiniert und bedarf aus Gründen der Rechtssicherheit der Schärfung. Nach rechtsmethodischem und insbesondere teleologischem Verständnis liegt auch diesem Tatbestandsmerkmal ein technisches und Cloud-spezifisches Verständnis zugrunde. Mit dem Tatbestandsmerkmal soll - wie bisher auch - die Stelle gemeint sein, die den skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen (§ 384 Nr. 5) technisch betreibt und damit die Cloud-spezifischen Risiken unmittelbar operativ kontrolliert. Das sind die Betreiber/Anbieter der technischen Infrastruktur (z.B.

		Hyperscaler). Der Begriff ist auf diese Akteure zu beziehen und insbesondere von den datenschutzrechtlichen Rollen des Verantwortlichen und Auftragsverarbeiter abzugrenzen, da es um eine davon abweichende Rolle geht. Ziel des § 393 SGB V ist es, die typischen Cloud-Risiken zu regulieren. In der Praxis können diese Rollen gleichwohl zusammenfallen. Die Etablierung eines gesonderten, für § 393 SGB V spezifischen Begriffes ist daher geboten und richtig. Dieser ist aber entsprechend legal zu definieren.
(2) Die Verarbeitung von Sozial- und Gesundheitsdaten im Wege des Cloud-Computing-Dienstes darf nur 1. im Inland, 2. in einem Mitgliedstaat der Europäischen Union oder 3. in einem diesem nach § 35 Absatz 7 des Ersten Bu- ches gleichgestellten Staat oder, sofern ein Angemes-	(2) Die Verarbeitung von Sozial- und Gesundheitsdaten im Wege des Cloud-Computing-Dienstes darf nur 1. im Inland, 2. in einem Mitgliedstaat der Europäischen Union oder 3. in einem diesem nach § 35 Absatz 7 des Ersten Bu- ches gleichgestellten Staat oder, sofern die Anforderungen der Art. 44 ff. ~~ein Angemessenheitsbeschluss gemäß Artikel 45~~ der Verordnung (EU) 2016/679 vorieg~~en~~t, in einem Drittstaat	I. Ersetzung der Formulierung: *„ein Angemessenheitsbeschluss gemäß Artikel 45“* durch *„die Anforderungen der Art. 44 ff.“.* Die bisherigen geographischen Anforderungen des Abs. 2 sind zu hinterfragen, weil sie bei strenger Lesart über die allgemeinen und ausreichenden Anforderungen der DSGVO hinausgehen. In der aktuellen Diskussion wird u.a. vertreten, dass sämtliche Datenzu- griffe aus oder in Drittstaaten ohne Angemessenheitsbeschluss oder deren bloße theoretische Möglichkeit dazu führen, dass die Voraussetzungen von § 393 SGB V nicht erfüllt sein sollen. Dieses Verständnis geht über die allgemeinen Anforderungen der DSGVO hinaus. Dafür besteht angesichts des schon durch Art. 44 ff. DSGVO erreichten hohen Schutzstandards kein Anlass. Ein Verweis auf die Geltung der Art. 44 ff. DSGVO ist ausreichend, um die legitimen Ziele des § 393 SGB V zu erreichen. Eine weitergehende Regulierung mit strengerem Maßstab wäre angesichts dessen auch nicht mit den

senheitsbeschluss gemäß Artikel 45 der Verordnung (EU) 2016/679 vorliegt, in einem Drittstaat erfolgen und sofern die datenverarbeitende Stelle über eine Niederlassung im Inland verfügt.	erfolgen. ~~und sofern~~ D~~d~~ie datenverarbeitende Stelle oder ein mit ihr verbundenes Unternehmen muss über eine Niederlassung in der Europäischen Union ~~im Inland~~ verfüg~~t~~en.	grundrechtlich geschützten Rechten der Anbieter, Anwender und Leistungserbringer zu vereinen. Die DSGVO führt zu einer Vollharmonisierung. Nationales Recht darf nur in solchen Fäl- len zusätzliche oder abweichende Anforderungen regeln, in denen die DSGVO eine Öffnungsklausel enthält. Art. 49 Abs. 5 DSGVO käme als einzige belastbare Öffnungsklausel für § 393 SGB V in Betracht. Hiernach darf u.a. nationales Recht die Übermittlung von personenbezogenen Daten in Drittstaaten ohne Angemessenheitsbeschluss *„aus wichtigen Gründen des öffentlichen Interesses“* beschränken. Diese Voraussetzungen sind nicht erfüllt, da die Regelungen der DSGVO hinreichend sind, um die spezifischen Risiken des Cloud-Computings zu adressieren. Mittels der Instrumente des Art. 46 Abs. 2 DSGVO kann auch im Rahmen des Cloud-Betriebs ein hinreichendes Datenschutzniveau erreicht werden. II. Einfügen des Tatbestandsmerkmals: *„oder ein mit ihr verbundenes Unternehmen“* und *„in der Europäischen Union“.* Dem Schutzzweck ist Genüge getan, wenn ein mit der datenverarbeitenden Stelle verbundenes Unternehmen seinen Sitz im Inland oder der Europäische Union hat. Die Zugriffsmöglichkeiten auf dieses Unternehmen sind hinreichend gesichert. Aus Gründen der EU- Rechtskonformität ist der Sitz zudem auf die Europäische Union auszuweiten, da eine Eingrenzung auf das Inland mit den Grundfreiheiten des EU-

		Primärrechts unvereinbar ist und insofern zur Unanwendbarkeit der Regelung führte.
3) Eine Verarbeitung nach Absatz 1 ist nur zulässig, wenn zusätzlich zu den Anforderungen des Absatzes 2 1. nach dem Stand der Technik angemessene technische und organisatorische Maßnahmen zur Gewährleis- tung der Informationssicherheit ergriffen worden sind, 2. ein aktuelles C5-Testat der datenverarbeitenden Stelle im Hinblick auf die C5-Basiskriterien für die im Rah- men des Cloud-Computing-	(3) Eine Verarbeitung nach Absatz 1 ist nur zulässig, wenn zusätzlich zu den Anforderungen des Absatzes 2 1. weitere nach dem Stand der Technik angemessene technische und organisatorische Maßnahmen zur Ge- währleistung der Informationssicherheit ergriffen worden sind, 2. ein aktuelles C5-Testat der datenverarbeitenden Stelle im Hinblick auf die C5-Basiskriterien für die im Rah- men des Cloud-Computing-Dienstes eingesetzten Cloud-Systeme und die eingesetzte Technik vorliegt und 3. die im Prüfbericht des Testats enthaltenen,	Einfügen des Tatbestandsmerkmals: *„weitere“.* Begründung s.u. zu Absatz (9) neu.

Dienstes eingesetzten Cloud-Systeme und die eingesetzte Technik vorliegt und 3. die im Prüfbericht des Testats enthaltenen, korrespon- dierenden Kriterien für Kunden umgesetzt sind.	korrespon- dierenden Kriterien für Kunden umgesetzt sind.	
(5) Technische und organisatorische Maßnahmen gelten als angemessen im Sinne von Absatz 3 Nummer 1, wenn folgende Anforderungen erfüllt werden: 1. in der vertragsärztlichen und vertragszahnärztlichen Versorgung die Voraussetzungen des § 390,	(5) Weitere t~~T~~echnische und organisatorische Maßnahmen gelten als angemessen im Sinne von Absatz 3 Nummer 1, wenn folgende Anforderungen erfüllt werden: 1. in der vertragsärztlichen und vertragszahnärztlichen Versorgung die Voraussetzungen des § 390, 2. in zugelassenen Krankenhäusern die Voraussetzun- gen des § 391 und	Einfügen des Tatbestandsmerkmals: *„weitere“.* Begründung s.u. zu Absatz (9) neu.

2. in zugelassenen Krankenhäusern die Voraussetzungen des § 391 und 3. von Krankenkassen die Voraussetzungen des Branchenspezifischen Sicherheitsstandards für gesetzliche Kranken- und Pflegeversicherer (B3S-GKV/PV).	von Krankenkassen die Voraussetzungen des Branchenspe- zifischen Sicherheitsstandards für gesetzliche Kranken- und Pflegeversicherer (B3S-GKV/PV).	
	(9) Die Anforderungen der Absätze 2 bis 4 gelten insgesamt als geeignete technische und organisatorische Maßnahmen gemäß Artikel 32 der Verordnung (EU) 2016/679.	Einfügen eines neuen Absatzes (9). Klärungs- und regelungsbedürftig ist das Verhältnis zwischen § 393 SGB V und der DSGVO. Für eine rechtssichere Anwendung muss dies ausdrücklich geregelt werden. Aktuell werden zu diesem Thema im Markt unterschiedliche Rechtsauffassungen vertreten, was Anbietern die Entwicklung von Geschäftsmodellen und Kunden den Umstieg und die Investitionsentscheidung erschwert. Es ist daher eine gesetzgeberische Klarstellung geboten. U.a. wird in der aktuellen Diskussion die Auffassung vertreten, dass es sich bei § 393 SGB V um eine Regelung gem. Art. 9 Abs. 4 DSGVO handle. Das ist unzutreffend und entsprechend

		klarzustellen. Nach Art. 9 Abs. 4 DSGVO können Mitgliedstaaten „zusätzliche Be- dingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist“. Hierbei geht es um eine Konkretisierung und Einschränkung der Erlaubnisgrundlagen für die Verarbeitung von Gesundheitsdaten. Eine Erlaubnisgrundlage enthält § 393 SGB V nicht, er regelt zweckunabhängig, auf welche Art und Weise Gesundheitsdaten verarbeitet werden dürfen. Bleibt es bei der aktuellen Regelung, wird der Einsatz von Cloud-Computing-Diens- ten im Gesundheitswesen unnötig erschwert und das gesetzgeberische Ziel damit letztlich konterkariert. Sowohl Kunden (Anwender/Leistungserbringer) als auch Anbieter werden in ihrem strategischen und operativen Tun durch Rechtsunsicherheit gehemmt, was der Digitalisierung des Gesundheitswesens entgegenläuft und dieses ausbremst. Nicht zuletzt würde sich § 393 SGB V bei restriktiver Auslegung seiner aktuellen Fassung aus den o.g. Gründen als unionsrechtswidrig erweisen und wäre schon aus diesem Grund anzupassen. Jenseits der Regelungen zur Drittstaatenübermittlung im Rahmen der (denkbaren, aber anzupassenden) Öffnung des Art. 49 Abs. 5 DSGVO (s.o.) kann § 393 SGB V allenfalls als Ausgestaltung der nach Art. 32 DSGVO geforderten technischen und organisatorischen Maßnahmen angesehen werden, indem konkretisiert wird, was im konkreten Fall angemessen ist.

		Werden die hier vorgeschlagenen Änderungen umgesetzt – namentlich die Klarstellung der Begrifflichkeiten und die Rückführung der geographischen Anforderungen auf den Maßstab der Art. 44 ff. DSGVO –, lässt sich § 393 SGB V seinem verbleibenden Regelungsgehalt nach als Konkretisierung technisch-organisatorischer Maßnahmen gemäß Art. 32 DSGVO einordnen. Entsprechende Anpassungen erfolgen in Absatz 3 und Absatz. 5.

Patientendaten in der Cloud

Rechtskonforme Nutzung von Cloud-Infrastrukturen im deutschen Gesundheitswesen zur Verbesserung von Sicherheit und Leistungsfähigkeit

A. Die Notwendigkeit der Cloud-Nutzung im modernen Gesundheitswesen

Die fortschreitende Digitalisierung des Gesundheitswesens ist eine unumgängliche Voraussetzung, um die medizinische Versorgung in Deutschland zukunftsfähig, effizient und sicher zu gestalten. Gleichzeitig stellen europäische Regulierungen im Rahmen der EU-Digitalstrategie, wie der European Health Data Space, hohe Anforderungen an die Interoperabilität, die Sicherheit und den grenzüberschreitenden Austausch von Gesundheitsdaten. Im Zentrum dieser Transformation steht die Fähigkeit, sensible Gesundheitsdaten in modernen IT-Infrastrukturen zu verarbeiten, die leistungsfähig, hochverfügbar und gleichzeitig sicher sind. Die Migration von traditionellen, lokal betriebenen Rechenzentren der einzelnen Gesundheitseinrichten in die Cloud ist dabei nicht nur eine Frage der Effizienz oder Kostenoptimierung, sondern eine strategische Notwendigkeit, um die Qualität und die Sicherheit der Patientenversorgung nachhaltig zu verbessern. Insbesondere fordern neue KI-basierte Softwareanwendungen eine besonders leistungsfähige und interoperable Infrastruktur, die derzeit und künftig nur durch Cloud-Infrastrukturen bereitgestellt werden kann.

Die Integration von Cloud-Infrastrukturen bietet dabei gegenüber den traditionellen On-Premise-Strukturen der einzelnen Gesundheitseinrichtungen entscheidende – nicht replizierbare – Vorteile:

- **Erhöhte Datensicherheit und Resilienz:** Die Verarbeitung von Gesundheitsdaten in der Cloud verbessert die Datensicherheit und Resilienz im Vergleich zu On-Premise-Systemen. Dies umfasst nicht nur die physische Sicherheit der Rechenzentren insbesondere großer Anbieter, sondern auch professionelle Redundanzarchitekturen, Notfallwiederherstellungsprozesse und ein proaktives, globales Bedrohungsmanagement, das rund um die Uhr auf Cyber-Bedrohungen reagiert. Die Auslagerung in eine dezentrale Cloud-Umgebung minimiert Risiken wie Datenverlust durch Hardware-Ausfälle, Naturkatastrophen, lokale Sicherheitsvorfälle oder Cyberangriffe, deren Komplexität und Frequenz stetig zunehmen.
- **Höhere Versorgungssicherheit:** Die erhöhte Datensicherheit und Resilienz führt gleichzeitig auch zu einer Verbesserung der Versorgungssicherheit. Die Kontinuität der Patientenversorgung profitiert von der georedundanten Infrastruktur, die die Cloud bietet; insbesondere das "Klumpenrisiko" eines Totalausfalls durch lokale Ereignisse (z.B. Naturkatastrophen, Stromausfälle) wird umgangen und eine durchgehende Verfügbarkeit aller relevanten Daten für die Patientenversorgung sichergestellt.
- **Verbesserung der Behandlungsqualität und Patientensicherheit:** Eine stabile und hochverfügbare sowie interoperable IT-Infrastruktur ist die technologische Basis für eine vernetzte Versorgung und eine funktionierende digitale Patientenakte. Sie ermöglicht den sicheren und schnellen Zugriff auf

relevante Patienteninformationen für das gesamte interdisziplinäre Behandlungsteam, unabhängig von Ort und Zeit. Behandlungsfehler, die durch unvollständige oder nicht rechtzeitig verfügbare Informationen entstehen, können reduziert werden. Moderne Krankenhausinformationssysteme (KIS) werden künftig zunehmend "cloud-native" sein, d.h. sie sind (ggf. ausschließlich) für den Betrieb in der Cloud konzipiert. Veraltete Systeme, die lokal betrieben werden ("on-premise"), bieten oft keine modernen Schnittstellen, was den nahtlosen und sicheren Datenfluss zwischen verschiedenen Anwendungen und Abteilungen verhindert. Ein cloud-basiertes KIS ist die Voraussetzung für eine interoperable Plattform, die eine echte Effizienzsteigerung und bessere Behandlungsergebnisse ermöglicht.

- **Sektoren- und standortübergreifende Datenverfügbarkeit:** Insbesondere für überregional und international agierende Klinikträger oder Betreiber von MVZ ist eine zentrale Cloud-Infrastruktur essenziell, um eine konsistente und lückenlose Patientenversorgung über Standort- und Sektorengrenzen hinweg zu gewährleisten. So kann sichergestellt werden, dass die Behandlungshistorie eines Patienten, der beispielsweise von einem Krankenhaus in Hessen in eine Spezialklinik in Bayern verlegt wird, dem neuen Behandlungsteam sofort vollständig, ohne Medienbrüche und im bekannten System zur Verfügung steht. Ein einheitliches System führt dabei erfahrungsgemäß zu erheblichen Effizienzgewinnen und damit zu besseren Behandlungsergebnissen für die Patienten. Auch können auf diese Weise Kosten eingespart werden. Der Aufbau einer vergleichbaren standortübergreifenden Verfügbarkeit mit einzelnen, dezentralen On-Premise-Rechenzentren würde hingegen zu zahlreichen unsicheren Datensilos führen und den Datenaustausch – insbesondere über System- und Anwendungsgrenzen hinweg - erschweren und verlangsamen.

- **Ermöglichung von medizinischem Fortschritt und Innovation:** Moderne medizinische Anwendungen, etwa in der KI-gestützten Anamnese, Diagnostik und Behandlung, erfordern Rechen- und Speicherkapazitäten, die nur durch flexible und annähernd unbegrenzt skalierbare Cloud-Infrastrukturen wirtschaftlich und technisch realisierbar sind. Ein konkretes Beispiel sind Large Language Models (LLMs), die als Basis für eine neue Generation von medizinischen Anwendungen ("Foundation Models") dienen. Diese Modelle, die de facto in der notwendigen Qualität, Leistungsfähigkeit und Funktionalität derzeit nicht von europäischen Anbietern entwickelt und bereitgestellt werden und in der Regel von US-Anbietern stammen, ermöglichen enorme Effizienzgewinne und Qualitätsverbesserungen:

    - Automatisierte Anamnese und Dokumentation: KI-basierte Anwendungen können Patientengespräche in Echtzeit transkribieren und strukturieren. Dies entlastet das ärztliche und sonstige Personal von administrativem Aufwand und reduziert Dokumentationsfehler, setzt aber ein leistungsstarkes KI-Foundation Model voraus.

    - Intelligente Arztbriefschreibung: LLMs können aus vergleichsweise unstrukturierten Daten (z.B. Befunden, Notizen) automatisch kohärente und vollständige Arztbriefe erstellen, diese bei Bedarf

zusammenfassen oder für internationale Fachkollegen automatisiert übersetzen.

- Klinische Entscheidungsunterstützung: Leistungsfähige KI-Systeme können die gesamte Patientenakte analysieren und dem Behandlungsteam themenbezogene Zusammenfassungen oder Hinweise auf mögliche Risiken liefern. Die Nutzung solcher global entwickelten Technologien ist für den medizinischen Fortschritt essenziell.

- **Optimierung klinischer Arbeitsabläufe:** Nahezu alle Arbeitsabläufe im Krankenhaus, von der Patientenaufnahme, Anamnese, Behandlung, Visite über die OP-Planung bis zur Entlassung und Abrechnung, sind datenintensiv. Eine durchgängige Cloud-Infrastruktur ist die Voraussetzung, um diese Arbeitsabläufe medienbruchfrei und standortübergreifend zu digitalisieren. Ein Beispiel ist die Spracherkennung ("Voice-to-Text"), die an jedem Arbeitsplatz im Krankenhaus – vom Arztzimmer bis zum OP – verfügbar sein muss, um eine durchgängige und effiziente Dokumentation zu gewährleisten. Dies ist nur mit einer zentralen, skalierbaren Cloud-Plattform realisierbar, nicht mit isolierten On-Premise-Lösungen, insbesondere wenn die Dokumentation und der Zugriff auf Patientendaten standortübergreifend möglich sein soll, um eine bestmögliche Versorgung der Patienten zu gewährleisten.
- **Wirtschaftlichkeit und Kosteneffizienz:** Cloud-Infrastrukturen ermöglichen eine signifikante Steigerung der Kosteneffizienz. Anstatt hohe (Vorab-)Investitionen in eigene Hardware, Lizenzen und Rechenzentrumsimmobilien tätigen zu müssen (welche zudem regelmäßig erneuert und modernisiert werden müssen), ermöglicht der Wechsel zu einer Cloud-Infrastruktur ein Modell mit variablen, nutzungsabhängigen Betriebskosten. Dies schafft finanzielle Flexibilität und Planbarkeit. Zudem ermöglicht die Elastizität der Cloud, Ressourcen dynamisch an den tatsächlichen Bedarf anzupassen, sodass nicht dauerhaft teure Kapazitäten für seltene Lastspitzen vorgehalten werden müssen. Indirekte Kosten für Energie, Kühlung, Raumnutzung und physische Sicherheit werden ebenfalls an den Anbieter verlagert und sind im Nutzungspreis enthalten.

Für die Aufrechterhaltung einer zeitgemäßen, sicheren IT-Infrastruktur im Gesundheitswesen ist der Rückgriff auf Cloud-Technologie auch zunehmend eine Voraussetzung, um gesetzliche Anforderungen an Informationssicherheit und Resilienz (z. B. nach sektoralen Sicherheitsstandards wie etwa NIS2) angemessen und standortübergreifend erfüllen zu können. Vor diesem Hintergrund ist die Nutzung von Cloud-Infrastrukturen – jedenfalls in größeren Verbünden – praktisch häufig nur mit global agierenden Hyperscalern realisierbar, die die erforderliche Skalierung, geographische Verteilung und standardisierte Sicherheitsarchitekturen mit Verschlüsselung, rollenbasiertem Berechtigungsmanagement, Sicherheits-Monitoring und umfangreichen Zertifizierungen (etwa nach ISO 27001 und C5) zur Verfügung stellen können. Daneben ist der Rückgriff auf global agierende Hyperscaler Voraussetzung des Zugangs zu einem integrierten Ökosystem aus Infrastruktur und fortschrittlicher Software. Insbesondere die für die Innovation entscheidenden Foundation Models

(LLMs) werden fast ausschließlich von US-Anbietern entwickelt und sind tief in deren Cloud-Plattformen integriert. Eine Trennung von Infrastruktur (Cloud) und Anwendung (KI-Modell) ist praktisch nicht möglich, da die Modelle auf die spezifische, hochkomplexe Systemarchitektur des jeweiligen Anbieters angewiesen sind. Europäische oder deutsche Anbieter können zwar eine reine Cloud-Infrastruktur (IaaS) bereitstellen und tun dies auch vermehrt, bieten aber nicht dieses unverzichtbare Ökosystem aus Plattformdiensten und Software. Zudem mangelt es diesen Anwendungen an Leistungsfähigkeit. Während der Aufbau digitaler Souveränität ein wichtiges Ziel bleibt, ist die deutsche und europäische Gesundheitsversorgung für den Anschluss an den medizinischen Fortschritt auf absehbare Zeit auf die genannten Technologien von US-Anbietern angewiesen.

B. Rechtliche Herausforderungen

Die Regulierung im Gesundheitsdatensektor ist vielschichtig und komplex. Gesundheitsdaten unterliegen als „besondere Kategorien personenbezogener Daten" nach Art. 9 DSGVO sowie als durch § 203 StGB geschützte Privatgeheimnisse einem hohen Schutzniveau. Die rechtlichen Herausforderungen lassen sich im Wesentlichen in die folgenden Kernbereiche gliedern:

1. **Zuständigkeit verschiedener Behörden und landesspezifischer „Flickenteppich":** Die größte Hürde für die Implementierung bundesweit einheitlicher digitaler Versorgungsstrukturen ist die Rechtszersplitterung in Deutschland. Neben bundesweiten Regelungen haben die 16 Bundesländer in ihren jeweiligen Landeskrankenhausgesetzen einen "Flickenteppich" an unterschiedlichen, teils widersprüchlichen Anforderungen an die Verarbeitung von Patientendaten durch externe Dienstleister erlassen. Dies erhöht die Komplexität für bundesweit agierende Klinikträger erheblich und macht einen völlig einheitlichen Roll-Out innovativer Anwendungen wie der oben genannten praktisch unmöglich. So kann beispielsweise die Nutzung eines cloud-basierten KIS in Mecklenburg-Vorpommern unter der Bedingung der Pseudonymisierung erlaubt sein, während in Hessen strengere oder andere Anforderungen gelten. Diese Rechtsunsicherheit führt zu enormen Systemkosten, verhindert Innovation und verzögert die notwendige technologische Modernisierung teilweise um Jahre. Hinzu kommt ggf. eine unterschiedliche Verwaltungspraxis bei der Rechtsanwendung durch Aufsichts- und Datenschutzbehörden. Zwar spricht viel dafür, dass die bundesgesetzliche Regelung des § 393 SGB V aufgrund der Gesetzgebungskompetenz des Bundes eine Sperrwirkung entfaltet und damit landesrechtliche Regelungen insoweit verdrängt, aber es fehlt hierzu bislang an gefestigter Rechtsprechung sowie vor allem an einer einheitlichen aufsichtsbehördlichen Praxis.
2. **Internationale Datenübermittlungen (Kapitel V DSGVO):** Seit dem „Schrems II"-Urteil des Europäischen Gerichtshofs bestehen hohe Hürden für die Übermittlung personenbezogener Daten in Drittländer wie etwa die USA. Da die Bereitstellung der Cloud-Infrastruktur und der darauf laufenden Foundation Models in dem notwendigen Umfang und der notwendigen Sicherheit vor allem durch Hyperscaler möglich ist, die in der Regel größere Anbieter mit Hauptsitz in den USA sind, muss das Risiko von Zugriffen durch

ausländische Sicherheitsbehörden effektiv adressiert werden. Diese Herausforderung besteht selbst dann, wenn die Daten primär in Rechenzentren innerhalb der EU gespeichert werden, da theoretisch Zugriffsmöglichkeiten im Rahmen von Support- oder Wartungsvorgängen nicht gänzlich ausgeschlossen werden können.

3. **Sozialrechtliche Vorgaben (§ 393 SGB V):** Das Fünfte Sozialgesetzbuch (SGB V) stellt in § 393 SGB V spezifische Anforderungen an den Einsatz von Cloud-Diensten durch Leistungserbringer wie Krankenhäuser. Die Norm verlangt unter anderem, dass die Verarbeitung von Gesundheitsdaten grundsätzlich nur im Inland, in der EU/EWR oder in einem Drittstaat mit Angemessenheitsbeschluss der EU-Kommission erfolgen soll. Zudem soll die datenverarbeitende Stelle über eine Niederlassung im Inland verfügen und ein aktuelles C5-Testat des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für die genutzten Cloud-Systeme vorweisen. Die Unionsrechtskonformität dieser speziellen Vorgaben im Spannungsfeld zur DSGVO ist derzeit nicht geklärt.
4. **Strafrechtliche Schweigepflicht (§ 203 StGB):** Berufsgeheimnisträger wie Ärzte und das Klinikpersonal müssen sicherstellen, dass das Patientengeheimnis auch bei der Einschaltung externer Dienstleister gewahrt bleibt. Der Cloud-Anbieter und dessen Personal gelten als „mitwirkende Personen" im Sinne des § 203 Abs. 3 S. 2 StGB. Die Wahrung der strafrechtlichen Schweigepflicht setzt voraus, dass der Dienstleister vertraglich umfassend zur Geheimhaltung verpflichtet wird.

Diese komplexe juristische Gemengelage führt zu erheblicher Rechtsunsicherheit, die den digitalen Fortschritt im Gesundheitswesen hemmt. Sie ist jedoch aus unserer Sicht durch einen risikobasierten und verantwortungsvollen Ansatz beherrschbar, der ein hohes Datenschutzniveau und Datensicherheit in der Cloud-Umgebung gewährleistet. Notwendig ist dazu sicherlich, dass der Gesetzgeber die entscheidenden Normen, wie § 393 SGB V, klarstellend nachschärft.

C. Klarstellung im Gesetzgebungsverfahren

Die dargestellte Rechtsunsicherheit beruht weniger darauf, dass der Einsatz von Cloud-Infrastruktur im Gesundheitswesen nach geltendem Recht grundsätzlich unzulässig wäre, sondern darauf, dass der bestehende Rechtsrahmen die maßgeblichen Anforderungen nicht hinreichend klar und konsistent formuliert. Dies führt in der Praxis dazu, dass sowohl Aufsichtsbehörden als auch Marktakteure bei der Auslegung und Anwendung der einschlägigen Vorschriften erheblich divergieren und kein einheitliches Verständnis darüber besteht, unter welchen Voraussetzungen der Cloud-Einsatz rechtssicher möglich ist. In der Folge fehlt es an einem klaren regulatorischen Signal, dass der Einsatz moderner Cloud-Infrastrukturen – unter Einhaltung hoher datenschutzrechtlicher und sicherheitstechnischer Standards – nicht nur zulässig, sondern angesichts der dargestellten Vorteile für Versorgungssicherheit, Datenschutz und Innovation vielfach sogar geboten ist.

Der Gesetzgeber ist daher aufgerufen, diese Unsicherheiten im Wege einer gezielten Klarstellung zu beseitigen. Zentrale Stellschraube hierfür ist § 393 SGB

V, der derzeit die maßgeblichen sozialrechtlichen Anforderungen an den Einsatz von Cloud-Infrastrukturen im Gesundheitswesen vorgibt, jedoch in seiner aktuellen Fassung weder hinreichend klar noch konsistent mit den unionsrechtlichen Vorgaben der DSGVO ausgestaltet ist:

1. **Konsistente Regelungen zu internationalen Datentransfers**: Erforderlich ist insbesondere ein ausdrücklicher Gleichlauf der sozialrechtlichen Anforderungen mit den Regelungen zu internationalen Datentransfers nach Kapitel V DSGVO. Nur so kann sichergestellt werden, dass Leistungserbringer und Cloud-Anbieter nicht mit widersprüchlichen oder überlagernden Anforderungen konfrontiert werden und ein unionsrechtskonformes, zugleich praktikables Datenschutzniveau erreicht wird.

2. **Klarheit zu erforderlichen technischen und organisatorischen Schutzmaßnahmen**: Darüber hinaus bietet eine Neufassung des § 393 SGB V die Chance, die für den Einsatz von Cloud-Infrastrukturen im Gesundheitswesen maßgeblichen technischen und organisatorischen Schutzmaßnahmen abschließend und rechtssicher zu kodifizieren. Dies würde nicht nur die bestehende Rechtsunsicherheit beseitigen, sondern zugleich einen hohen, transparenten und überprüfbaren Standard für den Schutz sensibler Gesundheitsdaten festschreiben.

3. **Eine bundesweit einheitliche Regelung**: Schließlich bedarf es einer klaren gesetzlichen Aussage zur bundesweiten Geltung dieser Regelungen. Eine auf § 393 SGB V gestützte bundesrechtliche Klarstellung würde als Ausübung der konkurrierenden Gesetzgebungskompetenz des Bundes wirken und damit divergierende landesrechtliche Vorgaben verdrängen. Nur auf diesem Weg lassen sich einheitliche, standort- und sektorenübergreifende digitale Versorgungsstrukturen realisieren, ohne dass bundesweit tätige Klinikträger weiterhin mit einem regulatorischen Flickenteppich konfrontiert sind.