Sicherung und Stärkung der Wettbewerbsfähigkeit von eHealth-Unternehmen bei der KI-Forschung im Gesundheitswesen

Die eHealth-Branche, in der wir als CompuGroup Medical SE & Co. KGaA tätig sind, ist eine tragende Säule der Gesundheitsversorgung in Deutschland. Sie ist zugleich ein unverzichtbarer Motor für Innovationen im hiesigen Gesundheitswesen.

Um die Gesundheitsversorgung zu stärken und unsere Wettbewerbsfähigkeit zu sichern, beschränken wir uns nicht auf die Entwicklung und Bereitstellung digitaler Anwendungen für die medizinische Versorgung. Ein bereits heute wesentlicher Teil unserer Tätigkeit ist vielmehr die evidenzbasierte Nutzung von Gesundheitsdaten zur Unterstützung der medizinischen Forschung. KI und die sich hieraus ergebenden Möglichkeiten können die Bedeutung dieses Tätigkeitsfeldes noch erheblich steigern. Unsere existierenden Lösungen und Visionen bieten dabei große Potenziale für den Standort Deutschland: Sie können für dringend benötigte Kosteneffizienz im Gesundheitswesen sorgen, hochwertige Arbeitsplätze schaffen und Deutschlands Vorreiterrolle in der digitalen Medizin, klinischen Forschung und KI-Entwicklung ausbauen.

Unserer Ansicht nach gefährden die jüngeren regulatorischen Entwicklungen jedoch die vielfältigen Potenziale der evidenzbasierten Nutzung von Gesundheitsdaten. Unklare, überbordende datenschutzrechtliche Anforderungen sowie ungleiche Wettbewerbsbedingungen von e-Health Unternehmen im Vergleich zu staatlichen Institutionen schaffen erhebliche Hürden. Sie bremsen Innovationen, erschweren Investitionen und mindern somit Deutschlands internationale Wettbewerbsfähigkeit. Es ist dringend geboten, den regulatorischen Rahmen zukünftig so auszugestalten, dass die rechtssichere Entwicklung digitaler Lösungen für das Gesundheitswesen und der Betrieb medizinischer Forschung gefördert werden, jedenfalls aber möglich bleiben.

Daher haben wir die aus unserer Sicht drängendsten Maßnahmen identifiziert, um Deutschlands Vorreiterrolle in Innovation, medizinischer Forschung und digitaler Gesundheitsversorgung zu sichern und auszubauen. All dies ist möglich, ohne den Staatshaushalt finanziell zu belasten. Auch Patienteninteressen können durch die existierenden technischen Schutzmaßnahmen gewahrt werden.

Gerne stehen wir Ihnen und Ihrem Haus für vertiefende Gespräche und einen fachlichen Austausch zur Verfügung, um gemeinsam tragfähige, praxisorientierte Lösungen zu entwickeln.

Zusammenfassung unserer wesentlichen Anliegen und Vorschläge

- **Datenschutzrechtliche Legitimation der Nutzung von pseudonymen Gesundheitsdaten:** eHealth-Unternehmen müssen nicht nur anonymisierte, sondern auch pseudonymisierte Gesundheitsdaten rechtssicher und diskriminierungsfrei verarbeiten können, um deren volles Forschungspotenzial nutzbar zu machen. Sie benötigen insofern die gleichen Bedingungen wie staatliche Akteure. Hierfür müssen § 6 GDNG auf privatwirtschaftliche Unternehmen erweitert und in § 27 Abs. 3 BDSG Klarstellungen vorgenommen werden, dass für Forschungszwecke verwendete (Gesundheit-)Daten nicht zwingend anonymisiert werden müssen.
- **Datenschutzrechtliche Legitimation der Nutzung zu innovationsgetriebenen Zwecken:** Die Nutzung pseudonymisierter Gesundheitsdaten muss für Zwecke der Forschung (analog zum Forschungsdatenzentrum des BMG), der Produktentwicklung und des KI-Trainings datenschutzkonform möglich sein. Hierfür sind ebenfalls die bestehenden datenschutzrechtlichen Rechtsgrundlagen für die Verarbeitung von Gesundheitsdaten und für Forschungszwecke zu öffnen bzw. weiterzuentwickeln.
- **Vereinheitlichung des Verständnisses der Anonymisierung von Daten in der DSGVO:** Wie von der Bundesregierung in den Vorschlägen zur Vereinfachung der DSGVO vom 23. Oktober 2025 bereits festgestellt, sorgen die Unsicherheiten hinsichtlich der Anforderungen und Konsequenzen einer Anonymisierung im Sinne der DSGVO für massive Innovationshemmnisse auch für eHealth-Unternehmen. Daher sollten anonymisierte Informationen explizit vom Anwendungsbereich der DSGVO ausgeschlossen sowie eine Legaldefinition des Begriffs der Anonymisierung auf Grundlage des Urteils des Europäischen Gerichtshofs in Sachen C-413/23 P eingeführt werden.
- **Spezifische Anonymisierungsregeln für Gesundheitsdaten:** Um den Besonderheiten der Verarbeitung von Gesundheitsdaten Rechnung zu tragen, bedarf es spezifischer Anonymisierungsregeln für Gesundheitsdaten auf nationaler Ebene. Dies kann durch die Etablierung klarer Standards und die Möglichkeit zur Anerkennung der Anonymisierung durch eine Zertifizierung erfolgen. Damit würde sich Deutschland an erfolgreichen Modellen aus dem US-amerikanischen Health Insurance Portability and Accountability Act (**HIPAA**) orientieren. Dieses Gesetz schafft Rechtssicherheit für innovative Forschung, indem Zweifel an der Anwendbarkeit datenschutzrechtlicher Anforderungen bei gleichzeitiger Wahrung von Patienteninteressen ausgeschlossen werden.
- **Zentrale und innovationsfördernde Datenschutzaufsicht:** Die in Deutschland bestehende föderale Datenschutzaufsicht erschwert die Bedingungen für eHealth-Unternehmen. Wir sprechen uns daher für eine zentrale und innovationsfördernde Datenschutzaufsicht auf Bundesebene aus, die Rechtssicherheit im Bundesgebiet gewährleistet.

Kapitel 1: Verarbeitung pseudonymisierter Gesundheitsdaten als Grundlage für die Forschung und Entwicklung durch eHealth-Unternehmen

A. Bedeutung dezentraler, sicherer Datenplattformen für Deutschland

Dezentrale, sichere Datenplattformen ermöglichen fortschrittliche Forschung auf Basis realer und repräsentativer Versorgungsdaten. Diese Daten müssen für die Allgemeinheit – einschließlich Forschender aus Wissenschaft, Wirtschaft und dem öffentlichen Sektor – barrierefrei zugänglich sein.

B. Regulatorische Rahmenbedingungen und zentrale staatliche Dateninfrastrukturen als Innovationshemmnisse

Die EHDS-Regulierung und das GDNG betonen den gesellschaftlichen Mehrwert einer effizienten, datenschutzkonformen Weiterverwendung von Gesundheitsdaten für Forschungszwecke („Sekundärnutzung“). Es soll die wertebasierte Entwicklung von innovativen medizinischen Anwendungen ermöglicht werden, um die Qualität medizinischer Versorgung zu steigern und zugleich Effizienzsteigerungen im Gesundheitssektor zu bewirken. Wir teilen die Ansicht zahlreicher Stakeholder – darunter auch das BMG –, dass trotz dieser Regulierungsansätze fehlende Infrastrukturen, rechtliche Unsicherheiten, mangelnde Datenkompetenz wesentliche Hindernisse für die Erreichung dieser Ziele darstellen und es einer forschungsfreundlichen Kommunikationskultur bedarf.

Die derzeitige staatliche Reaktion auf diese anerkannten Hindernisse in Form des Aufbaus einer zentralen, von staatlichen Institutionen kontrollierten Dateninfrastruktur (insbesondere durch das Forschungsdatenzentrum) sowie die Schaffung regulatorischer Vorteile für staatliche Institutionen führen zu einer unangemessenen Benachteiligung privatwirtschaftlicher eHealth-Unternehmen.

Darüber hinaus sieht das GDNG bislang vornehmlich Rechtsgrundlagen für die Datenverarbeitung durch öffentlich-rechtliche Einrichtungen oder Gesundheitseinrichtungen wie Krankenhäuser vor. Privatwirtschaftliche eHealth-Unternehmen, die über die erforderliche sektorspezifische Datenkompetenz verfügen (z.B. im Bereich der unstrukturierten Daten), werden hingegen nicht adressiert. Damit bleibt die Zulässigkeit der Verarbeitung von Gesundheitsdaten durch eHealth-Unternehmen rechtlich unsicher und die vom Gesetzgeber angestrebten Ziele können nicht erreicht werden. Diese Situation führt zu Innovationshemmnissen und Beschränkungen in der Möglichkeit zur Neu- und Weiterentwicklung von Versorgungsmodellen – jeweils zum Nachteil des eHealth-Standortes Deutschland.

C. Unser Lösungsansatz: Ermöglichung der Nutzung pseudonymisierter Gesundheitsdaten für private eHealth-Unternehmen

Der nationale Gesetzgeber sollte § 6 GDNG für private eHealth-Unternehmen öffnen und parallel in § 27 Abs. 3 BDSG klarstellen, dass für Forschungszwecke verwendete (Gesundheit-)Daten nicht zwingend anonymisiert werden müssen, sondern eine Pseudonymisierung ausreicht.

Die Verfügbarkeit und Nutzbarkeit umfassender Gesundheitsdaten sind für den Erfolg der Entwicklung innovativer – KI-basierter – Versorgungsmodelle zum Wohle der Patienten entscheidend. Sie ermöglichen die Analyse vollständiger Behandlungspfade über verschiedene Leistungserbringer hinweg, sodass der gesamte medizinische Versorgungskontext in die Forschung, Produktentwicklung und das Modelltraining einfließen kann. Das GDNG erkennt diese Problematik ausdrücklich an und betont die wesentliche Bedeutung valider Datenbestände. Die Verarbeitung umfassender Gesundheitsdaten wird jedoch unmöglich, wenn Daten absolut anonymisiert werden müssen – also jede Form des Personenbezugs vollständig und unwiderruflich entfernt wird.

Die Nutzung und Weitergabe von Gesundheitsdaten für legitime Nutzungszwecke nach § 6 GDNG darf nicht allein öffentlichen Einrichtungen vorbehalten sein. Auch privat- und gemischtwirtschaftliche Institutionen müssen von den Privilegierungen profitieren können, damit Innovationen im Gesundheitswesen entstehen können. § 6 GDNG beschränkt die Nutzung und Weitergabe von Gesundheitsdaten hingegen auf Gesundheitseinrichtungen. Datenschutzaufsichtsbehörden leiten daraus überschießend ab, dass sich lediglich diese Einrichtungen auf die Rechtsgrundlage des § 27 BDSG berufen dürften – das GDNG also für eine Einschränkung der Möglichkeit zur Verarbeitung von Gesundheitsdaten anstatt der vom Gesetzgeber intendierten Erweiterung führt.

In der Folge können ausschließlich staatliche Institutionen Gesundheitsdaten verknüpfen und auswerten (etwa aus der elektronischen Patientenakte), während die Rahmenbedingungen für privatwirtschaftlich tätige eHealth-Unternehmen mit Einführung des GDNG unverändert geblieben sind oder nach Auffassung von Datenschutzbehörden sogar limitiert wurden. Dies stellt nicht nur einen eklatanten Widerspruch zur Intention des Gesetzgebers dar, sondern benachteiligt privatwirtschaftliche Akteure, schränkt deren Innovationsmöglichkeiten erheblich ein und behindert folglich die digitale Transformation des Gesundheitswesens.

D. Unsere weiteren Ansätze für mehr Innovationen im Gesundheitswesen

Über die Klarstellung der Möglichkeit zur Nutzung pseudonymisierter Gesundheitsdaten hinaus, kann durch weitere Gesetzesänderungen ein innovationsfreundliches Umfeld für eHealth-Unternehmen geschaffen werden.

1. Erweiterung der Rechtsgrundlage des § 27 Abs. 1 BDSG für innovationsgetriebene Zwecke

§ 27 Abs. 1 BDSG sollte als Rechtsgrundlage zur Datenverarbeitung zu Forschungszwecken auf nationaler Ebene erweitert werden, um das volle Forschungspotenzial der Nutzung von Gesundheitsdaten auszuschöpfen. Diese Erweiterung sollte explizit die Erhebung, Aufbereitung und Weiterverarbeitung von Daten für privatwirtschaftliche Forschung und Produktentwicklung sowie das KI-Training legitimieren. Zur Sicherstellung übergreifender datenschutzrechtlicher Prinzipien wie Zweckbindung, Richtigkeit sowie Integrität und Vertraulichkeit können Pflichten zur Validierung, Aktualisierung und Überwachung der Modelle nach dem Vorbild des Medizinproduktrechts eingeführt werden.

Weiterhin darf Forschung im Sinne des § 27 BDSG nicht ausschließlich auf Tätigkeiten nicht-kommerzieller Institute und rein akademische Tätigkeiten beschränkt sein. Eine technologieoffene und umfassende Auslegung des Forschungsbegriffs ist essenziell, um datenbasierte Innovationen von Unternehmen und Start-ups in Deutschland zu ermöglichen. Auch spezialisierte Dienstleister und Datenintermediäre sollten als Forschungseinrichtungen anerkannt werden können, etwa wenn sie Daten statistisch für klinische Studien aufbereiten („Data Science“).

2. Weitere flankierende Maßnahmen

Weiterhin haben wir folgende Vorschläge für eine Verbesserung der regulatorischen Rahmenbedingungen:

- **Ausgewogene Regeln zur Nutzung pseudonymisierter Daten:** Für die Verarbeitung pseudonymisierter Daten sollte die Erteilung einer allgemeinen Transparenzinformation über die möglichen Verarbeitungsformen ausreichen, ohne dass diese bereits im Zeitpunkt der Erhebung der Primärdaten im Einzelnen feststehen müssen, um eine innovationsgetriebene Nutzung der Daten zu ermöglichen. Parallel können bestimmte Fälle unzulässiger Nutzungen, ähnlich der verbotenen Praktiken nach der KI-VO, bestimmt werden (bspw. personalisiertes Marketing oder Risk-Scoring).
- **Opt-out-Mechanismus statt „Broad Consent“ als flankierende Maßnahme:** Die Möglichkeit zur Nutzung von technisch geschützten pseudonymisierten Patientendaten für dezentrale, privatwirtschaftliche

Forschungsinfrastrukturen sollte nur im Falle einer spezifischen Ausschlusserklärung des jeweiligen Patienten (sog. „Opt-out“) unzulässig sein, wie dies etwa im GDNG bzw. hinsichtlich der elektronischen Patientenakte vorgesehen ist. Die Vorsehung eines „Opt-Outs“ statt „Opt-Ins“ ermöglicht die Entwicklung diverser und innovativer Forschungsmodelle jenseits von staatlich kontrollierten Einzelinstitutionen. Die von der Bundesregierung in den Vorschlägen zur Vereinfachung der DSGVO vom 23. Oktober 2025 vorgesehen Möglichkeit der Einholung eines sog. „Broad Consent“ von Patienten und Studienteilnehmern für verschiedene, im Einzelnen noch nicht feststehende Forschungsformen und -vorhaben mag für klinische Studien zielführend sein, wird jedoch absehbar nicht die notwendige Datenbasis schaffen können um nachhaltige eHealth Innovationen oder KI-Entwicklung im Gesundheitsbereich zu ermöglichen, die mit denen aus dem US-amerikanischen oder asiatischen Markt mithalten können.

- **Praxisgerechte Regelung der datenschutzrechtlichen Betroffenenrechte bei KI-Training:** Die datenschutzrechtlichen Betroffenenrechte wie Widerspruch, Widerruf der Einwilligung, Auskunft und Löschung sollten für jene Gesundheitsdaten, die zur Entwicklung und zum Training von KI-Modellen eingesetzt wurden oder bereits Teil anonymisierter Forschungsergebnisse sind, gesetzlich klar definierte Einschränkungen erfahren. Eine nachträgliche Entfernung von Daten aus einem trainierten KI-Modell (sog. „Untraining“) ist technisch nicht realisierbar und würde Forschungs- sowie Innovationsvorhaben erheblich behindern.
- **Sicherstellung der Veröffentlichungspflicht für Gesundheitsdatennutzer nach der EHDS-Regulierung:** Um das bestehende Ungleichgewicht zwischen staatlichen Institutionen und privaten eHealth-Unternehmen nicht weiter zu vertiefen, muss die Pflicht zur fristgemäßen Veröffentlichung der Resultate oder Ergebnisse der Sekundärnutzung von Gesundheitsdatennutzern nach der EHDS-Regulierung unbedingt europarechtskonform ausgestaltet werden. Nur so ist sichergestellt, dass die auf dem ggf. umfassenderen Datenbestand gewonnenen Erkenntnisse gemeinnützig, einschließlich von privaten eHealth-Unternehmen, weiterverwendet werden können.

Es ist dabei hervorzuheben, dass diese Ansätze technische Sicherheitsmaßnahmen zur Förderung des Datenschutzes nicht ersetzen sollen – zu diesen zählen bspw. das „Salted Hashing“ von Pseudonymen, die Trennung von Identitäts- und Nutzdaten sowie In- und Output-Kontrollen für KI-Modelle. Es soll jedoch ein angemessener Interessenausgleich geschaffen werden, der sicherstellt, dass datenschutzrechtliche Vorgaben eingehalten werden können und zugleich Innovationen in der Gesundheitsforschung möglich bleiben.

Kapitel 2: Anonymisierung von Gesundheitsdaten – Investitionshebel und Ordnungsrahmen für Innovationen

A. Behinderung von Innovationen durch fehlende einheitliche Standards

Während in den USA nach HIPAA längst praxistaugliche und rechtssichere Standards zur Anonymisierung etabliert sind, fehlen in Deutschland und Europa klare Standards, die Planungs- und Rechtssicherheit schaffen. HIPAA trennt binär zwischen identifizierbaren Daten („identifiable data“) und nicht-identifizierbaren Daten („non-identifiable data“). In Deutschland und Europa wird hingegen zwischen direkt identifizierbaren, pseudonymisierten, relativ anonymisierten sowie absolut anonymisierten Daten unterschieden, wobei bisher nur im letztgenannten Falle (z.B. in Form von aggregierten Tabellen, mit entsprechend reduzierter und für den eHealth-Bereich unbrauchbarer Datenqualität) die strengen Regelungen der DSGVO rechtssicher nicht greifen.

Im amerikanischen Gesundheitsdatenschutz bestehen zwei Wege zur wirksamen, rechtssicheren Anonymisierung („De-Identification“): Entweder wird die allenfalls äußerst geringe Möglichkeit der Rückführbarkeit der Daten durch einen qualifizierten Statistiker bestätigt („Expert Determination“) oder es werden insgesamt 18 Datenpunkte nach einer einheitlichen Checkliste entfernt („Safe Harbor“). Sind diese Vorgaben erfüllt, gilt eine rechtliche Vermutungswirkung für die datenschutzkonforme Anonymisierung – Unternehmen können sich darauf verlassen, dass die Daten nicht mehr unter die im Übrigen durchaus strengen Regelungen von HIPAA fallen. Die Nutzbarkeit von Patientendaten zur Forschung und Entwicklung wird so rechtssicher ermöglicht.

Im Gegensatz dazu existieren unter der DSGVO keine vergleichbaren, behördlich anerkannte Vorgaben oder einheitliche Mindeststandards zur Anonymisierung. Zwar ist die jüngste Rechtsprechung des Gerichtshofs der Europäischen Union zur relativen Anonymisierung (C-413/23 P) aus unserer Sicht zu begrüßen, dennoch nehmen wir bereits jetzt Bedenken zum Umgang mit dem Urteil durch die Datenschutzaufsichtsbehörden wahr. Für eHealth-Unternehmen und Investoren im Gesundheitssektor führt all dies zu erheblicher Rechtsunsicherheit und hemmt die Transformation zu patientenzentrierten, datenbasierten Geschäftsmodellen.

B. Weitere Hürden durch eine zersplitterte deutsche und europäische Datenschutzpraxis

Die föderale Datenschutzaufsicht und die datenschutzrechtlichen Bestimmungen in den auf Landesebene erlassenen Landeskrankenhausgesetzen führen durch nicht prognostizierbare, einzelfallbezogene Entscheidungen und divergierende

Anforderungen zu einem Höchstmaß an Rechtsunsicherheit für die eHealth-Branche. Aufgrund der in der DSGVO vorgesehenen Möglichkeit für EU-Mitgliedstaaten, im Bereich der Forschung eigene Rechtsgrundlagen (mit divergierenden Anforderungen) zu statuieren, entsteht für eHealth-Unternehmen in Deutschland und Europa ein undurchsichtiger regulatorischer Flickenteppich. Dies wiederum verhindert die Vornahme von im internationalen Umfeld erforderlichen Investitionen.

C. Bestehende technische und organisatorische Lösungsansätze

Unternehmen können durch verschiedene technische und organisatorische Maßnahmen sicherstellen, dass Daten wirksam (relativ) anonymisiert sind – es also unter Berücksichtigung der jeweiligen Einzelfallumstände äußerst unwahrscheinlich ist, dass der Datenempfänger die Datenpunkte einer natürlichen Person zuordnen kann:

- Die konsequente Trennung von Systemen, Rollen, Zugriffsrechten und Identitätsmanagement verhindert, dass ein einzelner Akteur Zugriff auf alle relevanten Datenpunkte hat. Gerade bei Cloud-Migrationen medizinischer IT-Infrastrukturen hilft dieses Prinzip, werthaltige Datensätze zu schützen und zugleich Forschung zu ermöglichen.
- Die Verwaltung und Pseudonymisierung von Patientendaten durch einen unabhängigen externen Treuhänder oder ein dezentral gespeicherter Schlüssel zur ID-Generierung können ebenfalls verhindern, dass ein einzelner Akteur über Zugriff auf alle relevanten Datenpunkte verfügt. Indirekte Identifikatoren können hierbei zusätzlich maskiert oder generalisiert werden. Durch diese Maßnahmen ist es möglich, Datenprofile verschiedener Leistungserbringer sicher und datenschutzkonform zusammenzuführen, ohne eine Re-Identifikation zuzulassen.

Praxisbeispiel: Unsere Lösung „CGM LIFE“ enthält ein Identitätsmanagement mit einer patientenzentrierten Verschlüsselung von Patientendaten, wobei die Schlüssel dezentral gespeichert werden. Für den Betreiber der Anwendung besteht damit keine Möglichkeit auf den Schlüssel zuzugreifen und die Daten der Patienten ggf. bestimmten Personen zuordnen zu können. Hierdurch werden Datenschutz, Verschlüsselung und Datenhoheit bei gleichzeitiger Analysefähigkeit der (relativ) anonymisierten Daten gewährleistet. Dennoch haben Datenschutzaufsichtsbehörden entsprechende Ansätze, soweit uns bekannt, bis zuletzt als reine Pseudonymisierung der Daten bewertet oder keine eindeutigen Aussagen getroffen. Auf Basis der bisherigen Rechtslage und der Praxis der Datenschutzbehörden ist die Nutzbarkeit der Daten für Sekundärzwecke erheblich eingeschränkt, obwohl die getroffene Maßnahme einen hinreichenden Schutz für die Daten bieten.

D. Unser Ansatz: Normierung notwendiger Klarstellungen im Datenschutzrecht

Entsprechend den Vorschlägen der Bundesregierung für die Vereinfachung der DSGVO sollten im Gesetzestext Rechtssicherheit schaffende Ergänzungen vorgenommen werden, unter welchen Voraussetzungen personenbezogene Daten als wirksam anonymisiert gelten. Die von der Bundesregierung vorgebrachten Ansätze, anonymisierte Informationen explizit vom Anwendungsbereich der DSGVO auszuschließen sowie eine Legaldefinition des Begriffs der Anonymisierung auf Grundlage des EuGH-Urteils in Sachen C-413/23 P einzuführen, erscheinen uns dabei begrüßenswert und sachgerecht.

Ferner sprechen wir uns für eine Klarstellung aus, dass die Anonymisierung personenbezogener Daten keine Verarbeitung im Sinne der DSGVO darstellt. Die Position der Bundesregierung in den Vereinfachungsvorschlägen zur DSGVO scheint hierzu noch unklar zu sein. Weder Wortlaut, Systematik noch Sinn und Zweck der DSGVO verlangen eine Auslegung, die den Begriff der Verarbeitung auf die Anonymisierung von Daten – also die Entfernung von identifizierenden Merkmalen – erstreckt. Ansonsten wäre jedenfalls klarzustellen, dass bei einer zulässigen Zweckänderung erhobener Daten – einschließlich besonders sensibler personenbezogener Daten wie Gesundheitsdaten – weiterhin die die Datenerhebung rechtfertigende Rechtsgrundlage gilt und eine vollständige und dauerhafte Anonymisierung stets als datenschutzkonform und gerechtfertigt einzustufen ist, unabhängig vom ursprünglichen Zweck der Datenerhebung. Ziel der Anonymisierung ist die Aufhebung des Personenbezugs, wodurch die in der DSGVO verankerten Prinzipien der Datenminimierung und Speicherbegrenzung zum Schutz der Privatsphäre umgesetzt werden. Die Anonymisierung stellt daher eine legitime Zweckänderung dar, sodass eine Einzelfallprüfung der Kompatibilität nicht erforderlich ist.

Unabhängig von den im Einzelnen nicht vorhersehbaren europäischen Entwicklungen besteht für den nationalen Gesetzgeber die Möglichkeit, national einheitlich geltende, sektorspezifische und praxistauglicher Standards zur Gesundheitsdatennutzung und Anonymisierung zu etablieren. Dies halten wir für unerlässlich, um kurzfristig Rechtssicherheit zu schaffen. Nach dem Vorbild des HIPAA kann dies durch Anforderungskataloge zu Aggregatsgrößen, Schwellenwerten und technischen Maßnahmen oder die Möglichkeit zur Vornahme von Zertifizierungen sichergestellt werden. Nur so lässt sich ein „level playing field“ für Forschung, KI-Modelltraining und den Betrieb datenbasierter Geschäftsmodelle schaffen.

Weiterhin sollten datenschutzrechtliche Anforderungen an die Verarbeitung und Nutzung von Gesundheitsdaten auf EU-Ebene, zumindest aber auf Bundesebene einheitlich geregelt und aus den Landeskrankenhausgesetzen entfernt werden. Denn Forschung und Entwicklung im eHealth-Bereich sind nicht auf den föderalen Einzugsbereich beschränkt, sondern erfolgen mit dem Ziel eines internationalen, jedenfalls aber EU- und bundesweiten, Markteintritts entwickelter Produktinnovationen.

Kapitel 3: Zentrale und innovationsfördernde Datenschutzaufsicht

Wir sprechen uns für die Einrichtung einer zentralen Datenschutzaufsichtsbehörde auf Bundesebene aus. Dies kann die wirtschaftliche Entwicklung gefährdende divergierende Interpretationen auf Landesebene beseitigen. Es muss dabei das Ziel sein, klare, einheitliche und praxisnahe Leitlinien zu etablieren, welche die besonderen Anforderungen datengetriebener Innovationen im Gesundheitswesen berücksichtigen. Die Ausrichtung einer solchen Datenschutzaufsichtsbehörde auf Bundesebene sollte sich an den bewährten, lösungsorientierten Prinzipien der Datenschutzaufsichtsbehörden aus Bayern und Baden-Württemberg orientieren. So können Rechtssicherheit, Planbarkeit und Wettbewerbsfähigkeit im gesamten Bundesgebiet gewährleistet werden.

Auf europäischer Ebene sollte ein verbindlicher Mechanismus geschaffen werden, der – über die bisherige, weitgehend konsultative Rolle des Europäischen Datenschutzausschusses als Diskussionsforum der nationalen Datenschutzbehörden auf europäischer Ebene hinausgehend – konkrete, zeitnah anwendbare und innovationsfördernde Leitlinien für das Datenschutzrecht im eHealth-Bereich entwickelt. Dies ist unerlässlich, um die Wettbewerbsfähigkeit des europäischen Standorts im Bereich digitaler Gesundheit nachhaltig zu sichern, innovative Versorgungsmodelle europaweit zu ermöglichen und diese auch global vertreiben zu können.

****