

# Hintergrundinformation

## Datenverarbeitung und Landeskrankenhausgesetze: Position Medtronic GmbH

Moderne, digitale Medizintechnik geht mit Datenverarbeitung einher. Medizinprodukte können heute zum Beispiel auf der Grundlage von Bilddaten individuell angepasst werden, Künstliche Intelligenz unterstützt während einer Operation oder Expert:innen werden telemedizinisch zugeschaltet. Findet dies im Rahmen einer Behandlung im Krankenhaus statt, unterliegt die Datenverarbeitung dem jeweiligen Landeskrankenhausgesetz - zusätzlich zu den ohnehin geltenden Bundesgesetzen (insbesondere Bundesdatenschutzgesetz und sozialgesetzliche Regelungen), der Datenschutzgrundverordnung der EU (DSGVO<sup>1</sup>) und dem jeweils anwendbaren Landesdatenschutzgesetz. Die meisten Landeskrankenhausgesetze regeln die Datenverarbeitung im Rahmen der Patientenbehandlung auf ihre jeweils eigene Art, nur wenige verweisen ausschließlich auf die Regelungen der DSGVO und der Bundesgesetze. In dieser heterogenen Landschaft muss jeder Vertrag eines Krankenhauses zur externen Datenverarbeitung (sogenannter Auftragsverarbeitungsvertrag) spezifisch geprüft und ggf. angepasst werden, unter Umständen auch in Bezug auf das jeweilige Kirchendatenschutzrecht und die verschiedenen Interpretationen der lokalen Aufsichtsbehörden und krankenhausinternen Datenschutzbeauftragten. Dies bedeutet für alle Beteiligten einen erheblichen bürokratischen Aufwand, Prozesse werden verlangsamt oder kommen der Versorgung gar nicht erst zugute.

Wir setzen uns daher für eine Vereinheitlichung der Regelungen ein, um den zeitlichen und personellen Aufwand für die Implementierung solcher Prozeduren sowohl bei den Krankenhäusern als auch bei Medizinprodukteherstellern oder Forschungspartnern zu verringern.

### Beispiele für Datenverarbeitung in digital unterstützten Prozeduren

#### **Digital Twin-Technologien: Digitale Simulation statt „Trial and Error“**

Digital Twins<sup>2</sup> kommen dann zum Einsatz, wenn anhand von vorhandenem Bildmaterial bevorstehende Eingriffe simuliert werden. Die Programme wurden mit entsprechendem Material trainiert und können für bevorstehende Fälle vor dem Eingriff errechnen, was mit den verschiedenen Optionen passieren würde. So sind Operateure vor dem Eingriff auf diesen konkreten Fall vorbereitet bzw. das richtige Material (z. B. Implantat) kann personalisiert ausgewählt werden. Software, mit der solche Berechnungen vorgenommen werden, sind Medizinprodukte oder Teil eines Medizinproduktes, denn sie unterstützen bei der Entscheidung für medizinische Handlungen. Sie unterliegen damit den medizinproduktespezifischen Regularien (MDR<sup>3</sup>, MPBetreibV<sup>4</sup>, ggf.

<sup>1</sup> <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679>

<sup>2</sup> <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-digital-twin-technology>

<sup>3</sup> <https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng>

<sup>4</sup> <https://www.buzer.de/MPBetreibV.htm>

AI Act<sup>5</sup>,...), die vor allem der Patientensicherheit dienen. Deswegen werden diese Programme besonders gesichert, dürfen nur von geschultem Personal bedient werden und werden stets an die neuesten Erkenntnisse angepasst. Die Verarbeitung der Simulation etwa als 3-D-Modell des Herzens ist aufwändig und stellt unter Umständen auch besondere Anforderungen an die Monitore, auf denen sie dargestellt werden.

Daher werden solche Programme oft so konstruiert, dass die Daten zum Algorithmus kommen. Die Simulation erfolgt beim Anbieter des Programms auf seinen Servern oder in seiner Cloud unter seinen sicheren IT-Bedingungen. Dafür müssen die notwendigen Daten des aktuellen Falles in das Programm übertragen werden. Verarbeitet wird nur die notwendige Information, etwa aus CT-Aufnahmen, um den digitalen Zwilling zu simulieren.

Bei den notwendigen Daten handelt es sich meistens um digitale Bilddaten. Namen, Geburtstag, Wohnort etc. werden vorher entfernt, so dass dort, wo mit diesen Daten simuliert wird, seitens der Anbieter keine Rückschlüsse auf die Person gezogen werden können (jedenfalls nicht ohne ergänzende Informationen und eine gewisse kriminelle Energie).

Medtronic bietet hier unter anderem folgende Produkte an:

[Harmony<sup>TM</sup>](#)<sup>6</sup> TPV, für Patientinnen und Patienten mit angeborenem Herzfehler.

Menschen mit angeborenen Herzfehlern können von einer individuellen Planung vor dem Eingriff profitieren, um eine optimale Klappenplatzierung zu unterstützen. Medtronic unterstützt bei der Dimensionierung der Klappe und Planung des Eingriffs durch die Verarbeitung von CT-Scans, die von medizinischem Fachpersonal zur Verfügung gestellt werden, um den Eingriff im Voraus zu planen. Krankenhäuser teilen pseudonymisierte CT-Scans mit Medtronic, das die Analyse mit einer speziellen Software und einem internen Bildgebungsteam durchführt, um einen Größenbericht zu erstellen.

[Smart Plan Pro Endoleak Risk Assessment](#)<sup>7</sup>: Präoperative Vorhersage zum Verhalten des Stentgraft mit Hilfe der Digital-Twin-Technologie

Stents stützen Blutgefäße, die nicht mehr stabil sind, und verhindern so ihren Riss – hier bei der Bauchaorta. Dieses Gefäß ist relativ groß und sehr individuell in der jeweiligen Anatomie. Sind Stent und Anatomie der Aorta nicht optimal aufeinander abgestimmt, droht ein sogenanntes Endoleak, also ein Leck, bei dem Blut außerhalb des Stentgrafts aber innerhalb des Aneurysmasacks fließt, nachdem ein Aneurysma behandelt wurde. Dies kann zu einem erneuten Wachstum des Aneurysmas führen und potenziell lebensbedrohlich sein, wenn es nicht behandelt wird. Anhand von prä-operativem Bildmaterial (CT) kann eine solche Operation geplant und das Verhalten und ihre Abdichtung verschieden großer Stents im Voraus simuliert werden.

---

<sup>5</sup> <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32024R1689>

<sup>6</sup> <https://www.medtronic.com/en-us/healthcare-professionals/products/cardiovascular/heart-valves/transcatheter-valves/harmony-transcatheter-pulmonary-valve.html>

<sup>7</sup> <https://europe.medtronic.com/xd-en/e/emea/cardiovascular/aortic-plus/smartplan.html#:~:text=With%20digital-twin%20technology%20we%20are%20now%20able%20to,you%20in%20the%20treatment%20decisions%20for%20your%20patients.>

## **Telemedizin bei Operationen**

Unter Telemedizin<sup>8</sup> wird jede Art von medizinischer Handlung verstanden, bei der die beteiligten Akteure nicht vor Ort zusammen sind, sondern sich technischer Hilfsmittel bedienen, um Patientinnen und Patienten zu versorgen. Rund um minimalinvasive Operationen, bei denen ohnehin Bildmaterial aus dem Körperinneren entsteht, bietet sich die Nutzung dieses Materials auch für weitere Zwecke des Krankenhauses an. Aber auch der Remote-Einsatz von Personal, das nicht vor Ort ist, bietet in Zukunft interessante Aspekte, um die Fachkräfte gezielt einsetzen zu können.

### Nutzung von Bildmaterial bei minimalinvasiven Eingriffen

Bei minimalinvasiven Operationen wird neben den Instrumenten auch eine Kamera in den Operationsbereich eingeführt, um die Instrumente im Körperinneren bedienen zu können. Das hierbei entstehende Bildmaterial kann in einer Bilddatenbank organisiert und archiviert werden, um künftige Eingriffe besser vorzubereiten und für Aus-, Fort- und Weiterbildung zu nutzen. Eine sinnvoll angelegte Datenbank, die schnellen Zugriff auf das gewünschte Material bietet, entsteht nicht von allein. Daher helfen spezielle Lösungen und künstliche Intelligenz beim Erstellen einer krankenhausindividuellen Datenbank.

TouchSurgery<sup>9</sup> ist eine KI- und cloud-basierte Videobibliothek, die mithilfe von Algorithmen chirurgische Prozeduren in die Hauptphasen aufteilt und so eine strukturierte Datenbank aufbaut. Die Cloud macht es möglich, dass Ärzt:innen ihre Videos jederzeit und überall zur Durchsicht und Ausbildungszwecken aufrufen können. Durch die Verschlagwortung der Videos wird die ärztliche Arbeitszeit verringert. Mithilfe von Lernkurven können Ärzt:innen ihren Fortschritt in der Ausbildung überblicken.

### Telechirurgische Eingriffe/Livestream zur Remote-Beteiligung von Expert:innen

Operateur:in und Patient:in sind während der OP nicht im gleichen Raum – das ist derzeit noch Zukunftsmusik in der Versorgung. Vor allem fehlt es an Übertragungstechnik für die Signale mit so wenig Verzögerung, dass ein solches Vorgehen im Alltag sinnvoll ist. Möglich kann das mit neuen Übertragungstechniken wie 6G aber bald werden und robotische Assistenzsysteme im OP-Saal stellen die dafür notwendige Technik schon heute bereit. Bereits heute können Spezialist:innen zur laufenden OP zugeschaltet werden und aufgrund der Bilder beraten, wenn auch nicht selbst operieren.

Wenn Bilder aus dem OP übertragen werden, sind in der Regel Übertragungssysteme beteiligt, die nicht komplett in der Hoheit der beteiligten Krankenhäuser liegen.

HUGO RAS<sup>10</sup>: Das robotische Assistenz-System HUGO wird für minimalinvasive Operationen im Bauchraum eingesetzt. Zusammen mit TouchSurgery kann ein umfassendes digitales System entstehen.

---

<sup>8</sup> <https://www.bundesgesundheitsministerium.de/service/begriffe-von-a-z/t/telemedizin/>

<sup>9</sup> <https://www.medtronic.com/en-us/healthcare-professionals/specialties/touch-surgery.html>

<sup>10</sup> <https://www.medtronic.com/en-us/healthcare-professionals/specialties/surgical-robotics/robotic-assisted-surgery.html>

## Problemlagen der Datenverarbeitung beim spezialisierten Dienstleister

Als Papierakten noch alle Daten für die Behandlung im Krankenhaus enthielten, verließen diese Akten das Krankenhaus in der Regel nicht. In einer digitalen Welt ist es jedoch oft sinnvoll, dass die Daten zum Programm geschickt werden, während die Patient:innen vor Ort von externer Expertise profitieren können. Es liegt auch im Interesse eines Krankenhauses, solche externen Services zu nutzen und nicht für ihren Betrieb und ihre Wartung operativ verantwortlich zu sein. Werden Patientendaten zur Anwendung übertragen, sind dafür sichere Bedingungen erforderlich. Nur notwendige Daten sollen übertragen werden und die Patientendaten sollen dem Schutz der DSGVO und allen weiteren bundes- und europaweit geltenden Gesetze unterliegen.

Krankenhäuser und Medizinproduktehersteller stehen angesichts der Landeskrankenhausgesetze der Bundesländer, ihrer Aufsichtsbehörden und den Datenschützern der Krankenhäuser immer wieder vor unterschiedlichen Verfahren, Interpretationen und Auslegungen. Vor jedem Vertragsabschluss müssen daher Verträge, Einwilligungserklärungen und Prozesse diskutiert und angepasst werden. Manche Krankenhäuser müssen zusätzliche Schritte der Datenverarbeitung vornehmen oder das Einwilligungsmanagement anpassen, während es bei anderen Häusern als nicht erforderlich eingeschätzt wird.

Sowohl die Krankenhäuser als auch die Hersteller würden daher von bundesweit einheitlichen Regelungen profitieren. Denn es geht im Wesentlichen immer wieder um die gleichen Fragen:

1. Welche Daten sind personenbezogene Daten?

Wann gelten Daten als personenbezogen? Ist eine CT-Aufnahme ohne direkt personenbezogene Merkmale wie Name und Geburtstag rückverfolgbar? Wie verhält es sich, wenn der Ort der Behandlung bekannt ist? Welche Verarbeitungsschritte muss das Krankenhaus etwa intern mit einer Bilddatei vor dem Versand unternehmen und ist diese Verarbeitung im Rahmen der Behandlung zulässig?

2. Ist eine spezifische Einwilligung in die Verarbeitung der Daten erforderlich?

Die Verarbeitung von Daten auf der Grundlage einer Einwilligung ist grundsätzlich immer möglich. Dies setzt jedoch eine aussagekräftige Einwilligungserklärung, eine patientenindividuelle Aufklärung und die entsprechende Dokumentation voraus. Werden Daten zur Behandlung eines Patienten/einer Patientin außerhalb des Krankenhauses ohne einen anderen Zweck verarbeitet, sollten die Rechtsgrundlagen so gestaltet sein, dass keine Einwilligung erforderlich ist.

3. Ist ein unberechtigter Zugriff auf personenbezogene Daten möglich?

Die bestehenden Datenschutzgesetze sollen ungerechtfertigten Zugriff auf personenbezogene Daten verhindern. Die Interpretation, wann ein solcher Zugriff ausgeschlossen ist, variiert. Ist der Zugriff von Technik-Teams von außerhalb Europas möglich? Wann sind verschlüsselte Daten wirklich verschlüsselt?

## Lösungsansätze:

DSGVO und Bundesgesetze sind ohnehin die Grundlage für die Nutzung von Gesundheitsdaten im Zusammenhang mit dem Behandlungsauftrag oder für weitere Zwecke wie das Training einer KI. Derzeit schränken die Landeskrankenhausgesetze die rechtlichen Grundlagen teilweise weiter ein oder verbinden sie mit eigenen Anforderungen an die Verfahren, was den bürokratischen Aufwand erhöht. So führen unterschiedliche Rechtsgrundlagen und Interpretationen letztendlich auch zu Unterschieden in der Versorgung: Wo die Regeln sehr eng sind oder sehr weitgehend interpretiert werden, kommen manche Angebote vielleicht nicht zum Einsatz. Daher schlagen wir vor:

- **DSGVO und Bundesgesetze<sup>11</sup> bieten einen umfassend ausformulierten Rechtsschutz für personenbezogene Daten.** Daher sollten Landeskrankenhausgesetze nur darauf verweisen, dass die entsprechenden Gesetze einzuhalten sind: „Patientendaten dürfen verarbeitet werden, soweit und wie dies durch eine Rechtsvorschrift zugelassen ist.“
- **Die Aufsichtsbehörden der Länder sollten sich in ihren Gremien so untereinander abstimmen, dass die Interpretation der DSGVO und der Bundesgesetze in allen Bundesländern gleichartig erfolgt.** Ähnlich dem Europäischen Datenschutzausschuss auf EU-Ebene sollte idealerweise eine zentrale Stelle bei Interpretationsfragen zuständig und mit entsprechenden Befugnissen ausgestattet sein, um eine bundeseinheitliche Auslegung sicherzustellen.
- **Eine vorliegende datenschutzrechtliche Freigabe aus einem Bundesland sollte in allen anderen Bundesländern anerkannt werden und keine weitere Prüfung erfordern.**

Im Folgenden stellen wir die jeweiligen Rechtsgrundlagen kurz vor, um den Handlungsbedarf in den verschiedenen Bundesländern darzustellen.

## Europäische und bundesweite Rechtsgrundlagen

In Europa gilt die Datenschutzgrundverordnung ([DSGVO](#)<sup>12</sup>), die den Datenschutz, die Persönlichkeitsrechte und Verfahren, damit umzugehen, regelt. Die europaweit geltende Regelung ergänzen nationale Gesetze, hierzulande das Bundesdatenschutzgesetz ([BDSG](#)<sup>13</sup>) sowie weitere bereichsspezifische Gesetze. Jedes Gesetz und jede Verordnung wird in der konkreten Anwendung durch die zuständigen Behörden und Datenschutzbeauftragten unterschiedlich gehandhabt. Außerdem gelten die sozialgesetzlichen Regelungen (§ 393 SGB V und SGB X). Neben diesen europaweit und bundesweit geltenden Regeln unterliegen Daten aus Krankenhäusern aber auch landesspezifischen Regelungen in den einzelnen Bundesländern.

---

<sup>11</sup> <https://www.buzer.de/BDSG.htm>, [SGB X Zehntes Buch Sozialgesetzbuch \(SGB X\) Sozialverwaltungsverfahren und Sozialdatenschutz](#) und weitere

<sup>12</sup> <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679>

<sup>13</sup> <https://www.buzer.de/BDSG.htm>

## Landesspezifische Rechtsgrundlagen

Die rechtliche Ausgestaltung und Organisation von Krankenhäusern sind Länderaufgabe. Länder planen die Krankenhauslandschaft und regeln, zumeist im Landeskrankenhausgesetz, die Aufgaben und Pflichten der Krankenhäuser und der stationären Versorgung. Viele Landeskrankenhausgesetze beinhalten spezielle Regeln, die den Umgang mit Patientendaten und den Verfahren dazu beschreiben. Dabei gehen die Regelungen teilweise über DSGVO und BDSG hinaus und beschreiben spezifische Abläufe, die im oder vom Krankenhaus einzuhalten sind. Bei der nachfolgenden Betrachtung landesspezifischer Regelungen gehen wir auf folgende Aspekte ein:

- Auftragsverarbeitung,
- Verarbeitung von Daten in Drittländern,
- spezielle Einschränkungen der Datennutzung personenbezogener Patientendaten im Hinblick auf die oben beschriebenen Zwecke.

## Baden-Württemberg

Das Landeskrankenhausgesetz Baden-Württemberg ([LKHG BW](#)) benennt das Thema des Datenschutzes, verweist zu den meisten Themen auf die jeweils geltenden Vorschriften (DSGVO und Bundesgesetze) und ist damit sehr schlank gehalten. Gemäß [§ 45 LKHG BW](#) dürfen Patientendaten unter anderem zur Versorgung, Qualitätssicherung und Aus-, Fort- und Weiterbildung verarbeitet werden, soweit diese Zwecke nicht mit anonymisierten Daten erreicht werden können und nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

Patientendaten dürfen unter anderem für die Versorgung an Personen und Stellen außerhalb des Krankenhauses übermittelt oder zugänglich gemacht werden, soweit dies nicht mit anonymisierten Daten geht und keine schutzwürdigen Interessen der Betroffenen entgegenstehen.

## Bayern

Das Bayerische Krankenhausgesetz ([BayKrG](#)) enthält ausdrückliche Regelungen zur Auftragsverarbeitung, diese gehen jedoch nicht über die DSGVO hinaus. [Artikel 27 BayKrG](#) regelt den Datenschutz. Sofern danach keine Einwilligung des Patienten/der Patientin vorliegt, ist die Erhebung und Aufbewahrung von Patientendaten nur erlaubt, soweit dies die zur Erfüllung der Aufgaben des Krankenhauses oder im Rahmen des krankenhausärztlichen Behandlungsverhältnisses erforderlich ist. Zudem enthält der Artikel weitere Besonderheiten bezüglich der zulässigen Datenverarbeitung, etwa dass Auskünfte von Ärzt:innen vermittelt werden sollen, soweit das mit Rücksicht auf den Gesundheitszustand geboten ist. Das Krankenhaus kann sich zur Verarbeitung anderer Stellen bedienen, die die gleichen Schutzmaßnahmen wie das Krankenhaus einhalten müssen. Es wird auf die Maßnahmen der DSGVO verwiesen, die einzuhalten sind.

## Berlin

Das Berliner Landeskrankenhausgesetz ([LKG](#)) hatte bis 2022 die restriktivsten Regelungen und auch nach den Änderungen noch sehr spezifische. Die Verarbeitung von Gesundheitsdaten wird auf die geltenden Rechtsgrundlagen (DSGVO, BDSG, Berliner Datenschutzgesetz ([BInDSG](#)) und LKG begrenzt. Bei der Verarbeitung von Gesundheitsdaten werden die bestehenden Regeln im [§ 24 LKG](#) konkretisiert: Gesundheitsdaten dürfen in Krankenhäusern nur für bestimmte definierte Zwecke

verarbeitet werden. Sollte die Datenverarbeitung zu Behandlungs- oder Qualitätssicherungszwecken erfolgen, ist dies nur zulässig, soweit diese Zwecke nicht mit anonymisierten oder pseudonymisierten Daten erreicht werden können und keine überwiegenden schutzwürdigen Interessen der Betroffenen entgegenstehen. Andere Auftragnehmer werden an ergänzende Bedingungen gebunden, insbesondere hinsichtlich der Datenübermittlung ins Ausland und Anzeigepflichten gegenüber der für Gesundheit zuständigen Senatsverwaltung. Die sehr spezifische Nennung und Beschreibung einzelner Regeln der DSGVO erzeugt zusätzlichen Interpretationsspielraum, die Anzeige ergänzende Bürokratie.

## **Brandenburg**

Das Brandenburger Krankenhausentwicklungsgesetz ([BbgKHEG](#)) beschreibt die Verarbeitung von Patientendaten zum Zweck der Behandlung und der damit erforderlichen Schritte, unter anderem Qualitätssicherung und Aus-, Fort- und Weiterbildung. Die Offenlegung von Patientendaten außerhalb des Krankenhauses wird ausgeschlossen, mit Ausnahme von erforderlichen Schritten zur Behandlung oder Qualitätssicherung, die mit anonymisierten Daten nicht erreicht werden kann und der keine schutzwürdigen Interessen Betroffener entgegenstehen. Auch das Brandenburger Datenschutzgesetz enthält Vorschriften zur Verarbeitung besonderer Kategorien von personenbezogenen Daten.

## **Bremen**

Das Bremische Landeskrankenhausgesetz ([BremKrhG](#)) erlaubt die Verarbeitung von Patientendaten auf einer bestehenden Rechtsgrundlage, mit Einwilligung sowie unter anderem zur Erfüllung des Behandlungsauftrages, zur Aus-, Fort- und Weiterbildung sowie Qualitätssicherung, wobei jeweils zu prüfen ist, ob die Datenverarbeitung erforderlich ist oder der Zweck auch mit anonymisierten/pseudonymisierten Daten erreicht werden kann. Die Auftragsverarbeitung ist insbesondere dann erlaubt, wenn der Betriebsablauf dies erfordert, die Verarbeitung günstiger ist oder die Datenverarbeitung vom Krankenhaus nur mit hohem Aufwand geleistet werden könnte. Spezifische Regeln zur Verarbeitung in Drittländern gibt es nicht, hier wird auf die DSGVO verwiesen.

## **Hamburg**

Das Hamburgische Krankenhausgesetz ([HmbKHG](#)) beschreibt im [§ 7 HmbKHG](#), dass die Verarbeitung von Patientendaten auf der Grundlage der DSGVO möglich ist. Die Offenlegung von Patientendaten zu bestimmten Zwecken ist in [§ 11 HmbKHG](#) geregelt. Die Übermittlung von Patientendaten ist zulässig, soweit dies zum Beispiel zur Durchführung der Behandlung erforderlich ist, die Daten dürfen nur für diese Zwecke verarbeitet werden. Auch eine automatisierte Übermittlung im Sinne von regelmäßigen Verfahren an bestimmte Empfänger:innen - diese hat das Krankenhaus jedoch aufzuzeichnen.

## **Hessen**

Das Hessische Krankenhausgesetz ([HKHG](#)) bezieht sich ausdrücklich auf die Geltung des DSGVO und das Hessische Datenschutz- und Informationsfreiheitsgesetz ([HDSIG](#)). Gemäß [§ 12 HKHG](#) Die Übermittlung von Patientendaten ist unter anderem für die Erfüllung des Behandlungsvertrages

zulässig, für die Mit- oder Nachbehandlung nach Hinweis, soweit Patient:innen nichts anderes bestimmt haben. Besondere Anforderungen an die Datenübermittlung oder Verarbeitung werden nicht gestellt.

### **Mecklenburg-Vorpommern**

Das Landeskrankhausgesetz Mecklenburg-Vorpommern ([LKHG M-V](#)) erlaubt in § 33 LKHG M-V die Verarbeitung von Personenbezogenen Daten durch das Krankenhaus nur zur Erfüllung des Behandlungsvertrages und der damit verbundenen Pflichten. Darüber hinaus sind gemäß § 34 LKHG M-V einige spezifisch benannte Umstände wie Aus-, Fort- und Weiterbildung zulässig, weitgehend beschränkt auf anonymisierte Daten, es sei denn, der Zweck ist nur mit pseudonymisierten Daten zu erreichen. Spätestens nach einem Jahr sind diese pseudonymisierten Daten zu löschen oder zu anonymisieren. Werden Daten im Auftrag verarbeitet, müssen die Kategorien dokumentiert werden und der Datenschutzbeauftragte des Krankenhauses ist zu beteiligen. Auftragsverarbeitung darf in Anspruch genommen werden, wenn der Betriebsablauf sonst gestört wäre oder die Verarbeitung kostengünstiger ist. Eine über drei Monate hinausgehende Speicherung beim Auftragsverarbeiter ist nur zulässig, wenn getrennte Datenträger verwendet werden. Dort dürfen Daten ohne explizite Einwilligung nur von Personen verarbeitet werden, die dem Berufsgeheimnis gemäß § 203 StGB unterliegen und zur Verschwiegenheit verpflichtet sind. Auftragsverarbeitung außerhalb des Geltungsbereichs des Grundgesetzes ist nur erlaubt, wenn ausdrücklich eingewilligt wurde oder das Sitzland des Auftragsverarbeiters gesetzlichen Geheimhaltungspflichten unterliegt.

Damit geht Mecklenburg-Vorpommern deutlich über die DSGVO hinaus, bleibt aber unpräzise, denn die gesetzliche Geheimhaltungspflicht wird nicht weiter spezifiziert.

### **Niedersachsen**

Im niedersächsischen Krankenhausgesetz ([NKHG](#)) wird seit der Neufassung vom 31. Januar 2025 nur noch der Datenaustausch zwischen Krankenhäusern und Ministerium in Bezug auf dessen spezifische Aufgaben geregelt.

### **Nordrhein-Westfalen**

Nordrhein-Westfalen hat sein Gesundheitsdatenschutzgesetz zum 1. Juli 2025 aufgehoben. Es gelten ausschließlich die DSGVO und die Bundesgesetze sowie das [Datenschutzgesetz NRW \(DSG\)](#).

### **Rheinland-Pfalz**

Das rheinland-pfälzische Landeskrankhausgesetz ([LKG](#)) definiert im § 36 LKG enge Grenzen für die zulässige Verarbeitung von Patientendaten: Behandlung, Qualitätssicherung, aber auch eine vorliegende Rechtsvorschrift oder die Einwilligung. Wobei an die Einwilligung noch eigene Anforderungen gestellt werden. Die Übermittlung von Patientendaten an Dritte ist ebenfalls an strenge Auflagen gebunden, die § 36 LKG im Einzelnen beschreibt, darunter etwa die Erforderlichkeit für die Durchführung des Behandlungsvertrages, soweit die Patientin oder der Patient nach dem Hinweis auf die beabsichtigte Übermittlung nichts anderes bestimmt hat. Die

Ausgestaltung der Auftragsverarbeitung verweist auf die DSGVO und stellt keine eigenen Anforderungen.

## **Saarland**

Das Saarländische Krankenhausgesetz ([SKHG](#)) beschreibt den Patientendatenschutz in [§ 13 SKHG](#) ausführlich und eng abgrenzend, orientiert an der Erforderlichkeit für die Behandlung. Die Auftragsverarbeitung gemäß [§ 13a SKHG](#) verlangt von den Krankenhäusern eine Begründung, wenn sie Auftragsverarbeiter einsetzen (u. a. Betriebsablaufstörungen oder Kostenersparnis). Der Auftragsverarbeitungsvertrag muss an das Unabhängige Datenschutzzentrum Saarland und die Krankenhausaufsichtsbehörde übermittelt werden, der Auftragsverarbeiter muss sich der Kontrolle des Landesbeauftragten für Datenschutz und Informationsfreiheit unterwerfen. Bei einer Speicherung der Daten länger als drei Monate hat diese beim Auftragsverarbeiter auf getrennten Datenträgern zu erfolgen. Es gibt keine spezifischen Regelungen zur Drittlandübermittlung.

## **Sachsen**

Das Sächsische Krankenhausgesetz ([SächsKHG](#)) schränkt mit [§ 28 SächsKHG](#) die Übermittlung von Patientendaten außerhalb des Krankenhauses ohne Einwilligung im Wesentlichen auf die Erfüllung und die Durchführung des Behandlungsvertrages und der Nachbehandlung ein. Nach Ablauf der Behandlung unterliegen die Daten (mit wenigen Ausnahmen) dem alleinigen Zugriff der jeweiligen Fachabteilung. Auftragsverarbeitung ist möglich, der Auftragsverarbeiter muss einen Datenschutzbeauftragten ernennen und sich zur Geheimhaltung verpflichten. Es gibt keine spezifischen Regeln zur Drittlandsübermittlung.

## **Sachsen-Anhalt**

Das Krankenhausgesetz Sachsen-Anhalt ([KHG LSA](#)) regelt die Verarbeitung von Patientendaten in [§ 16 KHG LSA](#). Patientendaten dürfen verarbeitet werden, wenn das Gesetz oder eine eigene Rechtsvorschrift dies erlaubt, sowie mit Einwilligung. Damit ist ein guter allgemeiner Rahmen gesetzt, der andere gesetzliche Grundlagen nicht einschränkt. Krankenhäuser dürfen Auftragsverarbeiter einsetzen, wenn die Inanspruchnahme von Auftragsverarbeitern erforderlich ist und schutzwürdige Belange der betroffenen Personen nicht beeinträchtigt werden. Die Auftragsverarbeiter müssen sich an die DSGVO halten und zur Verschwiegenheit verpflichtet werden. Die Krankenhäuser müssen die Patienten über die Auftragsverarbeitung vorab informieren und ihnen die Möglichkeit geben, der Verarbeitung zu widersprechen. Es gibt keine spezifischen Regelungen zur Drittlandübermittlung.

## **Schleswig-Holstein**

Das Krankenhausgesetz für das Land Schleswig-Holstein ([LKHG](#)) regelt die Datenverarbeitung im Krankenhaus in [§ 36 LKHG](#). Patientendaten dürfen verarbeitet werden, sofern es dafür eine Rechtsgrundlage gibt und unter anderem zur Erfüllung des Behandlungsvertrages, zur Aus-, Fort- und Weiterbildung, sofern die Zwecke mit anonymisierten oder pseudonymisierten Daten nicht erreichbar sind. Zur Einwilligung wird auf die DSGVO verwiesen. Krankenhäuser dürfen gemäß [§ 37 LKHG](#) ihrem Auftragsverarbeiter Daten nur offenlegen, soweit dies für die Auftragserfüllung erforderlich ist. Die Daten sind zu anonymisieren oder zumindest zu pseudonymisieren, wenn der

Auftragszweck damit erreicht werden kann. Eine spezifische Regelung zur Drittlandübermittlung gibt es nicht.

## Thüringen

Das Thüringer Krankenhausgesetz ([ThürKHG](#)) beschreibt in [§ 27 ThürKHG](#) den Schutz der Persönlichkeit und Datenschutz. Demnach ist die Übermittlung von Patientendaten an Empfänger außerhalb des Krankenhauses nur gemäß der dortigen Vorgaben zulässig, etwa zur Erfüllung gesetzlich vorgeschriebener Mitteilungspflichten oder aufgrund einer Einwilligung. Diese Daten dürfen nur zum entsprechenden Zweck verwendet und müssen geheim gehalten werden. Sie sind zu löschen, wenn sie nicht mehr gebraucht werden. Die Auftragsverarbeitung ([§ 27b ThürKHG](#)) ist nur zulässig, wenn Betriebsablaufstörungen vermieden oder Kosten gespart werden, die Datenschutzbestimmungen gesichert sind, und die Anforderungen an die Schweigepflicht ([§ 203 StGB](#)) eingehalten werden. Das Krankenhaus muss der Aufsichtsbehörde die Auftragsverarbeitung vorab anzeigen, der Auftragsverarbeiter muss Kontrollen jederzeit ermöglichen. Es gibt keine spezifischen Regelungen zur Drittlandsübermittlung.

Diese Hintergrundinformation wurde bereitgestellt von:

Medtronic GmbH

Earl-Bakken-Platz 1

40670 Meerbusch

Geschäftsführung: Irene Holler, Rudolf Matzenberger,

Dorothee Stamm, Jörg Vollmann

Sitz der Gesellschaft: Meerbusch

Handelsregister: Amtsgericht Neuss HRB 14798

Für weitere Fragen kontaktieren Sie gerne:

- Dorothee Stamm, Director Governmental Affairs:

[dorothee.stamm@medtronic.com](mailto:dorothee.stamm@medtronic.com)

- Pia Maier, Governmental Affairs Specialist:

[pia.maier@medtronic.com](mailto:pia.maier@medtronic.com)