



Bundesministerium
für Forschung, Technologie
und Raumfahrt



DATATREE
YOUR COMPLIANCE PROVIDER



RECHTSRAHMEN für Daten & KI im Gesundheitswesen

KI-basierte Anonymisierung in der Medizin

// INHALT

1. DATENSCHUTZGESETZE

1.1 Europäische Datenschutz-Grundverordnung (DSGVO)	6
1.2 Bundesdatenschutzgesetz (BDSG)	9
1.3 Datenschutzgesetz Nordrhein-Westfalen (DSG NRW)	9
1.4 Gesetz über den Kirchlichen Datenschutz (KDG)	9
1.5 Datenschutzgesetz der Evangelischen Kirche in Deutschland (DSG-EKD)	10

2. GESUNDHEIT / PATIENTENRECHTE

2.1 Europäischer Gesundheitsdatenraum (EHDS)	12
2.2 Patientendaten-Schutz-Gesetz (PDSG)	13
2.3 Sozialgesetzbuch (SGB V)	13
2.4 Digitale-Versorgung-Gesetz (DVG)	14
2.5 Digitale-Versorgung-und-Pflege-Modernisierung-Gesetz (DVPMG)	14
2.6 Telekommunikation-Telemedien-Datenschutz-Gesetz (TDDDG)	14
2.7 Digitale-Gesundheitsanweisungen-Verordnungen (DiGAV)	15
2.8 Patients' Rights Directive	15
2.9 Gesundheitsdatennutzungsgesetz (GDNG)	15
2.10 Krankenhausgestaltungsgesetz NRW (KHGG NRW)	16
2.11 Krankenhauszukunftsgesetz-Durchführungsverordnung NRW (KHZG-DVO NRW)	16

3. KI / DIGITALISIERUNG

3.1 EU Artificial Intelligence Act (EU AI Act)	18
3.2 Produkthaftungsrichtlinie (PLD)	21
3.3 Arbeitnehmervertretung und KI-Einsatz	21
3.4 Data Governance Act (DGA)	21

4. MEDIZIN / PRODUKTE / ARZNEIMITTEL

4.1 Medical Device Regulation (MDR)	23
4.2 Medizinprodukte-Durchführungsgesetz (MPDG)	25
4.3 Arzneimittelgesetz (AMG)	25
4.4 EU Clinical Trials Regulation (CTR)	25
4.5 Heilmittelwerbegesetz (HWG)	26
4.6 Medizinrecht	26

// INHALT

5. IT-SICHERHEIT / CYBER

5.1 Netzwerk- und Informationssicherheitsrichtlinie 2 (NIS2)	28
5.2 IT-Sicherheitsgesetz 2.0 (BSIG)	30
5.3 Cyber Resilience Act (CRA)	31
5.4 Cybersecurity Act (CSA)	31
5.5 KRITIS-Verordnung	31

6. WETTBEWERBS- UND WIRTSCHAFTSRECHT

6.1 Data Act	33
6.2 Digital Services ACT (DSA)	34
6.3 Digital Markets Act (DMA)	34
6.4 Gesetz gegen den unlauteren Wettbewerb (UWG)	34
6.5 Urheberrechtsgesetz (UrhG)	34
6.6 Vertragsrecht	34

7. STRAF- UND HAFTUNGSRECHT

7.1 Strafgesetzbuch (StGB)	36
7.2 Haftungsrechtliche Einordnung ärztlicher KI-Nutzung	37

8. BERUFSRECHT

8.1 Heilberufegesetz NRW (HeilBerG NRW)	39
8.2 Muster-Berufsordnung für Ärzte (MBO-Ä)	40

9. VERWALTUNG / STAAT

9.1 Betriebsverfassungsgesetz (BetrVG)	42
9.2 Onlinezugangsgesetz (OZG)	43
9.3 E-Government-Gesetze (EGovG)	43
9.4 European Accessibility Act (EAA)	44
9.5 Landeshochschulgesetz NRW (HG NRW)	44
9.6 Digitalisierung von Verwaltungsprozessen im Klinikbetrieb	44

IMPRESSUM	46
-----------	----

Der Rechtsrahmen für Daten & KI im Gesundheitswesen

Der verantwortungsvolle Umgang mit Daten ist die Grundvoraussetzung für den sicheren und wirksamen Einsatz von Künstlicher Intelligenz (KI) im Gesundheitswesen. KI-Systeme benötigen umfangreiche und qualitativ hochwertige Datenbestände, die häufig besonders sensible Gesundheitsinformationen umfassen. Ihr Schutz ist entscheidend für Patientensicherheit, Vertrauen und Rechtssicherheit im gesamten KI-Lebenszyklus.

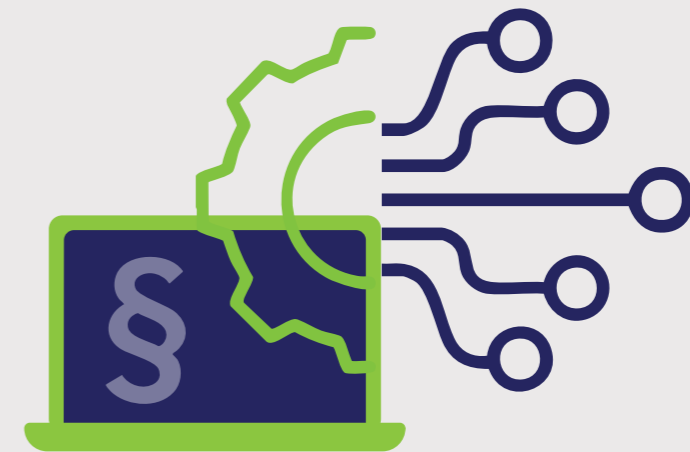
Pseudonymisierung und Anonymisierung sind dabei zentrale Schutzmechanismen. Während die Pseudonymisierung die Identität lediglich durch zusätzliche Informationen wiederherstellbar macht, wird bei der Anonymisierung der Personenbezug vollständig und dauerhaft entfernt. Beide Verfahren ermöglichen es, Gesundheitsdaten für Analyse, Forschung und Entwicklung zu nutzen, ohne die Rechte der betroffenen Personen zu beeinträchtigen.

Im Rahmen des Förderprojekts KI-AIM werden diese Verfahren sowie die datenschutzkonforme Nutzung von Daten aus rechtlicher, technischer und organisatorischer Perspektive systematisch betrachtet. Ziel ist es, Anforderungen, Risiken und Schutzmaßnahmen über den gesamten Daten- und KI-Lebenszyklus hinweg transparent darzustellen und eine fundierte Grundlage für rechtssichere und belastbare Entscheidungsprozesse zu schaffen.

Die Anwender*innen dieses Moduls sind verpflichtet, die für ihren jeweiligen Anwendungsfall maßgeblichen gesetzlichen Vorgaben eigenständig zu prüfen und zu berücksichtigen. Die rechtlichen Rahmenbedingungen unterscheiden sich je nach Rechtsraum, Datenart, Zweck der Verarbeitung sowie der eingesetzten technischen Verfahren. Diese Vorgaben sind frühzeitig zu berücksichtigen und in die Planung, Implementierung und Bewertung von KI-Systemen verbindlich einzubeziehen.

Dieses Kapitel stellt einen konsistenten und praxisorientierten Überblick über die rechtlichen Grundlagen von Pseudonymisierung, Anonymisierung und datenschutzgerechter Datennutzung bereit. Es soll dazu beitragen, KI-Systeme in medizinischen Kontexten verantwortungsvoll, transparent und im Einklang mit Datenschutz-, Sicherheits- und Berufsrechtsgaben einzusetzen und damit die Grundlage für eine vertrauenswürdige und zukunftsfähige Digitalisierung im Gesundheitswesen zu schaffen.

Gesetzliche Anforderungen



Der Einsatz von Künstlicher Intelligenz (KI) im Gesundheitswesen eröffnet neue Möglichkeiten, um Diagnosen zu verbessern, Behandlungsprozesse zu optimieren und das medizinische Personal zu entlasten. Damit verbunden ist jedoch auch eine erhebliche Verantwortung im Umgang mit sensiblen Gesundheitsdaten. KI-Systeme benötigen große Datenmengen, um verlässliche Ergebnisse zu liefern, wobei es sich häufig um besonders schützenswerte Informationen über den Gesundheitszustand, das Verhalten oder die Identität von Patient*innen handelt.

In den vergangenen Jahren hat die Europäische Union zentrale Regelwerke geschaffen, um die Verarbeitung personenbezogener Daten, den Austausch von Gesundheitsinformationen und den verantwortungsvollen Einsatz von KI europaweit zu regulieren. Datenschutz spielt dabei eine zentrale Rolle, weil er das Fundament für Vertrauen, Sicherheit und Fairness bildet. Nur wenn der Schutz persönlicher Daten gewährleistet ist, können Patient*innen und Mitarbeitende darauf vertrauen, dass KI-Systeme verantwortungsvoll eingesetzt werden. Ein bewusster und transparenter Umgang mit Daten stärkt die Akzeptanz neuer Technologien und verhindert, dass KI zu Intransparenz, Überwachung

oder unbeabsichtigter Diskriminierung führt. Zugleich trägt Datenschutz dazu bei, Fehler und Risiken zu minimieren. Eine unreflektierte Nutzung von Gesundheitsdaten kann falsche Schlussfolgerungen, verzerrte Ergebnisse oder unfaire Behandlungsentscheidungen begünstigen.

Durch klare Datenschutzprinzipien, etwa Datenminimierung, Zweckbindung und Transparenz, wird sichergestellt, dass KI-Systeme verlässlich, nachvollziehbar und verantwortbar arbeiten. Datenschutz wird im KI-Kontext somit nicht als Hemmnis, sondern als Qualitätsmerkmal verstanden: Er schafft die Grundlage für ethische Innovation, schützt die Rechte der Betroffenen und unterstützt eine nachhaltige, vertrauenswürdige Digitalisierung im Gesundheitswesen.



1. Datenschutzgesetze

Der Datenschutz bildet die Grundlage für den sicheren Umgang mit personenbezogenen und insbesondere sensiblen Gesundheitsdaten. Europäische und nationale Rechtsvorschriften regeln deren Verarbeitung, Speicherung und Schutz, um sicherzustellen, dass die Rechte der betroffenen Personen jederzeit gewahrt bleiben.

1.1 Europäische Datenschutz-Grundverordnung (DSGVO)

Die Datenschutz-Grundverordnung gilt seit dem 25. Mai 2018 unmittelbar in allen Mitgliedstaaten der Europäischen Union und des Europäischen Wirtschaftsraums. Als Unionsrecht besitzt sie Anwendungsvorrang gegenüber nationalen Regelungen, sodass Behörden und Gerichte nationale Vorschriften, die der DSGVO widersprechen, unangewendet lassen müssen.

Gerade im Gesundheitswesen und beim Einsatz von Künstlicher Intelligenz (KI) kommt der DSGVO eine zentrale Bedeutung zu. Sie verpflichtet Verantwortliche dazu, personenbezogene Daten nur auf einer rechtmäßigen Grundlage zu verarbeiten und geeignete Schutzmaßnahmen zu implementieren. Ein Verantwortlicher nach Art. 4 Nr. 7 DSGVO ist die Stelle, die allein oder gemeinsam mit anderen darüber entscheidet, zu welchen Zwecken und mit welchen Mitteln personenbezogene Daten verarbeitet werden. Gesundheitsdaten zählen zu den besonders sensiblen Kategorien personenbezogener Daten. Ihre unbefugte Offenlegung oder missbräuchliche Nutzung kann erhebliche Risiken mit sich bringen, wie Diskriminierung, Stigmatisierung oder soziale Nachteile.

Nach Art. 4 Nr. 1 DSGVO umfassen personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Eine Identifizierbarkeit liegt vor, wenn die Person direkt oder indirekt über Merkmale wie Name, Kennnummer, Standortdaten, Online-Kennung oder biometrische bzw. genetische Eigenschaften bestimmbar ist.

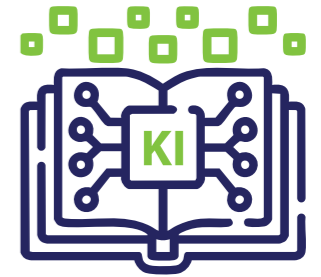
Die DSGVO unterscheidet insbesondere zwischen:

Pseudonymisierten Daten (Art. 4 Nr. 5 DSGVO): Daten werden so verarbeitet, dass sie ohne zusätzliche Informationen nicht mehr einer Person zugeordnet werden können. Diese Zusatzinformationen müssen getrennt und besonders gesichert aufbewahrt werden.

Pseudonymisierte Daten gelten weiterhin als personenbezogen, da eine Re-Identifizierung möglich bleibt. Sie unterliegen daher vollständig den Anforderungen der DSGVO, tragen jedoch zur Risikominderung bei, insbesondere in Bezug auf Art. 25 (Datenschutz durch Technikgestaltung) und Art. 32 (Datensicherheit).

Anonymisierten Daten (Erwägungsgrund 26 DSGVO): Anonymisierte Daten sind solche, bei denen die Identität der betroffenen Person weder direkt noch indirekt festgestellt werden kann. Sie fallen nicht in den Anwendungsbereich der DSGVO. Eine wirksame Anonymisierung setzt voraus, dass auch durch Kombination mit weiteren Datenquellen keine Identifizierbarkeit möglich ist.

Der Europäische Gerichtshof (EuGH) hat am 4. September 2025 klargestellt, dass pseudonymisierte Daten für die Stelle, die über die zur Identifizierung erforderlichen Zusatzinformationen verfügt, personenbezogene Daten bleiben. Entscheidend ist, ob eine Re-Identifizierung mit rechtlich zulässigen und praktisch verfügbaren Mitteln möglich ist. Eine rein theoretische Möglichkeit genügt nicht. Für Dritte ohne Zugriff auf die Zusatzinformationen können dieselben Daten als anonym gelten.



Beispiel zur Pseudonymisierung:

Ein Krankenhaus betreibt ein zentrales Labor, das täglich zahlreiche Blutproben analysiert. Um diese Daten für die interne Qualitätssicherung oder Forschung zu nutzen, werden sie pseudonymisiert. Statt des Namens oder Geburtsdatums erhält jeder Datensatz eine Zufalls-ID (z.B. Patientennummer „PZ-84726“). Nur ein getrennt und verschlüsselt geführtes Verzeichnis enthält die Zuordnung zur Identität der Patient*innen. So bleiben die Daten für Forschungszwecke nutzbar, ohne dass ein direkter Personenbezug besteht.

Bei KI-Projekten spielt zudem die gemeinsame Verantwortlichkeit nach Art. 26 DSGVO eine zentrale Rolle. Diese liegt vor, wenn zwei oder mehr Stellen gemeinsam über Zwecke und Mittel der Verarbeitung entscheiden etwa bei der Entwicklung, dem Training oder Betrieb eines KI-Systems im Gesundheitswesen. In solchen Fällen müssen die Verantwortlichen in einer Art. 26 Vereinbarung klar regeln, wer welche Pflichten übernimmt, insbesondere in Bezug auf Transparenz, Betroffenenrechte, technische und organisatorische Maßnahmen sowie die Meldung von Datenschutzverletzungen.

Krankenhäuser sollten daher ein besonderes Augenmerk auf Datenminimierung, risikoorientierte Bewertungen, die strikte Trennung identifizierender Informationen, geeignete technische Schutzmaßnahmen sowie eine sorgfältige Dokumentation aller Verarbeitungsschritte legen. Einrichtungen, die Anonymisierungs- oder Analyseverfahren einsetzen, tragen die Verantwortung für verbleibende Re-Identifizierungsrisiken und sollten zur Absicherung klare interne Richtlinien, regelmäßige Schulungen sowie wirksame Kontrollmechanismen etablieren.

Nach Art. 9 Abs. 1 DSGVO ist die Verarbeitung besonderer Kategorien personenbezogener Daten darunter Gesundheitsdaten, genetische und biometrische Daten grundsätzlich untersagt. Sie ist nur in den in Art. 9 Abs. 2 DSGVO vorgesehenen Ausnahmefällen zulässig, etwa bei ausdrücklicher Einwilligung der betroffenen Person oder bei medizinischer Erforderlichkeit.

Im Kontext von KI spielt zudem der Begriff der Synthetisierung eine zentrale Rolle. Dieser bezeichnet die Zusammenführung unterschiedlicher Datensätze oder Merkmale, aus denen neue, potenziell besonders sensible Informationen entstehen können. Ein solcher Vorgang kann eine Zweckänderung darstellen und damit eine neue Rechtsgrundlage erfordern. Werden beispielsweise Bewegungs-, Medikations- und Sprachdaten kombiniert, kann hierdurch ein neues Gesundheitsdatum mit erhöhtem Schutzbedarf entstehen. Daher sind bei KI-Projekten eine frühzeitige rechtliche Bewertung, größtmögliche Transparenz gegenüber den betroffenen Personen, gegebenenfalls die Durchführung einer Datenschutzfolgenabschätzung sowie technische Maßnahmen wie Pseudonymisierung und restriktive Zugriffsbeschränkungen zwingend erforderlich.

Tab. 1 DSGVO

Normen	Inhalte	Praxisrelevanz
Art. 5 DSGVO	Grundsätze der Datenverarbeitung (Rechtmäßigkeit, Transparenz, Zweckbindung etc.)	Alle Datenverarbeitungen müssen diesen Prinzipien entsprechen
Art. 6 DSGVO	Rechtsgrundlagen für die Datenverarbeitung	z. B. Einwilligung, Vertragserfüllung (z. B. Behandlungsvertrag)
Art. 9 DSGVO	Verarbeitung besonderer Kategorien personenbezogener Daten (z. B. Gesundheitsdaten)	Nur mit ausdrücklicher Einwilligung oder medizinischer Notwendigkeit erlaubt
Art. 12 DSGVO	Transparente Information der Betroffenen	Informationspflicht zu Art, Zweck und Umfang der Datenverarbeitung
Art. 13/14 DSGVO	Informationspflicht bei direkter/indirekter Datenerhebung	Aufklärung über Verarbeitungszwecke, Dauer, Empfänger
Art. 17 DSGVO	Recht auf Löschung („Recht auf Vergessenwerden“)	Besonders relevant bei Daten, die zu KI-Trainingszwecken verarbeitet wurden
Art. 21 DSGVO	Widerspruchsrecht gegen Datenverarbeitung	Betroffene können automatisierte Verarbeitung (z. B. durch KI) ablehnen
Art. 25 DSGVO	Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen	Pseudonymisierung, Verschlüsselung, Datensparsamkeit von Anfang an
Art. 33 DSGVO	Meldung von Datenschutzverletzungen	Pflicht zur Meldung an Aufsichtsbehörde und ggf. Betroffene (innerhalb von 72 h)
Art. 35 DSGVO	Datenschutz-Folgenabschätzung (DSFA)	Pflicht bei hohem Risiko durch KI-Systeme
Art. 44 ff. DSGVO	Datenübermittlung in Drittländer außerhalb der EU	Nur zulässig bei angemessenem Datenschutzniveau oder geeigneten Garantien
Art. 77–79 DSGVO	Rechte auf Beschwerde, gerichtlichen Rechtsbehelf und Schadenersatz	Betroffene können Verstöße melden und ggf. Schadenersatz verlangen

a) Internationale Datenschutzgesetze verfolgen teilweise abweichende Ansätze:

In Südkorea unterscheidet der Personal Information Protection Act (PIPA) klar zwischen pseudonymisierten und anonymisierten Daten. Pseudonymisierte Daten bleiben dem Datenschutzrecht unterworfen, während anonymisierte Daten davon ausgenommen sind. Der PIPA verpflichtet zu umfassenden technischen und organisatorischen Maßnahmen, zur Dokumentation der Anonymisierungsverfahren. Außerdem sieht das Gesetz die Benennung eines Privacy Officers (mit Ausnahmen für Kleinstunternehmen) vor. Datenübermittlungen ins Ausland erfordern grundsätzlich eine Einwilligung, es bestehen jedoch Ausnahmenvorschriften (z.B. vertragliche Erforderlichkeit oder Angemessenheitsentscheidungen).

In Japan ist der Umgang mit anonymisierten Daten im Act on the Protection of Personal Information (APPI) ausdrücklich geregelt. Das Gesetz definiert „Anonymously Processed Information“ und verlangt, dass identifizierende Merkmale vollständig entfernt werden und eine Re-Identifizierung ausgeschlossen ist. Zudem ist die Kombination anonymisierter Daten mit an-

deren Informationen untersagt. Unternehmen sind verpflichtet, den gesamten Anonymisierungsprozess nachvollziehbar zu dokumentieren und offenzulegen.

Im Vergleich dazu definiert die Europäische Union die Anonymisierung im Rahmen der DSGVO nicht ausdrücklich, sondern orientiert sich an den jeweils aktuellen technischen Möglichkeiten sowie den tatsächlichen Re-Identifizierungsrisiken. Dieser funktionale und flexible Ansatz bietet zwar erheblichen Gestaltungsspielraum, führt jedoch in der praktischen Umsetzung zu einer geringeren Rechtssicherheit.

1.2 Bundesdatenschutzgesetz (BDSG)

Das Bundesdatenschutzgesetz konkretisiert seit dem 25. Mai 2018 die Vorgaben der DSGVO auf nationaler Ebene. Es gilt für öffentliche Stellen des Bundes sowie für nicht-öffentliche Stellen, sofern keine spezielleren Landesregelungen Anwendung finden. Das BDSG enthält unter anderem Bestimmungen zur Verarbeitung besonderer Kategorien personenbezogener

Daten (§ 22 BDSG), zum Beschäftigtendatenschutz (§ 26 BDSG) sowie zur Verpflichtung von Verantwortlichen zur Umsetzung angemessener technischer und organisatorischer Maßnahmen (TOMs). Dazu zählen Zugriffsbeschränkungen, Protokollierung, Verschlüsselung, Notfallmanagement und interne Datenschutzrichtlinien.

Tab. 2 BDSG

Normen	Inhalte
§ 22 BDSG	Verarbeitung besonderer Kategorien personenbezogener Daten
§ 26 BDSG	Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

1.3 Datenschutzgesetz Nordrhein-Westfalen (DSG NRW)

Das Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) regelt die Verarbeitung personenbezogener Daten durch öffentliche Stellen des Landes, einschließlich kommunaler Krankenhäuser und Universitätskliniken. Es ergänzt die DSGVO in Bereichen, in denen nationale Gestaltungsspielräume bestehen, wie etwa bei Datenschutz-Folgenabschätzungen, Betroffenenrechten oder den Anforderungen an Datenschutzauftragte.

Für öffentliche Gesundheitseinrichtungen ist das DSG NRW insbesondere im Kontext digitaler Systeme und KI-Anwendungen von Bedeutung. Es schreibt vor, unter welchen Voraussetzungen Gesundheitsdaten verarbeitet werden dürfen, welche Schutzmaßnahmen zu implementieren sind, und in welchen Fällen eine Datenschutz-Folgenabschätzungen verpflichtend ist.

1.4 Gesetz über den Kirchlichen Datenschutz (KDG)

Das Gesetz über den kirchlichen Datenschutz (KDG) gilt für katholische Einrichtungen in Deutschland und beruht auf dem kirchlichen Selbstbestimmungsrecht (Art. 140 GG i. V. m. Art. 137 Abs. 3 WRV). Es stellt ein eigenständiges Datenschutzrecht dar, das auf Grundlage des kirchlichen Selbstverwaltungsrechts parallel zur DSGVO gilt und ein gleichwertiges Schutzniveau gewährleistet.

Das KDG regelt seit dem 24. Mai 2018 die Verarbeitung personenbezogener Daten in katholischen Einrichtungen wie Bistümern, Pfarreien, Caritasverbänden, kirchlichen Krankenhäusern, Ordensgemeinschaften und sonstigen kirchlichen Rechtsträgern. Es übernimmt die zentralen Datenschutzprinzipien der DSGVO – darunter Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung, Speicherbegrenzung sowie Integrität und Vertraulichkeit und enthält spezifische kirchenrechtliche Ausgestaltungen. Eine besondere Rolle spielt die Verarbeitung sensibler personenbezogener Daten (z. B. Gesundheits-, Sozial- und Beschäftigtendaten), die in vielen kirchlichen Einrichtungen regelmäßig erfolgt und besonders hohe Anforderungen an technische und organisatorische Maßnahmen stellt. Ein zentraler Unterschied zur staatlichen Datenschutzaufsicht besteht darin, dass die Kontrolle im Bereich des KDG nicht durch staatliche Behörden erfolgt, sondern durch unabhängige kirchliche Datenschutzaufsichtsstellen. Hierzu gehören insbesondere die Katholischen Datenschutzaufsichten (KDSA) der jeweiligen Kirchenprovinzen. Diese überwa-

chen die Einhaltung des KDG, beraten die Einrichtungen, führen Prüfungen durch und können bei Verstößen verbindliche Maßnahmen anordnen. Die kirchlichen Aufsichtsbehörden sind damit Teil der kirchlichen Selbstverwaltung und unterliegen nicht der staatlichen Datenschutzaufsicht. Sie handeln eigenständig, dialogorientiert und kirchenrechtlich legitimiert, besitzen aber zugleich wirksame Eingriffsbefugnisse, um Verstöße zu ahnden und rechtmäßige Zustände wiederherzustellen. Für Verantwortliche bestehen umfangreiche Pflichten, darunter das Führen eines Verzeichnisses der Verarbeitungstätigkeiten, geeignete technische und organisatorische Maßnahmen, datenschutzfreundliche Voreinstellungen, Datenschutz-Folgenabschätzungen, Verpflichtung auf das Datengeheimnis sowie umfassende Dokumentations- und Nachweispflichten. Ebenso garantiert das KDG Betroffenenrechte wie Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch und Rechte bei automatisierten Entscheidungen. Insgesamt stellt das KDG ein umfassendes, eigenständiges und vollwertiges Datenschutzgesetz dar, das die Besonderheiten der katholischen Organisationsstruktur berücksichtigt und gleichzeitig sicherstellt, dass personenbezogene Daten in katholischen Einrichtungen auf einem Schutzniveau verarbeitet werden, das der DSGVO vollständig entspricht.

1.5 Datenschutzgesetz der Evangelischen Kirche in Deutschland (DSG-EKD)

Das Datenschutzgesetz der Evangelischen Kirche in Deutschland (DSG-EKD) regelt seit Mai 2018 die Verarbeitung personenbezogener Daten in Einrichtungen der Evangelischen Kirche, darunter Kirchengemeinden, diakonische Dienste und evangelische Krankenhäuser. Es beruht auf Art. 91 DSGVO, der den Kirchen die Ausgestaltung eigener Datenschutzregelungen ermöglicht, und orientiert sich inhaltlich eng an der DSGVO.

Ergänzend enthält das DSG-EKD spezifisch kirchliche Vorgaben, insbesondere zur kirchlichen Aufsicht, zu organisatorischen Zuständigkeiten und zur Umsetzung kirchenrechtlicher Besonderheiten. Die Kontrolle erfolgt nicht durch staatliche Stellen, sondern durch kirchliche Datenschutzaufsichtsbehörden wie die Evangelische Datenschutzaufsicht (DSA-EKD).

Diese kirchlichen Aufsichtsbehörden sind eigenständige, unabhängige Stellen, die im Rahmen des kirchlichen Selbstbestimmungsrechts handeln und nicht der staatlichen Datenschutzaufsicht unterliegen. Sie beraten die Einrichtungen, führen Prüfungen durch und können bei Verstößen verbindliche Maßnahmen anordnen, wobei der Aufsichtsstil dialogorientiert, aber rechtlich verbindlich ist.

Das DSG-EKD verpflichtet zur Einhaltung der Grundprinzipien der Datenverarbeitung, darunter Rechtmäßigkeit, Zweckbindung, Datenminimierung und die Wahrung der Betroffenenrechte.

Von besonderer Bedeutung ist das DSG-EKD im diakonischen Bereich, in dem regelmäßig besonders schützenswerte personenbezogene Daten, insbesondere Gesundheits-, Sozial- und Beratungsdaten verarbeitet werden. Hier gelten erhöhte Anforderungen an Transparenz, technische und organisatorische Maßnahmen sowie an die interne Verantwortlichkeit.

Von besonderer Bedeutung ist das DSG-EKD im diakonischen Bereich, in dem regelmäßig besonders schützenswerte personenbezogene Daten insbesondere Gesundheits-, Sozial- und Beratungsdaten verarbeitet werden. Hier gelten erhöhte Anforderungen an Transparenz, technische und organisatorische Maßnahmen sowie an die interne Verantwortlichkeit. Evangelische Einrichtungen sind verpflichtet, hohe Datenschutzstandards einzuhalten und umfangreiche Pflichten zu erfüllen, darunter technische und organisatorische Maßnahmen, Datenschutz-Folgenabschätzungen, Verzeichnisse von Verarbeitungstätigkeiten, datenschutzfreundliche Voreinstellungen sowie Dokumentations- und Nachweispflichten. Insgesamt stellt das DSG-EKD ein eigenständiges, vollwertiges Datenschutzgesetz dar, das den Schutz personenbezogener Daten im evangelischen Bereich gewährleistet, kirchliche Strukturen berücksichtigt und zugleich das durch Art. 91 DSGVO garantierte Selbstbestimmungsrecht der Kirche wahrt.



Merktafel

Datenschutz-Grundverordnung (DSGVO):

- Verarbeitung nur auf Rechtsgrundlage und zu festgelegtem Zweck
- Gesundheitsdaten nur mit Einwilligung oder gesetzlicher Grundlage verarbeiten
- Transparente Information der Betroffenen
- Datenminimierung und Zweckbindung
- Pseudonymisierung oder Verschlüsselung einsetzen
- Technische und organisatorische Schutzmaßnahmen (TOMs) umsetzen
- Datenschutz-Folgenabschätzung bei hohem Risiko
- Datenschutzvorfälle binnen 72 Stunden melden
- Rechte der Betroffenen (Auskunft, Löschung, Widerspruch) wahren
- Datenübermittlungen in Drittländer nur bei angemessenem Schutzniveau

Bundesdatenschutzgesetz (BDSG):

- Ergänzt DSGVO auf nationaler Ebene
- Verarbeitung besonderer Daten nur auf spezieller Grundlage
- Beschäftigtendaten nur bei Erforderlichkeit verarbeiten
- TOMs verpflichtend (Zugriffsschutz, Protokollierung, Verschlüsselung)
- Datenschutzkonzept und interne Kontrollen erforderlich

Datenschutzgesetz NRW (DSG NRW):

- Gilt für öffentliche Stellen (z.B. Krankenhäuser, Kliniken)
- Datenschutzbeauftragte müssen benannt werden
- Neue oder risikoreiche Verarbeitungen dokumentieren
- Datenschutz-Folgenabschätzung bei Gesundheits- oder KI-bezogenen Daten erforderlich
- Sicherheitsmaßnahmen regelmäßig prüfen und anpassen

Gesetz über den kirchlichen Datenschutzgesetz (KDG):

- Eigenständiges kirchliches Datenschutzrecht auf Grundlage des kirchlichen Selbstverwaltungsrechts
- Gleichwertiges Schutzniveau zur DSGVO
- Aufsicht durch kirchliche Datenschutzbehörden (nicht staatlich)
- Hohe Anforderungen bei Gesundheits-, Sozial- und Beschäftigtendaten

Datenschutzgesetz der Evangelischen Kirche in Deutschland (DSG-EKD):

- Eigenständiges Datenschutzrecht im evangelischen Bereich gemäß Art. 91 DSGVO
- Unabhängige kirchliche Datenschutzaufsicht (DSA-EKD)
- Strenge Vorgaben für Einrichtungen der Diakonie aufgrund sensibler Datenverarbeitung
- Verpflichtung zu umfangreichen technischen, organisatorischen und dokumentarischen Maßnahmen



2. Gesundheit / Patientenrechte

Der Schutz von Gesundheits- und Patientendaten unterliegt besonders strengen rechtlichen und organisatorischen Vorgaben. Diese Daten bilden die Grundlage für eine vertrauenswürdige, sichere und verantwortungsvolle Gesundheitsversorgung. Die einschlägigen europäischen und nationalen Regelwerke legen fest, unter welchen Bedingungen Gesundheitsdaten verarbeitet, übermittelt und genutzt werden dürfen, stärken die Rechte der Patient*innen und schaffen zugleich den rechtlichen Rahmen für Innovation, Digitalisierung und den Einsatz von KI im medizinischen Umfeld.

2.1 Europäischer Gesundheitsdatenraum (EHDS).

Der Europäische Gesundheitsdatenraum (European Health Data Space, EHDS) ist eine zentrale EU-Verordnung (2025/327). Sie wurde am 26. März 2025 verabschiedet, tritt jedoch mit gestaffelten Übergangsfristen in Kraft und entfaltet ihre volle Anwendung erst in den folgenden Jahren. Er schafft erstmals einen verbindlichen Rechtsrahmen für den sicheren und grenzüberschreitenden Austausch sowie die kontrollierte Nutzung elektronischer Gesundheitsdaten in allen Mitgliedstaaten. Ziel ist es, sowohl die Primärnutzung – zur unmittelbaren medizinischen Versorgung – als auch die Sekundärnutzung – für Forschung, Innovation, öffentliche Gesundheit und Politikgestaltung – unter strengen Datenschutz-, Transparenz- und Sicherheitsanforderungen zu ermöglichen.

Patient*innen erhalten durch den EHDS deutlich gestärkte Rechte. Sie sollen jederzeit Zugang zu ihren elektronischen Gesundheitsdaten haben, diese zwischen Leistungserbringenden übertragen sowie die Zugriffsrechte Dritter selbst steuern können. Die Verordnung stärkt damit die informationelle Selbstbestimmung und verankert einen europaweit einheitlichen Anspruch auf digitale Gesundheitsinformationen. Gesundheitsdienstleister und Anbieter elektronischer Patientenakten werden verpflichtet, Gesundheitsdaten interoperabel, sicher und über MyHealth@EU europaweit zugänglich zu machen. Hierfür definiert der EHDS gemeinsame technische Standards, einheitliche Schnittstellen und verbindliche Sicherheitsanforderungen.

Für die Sekundärnutzung von Gesundheitsdaten werden in allen Mitgliedstaaten sogenannte Health Data Access Bodies (HDABs) eingerichtet. Diese nationalen Zugangsstellen prüfen und genehmigen Anträge auf Datennutzung, führen Daten-

kataloge, überwachen die Einhaltung der gesetzlichen Vorgaben und stellen sicher, dass Gesundheitsdaten ausschließlich zu zulässigen Zwecken verarbeitet werden. Der EHDS legt klar fest, dass eine Sekundärnutzung nur für wissenschaftliche Forschung, Innovation, öffentliche Gesundheit, Statistik oder die Entwicklung von Medizinprodukten und KI-Systemen zulässig ist. Nutzungen für Werbung, personalisierte Versicherungsprodukte, Kredit scoring oder arbeitsrechtliche Bewertungen sind ausdrücklich verboten.

Ein besonderer Schwerpunkt des EHDS liegt auf Datenschutz, IT-Sicherheit und Anonymisierung. Alle Zugriffe auf Gesundheitsdaten müssen protokolliert werden; Re-Identifizierungen pseudonymisierter oder anonymisierter Datensätze sind untersagt. Zudem gelten strenge Vorgaben zu Zweckbindung, Datenminimierung und sicherer Speicherung. Die Anwendung des EHDS erfolgt gestaffelt über mehrere Jahre: Erste Pflichten gelten erst nach Ablauf der Übergangsfristen ab 2026/2027. Prioritäre technische Standards und ausgewählte Datendomänen werden schrittweise bis 2029 verbindlich. Die vollständige Umsetzung des EHDS wird je nach Mitgliedstaat und betroffener Datenkategorie im Zeitraum von 2030 bis 2034 erwartet.

Damit markiert der EHDS einen bedeutenden Meilenstein der europäischen Gesundheits- und Digitalpolitik, dessen Wirkung aufgrund der gestaffelten Einführung erst in den kommenden Jahren vollständig sichtbar wird. Er verbindet ein hohes Datenschutzniveau mit der Förderung datengetriebener Innovation und bildet die Grundlage für eine interoperable, vertrauenswürdige und KI-fähige Gesundheitsversorgung in Europa.

Tab. 3 EHDS

Normen	Inhalte
Art. 3 EHDS	Definitionen
Art. 7-9 EHDS	Rechte der Patient*innen: Zugang, Kontrolle und Datenübertragbarkeit im Rahmen der Primärnutzung
Art. 14-16 EHDS	Pflichten der Gesundheitsdienstleister und EHR-Systemanbieter: interoperable, sichere und grenzüberschreitende Bereitstellung über MyHealth@EU
Art. 34-36 EHDS	Einrichtung und Aufgaben der Health Data Access Bodies – Prüfung, Genehmigung und Überwachung der Sekundärnutzung
Art. 45 EHDS	Zulässige Zwecke der Sekundärnutzung: Forschung, Innovation, öffentliche Gesundheit, Statistik, Entwicklung von Medizinprodukten oder KI-Systemen
Art. 55 EHDS	Ausgeschlossene Nutzungen: Werbung, personalisierte Versicherungen, Kredit scoring, arbeitsrechtliche Bewertungen, Entwicklung gefährlicher Produkte
Art. 57-59 EHDS	Datenschutz- und Sicherheitsmaßnahmen: Datenminimierung, Pseudonymisierung/Anonymisierung, Re-Identifizierungsverbot, Protokollierung aller Zugriffe
Art. 63-65 EHDS	Zusammenarbeit der Behörden, Einrichtung des EHDS-Boards und Koordination der nationalen Stellen
Art. 70-72 EHDS	Übergangsbestimmungen, Durchführungsakte, Inkrafttreten (März 2025) und gestaffelte Anwendung ab 2026 bis 2030

2.2 Patientendaten-Schutz-Gesetz (PDSG)

Das Patientendaten-Schutz-Gesetz (PDSG) gilt seit Oktober 2020. Es ergänzt das Digitale-Versorgung-Gesetz (DVG) und definiert den verbindlichen Rechtsrahmen für die sichere Einführung und Nutzung der elektronischen Patientenakte (ePA) sowie digitaler Anwendungen im Gesundheitswesen. Das Gesetz verfolgt zwei zentrale Ziele: die Stärkung der digitalen Souveränität der Patient*innen sowie den umfassenden Schutz ihrer besonders sensiblen Gesundheitsdaten.

Im Mittelpunkt des PDSG steht die Verpflichtung der gesetzlichen Krankenkassen, allen Versicherten eine elektronische

Patientenakte bereitzustellen. Diese muss über fein abgestufte Zugriffsrechte verfügen, die von den Patient*innen selbst verwaltet und kontrolliert werden können. Ergänzend regelt das PDSG die Anforderungen an den Einsatz telemedizinischer Verfahren, die Nutzung elektronischer Rezepte (E-Rezepte), digitaler Identitäten sowie den strukturierten und sicheren Datenaustausch zwischen Leistungserbringenden darunter Ärzt*innen, Kliniken und Apotheken.

2.3 Sozialgesetzbuch (SGB V)

Das Sozialgesetzbuch bildet die rechtliche Grundlage für das deutsche Sozialversicherungssystem. Es ist in mehrere Bücher gegliedert, die unter anderem die gesetzliche Kranken-, Renten- und Unfallversicherung sowie Leistungen für Kinder, Jugendliche und Menschen mit Beeinträchtigungen regeln. Auch wenn das SGB primär sozialrechtliche Aufgaben verfolgt, enthält es in verschiedenen Bereichen datenschutzrechtlich relevante Vorgaben. Diese betreffen insbesondere den Umgang mit personenbezogenen Daten in der Gesundheitsversorgung und sind bei entsprechenden Verarbeitungen zu berücksichtigen.

Besonders relevant sind die IT-sicherheitsrechtlichen Spezialvorschriften des SGB V: § 391 SGB V verpflichtet Krankenhäuser zur Umsetzung der BSI-Mindeststandards sowie branchenspezifischer Sicherheitsvorgaben, während § 393 SGB V den sicheren Einsatz von Cloud-Diensten regelt und nur zertifizierte Anbieter mit Datenspeicherung innerhalb der EU zulässt.

Tab. 4 SGB V

Normen	Inhalte
§ 391 SGB V	IT-Sicherheit in Krankenhäusern (BSI-Mindeststandards, branchenspezifische Sicherheitsvorgaben)
§ 393 SGB V	Cloud-Einsatz im Gesundheitswesen (zertifizierte Anbieter, EU-Speicherort)

2.4 Digitale-Versorgung-Gesetz (DVG)

Das Digitale-Versorgung-Gesetz (DVG) bildet die Grundlage für die Einführung digitaler Gesundheitsanwendungen in die Regelversorgung. Es schafft den rechtlichen Rahmen, damit auch KI-basierte Anwendungen erstattet werden können, sofern sie einen nachweisbaren Patient*innenrelevanten Nutzen erbringen.

Damit eröffnet das DVG den Zugang zu digitalen Präventions- und Therapieangeboten, stellt jedoch zugleich hohe Anforderungen an Datenschutz, Informationssicherheit und Interoperabilität. Nur Anwendungen, die diese Vorgaben erfüllen, können in das Versorgungssystem aufgenommen werden.

2.5 Digitale-Versorgung-und-Pflege-Modernisierung-Gesetz (DVPMG)

Das Digitale-Versorgung-und-Pflege-Modernisierung-Gesetz (DVPMG) baut auf den Regelungen des DVG auf und erweitert dessen Anwendungsbereich, insbesondere auf die pflegerische Versorgung. Es stärkt die Nutzung der elektronischen Patientenakte (ePA) und des E-Rezepts und schafft zusätzliche Einsatzmöglichkeiten für digitale und KI-gestützte Anwendungen.

Dazu zählen unter anderem die Analyse von Verlaufsdaten sowie der Einsatz digitaler Pflegeanwendungen (DiPA). Für KI-Systeme bedeutet dies eine stärkere Einbindung in medizinische und pflegerische Prozesse. Gleichzeitig verlangt das DVPMG Transparenz, Nachvollziehbarkeit und eine klare Verantwortungszuordnung, um die ärztliche und pflegerische Entscheidungsbefugnis nicht zu beeinträchtigen.

2.6 Telekommunikation-Telemedien-Datenschutz-Gesetz (TDDDG)

Das Telekommunikation-Telemedien-Datenschutz-Gesetz (TDDDG), das seit Mai 2024 gilt, regelt die Vertraulichkeit in Telekommunikation und Telemedien. Es ist besonders relevant für KI-gestützte Telemedizin und digitale Gesundheitsanwendungen, die Kommunikations- oder Nutzungsdaten verarbeiten. Das Gesetz legt klare Grenzen für die Erhebung, Speicherung und Analyse solcher Daten fest. Tracking, Profilbildung

und vergleichbare Auswertungen sind nur mit ausdrücklicher Einwilligung zulässig. Auf diese Weise verhindert das TDDDG verdeckte oder unkontrollierte Datenanalysen in digitalen Gesundheitsportalen, Chatbots und telemedizinischen Plattformen.

Tab. 5 TDDDG

Normen	Inhalte
§ 3 TDDDG	Anforderungen an Sicherheit, Funktionstüchtigkeit, Qualität und Interoperabilität
§ 4 TDDDG	Anforderungen an Datenschutz und Datensicherheit
§ 5 TDDDG	Nachweis positiver Versorgungseffekte
§ 7 TDDDG	Anforderungen an die Bewertung durch das BfArM

2.7 Digitale-Gesundheitsanweisungen-Verordnungen (DiGAV)

Die Digitale-Gesundheitsanweisungen-Verordnung (DiGAV) konkretisiert die Vorgaben des Digitale-Versorgung-Gesetzes (DVG) und regelt das Verfahren zur Aufnahme digitaler Gesundheitsanwendungen (DiGA) in das offizielle Verzeichnis des Bundesinstituts für Arzneimittel und Medizinprodukte (BfArM). Die Verordnung ist am 21. April 2020 in Kraft getreten.

müssen einen medizinischen Zweck erfüllen, nicht invasiv und nicht diagnostisch sein und Patient*innen bei der Erkennung, Überwachung oder Behandlung von Krankheiten unterstützen. Die Verordnung stellt hierfür verbindliche Anforderungen an Datenschutz, Informationssicherheit, Interoperabilität und wissenschaftliche Evidenz.

Sie legt fest, unter welchen Voraussetzungen digitale Gesundheitsanwendungen – darunter Gesundheits-Apps und webbasierte Lösungen – erstattungsfähig sind. DiGAs

2.8 Patients' Rights Directive

Die Patients' Rights Directive (Richtlinie 2011/24/EU) gilt seit dem 9. März 2011 und regelt die grenzüberschreitende Gesundheitsversorgung innerhalb der Europäischen Union. Sie sichert Patient*innen das Recht, medizinische Leistungen auch in anderen EU-Mitgliedstaaten in Anspruch zu nehmen und die Kosten unter bestimmten Voraussetzungen erstatten zu lassen. Darüber hinaus verpflichtet die Richtlinie zu umfassender Transparenz hinsichtlich Qualitäts- und Sicherheitsstandards sowie zur Bereitstellung verständlicher Gesundheitsinformationen.

Ein zentrales Element ist die Zusammenarbeit der nationalen Gesundheitssysteme, unter anderem über nationale Kontaktstellen, die Patient*innen bei grenzüberschreitenden Behandlungen unterstützen. Für KI-basierte Gesundheitsanwendungen ist die Richtlinie relevant, wenn digitale Dienste oder Informationen länderübergreifend nutzbar sind und damit in den Anwendungsbereich der grenzüberschreitenden Versorgung fallen.

2.9 Gesundheitsdatennutzungsgesetz (GDNG)

Das Gesundheitsdatennutzungsgesetz (GDNG) ist am 26. März 2024 in Kraft getreten und bildet den nationalen Rechtsrahmen für die Sekundärnutzung von Gesundheitsdaten zu Forschungszwecken, zur Qualitätssicherung und zur Weiterentwicklung des Gesundheitswesens.

Besondere Schutzmechanismen ergeben sich aus dem Forschungsgeheimnis (§§ 7–9 GDNG), das die unbefugte Nutzung oder Weitergabe von Forschungsdaten sanktioniert und strenge organisatorische und technische Sicherheitsanforderungen vorsieht. Zudem besteht eine Pflicht zur Registrierung und Veröffentlichung von Forschungsvorhaben (§ 8 GDNG). Eine wesentliche Neuerung ist die Opt-out-Regelung: Daten aus der elektronischen Patientenakte dürfen für Forschungszwecke genutzt werden, sofern die betroffene Person nicht widersprochen hat.

Das Gesetz wird schrittweise umgesetzt, der vollständige Aufbau des Forschungsdatenökosystems erstreckt sich voraussichtlich bis 2026/2027.

Zentrale Instrumente des Gesetzes sind das Forschungsdatenzentrum Gesundheit (FDZ) sowie die beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) angesiedelte Datenzugangs- und Koordinierungsstelle. Diese koordinieren die Bereitstellung pseudonymer Gesundheitsdaten und prüfen Anträge auf Datennutzung, führen Daten aus verschiedenen Registern zusammen und stellen sichere Verarbeitungs-umgebungen bereit.

Für KI-Anwendungen schafft das GDNG eine wichtige Grundlage: Durch strukturierten, qualitätsgesicherten und pseudonymisierten Datenzugang können KI-Systeme entwickelt, trainiert, validiert und zur Verbesserung diagnostischer und prädiktiver Verfahren eingesetzt werden. Dabei gelten weiterhin die DSGVO, das BDSG, die Regeln des Forschungsgeheimnisses und – künftig – die Anforderungen des EU AI Act, insbesondere im Hinblick auf Datenqualität, Sicherheitsstandards und Re-Identifizierungsrisiken.

Nach § 6 GDNG ist die Verarbeitung von Gesundheitsdaten unter bestimmten Voraussetzungen auch ohne individuelle Einwilligung zulässig, insbesondere zu wissenschaftlichen Forschungszwecken, zur Gesundheitsberichterstattung oder zur Qualitätssicherung des Gesundheitswesens.

2.10 Krankenhausgestaltungsgesetz NRW (KHGG NRW)

Das Krankenhausgestaltungsgesetz Nordrhein-Westfalen (KHGG NRW) bildet die zentrale landesrechtliche Grundlage für die Planung, Struktur und Förderung der Krankenhäuser in Nordrhein-Westfalen. Es regelt insbesondere die Aufstellung des Krankenhausplans, legt Versorgungsaufträge fest und definiert die Voraussetzungen für die Vergabe von Investitionsmitteln.

Ziel des Gesetzes ist eine bedarfsgerechte, leistungsfähige und zukunftsfähige Krankenhausversorgung.

Mit dem Fünften Gesetz zur Änderung des KHGG NRW vom 11. Februar 2025 wurden unter anderem die Regelungen zum Nachweis freier Behandlungskapazitäten (§ 10), zur Rechtsaufsicht (§ 11) sowie zur Investitionsförderung (§§ 20, 21) angepasst. Die novellierten Vorgaben präzisieren die Meldepflichten der Krankenhäuser gegenüber den Leitstellen und schaffen zusätzliche Flexibilität bei der Finanzierung und Absicherung von Investitionen, insbesondere im Zusammenhang mit Schließungen und Insolvenzsituationen.

Tab. 6 KHGG NRW

Normen	Inhalte
§10 KHGG NRW	<ul style="list-style-type: none"> Nachweis freier Behandlungskapazitäten und Meldung der Auslastung an die einheitlichen Leitstellen nach dem Rettungsgesetz NRW Grundlage für die Steuerung des Belegungsmanagements sowie die Bewältigung von Großereignissen und Katastrophen
§34 c KHGG NRW	<ul style="list-style-type: none"> Sicherung und Aufbewahrung von Patientenunterlagen (analog und digital) auch im Fall einer drohenden Schließung des Krankenhauses Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit sowie Wahrung der Rechte der Patientinnen und Patienten Regelmäßiger Nachweis der getroffenen Sicherungsmaßnahmen gegenüber der Aufsichtsbehörde

Das KHGG NRW integriert damit datenschutz- und informationssicherheitsrelevante Anforderungen in das Krankenhausrecht und stärkt die Verantwortung der Krankenhausträger für Datenverfügbarkeit und die Nachvollziehbarkeit klinischer Dokumentation. Zugleich bildet es im Zusammenspiel mit dem bundesrechtlichen Krankenhauszukunftsgesetz eine rechtliche Grundlage für die technische und digitale Modernisierung der Krankenhauslandschaft in Nordrhein-Westfalen.

2.11 Krankenhauszukunftsgesetz-Durchführungsverordnung NRW (KHZG-DVO NRW)

Die Krankenhauszukunftsgesetz-Durchführungsverordnung Nordrhein-Westfalen (KHZG-DVO NRW) konkretisiert die landesrechtlichen Vorgaben zur Umsetzung des bundesweiten Krankenhauszukunftsgesetzes und regelt die Voraussetzungen für die Bewilligung von Fördermitteln, das Verfahren zur Antragstellung, die sachgerechte Mittelverwendung sowie die Dokumentations- und Prüfpflichten der Krankenhäuser.

Gefördert werden auf Grundlage des bundesrechtlichen KHZG insbesondere Projekte wie digitale Notaufnahmen, Patientenportale, IT-Sicherheitsmaßnahmen, elektronische Dokumentationssysteme und telemedizinische Anwendungen.

Ein zentraler Bestandteil der KHZG-DVO NRW sind die umfangreichen Nachweis- und Berichtspflichten. Krankenhäuser müssen belegen, dass die gewährten Fördermittel zweckentsprechend eingesetzt wurden und die geplanten Maßnahmen

ordnungsgemäß umgesetzt wurden. Dazu gehören regelmäßige Sachstandsberichte, Nachweise zur Zielerreichung sowie zur Einhaltung technischer und organisatorischer Spezifikationen. Darüber hinaus enthält die Verordnung Vorgaben zur Aufbewahrung relevanter Unterlagen sowie zur Prüfung der geförderten Maßnahmen durch das Land Nordrhein-Westfalen.

Insgesamt schafft die KHZG-DVO NRW einen verbindlichen rechtlichen Rahmen für die digitale Transformation der Krankenhauslandschaft in Nordrhein-Westfalen. Sie unterstützt Krankenhäuser gezielt bei der Modernisierung ihrer IT- und Kommunikationssysteme und schafft einen verbindlichen Rahmen für den Einsatz der Fördermittel, einschließlich der Nachweis- und Dokumentationspflichten.



Merktafel

Europäischer Gesundheitsdatenraum (EHDS):

- Regelt EU-weit den sicheren Austausch und die Nutzung elektronischer Gesundheitsdaten
- Patient*innen erhalten digitale Zugriffs- und Kontrollrechte
- Nutzung nur für Versorgung, Forschung, Innovation und öffentliche Gesundheit
- Werbung und Profilbildung sind verboten
- Umsetzung schrittweise bis 2034

Patientendaten-Schutz-Gesetz (PDSG):

- Krankenkassen müssen ePA bereitstellen; Patient*innen steuern Zugriffsrechte selbst
- Regelt Telemedizin, E-Rezepte, digitale Identitäten und schützt Gesundheitsdaten

Sozialgesetzbuch V (SGB V):

- Für KRITIS-Krankenhäuser gelten verpflichtend die BSI-Mindeststandards zur IT-Sicherheit (§ 391 SGB V)
- Cloud-Anbieter müssen zertifiziert sein und Daten in der EU speichern (§ 393 SGB V)

Digitale-Versorgung-Gesetz (DVG):

- Erlaubt Erstattung digitaler Gesundheitsanwendungen (DiGA)
- Apps müssen Datenschutz, Interoperabilität und Nutzen nachweisen

Digitale-Versorgung-und-Pflege-Modernisierungsgesetz (DVPMG):

- Erweiterung des DVG auf Pflege und digitale Pflegeanwendungen (DiPA)
- KI-Nutzung zulässig, sofern Transparenz und Verantwortlichkeit gewährleistet sind

Telekommunikation-Telemedien-Datenschutz-Gesetz (TDDDG):

- Schützt Kommunikations- und Nutzungsdaten in Telemedizin
- Tracking und Profilbildung nur mit Einwilligung

Digitale-Gesundheitsanwendungen-Verordnung (DiGAV):

- Regelt Zulassung und Erstattung von DiGA über das BfArM
- Anforderungen: Datenschutz, Sicherheit, Interoperabilität, Evidenz

Patients' Rights Directive (EU):

- Sichert grenzüberschreitende Gesundheitsversorgung und Kostenerstattung
- Verlangt Transparenz zu Qualitäts- und Sicherheitsstandards

Gesundheitsdatennutzungsgesetz (GDNG):

- Erlaubt Sekundärnutzung von Gesundheitsdaten für Forschung auch ohne Einwilligung (§ 6 GDNG)
- Enthält Opt-out-Regelung für ePA-Daten (§ 14 GDNG)
- Forschung unterliegt strengen Pseudonymisierungs- und Geheimhaltungspflichten

Krankenhausgestaltungsgesetz (KHGG NRW):

- Digitale Meldung freier Behandlungskapazitäten (§ 10 KHGG NRW)
- Vorgaben zur sicheren digitalen Aufbewahrung von Patientenunterlagen (§ 34c KHGG NRW)

Krankenhauszukunftsgesetz-Durchführungsverordnung NRW (KHZG-DVO NRW):

- Regelt Förderung digitaler Krankenhausprojekte in NRW
- Fördermittel müssen zweckentsprechend und nachweisbar eingesetzt werden



3. KI / Digitalisierung

Mit dem zunehmenden Einsatz digitaler Technologien und Künstlicher Intelligenz (KI) im Gesundheitswesen steigen die Anforderungen an Sicherheit, Transparenz und rechtliche Kontrolle. Europäische und nationale Regelungen schaffen hierfür einen verbindlichen Rahmen, der Innovation ermöglicht und zugleich Grundrechte, Datenschutz und Patient*innensicherheit sicherstellt.

3.1 EU Artificial Intelligence Act (EU AI Act)

Der EU AI Act ist am 1. August 2024 in Kraft getreten. Seine Anwendung erfolgt gestaffelt: Erste Transparenzpflichten und Verbote bestimmter KI-Praktiken gelten ab dem 2. Februar 2025. Die Pflichten für generative KI-Modelle (GPAI) treten ab dem 2. August 2025 in Kraft – für bereits zuvor in Verkehr gebrachte Modelle gelten verlängerte Übergangsfristen bis 2027. Die Vorgaben für Hochrisiko-KI-Systeme gelten ab dem 2. August 2026. Eine zusätzliche Übergangsfrist für die Einstufung nach Art. 6 Abs. 1 gilt bis zum 2. August 2027.

Die Europäische Kommission wird zwischen 2025 und 2027 mehrere delegierte Rechtsakte und Implementing Acts veröffentlichen, die technische Detailanforderungen, Meldepflichten, Leitlinien zur Risikoklassifizierung und Dokumentationsstandards weiter präzisieren. Die vollständige Anwendung des AI Act hängt daher auch von diesen ergänzenden Rechtsakten ab.

Der AI Act schafft erstmals einen verbindlichen europäischen Rechtsrahmen für die Entwicklung und Nutzung von KI-Systemen. Von zentraler Bedeutung ist die Risikoklassifizierung. KI-Anwendungen im Gesundheitswesen – etwa in Diagnostik, Therapie oder klinischer Entscheidungsunterstützung – gelten in der Regel als Hochrisiko-Systeme und unterliegen strengen Anforderungen. Sie sind in einer zentralen EU-Datenbank zu registrieren und müssen vor ihrer Inbetriebnahme ein Konformitätsbewertungsverfahren durchlaufen.

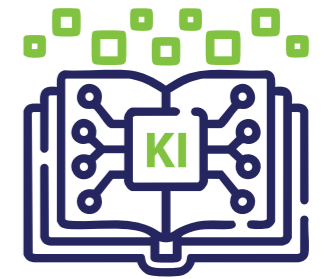
Der AI Act verpflichtet Anbieter und Betreiber zu umfangreichen Maßnahmen. Dazu zählen ein Risikomanagementsystem (Art. 9 EU AI Act), Anforderungen an Datenqualität und Daten-

Governance (Art. 10 EU AI Act), eine vollständige technische Dokumentation (Art. 11 EU AI Act) sowie lückenlose Aufzeichnungen (Art. 12 EU AI Act). Nach Art. 13 EU AI Act müssen Informationen zur Funktionsweise, Leistung und zu den Beschränkungen der Systeme transparent offengelegt werden. Ein Anbieter nach dem EU AI Act ist die natürliche oder juristische Person, die ein KI-System entwickelt oder entwickeln lässt und es anschließend unter eigenem Namen oder eigener Marke in Verkehr bringt. Ein Betreiber ist die Stelle, die ein KI-System in eigener Verantwortung einsetzt und dessen Anwendung im praktischen Betrieb steuert, etwa ein Krankenhaus, das eine KI-Lösung im klinischen Alltag verwendet.

Einzelheiten zur technischen Dokumentation und zu den Anforderungen an Trainings- und Testdaten werden zusätzlich durch künftige Implementing Acts konkretisiert werden.

Ein zentrales Prinzip ist die menschliche Aufsicht. Art. 14 EU AI Act schreibt vor, dass KI-Systeme nicht ohne menschliche Kontrolle betrieben werden dürfen. Die letztverantwortliche Entscheidung verbleibt stets bei einer natürlichen Person; vollautomatisierte Letztentscheidungen sind unzulässig. Art. 15 EU AI Act ergänzt dies durch Anforderungen an Genauigkeit, Robustheit und Cybersicherheit.

Art. 7 EU AI Act verbietet irreführende Angaben zu Zweck, Funktion oder Leistungsfähigkeit eines KI-Systems.



Ein Beispiel für eine MDR-konforme Formulierung:

„Unsere App unterstützt die ärztliche Beurteilung von Hautveränderungen durch eine KI-gestützte Voranalyse. Die abschließende Diagnose trifft ein Facharzt*innen.“

Für medizinische Hochrisiko-Systeme fordert Art. 61 EU AI Act eine klinische Bewertung, die Sicherheit, Leistungsfähigkeit und klinischen Nutzen nachweist. Vor dem Marktzugang ist eine Konformitätsbewertung nach Art. 43 EU AI Act durchzuführen, sie erfolgt durch eine benannte Stelle und endet mit der CE-Kennzeichnung.

Auch für klinische Bewertungsanforderungen werden bis 2027 weitere Durchführungsrechtsakte erwartet, insbesondere zur Harmonisierung mit der MDR.

Auch im laufenden Betrieb gelten umfangreiche Pflichten. Betreiber müssen ein kontinuierliches Risikomanagement sowie ein Post-Market-Monitoring etablieren. Schwere Vorfälle sind gemäß Art. 73 EU AI Act innerhalb festgelegter Fristen zu melden: in der Regel innerhalb von 15 Tagen, bei Todesfällen innerhalb von 10 Tagen und in besonders gravierenden Fällen innerhalb von 2 Tagen; eine Vorabmeldung ist zulässig. Die konkreten Meldeformate, Schwellenwerte und technischen Übermittlungspflichten werden durch Implementing Acts weiter ausgestaltet.

Verstöße können nach Art. 112 EU AI Act mit erheblichen Bußgeldern geahndet werden.

Der AI Act basiert auf ethischen Grundprinzipien wie Transparenz, Fairness, Sicherheit, menschlicher Aufsicht und Diskriminierungsfreiheit. Praktiken wie Social Scoring sind ausdrücklich verboten.

Der AI Act ist eng mit dem Data Act verzahnt (siehe Punkt 1.6.1). Während der Data Act den Zugang zu Daten – insbesondere IoT-Daten – regelt, bestimmt der AI Act die Bedingungen für Entwicklung und Einsatz von KI-Systemen. Werden IoT-Daten aus dem Data Act als Trainingsdaten verwendet, gelten zusätzlich die Vorgaben des AI Act zu Datenqualität, Repräsentativität und Dokumentation. Beide Verordnungen wirken ergänzend zur DSGVO; personenbezogene Daten dürfen weiterhin nur auf einer rechtmäßigen Grundlage verarbeitet werden.

Die vollständige Wirksamkeit des AI Act wird schrittweise bis 2027 erreicht. Einrichtungen im Gesundheitswesen sollten daher frühzeitig eine integrierte Compliance-Strategie für Daten- und KI-Regelungen entwickeln.

Dabei ist zu berücksichtigen, dass zentrale Pflichten erst mit Veröffentlichung der Implementing Acts rechtssicher anwendbar werden und Compliance-Systeme deshalb flexibel anpassbar bleiben müssen.

Praxisbezug:

Risikoklassifizierung vor Projektstart:

- Frühzeitige Prüfung, ob die Anwendung als Hochrisiko-System einzustufen ist
- Dokumentation der Einstufung anhand von Anhang III AI Act

Technische Dokumentation:

- Erstellung vollständiger Unterlagen (Systemarchitektur, Modellbeschreibung, Trainingsdaten)
- Vorbereitung der Konformitätsbewertung nach Art. 43 EU AI Act

Data-Governance:

• Etablierte Prozesse zur Auswahl, Prüfung und Dokumentation von Trainingsdaten nach Art. 10 EU AI Act bilden:

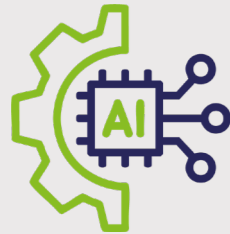
- Quellenangaben der Daten (Nachvollziehbarkeit, woher die Daten kommen: klinische Studie, Patientenakten, öffentliche Datensätze; DSGVO-Konformität sicherstellen)
- Maßnahmen zur Bias-Reduktion (z. B. dokumentierte Fairness-Analyse und Gegenmaßnahmen)
- Prüfung auf Repräsentativität (Werden alle relevanten Patientengruppen abgebildet? Analyse der Verteilung)
- Aktualitätsbewertung (Review-Prozess zur kontinuierlichen Bewertung der Aktualität der Daten)

Menschliche Aufsicht:

- Rollen- und Prozessbeschreibungen definieren, wer für die Überwachung des KI-Systems im Klinikalltag zuständig ist

Vorbereitung auf Meldepflichten:

- Aufbau von Prozessen, um Vorfälle gemäß Art. 73 EU AI Act frühzeitig zu erkennen und zu melden



Verhältnis zwischen EU AI Act und MDR:

KI-basierte Medizinprodukte unterliegen einer doppelten Regulierung. Sie müssen sowohl die Anforderungen der MDR (Produktsicherheit, klinische Bewertung, CE-Kennzeichnung) als auch die Pflichten des EU AI Act erfüllen. Der AI Act stuft medizinische KI-Anwendungen grundsätzlich als Hochrisiko-KI-Systeme ein, sodass Hersteller neben der MDR-Konformitätsbewertung zusätzlich ein KI-spezifisches Risikomanagement, Datenqualitätsanforderungen, technische Dokumentation und Transparenzpflichten erfüllen müssen. Ein Hersteller im Sinne der MDR ist jede natürliche oder juristische Person, die ein Medizinprodukt entwickelt, herstellt, verpackt oder unter ihrem Namen in Verkehr bringt und damit die Verantwortung für dessen Sicherheit, Leistungsfähigkeit und Konformität übernimmt. Die Konformitätsbewertung nach MDR und AI Act wird künftig eng verzahnt, da der AI Act eine Integration der KI-Anforderungen in bestehende MDR-Prozesse vorsieht. Die vollständige Harmonisierung beider Regelwerke wird bis 2027 durch Implementing Acts konkretisiert.

3.2 Produkthaftungsrichtlinie (PLD)

Die Produkthaftungsrichtlinie (2024/2853) wurde im März 2024 verabschiedet und modernisiert erstmals seit 1985 den europäischen Haftungsrahmen. Sie bezieht Software, KI-Systeme und digitale Komponenten ausdrücklich in den Produktbegriff ein.

Hersteller haften künftig nicht nur für physische, sondern auch für digitale Produktmängel, etwa fehlerhafte Algorithmen, unzureichende Sicherheitsmechanismen oder fehlende Updates. Gerichte können Beweisvermutungen zugunsten geschädigter Personen anstellen, insbesondere wenn technische Komplexität oder unzureichende Herstellerinformationen den Nachweis erschweren.

3.3 Arbeitnehmervertretung und KI-Einsatz

Der Einsatz von KI am Arbeitsplatz unterliegt der Mitbestimmung. Nach § 87 Abs. 1 Nr. 6 BetrVG hat der Betriebsrat ein zwingendes Mitbestimmungsrecht, wenn technische Einrichtungen eingesetzt werden, die Verhalten oder Leistung der Beschäftigten überwachen können. Da KI-Systeme Arbeitsabläufe, Leistungsbewertungen oder Entscheidungsprozesse beeinflussen können, ist ihre Einführung grundsätzlich mitbestimmungspflichtig.

Die 2021 eingeführte KI-Novelle des BetrVG verpflichtet Arbeitgeber, den Betriebsrat bei der Einführung, Anwendung

und Bewertung von KI-Systemen sachkundig zu unterstützen (§ 80 Abs. 3 BetrVG). Der Betriebsrat kann hierzu externe Sachverständige hinzuziehen.

Für Hersteller und Betreiber von KI-Systemen im Gesundheitswesen bedeutet dies umfassende Pflichten über den gesamten Lebenszyklus: Sicherstellung der Systemstabilität, Bereitstellung von Updates, Dokumentation von Änderungen sowie zügige Behebung von Sicherheitsproblemen. Krankenhäuser und Forschungseinrichtungen müssen den Einsatz ihrer KI-Systeme regelmäßig prüfen und Beschäftigte entsprechend schulen.

Die Richtlinie muss bis zum 9. Dezember 2026 in nationales Recht umgesetzt werden und gilt danach verbindlich für alle neuen Produkte und Softwareversionen.

Ziel ist es, Transparenz, Datenschutz und die Wahrung der Persönlichkeitsrechte der Beschäftigten sicherzustellen und sie auf den technologischen Wandel vorzubereiten.

3.4 Data Governance Act (DGA)

Der Data Governance Act (DGA) ist am 23. Juni 2022 in Kraft getreten und gilt seit September 2023 unmittelbar in allen EU-Mitgliedstaaten. Er bildet einen zentralen Bestandteil der europäischen Datenstrategie und schafft einen Rahmen für eine sichere, faire und vertrauenswürdige Datennutzung.

Der DGA fördert die Wiederverwendung geschützter öffentlicher Daten, regelt die Tätigkeit von Datenmittlern und schafft den rechtlichen Rahmen für Datenaltruismus – also die freiwillige Bereitstellung personenbezogener Daten zu gemeinwohlorientierten Zwecken. Die Verordnung stärkt zudem die Kontrolle betroffener Personen über ihre Daten und verpflichtet Datenmittler zu Neutralität, Datenschutz und Informationssicherheit. Zusätzlich enthält sie Schutzmechanismen gegen unrechtmäßigen Drittstaatenzugriff.

Für den Gesundheitssektor ist der DGA von besonderer Bedeutung. Er ermöglicht eine vertrauenswürdige Sekundärnutzung von Gesundheitsdaten für Forschung und Innovation. Krankenhäuser, Forschungseinrichtungen und Gesundheitsplatt-

formen können Daten bereitstellen, sofern sie die strengen Transparenz-, Sicherheits- und Schutzanforderungen erfüllen. Dadurch entstehen neue Möglichkeiten zur Entwicklung und Validierung von KI-Systemen, ohne die Grundrechte der Patient*innen zu gefährden.

Insgesamt stärkt der DGA den Aufbau einer europäischen Datenökonomie und schafft neue Handlungsspielräume, um Gesundheits- und Forschungsdaten rechtssicher und patientenorientiert zu nutzen.

Der DGA wirkt zudem als flankierende Regelung zum European Health Data Space (EHDS). Während der EHDS den sektoralen Rahmen für die Primär- und Sekundärnutzung von Gesundheitsdaten schafft, legt der DGA die übergreifenden Mechanismen für Datenmittler, Datenaltruismus und den sicheren Datenaustausch fest. Beide Verordnungen ergänzen sich und bilden gemeinsam die Grundlage für eine interoperable und vertrauenswürdige europäische Gesundheitsdateninfrastruktur.



Merktafel

EU Artificial Intelligence Act (EU AI Act):

- Seit 1. August 2024 in Kraft, gestaffelte Anwendung bis 2027
- Verbote unzulässiger KI-Praktiken ab Februar 2025, generative KI ab August 2025, Hochrisiko-KI ab August 2026
- Hochrisiko-KI-Systeme müssen registriert und einer Konformitätsbewertung unterzogen werden, die in der Regel mit einer CE-Kennzeichnung abschließt
- Social Scoring und manipulative KI sind verboten
- Trainingsdaten müssen hochwertig, repräsentativ und dokumentiert sein
- KI darf nicht ohne menschliche Aufsicht eingesetzt werden
- Betreiber müssen Risikomanagement, Überwachung und Meldeprozesse einrichten
- Verstöße können zu hohen Bußgeldern führen
- Der Data Act regelt den Datenzugang (insbesondere IoT-Daten) und wirkt ergänzend zum AI Act, der die Entwicklung und Nutzung von KI-Systemen reguliert.

Produkthaftungsrichtlinie (PLD)

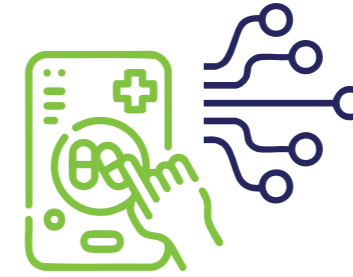
- Gilt für Software, KI-Systeme und digitale Produkte
- Hersteller haften auch für digitale Fehler und mangelhafte Updates
- Sicherheits- und Dokumentationspflichten über den gesamten Lebenszyklus
- Umsetzung in nationales Recht bis 9. Dezember 2026

Arbeitnehmerschutz & KI

- Der Betriebsrat hat Mitbestimmungsrechte beim Einsatz von KI
- KI darf nicht zur verdeckten Überwachung genutzt werden
- Der Betriebsrat kann Sachverständige für KI hinzuziehen
- Ziel ist eine faire, transparente und rechtskonforme Nutzung von KI am Arbeitsplatz sowie die Wahrung der Persönlichkeitsrechte der Beschäftigten.
- Arbeitgeber müssen den Betriebsrat bei der Einführung und Anwendung von KI sachkundig unterstützen (§ 80 Abs. 3 BetrVG)

Data Governance Act (DGA)

- Gilt seit September 2023
- Ziel: Vertrauenswürdige Datennutzung und Förderung der Datenweitergabe in der EU
- Regelt Wiederverwendung geschützter öffentlicher Daten, Datenmittler und Datenaltruismus
- Stärkt Transparenz, Neutralität und Datenschutz bei Datenaustauschdiensten
- Enthält Schutzmechanismen gegen unrechtmäßige Drittstaatenzugriffe
- Ermöglicht rechtssichere Sekundärnutzung von Gesundheitsdaten für Forschung und KI
- Der DGA ergänzt den EHDS, indem er sektorübergreifende Mechanismen für Datenmittler, Datenaltruismus und sicheren Datenaustausch bereitstellt



4. Medizin / Produkte / Arzneimittel

Für Arzneimittel, Medizinprodukte und klinische Prüfungen gelten in der Europäischen Union und in Deutschland umfassende regulatorische Vorgaben. Sie gewährleisten Sicherheit, Qualität und Wirksamkeit medizinischer Produkte und stellen eine rechtskonforme Forschungspraxis sicher. Diese Regelwerke bilden zugleich die Grundlage für eine vertrauenswürdige Nutzung digitaler und KI-gestützter Technologien im Gesundheitswesen.

4.1 Medical Device Regulation (MDR)

Die Verordnung (EU) 2017/745 über Medizinprodukte (Medical Device Regulation, MDR) gilt seit dem 26. Mai 2021 unmittelbar in allen EU-Mitgliedstaaten. Sie legt umfassende Anforderungen an Sicherheit, Leistungsfähigkeit und Marktüberwachung von Medizinprodukten fest – einschließlich Software und KI-Systemen mit medizinischer Zweckbestimmung. Ziel ist ein hohes Maß an Patientensicherheit, Transparenz und Qualität sowie die Förderung verantwortungsvoller Innovation.

Der Anwendungsbereich der MDR umfasst alle Produkte, die zu medizinischen Zwecken in Verkehr gebracht werden. Die Klassifizierung erfolgt risikobasiert nach Anhang VIII. Besonders relevant ist Regel 11, die Software betrifft. KI-Anwendungen in Diagnostik, Therapie oder Überwachung werden häufig höheren Risikoklassen (IIa, IIb oder III) zugeordnet, da sie direkten Einfluss auf medizinische Entscheidungen haben.

Hersteller müssen gemäß Art. 5 und 10 MDR nachweisen, dass ihr Produkt die grundlegenden Sicherheits- und Leistungsanforderungen erfüllt. Dazu gehören Risikominimierung, Fehlererkennung, Reproduzierbarkeit der Ergebnisse und Maßnahmen gegen algorithmische Verzerrungen (Bias). Art. 61 MDR verlangt eine klinische Bewertung, die Sicherheit, Leistungsfähigkeit und klinischen Nutzen belegt. Diese kann sowohl auf retrospektiven Daten als auch auf prospektiven Studien beruhen. Zur Sicherstellung der kontinuierlichen Produktsicherheit

schreibt Art. 83 MDR ein Post-Market-Surveillance-System vor, in dessen Rahmen Vorfälle gemeldet, Anwendungsdaten ausgewertet und gegebenenfalls Korrekturmaßnahmen durchgeführt werden. Art. 7 untersagt irreführende Angaben zu Zweck, Funktion und Wirksamkeit. KI-gestützte Systeme müssen nachvollziehbar und erklärbar sein – gegenüber medizinischem Fachpersonal ebenso wie gegenüber Patient*innen.

Beispiel für MDR-konforme Kommunikation:

„Unsere App unterstützt die ärztliche Beurteilung von Hautveränderungen durch eine KI-gestützte Voranalyse. Die abschließende Diagnose trifft eine Fachärztin oder ein Facharzt.“

Nach Art. 52 MDR unterliegen KI-basierte Medizinprodukte – abhängig von ihrer Risikoklasse – einer Konformitätsbewertung durch eine benannte Stelle. Bei erfolgreicher Bewertung erfolgt die CE-Kennzeichnung, die den Marktzugang in der EU ermöglicht.

Der Zertifizierungsprozess unter der MDR umfasst im Wesentlichen folgende Schritte:

1. Risikoklassifizierung

Zunächst wird das Produkt gemäß Art. 51 in eine Risikoklasse (I, IIa, IIb, III) eingestuft abhängig von Zweck, Einsatzbereich und potenziellem Schaden im Fehlerfall.

2. Erstellung der technischen Dokumentation

Der Hersteller erstellt eine umfassende Dokumentation, in der u. a. Sicherheit, Leistungsfähigkeit, klinische Bewertung, Softwarearchitektur und Risikomanagement dargelegt sind.

3. Konformitätsbewertung

Je nach Klasse erfolgt eine Prüfung der Unterlagen durch eine benannte Stelle. Diese kann zusätzlich Produktprüfungen oder Audits durchführen (ab Klasse IIa zwingend).

4. CE-Kennzeichnung und Marktzugang

Bei erfolgreicher Prüfung wird eine CE-Kennzeichnung erteilt, die das Produkt zur Vermarktung in der EU berechtigt.

5. Post-Market-Surveillance (PMS)

Auch nach dem Inverkehrbringen müssen Hersteller ihre Produkte kontinuierlich überwachen, Zwischenfälle melden und ggf. Verbesserungen vornehmen (Art. 83). (Inverkehrbringen bedeutet die erstmalige Bereitstellung eines Medizinprodukts oder KI-Systems auf dem EU-Binnenmarkt, das heißt der Moment, in dem das Produkt einem Anwender oder einer Organisation erstmals kommerziell zur Verfügung gestellt wird).



Beispiele für KI-gestützte Medizinprodukte und Risikoklassen:

1. Dermanostic App - Klasse IIa nach Regel 11 MDR

Diese App erlaubt es Nutzern, Hautveränderungen per Foto digital einreichen zu lassen und erhält daraufhin eine ärztliche Diagnose. Da sie nicht selbstständig Entscheidungen trifft, sondern den ärztlichen Diagnoseprozess unterstützt, fällt sie vermutlich in Klasse IIa als ein aktives diagnostisches System mit mittlerem Risiko.

2. KI zur automatischen Tumorerkennung in MRT-Bildern – Klasse IIb oder III

Systeme, die selbstständig medizinisch relevante Auffälligkeiten identifizieren (z. B. potenziell maligne Tumoren), greifen direkt in die Diagnostik ein. Aufgrund der hohen Tragweite der Entscheidungen (z. B. Krebsdiagnose oder nicht) erfolgt in der Regel eine Einstufung in Klasse IIb oder sogar Klasse III, je nach Grad der Autonomie und Risiko.

3. Blutzucker-Vorhersagesystem für Diabetiker (z. B. KI in einem CGM-System) – Klasse IIb

Systeme, die Blutzuckerwerte kontinuierlich messen und mit KI vorhersagen, ob eine Hypoglykämie droht, sind therapierelevant. Aufgrund des Risikos durch Fehlalarme oder -prognosen wird meist Klasse IIb angenommen.

4.2 Medizinprodukte-Durchführungsgesetz (MPDG)

Das Medizinprodukte-Durchführungsgesetz (MPDG) gilt seit dem 26. Mai 2021 und ergänzt die MDR sowie die Verordnung (EU) 2017/746 über In-vitro-Diagnostika (IVDR) auf nationaler Ebene. Das MPDG regelt die Zuständigkeiten der Behörden, die Aufgaben der Ethikkommissionen, die Genehmigung und Überwachung klinischer Prüfungen sowie Melde- und Sanktionsverfahren.

Für Krankenhäuser, Forschungseinrichtungen und Hersteller KI-basierter Medizinprodukte konkretisiert das MPDG die rechtlichen Pflichten in klinischen Prüfungen, beim Umgang mit Sicherheitsvorfällen und in der Zusammenarbeit mit benannten Stellen. Besonders relevant sind:

Tab. 7 MPDG

Normen	Inhalte
§3 MPDG	Anwendungsbereich
§§4-8 MPDG	Ethikkommissionen und Genehmigung klinischer Prüfung
§16 MPDG	Pflichten des Prüfers in klinischen Prüfungen
§§33-35 MPDG	Beobachtungs- und Meldepflichten bei klinischer Prüfung
§40-42 MPDG	Zuständigkeiten der Behörden
§74 MPDG	Bußgeldvorschriften bei Verstößen

4.3 Arzneimittelgesetz (AMG)

Das Arzneimittelgesetz (AMG) regelt die Sicherheit, Qualität und Zulassung von Arzneimitteln in Deutschland. Zentrale Bestimmungen sind die Zulassungspflicht (§ 21 AMG), das Verbot bedenklicher Arzneimittel (§ 5 AMG), die Apothekenpflicht (§ 43 AMG) sowie die Straf- und Bußgeldvorschriften (§§ 94 ff.

AMG). Ziel ist der Schutz der öffentlichen Gesundheit und der sichere Umgang mit Arzneimitteln in Entwicklung, Herstellung und Anwendung.

4.4 EU Clinical Trials Regulation (CTR)

Die Clinical Trials Regulation (EU) 536/2014 gilt seit dem 31. Januar 2022 vollständig. Sie ersetzt die Richtlinie 2001/20/EG und harmonisiert die Genehmigung, Durchführung und Überwachung klinischer Prüfungen in der EU. Zentrales Instrument ist das Clinical Trials Information System (CTIS). Dieses Portal ermöglicht digitale Antragstellung, Genehmigungen und Meldungen.

Die CTR erhöht Transparenz und Patientenschutz, da alle Studienergebnisse veröffentlicht werden müssen. Sie gilt für neue klinische Prüfungen seit Januar 2022; bestehende Studien müssen spätestens bis Januar 2025 umgestellt sein. KI-Systeme fallen nur dann unter die CTR, wenn sie Teil des Prüfprodukts oder der Prüfmethode in einer Arzneimittelstudie sind.

Tab. 8 CTR

Normen	Inhalte
Art. 2 CTR	Begriffsbestimmungen
Art. 4 CTR	Einwilligung bei nichteinwilligungsfähigen Personen
Art. 5 CTR	Einwilligung bei Minderjährigen
Art. 6 CTR	Einwilligung bei schwangeren oder stillenden Frauen
Art. 25 CTR	Antrag auf Genehmigung klinischer Prüfung
Art. 49 CTR	Überwachung und Berichterstattung schwerwiegender unerwünschter Ereignisse
Art. 57 CTR	Vertraulichkeit und Datenschutz
Art. 73 ff. CTR	EU-Datenbank und Veröffentlichungspflichten
Art. 81 CTR	Übergangsbestimmungen

4.5 Heilmittelwerbe-gesetz (HWG)

Das Heilmittelwerbe-gesetz schützt Verbraucher*innen vor irreführender Werbung für Arzneimittel, Medizinprodukte und Heilverfahren. Kernregelungen umfassen das Irreführungsverbot (§ 3 HWG), Werbebeschränkungen für verschreibungspflichtige Arzneimittel und Krankengeschichten

(§ 11 HWG) sowie Einschränkungen bei Werbeaktionen, Gewinnspielen und Sonderangeboten (§ 12 HWG). Das HWG stellt sicher, dass medizinische Informationen sachlich, transparent und patientenschutzorientiert kommuniziert werden.

4.6 Medizinrecht

Das Medizinrecht umfasst sämtliche rechtlichen Anforderungen an medizinische Behandlung, Forschung und Digitalisierung. Mit dem Einsatz von KI in Diagnostik und Therapie entstehen erweiterte Anforderungen an Transparenz, Aufklärung und Einwilligung. Patient*innen müssen nachvollziehen können, wie KI-gestützte Entscheidungen zustande kommen. Ärzt*innen tragen weiterhin die Letztverantwortung und dürfen sich nicht ausschließlich auf KI-Systeme stützen.

mittelbar der Behandlung dienen (z. B. Training, Forschung, Modellverbesserung). Künftig schafft der Europäische Gesundheitsdatenraum hierfür eine einheitliche Grundlage. Ergänzend gelten die Vorgaben des EU AI Act zu Transparenz, Dokumentation und Diskriminierungsfreiheit.

Haftungsfragen sind im Wandel: Primär haftet weiterhin die behandelnde Person. Je nach Fallkonstellation können jedoch auch Hersteller oder Betreiber KI-basierter Systeme verantwortlich sein – insbesondere nach MDR und PLD (2024/2853).

Die informierte Einwilligung ist erforderlich, wenn Gesundheitsdaten für Zwecke verarbeitet werden, die nicht un-



Merktafel

Medical Device Regulation (MDR):

- Gilt seit 26. Mai 2021 verbindlich in allen EU-Mitgliedstaaten
- Regelt Sicherheit, Leistungsfähigkeit und Marktüberwachung aller Medizinprodukte, einschließlich KI-Software
- Einstufung von KI nach Risikoklassen I, IIa, IIb und III (Software nach Regel 11)
- Hersteller müssen eine klinische Bewertung durchführen und die Sicherheit und Wirksamkeit belegen
- Risikomanagement und Post-Market-Surveillance (Art. 83) sind verpflichtend
- KI-Entscheidungen müssen nachvollziehbar und erklärbar sein
- Irreführende Aussagen über Funktion oder Zweck sind verboten (Art. 7)
- Hochrisiko-Produkte benötigen eine Konformitätsbewertung durch eine benannte Stelle (Art. 52)
- CE-Kennzeichnung ist Voraussetzung für den Marktzugang in der EU
- Hersteller tragen Verantwortung für Sicherheit und ordnungsgemäße Anwendung
- KI-Medizinprodukte müssen zusätzlich die Hochrisiko-Pflichten des EU AI Act erfüllen (z. B. Art. 9–15, Art. 61 AI Act)

Medizinprodukte-recht-Durchführungsgesetz (MPDG):

- Ergänzt die MDR national Ebene seit 26. Mai 2021
- Regelt klinische Prüfungen, Ethikkommissionen, Marktüberwachung und Bußgelder
- Klinische Prüfungen mit Medizinprodukten bedürfen der Genehmigung durch eine Ethikkommission (§§ 4–8 MPDG)
- Prüfer und Einrichtungen müssen Sicherheits- und Meldepflichten erfüllen (§§ 33–35 MPDG)
- Verstöße können mit Bußgeldern (§ 74 MPDG) geahndet werden

Arzneimittel-gesetz (AMG):

- Regelt Zulassung, Herstellung, Qualität und Abgabe von Arzneimitteln
- Arzneimittel benötigen eine Zulassung nach § 21 AMG
- Bedenkliche Arzneimittel sind verboten (§ 5 AMG)
- Apothekenpflicht gilt für verschreibungspflichtige Medikamente (§ 43 AMG)
- Verstöße werden nach §§ 94 ff. AMG straf- oder bußgeldrechtlich verfolgt

EU Clinical Trials Regulation (CTR):

- Gilt seit 31. Januar 2022 für klinische Prüfungen mit Humanarzneimitteln
- Vereinheitlicht und digitalisiert Genehmigungen und Meldungen über das CTIS-Portal
- Veröffentlichung aller Studienergebnisse erforderlich (Art. 73 ff.)
- KI-gestützte Verfahren in Arzneimittelstudien fallen ebenfalls unter die CTR
- KI-Verfahren fallen nur dann unter die CTR, wenn sie Teil des Prüfprodukts oder der Prüfmethode in einer Arzneimittelstudie sind
- Bestehende Studien müssen bis Januar 2025 vollständig umgestellt sein

Heilmittelwerbe-gesetz (HWG):

- Schützt Verbraucher*innen vor irreführender oder unzulässiger Heilmittelwerbung
- Werbung für verschreibungspflichtige Arzneimittel ist verboten (§ 11 HWG)
- Irreführende Angaben zu Wirkung oder Erfolg sind untersagt (§ 3 HWG)
- Werbung mit Krankengeschichten oder Gewinnspielen ist eingeschränkt (§ 12 HWG)

Medizinrecht:

- Ärzt*innen behalten stets die medizinische Letztverantwortung bei KI-Einsatz
- Patient*innen müssen über den Einsatz und die Funktionsweise von KI aufgeklärt werden
- Eine Einwilligung ist nur erforderlich, wenn KI-Datenverarbeitung nicht unmittelbar der Behandlung dient (z. B. Training, Forschung)
- Der EHDS soll künftig eine einheitliche EU-Grundlage für Datennutzung schaffen
- Haftung kann neben Behandelnden auch Hersteller oder Betreiber treffen (nach MDR/PLD)
- KI-Systeme müssen transparente, diskriminierungsfreie und dokumentierte Entscheidungsprozesse aufweisen
- Bei medizinischer KI gilt stets die „doppelte Regulierung“: MDR und EU AI Act.



5. IT-Sicherheit / Cyber

Digitale Infrastrukturen im Gesundheitswesen gehören zu den besonders schutzbedürftigen Bereichen. Cyberangriffe oder IT-Ausfälle können die Patientenversorgung unmittelbar gefährden. Europäische und nationale Regelwerke verpflichten Krankenhäuser, Forschungseinrichtungen und Dienstleister daher zu wirksamen technischen und organisatorischen Maßnahmen, zu strukturierten Risikobewertungen und zu kontinuierlichen Verbesserungen ihrer Informationssicherheitsstrukturen.

5.1 Netzwerk- und Informationssicherheitsrichtlinie 2 (NIS2)

Die Richtlinie (EU) 2022/2555 (NIS2) stärkt die Cybersicherheit in der Europäischen Union durch einheitliche Mindeststandards und erweiterte Pflichten für sogenannte „besonders wichtige“ und „wichtige“ Einrichtungen in bestimmten Sektoren (u. a. Gesundheitsdienstleistungen). Für das Gesundheitswesen bedeutet dies verschärfte Anforderungen an Informationssicherheits-Management, Dokumentation und Meldepflichten.

Nach Art. 21 NIS2 müssen Organisationen ein dokumentiertes Informationssicherheits-Managementsystem (ISMS) einführen, Notfall- und Wiederanlaufpläne (Business Continuity Management, BCM) vorhalten, Lieferantenbeziehungen sicherheitsbezogen prüfen und Mitarbeitende regelmäßig zu Cyberhygiene schulen. Sicherheitsvorfälle, die als erheblich eingestuft werden, unterliegen einem dreistufigen Meldesystem nach Art. 23 NIS2: eine Erstmeldung („Early Warning“) innerhalb von 24 Stunden, eine weitere Meldung innerhalb von 72 Stunden und ein Abschlussbericht spätestens innerhalb eines Monats. Art. 32 NIS2 regelt hingegen die Aufsichts- und Durchsetzungsmaßnahmen der Behörden gegenüber besonders wichtigen Einrichtungen.

Technische Maßnahmen wie Verschlüsselung, Patchmanagement, Identitäts- und Zugriffskontrolle sowie Multi-Faktor-Authentifizierung sind nach dem Stand der Technik umzusetzen. Durchführungsrechtsakte wie die Durchführungsverordnung (EU) 2024/2690 konkretisieren sektorspezifische Anforderungen weiter.

Deutschland setzt die Richtlinie mit dem NIS2-Umsetzungsgesetz um, das im November 2025 beschlossen wurde und das BSI-Gesetz umfassend novelliert. Ein Inkrafttreten zum Jahreswechsel 2025/2026 ist vorgesehen.

Die Schwellenwerte der BSI-KRITIS-Verordnung (z. B. mehr als 30.000 stationäre Fälle pro Jahr für Krankenhäuser) bleiben bis zur Vollanwendung des KRITIS-Dachgesetzes relevant.

Tab. 9 NIS2

Unternehmensgrößen
Mittelgroßes Unternehmen:
- Mehr als 50 Mitarbeitende
- Mehr als 10 Mio. € Umsatz
- Mehr als 10 Mio. € Bilanzsumme
Großes Unternehmen:
- Mehr als 250 Mitarbeitende
- Mehr als 50 Mio. € Umsatz
- Mehr als 43 Mio. € Bilanzsumme
Betreiber kritischer Anlagen:
- Unternehmen, die mehr als 500.000 Menschen versorgen
Kritische Betreiber – Krankenhäuser:
- Mehr als 30.000 vollstationäre Patient*innen pro Jahr



Als wichtige bzw. besonders wichtige Einrichtungen im Sinne der NIS2 gelten mittelgroße bzw. große Unternehmen nur, wenn sie einem der in Anhang I oder II genannten Sektoren zugeordnet sind (u.a. Gesundheitsdienstleistungen). In bestimmten Fällen können auch kleinere Unternehmen erfasst sein, etwa bestimmte digitale Infrastrukturdienste.

Die Anforderungen lassen sich in zehn zentrale Punkte unterteilen.

- 1. Konzepte zur Risikoanalyse:** Für das Risikomanagement müssen dokumentierte Abläufe vorhanden sein. Diese können als Richtlinien oder in Form eines Informationssicherheits-Managementsystems umgesetzt werden. Das ISMS besteht aus Verfahren und Regeln, die in einem Unternehmen umgesetzt werden sollen, um Informationssicherheit zu gewährleisten.
- 2. Bewältigung von Sicherheitsvorfällen:** Gemäß Art. 23 NIS2 und § 32 BSIG neu muss ein geregeltes Verfahren zur Erkennung, Behandlung und Meldung von Sicherheitsvorfällen vorhanden sein, bei dem die Abläufe dokumentiert werden und das dreistufige Melderegime (24 Stunden Meldung, 72 Stunden Meldung, Abschlussbericht spätestens nach einem Monat) eingehalten wird.
- 3. Betriebliches Kontinuitätsmanagement (BCM):** Gemäß dem gängigen BSI-Standard 200-4 ist das Ziel die Aufrechterhaltung und Wiederherstellung des Geschäftsbetriebs in Notlagen. Innerhalb des BCMs steht die Durchführung des Assessments einzelner Abteilungen im Vordergrund. Angelehnt an den Standard werden dann Maßnahmen abgeleitet.
- 4. Lieferanten:** Es muss eine Lieferantenüberprüfung geben und Lieferanten müssen auf die Informationssicherheit verpflichtet werden.
- 5. Sicherheitsmaßnahmen von IT-Systemen:** Es muss ein wirksamer Einsatz von sicherheitstechnischen Lösungen nach dem Stand der Technik geben. Dazu gehört Patchmanagement und Backupsysteme, ergänzt um Protokollierung und Angriffserkennung für kritische Systeme.
- 6. Risikomanagementmaßnahmen:** Gemäß § 30 BSIG neu müssen Cyberrisiken systematisch im unternehmensweiten Risikomanagement berücksichtigt und die daraus abgeleiteten Entscheidungen sowie Maßnahmen nachvollziehbar dokumentiert werden.
- 7. Cyberhygiene und Schulungen:** Sowohl Mitarbeitende als auch Führungskräfte müssen geschult werden. Das kann durch Pflichtschulungen, Phishing-Kampagnen usw. umgesetzt werden.
- 8. Kryptografie:** Es muss ein Kryptografie-Konzept entwickelt werden, welches nach dem Stand der Technik funktioniert und sowohl Data-In-Motion als auch Data-In-Rest behandelt.
- 9. Personalsicherheit und Zugriffskontrolle:** Bei der Auswahl von Personal muss es einen geregelten Auswahlprozess geben und eine Richtlinie für Zugriffe entwickelt werden. Admin und Benutzerkonten müssen getrennt werden.
- 10. Multi-Faktor-Authentifizierung:** Ist insbesondere für privilegierte Zugänge, Remote-Zugriffe und besonders schützenswerte Systeme einzusetzen; der Einsatz richtet sich nach einer risikobasierten Bewertung im Sinne von Art. 21 NIS2 und § 30 BSIG neu.

5.2 IT-Sicherheitsgesetz 2.0 (BSIG)

Das IT-Sicherheitsgesetz 2.0 erweitert das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) und stärkt den Schutz kritischer Infrastrukturen. Das BSIG gilt im Gesundheitssektor jedoch nur für Krankenhäuser, die als Betreiber Kritischer Infrastrukturen eingestuft sind. Dies betrifft Einrichtungen mit mehr als 30.000 vollstationären Fällen pro Jahr gemäß BSI-Kritisverordnung.

KRITIS-Krankenhäuser müssen nach § 8a BSIG ein Informationssicherheits-Managementsystem betreiben, angemessene technische und organisatorische Maßnahmen nach dem

Stand der Technik umsetzen und erhebliche IT-Störungen sowie Sicherheitsvorfälle unverzüglich an das BSI melden. Sie sind verpflichtet, regelmäßige Sicherheitsaudits durchzuführen, Angriffserkennungssysteme einzusetzen und Notfall- sowie Wiederanlaufkonzepte vorzuhalten. KI-Systeme in der Patientenversorgung unterliegen den BSIG-Pflichten nur dann, wenn das Krankenhaus KRITIS-Einrichtung ist. In nicht-KRITIS-Krankenhäusern gelten hingegen ausschließlich die Anforderungen der DSGVO sowie der sektorspezifischen Gesundheitsgesetzgebung.

5.3 Cyber Resilience Act (CRA)

Der Cyber Resilience Act (EU) 2024/2847 wurde am 10. Dezember 2024 veröffentlicht und verpflichtet Hersteller dazu, Software und Hardware nach dem Prinzip „Security by Design and by Default“ zu entwickeln. Sicherheitslücken müssen über den gesamten Lebenszyklus überwacht und durch Updates geschlossen werden – für die geschätzte Lebensdauer des Produkts oder mindestens fünf Jahre.

Zeitplan:

Ab 11. September 2026: Beginn der Meldepflichten für aktiv ausgenutzte Schwachstellen und Sicherheitsvorfälle.

Ab 11. Dezember 2027: Anwendung aller weiteren Pflichten (einschließlich CE-Kennzeichnung, Konformitätsbewertungsverfahren und Marktüberwachung).

Hersteller, Importeure und Händler sind gleichermaßen verpflichtet. Werden Schwachstellen aktiv ausgenutzt, müssen sie unverzüglich, spätestens innerhalb von 24 Stunden, an die zuständige nationale Behörde gemeldet werden. Für Krankenhäuser bedeutet dies, dass künftig ausschließlich CRA-konforme Hard- und Software beschafft werden dürfen.

Tab. 10 CRA

Normen	Inhalte
Art. 3 CRA	Anwendungsbereiche und Ausnahmen
Art. 6 CRA	Wesentliche Cybersicherheitsanforderungen an Produkte mit digitalen Elementen
Art. 10 CRA	Verpflichtungen der Hersteller
Art. 11-14 CRA	Konformitätsbewertung, CE-Kennzeichnung sowie Pflichten für Importeure und Händler
Art. 18 ff. CRA	Marktüberwachung, Meldepflichten für Schwachstellen und aktiv ausgenutzte Sicherheitsvorfälle
Art. 30 CRA	Sanktionen und Durchsetzungsmaßnahmen

5.4 Cybersecurity Act (CSA)

Der Cybersecurity Act gilt seit dem 27. Juni 2019 und verleiht der EU-Agentur ENISA ein dauerhaftes Mandat. Die Verordnung etabliert einen EU-weiten Zertifizierungsrahmen für Informations- und Kommunikationstechnologien (Art. 46 ff.) mit drei Vertrauensstufen: basic, substantial und high.

Für das Gesundheitswesen schafft der CSA die Grundlage, medizinische KI-Systeme, Cloud-Dienste oder vernetzte Medizingeräte künftig nach einheitlichen europäischen Sicherheits-

standards zertifizieren zu lassen. Diese Zertifikate können im Rahmen des EU AI Act als Nachweis für technische Sicherheit und Robustheit dienen.

Der CSA bildet zudem die regulatorische Basis für den Cyber Resilience Act, der ab 2027 zusätzliche Anforderungen an vernetzte digitale Produkte festlegt. Beide Verordnungen ergänzen sich zu einem kohärenten europäischen Cybersicherheitsrahmen.

5.5 KRITIS-Verordnung

Die BSI-KRITIS-Verordnung definiert in Deutschland, welche Einrichtungen als kritische Infrastrukturen gelten. Im Gesundheitswesen betrifft dies insbesondere Krankenhäuser mit mehr als 30.000 vollstationären Fällen pro Jahr.

Betreiber müssen gemäß § 8a BSIG nachweisen, dass sie technische und organisatorische Maßnahmen nach dem Stand

der Technik umsetzen. Sicherheitsvorfälle müssen unverzüglich an das BSI gemeldet werden, und eine dauerhaft erreichbare Kontaktstelle ist vorzuhalten.

Die Verordnung wird im Zuge der NIS2-Umsetzung künftig durch das KRITIS-Dachgesetz ersetzt, das harmonisierte europäische Anforderungen integrieren soll.



Merktafel

NIS2-Richtlinie (NIS 2):

- Seit Oktober 2024 EU-weiter Rahmen für Cybersicherheit
- Betrifft u. a. Krankenhäuser, Labore und IT-Dienstleister im Gesundheitswesen
- Verpflichtung zur Einführung eines Informationssicherheits-Managementsystems (ISMS)
- Meldepflichten für Sicherheitsvorfälle und Schwachstellen
- Zehn Kernmaßnahmen: Risikoanalyse, BCM, Lieferantenprüfung, Patchmanagement, Schulungen, Zugriffskontrolle, Verschlüsselung, MFA, Protokollierung und Monitoring, Sicherheit in der Lieferkette
- Bußgelder bis zu 10 Mio. € oder 2 % des Jahresumsatzes

IT-Sicherheitsgesetz 2.0 (BSIG):

- Stärkt Schutz kritischer Infrastrukturen (KRITIS)
- Krankenhäuser, die als KRITIS-Einrichtung gelten, müssen nach § 8a BSIG technische und organisatorische Schutzmaßnahmen umsetzen
- Pflicht zur unverzüglichen Meldung von Sicherheitsvorfällen an das BSI
- KI-Systeme in der Patientenversorgung unterliegen denselben Pflichten

Cyber Resilience Act (CRA):

- EU-Verordnung für sichere digitale Produkte und Software
- Verpflichtet zu „Security by Design & Default“ und lebenszyklusweiten Updates
- Meldepflichten ab 11.09.2026, vollständige Anwendung ab 11.12.2027
- Sicherheitslücken müssen innerhalb von 24 Stunden gemeldet werden
- Krankenhäuser sollen nur CRA-konforme Systeme beschaffen

Cybersecurity Act (CSA):

- Gilt seit 27. Juni 2019
- Stärkt ENISA als EU-Agentur für Cybersicherheit
- Etabliert ein EU-weites Zertifizierungssystem für ICT-Produkte, -Dienste und -Prozesse
- Zertifikate belegen technische Sicherheit und Robustheit
- Relevanz für medizinische KI-, Cloud- und IoT-Systeme
- Grundlage für den Cyber Resilience Act (ab 2027)

KRITIS-Verordnung:

- Gilt für Krankenhäuser mit mehr als 30.000 stationären Fällen pro Jahr
- Nachweis technischer und organisatorischer Sicherheitsmaßnahmen nach § 8a BSIG
- Verpflichtung zur Meldung von IT-Störungen an das BSI
- Wird im Zuge der NIS2-Umsetzung durch das KRITIS-Dachgesetz ersetzt



6. Wettbewerbs- und Wirtschaftsrecht

Digitale Gesundheitsanwendungen und KI-gestützte Systeme unterliegen nicht nur datenschutz- und gesundheitsrechtlichen Vorgaben, sondern auch umfassenden wirtschafts-, vertrags- und wettbewerbsrechtlichen Regelungen. Diese Rechtsgebiete stellen sicher, dass digitale Dienste fair betrieben, geistiges Eigentum geschützt, Geschäftsbeziehungen transparent gestaltet und Marktmissbrauch verhindert wird. Für KI-Anwendungen im Gesundheitswesen sind diese Vorschriften besonders relevant, da sie häufig auf Daten zugreifen, digitale Dienste erbringen oder wirtschaftlich verwertet werden.

6.1 Data Act

Der Data Act ist eine zentrale EU-Verordnung, die am 11. Januar 2024 in Kraft trat und ab dem 12. September 2025 unmittelbar in allen Mitgliedstaaten gilt. Zusammen mit dem Data Governance Act (DGA) bildet er das Fundament der europäischen Datenstrategie. Ziel ist es, einen fairen, sicheren und innovationsfreundlichen Datenmarkt zu schaffen und rechtliche, technische sowie wirtschaftliche Hürden beim Datenaustausch abzubauen.

Der Data Act regelt, wer unter welchen Bedingungen auf Daten zugreifen und sie nutzen darf. Betroffen sind insbesondere Hersteller, Nutzer und Anbieter vernetzter Geräte und digitaler Dienste, darunter medizinische Geräte, Wearables, Sensoren, Krankenhaus-IT-Systeme und Cloud-Plattformen. Die Verordnung definiert verbindliche Regeln für Datenbeziehungen zwischen Unternehmen, Verbraucher*innen und öffentlichen Stellen (B2B, B2C und B2G).

Zentral ist die Stärkung der Rechte von Datennutzenden. Nutzer*innen vernetzter Geräte erhalten ein Recht auf Zugriff sowie ein Recht, die Weitergabe ihrer Daten an Dritte zu veranlassen. Dabei dürfen Nutzer*innen jedoch nur solche Daten weitergeben, für die sie selbst berechtigt sind; Datenrechte Dritter dürfen nicht beeinträchtigt werden. Hersteller müssen technische Exportfunktionen bereitstellen und Daten in einem sicheren, strukturierten und maschinenlesbaren Format zur Verfügung stellen. Gleichzeitig verpflichtet der Data Act Anbieter zu wirksamen Sicherheitsmaßnahmen, einschließlich Zugriffskontrollen, Verschlüsselung und Protokollierung.

Ein wesentlicher Schwerpunkt liegt auf Interoperabilität. Systeme und Daten müssen technisch und semantisch kompatibel sein, um einen nahtlosen sektorenübergreifenden Austausch zu ermöglichen. Gerade im Gesundheitswesen – etwa zwischen Kliniken, Forschungseinrichtungen, Pflegeeinrichtungen und mobilen Gesundheitsanwendungen – ist dies entscheidend für eine präzise Versorgung, effiziente Prozesse und verlässliche KI-Modelle.

Der Data Act stärkt darüber hinaus faire Wettbewerbsbedingungen, indem er missbräuchliche Vertragsklauseln großer Anbieter gegenüber kleinen und mittleren Unternehmen für unwirksam erklärt. Für die öffentliche Hand schafft die Verordnung klare Regeln für Datenzugriffe in außergewöhnlichen Situationen, etwa bei Pandemien oder Naturkatastrophen, unter strengen Anforderungen an Verhältnismäßigkeit und Datenschutz.

Für das Gesundheitswesen eröffnet der Data Act erstmals einen vollständig harmonisierten Rechtsrahmen für interoperable, sektorenübergreifende und datenschutzkonforme Nutzung von Gesundheits- und Forschungsdaten. Er ist eng verzahnt mit dem EU AI Act, dem European Health Data Space und der Medical Device Regulation. Gemeinsam fördern diese Rechtsakte eine vertrauenswürdige, sichere und datengetriebene Digitalisierung.

6.2 Digital Services Act (DSA)

Der Digital Services Act gilt seit dem 17. Februar 2024 und schafft einheitliche Regeln für den sicheren, transparenten und verantwortungsvollen Betrieb digitaler Dienste und Plattformen in der EU. Er verpflichtet Anbieter zu Maßnahmen gegen illegale Inhalte, zu Transparenz über algorithmische Empfehlungssysteme und zum Umgang mit systemischen Risiken. Für das Gesundheitswesen ist der DSA relevant, wenn Plattfor-

men Gesundheitsinformationen bereitstellen oder telemedizinische Inhalte vermitteln. Betreiber müssen sicherstellen, dass bereitgestellte Inhalte – insbesondere medizinische – korrekt, überprüfbar und nicht irreführend sind. Zudem müssen KI-generierte Inhalte oder automatisierte Empfehlungen eindeutig als solche gekennzeichnet werden. Dies erhöht Transparenz, Vertrauenswürdigkeit und Patientensicherheit.

6.3 Digital Markets Act (DMA)

Der seit dem 2. Mai 2023 anwendbare Digital Markets Act richtet sich an sogenannte Gatekeeper-Plattformen – große Anbieter zentraler digitaler Dienste wie Cloud-Infrastrukturen, Suchmaschinen oder App-Stores. Ziel ist es, fairen Wettbewerb sicherzustellen und marktbeherrschende Strukturen zu verhindern.

nicht missbräuchlich nutzen. Für KI- und Digitalisierungsprojekte im Gesundheitswesen schafft der DMA damit verlässliche Zugangsbedingungen zu Cloud-Diensten, Analyseplattformen oder Schnittstellen großer Anbieter. Dies verbessert die Marktchancen kleinerer Unternehmen und trägt zu einem fairen digitalen Gesundheitsökosystem bei.

Gatekeeper müssen Interoperabilität gewährleisten, dürfen Geschäftskunden nicht diskriminieren und dürfen Daten

6.4 Gesetz gegen den unlauteren Wettbewerb (UWG)

Das Gesetz gegen den unlauteren Wettbewerb schützt Verbraucher*innen und Unternehmen vor irreführenden, aggressiven oder sonstigen unlauteren geschäftlichen Handlungen. Für digitale Gesundheits- und KI-Anwendungen bedeutet dies insbesondere, dass Werbung für diagnostische oder therapeutische Software sachlich, überprüfbar und frei von Täuschungen sein muss. Aussagen zur Leistungsfähigkeit, Genauigkeit oder Wirksamkeit eines Systems dürfen nur gemacht werden,

wenn sie nachweisbar und fachlich korrekt sind. Unzulässige vergleichende Werbung, übertriebene Heilversprechen oder die Ausnutzung von Unsicherheiten und Ängsten sind ebenso verboten wie die unbefugte Nutzung vertraulicher Daten oder Geschäftsgeheimnisse für eigene wirtschaftliche Zwecke. Verstöße gegen das UWG können Unterlassungsansprüche, Abmahnungen sowie empfindliche Bußgelder nach sich ziehen.

6.5 Urheberrechtsgesetz (UrhG)

Auch das Urheberrecht spielt beim Training und Einsatz von KI eine zentrale Rolle. Urheberrechtlich geschützte Werke dürfen grundsätzlich nur genutzt werden, wenn keine Opt-out-Erklärung des Rechteinhabers vorliegt oder eine gesetzliche Ausnahme greift. KI-generierte Inhalte sind nur dann geschützt, wenn eine menschliche schöpferische Leistung erkennbar beteiligt war; rein KI-generierte Inhalte sind nicht urheberrechtlich geschützt.

Anbieter von General-Purpose-AI-Modellen müssen offenlegen, welche Trainingsdaten verwendet wurden, und Strategien zur Einhaltung des Urheberrechts bereitstellen. Dies schafft Transparenz und Rechtssicherheit für Anwender*innen.

6.6 Vertragsrecht

Im Gesundheitswesen müssen vertragliche Vereinbarungen zwischen Krankenhäusern, Softwareanbietern und Dienstleistern die rechtlichen Anforderungen digitaler Systeme eindeutig und umfassend abbilden. Dies umfasst insbesondere verbindliche Regelungen zu Datenschutz und Datennutzung im Einklang mit der DSGVO und dem European Health Data Space, zur Produktsicherheit nach MDR und Produkthaftungsrichtlinie sowie zur Informationssicherheit gemäß BSIG, NIS2 und Cyber Resilience Act. Zusätzlich müssen vertragliche Vereinbarungen die verpflichtenden KI-Sicherheits- und Risikomanagementanforderungen des EU AI Act (Art. 9–15)

ausdrücklich abbilden. Hinzu kommen klare Bestimmungen zu Haftung, Gewährleistung, Update- und Supportpflichten sowie zur Meldung, Behandlung und Dokumentation von Fehlern oder Sicherheitsvorfällen. Auch im Verhältnis zu Patient*innen besteht eine Pflicht zur Transparenz: Der Einsatz KI-gestützter Systeme in Diagnostik, Therapie oder Entscheidungsunterstützung muss offen kommuniziert werden. Nur durch eindeutig definierte vertragliche Verantwortlichkeiten können rechtliche Sicherheit, eine verlässliche digitale Versorgung und der Schutz der Patient*innen gewährleistet werden.



Merktafel

Data Act:

- Gilt ab 12. September 2025 unmittelbar in allen EU-Mitgliedstaaten
- Ziel: Fairer, sicherer und interoperabler Datenaustausch
- Nutzer*innen entscheiden, wer auf ihre Daten zugreifen darf
- Hersteller müssen technisch interoperable Schnittstellen schaffen
- Unfaire B2B-Vertragsklauseln zum Datenaustausch sind unzulässig
- Datenzugriffe erfordern eine wirksame Zustimmung und müssen vor unbefugtem Zugriff geschützt werden
- Fördert KI-Training auf hochwertigen, strukturierten und standardisierten Datensätzen
- Zentrale Grundlage für den Europäischen Gesundheitsdatenraum (EHDS)
- Der Data Act verpflichtet zusätzlich zu Interoperabilität und Wechselseitigkeiten bei Cloud-Diensten (Art. 26–30)

Digital Services Act (DSA):

- Gilt seit Februar 2024
- Regelt Sicherheit und Transparenz digitaler Plattformen
- Verpflichtet zur schnellen Entfernung illegaler Inhalte und Desinformation
- Offenlegung von Algorithmus- und Empfehlungssystemen
- KI-generierte Inhalte sind als solche kenntlich zu machen
- Relevant für Patientenportale, Telemedizin, Gesundheitsplattformen

Digital Markets Act (DMA):

- Gilt seit Mai 2023
- Richtet sich an große Plattformanbieter („Gatekeeper“)
- Verpflichtung zur Interoperabilität und zu fairen Zugangsbedingungen für Geschäftskunden
- Verbot von Selbstbevorzugung und missbräuchlicher Nutzung von Geschäftsdaten
- Stärkt Wettbewerb, Innovationsfreiheit und Markttransparenz
- Erleichtert im Gesundheitssektor den Zugang zu Cloud- und IT-Diensten

Gesetz gegen den unlauteren Wettbewerb (UWG):

- Schützt Verbraucher*innen und Unternehmen vor irreführenden oder aggressiven geschäftlichen Handlungen
- Werbung für KI- oder Gesundheitssoftware muss sachlich, korrekt und transparent sein
- Übertriebene Leistungsversprechen und Täuschungen sind verboten
- Nutzung vertraulicher Daten oder Geschäftsgeheimnisse zu Wettbewerbszwecken ist unzulässig
- Verstöße können Abmahnungen, Unterlassungsansprüche und Bußgelder auslösen

Urheberrechtsgesetz (UrhG):

- Regelt die Nutzung urheberrechtlich geschützter Werke im digitalen Umfeld und im Kontext von KI-Systemen
- KI darf geschützte Inhalte nur nutzen, wenn kein Opt-out erfolgt ist oder eine Ausnahme greift
- Rein KI-generierte Inhalte ohne menschliche Mitwirkung genießen keinen Urheberrechtsschutz
- Anbieter von Generative AI müssen verwendete Trainingsdaten offenlegen (Diese Transparenzpflicht ergibt sich aus Art. 53 EU AI Act)
- Wichtig für KI-Systeme, die mit Bildern, Texten oder Audio trainiert werden

Vertragsrecht:

- Regelt Haftung, Pflichten und Verantwortlichkeiten beim Einsatz digitaler Systeme und KI
- Verträge müssen Datenschutz, Wartung, Updates, Sicherheitsmaßnahmen und Zulassungspflichten abdecken
- Transparenzpflicht: Einsatz von KI-Systemen muss im Behandlungsvertrag offengelegt werden
- Verträge müssen die verpflichtenden KI-Risikomanagement-, Datenqualitäts- und Transparenzanforderungen aus Art. 9–15 EU AI Act enthalten
- Verantwortlichkeiten zwischen Betreiber, Hersteller und Dienstleister sind klar festzulegen
- Schulungspflichten gewährleisten einen sicheren und rechtssicheren Betrieb von KI-Systemen



7. Straf- und Haftungsrecht

Das Straf- und Haftungsrecht legt fest, wer im Umgang mit Daten, digitalen Technologien und medizinischen Anwendungen Verantwortung trägt. Es definiert die Folgen von Pflichtverletzungen, fahrlässigem Verhalten oder technischen Fehlern und stellt sicher, dass Patientensicherheit, Datenschutz und berufliche Sorgfalt gewahrt bleiben. Gerade im Einsatz von KI-Systemen haben diese Vorgaben wachsende Bedeutung, da neue digitale Verarbeitungsszenarien zusätzliche Risiken und Verantwortlichkeiten erzeugen.

7.1 Strafgesetzbuch (StGB)

Das Strafgesetzbuch bildet die zentrale Grundlage des deutschen Strafrechts. Besonders relevant für das Gesundheitswesen und die digitale Datenverarbeitung ist § 203 StGB, der die Verletzung von Privatgeheimnissen unter Strafe stellt. Ärzt*innen, Pflegekräfte sowie weitere Berufsgeheimnisträger sind verpflichtet, patientenbezogene Informationen vertraulich zu behandeln.

Diese Verschwiegenheitspflichten gelten unverändert auch beim Einsatz digitaler Systeme und KI-gestützter Datenverarbeitung. Insbesondere müssen Trainings-, Analyse- und Betriebsdaten so verarbeitet werden, dass eine Identifizierung einzelner Patient*innen ausgeschlossen bleibt, beispielsweise durch Anonymisierung, Verschlüsselung, Zugriffsbeschränkungen oder den Abschluss geeigneter Auftragsvertragsverträge.

Die Übermittlung von Patientendaten an ein KI-System kann grundsätzlich eine Offenbarung von Privatgeheimnissen darstellen und ist strafrechtlich relevant, sofern keine gesetzliche Befugnis oder wirksame Einwilligung vorliegt. Eine pauschale Schweigepflichtentbindung ist im Rahmen automatisierter, großskaliger oder hochsensibler KI-Verarbeitungen regelmäßig nicht ausreichend. Landesrechtliche Offenbarungsbefugnisse können Ausnahmen vorsehen; in Nordrhein-Westfalen bestehen jedoch keine spezifischen Regelungen für KI-Anwendungen. Die Datenoffenbarung ist daher ausschließlich im Rahmen der allgemeinen Rechtsgrundlagen – insbesondere § 203 StGB in Verbindung mit Art. 6 und Art. 9 DSGVO zulässig.

Tab. 11 StGB

Normen	Inhalte
§ 203 StGB	Verletzung von Privatgeheimnissen

7.2 Haftungsrechtliche Einordnung ärztlicher KI-Nutzung

Mit dem Einsatz von KI-Systemen in Diagnostik, Therapie und Entscheidungsunterstützung stellt sich zunehmend die Frage der haftungsrechtlichen Verantwortung. Auch wenn KI wertvolle Unterstützung bietet, bleibt die medizinische Letztverantwortung vollständig bei den behandelnden Ärzt*innen. Sie sind verpflichtet, die Ergebnisse der KI fachlich zu prüfen und in den klinischen Kontext einzuordnen.

Ein Blindvertrauen in KI-Ergebnisse kann als Behandlungsfehler gemäß §§ 630a, 823 BGB gewertet werden. Darüber hinaus kann ein Organisationsverschulden des Krankenhauses oder des Trägers vorliegen, wenn fehlerhafte oder ungeeignete KI-Systeme eingesetzt, wenn Systeme unzureichend geprüft oder wenn das Personal nicht angemessen geschult wurde.

Liegt der Schaden an einem technischen Defekt, einer fehlerhaften Programmierung oder einer unzureichenden Datenbasis, kann zusätzlich eine Produkthaftung des Herstellers greifen – insbesondere nach der neuen EU-Produkthaftungsrichtlinie (PLD 2024/2853), die Software, KI-Systeme und digitale Komponenten ausdrücklich umfasst.

Wesentlich sind auch die ärztlichen Aufklärungspflichten nach § 630e BGB. Patient*innen müssen über Art, Umfang und Bedeutung des KI-Einsatzes informiert werden, sofern dieser das Behandlungsergebnis wesentlich beeinflusst. Eine fehlende, unzureichende oder irreführende Aufklärung kann eigenständige haftungsrechtliche Konsequenzen nach sich ziehen.



Tab. 12 Haftungsrechtliche Einordnung

Normen	Inhalte
Behandlungsfehler gem. §630 a BGB i.V.m. §823 BGB	Wenn sich Ärzte blind auf KI-Systeme verlassen, ohne das Ergebnis kritisch zu hinterfragen, kann dies als Behandlungsfehler gewertet werden.
Organisationsverschulden gem. §823, §31 BGB analog	Wenn das Krankenhaus oder die Trägerorganisation ungeeignete oder nicht ausreichend geprüfte KI-Systeme einsetzt, kann ein sogenanntes Organisationsverschulden vorliegen.
Produkthaftung	Falls der Schaden auf einem technischen Fehler des KI-Systems beruht (z. B. falsche Programmierung, unzureichende Schulung, fehlerhafte Datenbasis), kann auch eine Produkthaftung des Herstellers greifen. (Das Produkt erfüllt die Merkmale eines Medizinprodukts und war fehlerhaft)
Aufklärungspflichten gem. §630 e BGB	Bei komplexeren KI-Anwendungen etwa bei Entscheidungsunterstützungssystemen in der Onkologie kann es notwendig sein, Patienten über die Rolle der KI aufzuklären, insbesondere wenn sie eine erhebliche Bedeutung für die Entscheidung hat. Fehlende oder irreführende Aufklärung kann haftungsrechtlich relevant sein.



Merktafel

Strafgesetzbuch (StGB):

- Verbot der unbefugten Weitergabe vertraulicher Patientendaten
- Gilt auch für digitale Systeme und KI-Anwendungen
- KI-bezogene Datenverarbeitungen müssen so erfolgen, dass keine Offenbarung nach § 203 StGB erfolgt (technische und organisatorische Schutzmaßnahmen ergeben sich aus Art. 32 DSGVO)
- Offenbarung nur bei gesetzlicher Grundlage oder Einwilligung erlaubt
- In NRW keine Sonderregelung für KI, daher Anwendung von § 203 StGB und DSGVO

Haftungsrecht bei KI-Nutzung:

- Ärzt*innen behalten Letztverantwortung für Diagnosen und Entscheidungen
- KI-Fehler entbinden nicht von ärztlicher Sorgfaltspflicht
- Kliniken müssen sichere, geprüfte Systeme einsetzen und Personal schulen

Zentrale Haftungstatbestände:

- Behandlungsfehler (§ 630a BGB i. V. m. § 823 BGB): Haftung bei blindem Vertrauen in KI-Ergebnisse ohne Prüfung.
- Organisationsverschulden (§ 823, § 31 BGB analog): Krankenhaus haftet für ungeeignete, fehlerhafte oder unzureichend geprüfte KI-Systeme.
- Produkthaftung (PLD 2024/2853): Hersteller haftet für Softwarefehler, fehlerhafte Algorithmen oder mangelhafte Updates.
- Aufklärungspflicht (§ 630e BGB): Patient*innen müssen über den Einsatz und die Bedeutung von KI informiert werden. Fehlende Aufklärung kann haftungsrechtlich relevant sein.



8. Berufsrecht

Das Berufsrecht konkretisiert die ärztliche Verantwortung beim Einsatz digitaler Technologien, Künstlicher Intelligenz und sensibler Gesundheitsdaten. Es legt verbindliche Standards für die Berufsausübung fest und gewährleistet, dass medizinische Qualität, Datenschutz und ethische Grundsätze auch in einer zunehmend digitalisierten Versorgung eingehalten werden. Die berufsrechtlichen Vorgaben wirken ergänzend zu Datenschutz-, Medizin- und Haftungsrecht und stellen sicher, dass moderne Technologien verantwortungsvoll eingesetzt werden.

8.1 Heilberufegesetz NRW (HeilBerG NRW)

Das Heilberufegesetz Nordrhein-Westfalen regelt Organisation, Aufgaben und Berufspflichten der Heilberufskammern – einschließlich Kammern der Ärzt*innen, Zahnärzt*innen, Psychotherapeut*innen, Tierärzt*innen sowie Apotheker*innen. Es dient dem Schutz der öffentlichen Gesundheit, der Sicherstellung qualitativ hochwertiger medizinischer Versorgung und der Wahrung der beruflichen Eigenverantwortung.

Zentrale Berufspflichten umfassen eine gewissenhafte, rechtlich korrekte und verantwortungsvolle Ausübung des Berufs, die Pflicht zur kontinuierlichen Fortbildung und die Wahrung der Verschwiegenheit über alle im Rahmen der Berufsausübung anvertrauten oder bekannt gewordenen Geheimnisse. Die Schweigepflicht nach § 30 HeilBerG NRW ergänzt die strafrechtliche Norm des § 203 StGB und bildet eine eigenständige berufsrechtliche Grundlage für den Schutz von Patientendaten.

Darüber hinaus verpflichtet das HeilBerG NRW zur sorgfältigen Dokumentation und zur sicheren Aufbewahrung von Behandlungsunterlagen. Diese Pflichten stehen in engem Zusammenhang mit den datenschutzrechtlichen Anforderungen der DSGVO, insbesondere Rechenschaftspflicht, Integrität, Vertraulichkeit und technischer Sicherheit.

Die Heilberufskammern übernehmen eine zentrale Funktion in der berufsständischen Selbstverwaltung. Sie fördern Fort- und Weiterbildung, sichern die Qualität der Berufsausübung und überwachen die Einhaltung der Berufspflichten. Berufsordnungen der Kammern konkretisieren diese Pflichten – etwa zur Datenverarbeitung, Dokumentation, Schweigepflicht sowie zur ordnungsgemäßen Führung und Aufbewahrung von Patientendaten. Verstöße gegen berufsrechtliche Verpflichtungen können durch berufsgerichtliche Maßnahmen sanktioniert werden, die je nach Schwere von einem Verweis über Geldbußen bis hin zum Ruhen oder Widerruf der Approbation reichen können.

Obwohl sich das HeilBerG NRW primär an einzelne Angehörige der Heilberufe richtet, entfaltet es Wirkung auf Krankenhäuser und andere Versorgungseinrichtungen, die organisatorisch sicherstellen müssen, dass berufsrechtliche Anforderungen eingehalten werden. Damit verbindet das Gesetz staatliche Aufsicht, datenschutzrechtliche Verpflichtungen und ärztliche Eigenverantwortung und gewährleistet, dass digitale Anwendungen und KI-Systeme im Gesundheitswesen mit hoher Professionalität, ethischer Verantwortung und Datenschutz umgesetzt werden.

Tab. 13 HeilBerG NRW

Normen	Inhalte
§ 30 HeilBerG NRW	<ul style="list-style-type: none"> • Verpflichtet Angehörige der Heilberufe zur Verschwiegenheit über alle im Rahmen der Berufsausübung anvertrauten oder bekannt gewordenen Geheimnisse • gilt auch nach dem Tod von Patient*innen • Pflicht zur sorgfältigen Dokumentation und sicheren Aufbewahrung von Patientenunterlagen
§ 31 HeilBerG NRW	<ul style="list-style-type: none"> • Verpflichtet alle Kammerangehörigen zur regelmäßigen beruflichen Fortbildung, um ihre fachliche Kompetenz und die Qualität der Versorgung auf aktuellem Stand zu halten • Die Kammern können Nachweise verlangen oder Vorgaben in den Berufsordnungen regeln

8.2 Muster-Berufsordnung für Ärzte (MBO-Ä)

Die Muster-Berufsordnung für in Deutschland tätige Ärzt*innen (MBO-Ä) konkretisiert die allgemeinen Berufspflichten und dient als Grundlage für die Berufsordnungen der Landesärztekammern.

Sie dient als Orientierung für eine einheitliche Berufsausübung und stärkt das Vertrauensverhältnis zwischen Ärzt*innen und Patient*innen.

Die MBO-Ä gilt somit nicht unmittelbar, sondern wird erst durch Beschluss der Landesärztekammern in regionale Berufsordnungen überführt. Dies führt zu länderspezifischen Ausgestaltungen, während der Kern der Pflichten bundesweit übereinstimmt. Von besonderer Bedeutung sind § 9 MBO-Ä (Schweigepflicht) und § 10 MBO-Ä (Dokumentationspflicht). Ärzt*innen sind verpflichtet, alle ihnen anvertrauten persönlichen Informationen vertraulich zu behandeln und diese nur weiterzugeben, wenn eine gesetzliche Befugnis oder eine wirksame Einwilligung der betroffenen Person vorliegt. Die Schweigepflicht ist zeitlich unbegrenzt und gilt auch nach dem Tod von Patient*innen.

Die Dokumentationspflicht nach § 10 MBO-Ä stellt sicher, dass der Behandlungsverlauf vollständig, nachvollziehbar und prüfbar festgehalten wird. Ärzt*innen müssen alle wesentlichen diagnostischen Maßnahmen, Befunde und therapeutischen Entscheidungen dokumentieren und die Unterlagen ordnungsgemäß, vollständig und sicher aufbewahren.

Im Kontext digitaler Technologien und KI-gestützter Anwendungen betont die MBO-Ä die ärztliche Verantwortung, innovative Systeme nur unter Wahrung berufsethischer Grundsätze und datenschutzrechtlicher Vorgaben einzusetzen. Dies schließt eine kritische Prüfung von KI-Ergebnissen, Transparenz gegenüber Patient*innen sowie die Wahrung der ärztlichen Entscheidungs- und Aufklärungspflichten ein.

Zivilrechtliche Ergänzung:

Neben den berufsrechtlichen Dokumentationspflichten nach § 10 MBO-Ä gelten für Krankenhäuser und Ärzt*innen auch die zivilrechtlichen Anforderungen des § 630f BGB. Die Vorschrift verpflichtet Leistungserbringende dazu, die Behandlung in einer Patientenakte vollständig, richtig und zeitnah zu dokumentieren.

Die Patientenakte muss alle aus fachlicher Sicht wesentlichen Maßnahmen, Befunde, Diagnosen, Therapien, Einwilligungen sowie Aufklärungen enthalten. Nachträgliche Änderungen sind nur zulässig, wenn erkennbar bleibt, wann und von wem die Änderung vorgenommen wurde eine rückwirkende Manipulation ist unzulässig.

§ 630f Abs. 3 BGB schreibt zudem vor, dass Patientenakten unabhängig vom Medium mindestens zehn Jahre aufzubewahren sind, soweit nicht spezialgesetzliche Regelungen längere Fristen verlangen. Dies umfasst auch digitale Dokumentationen sowie KI-gestützte Aufzeichnungen und Analysen.

Die zivilrechtlichen Dokumentationspflichten sind für die Haftung besonders relevant: Dokumentationsmängel können zu einer Beweislastumkehr zulasten des Krankenhauses oder der behandelnden Ärzt*innen führen. Daher muss jede digitale oder KI-gestützte Dokumentationslösung technisch sicherstellen, dass Vollständigkeit, Integrität, Unveränderbarkeit und Nachvollziehbarkeit gemäß § 630f BGB gewährleistet bleiben.



Merktafel

Heilberufegesetz NRW (HeilBerG NRW):

- Gilt für alle Heilberufskammern in NRW (Ärzte, Zahnärzte, Psychotherapeuten, Apotheker, Tierärzte)
- Ergänzt Datenschutzrecht durch berufsrechtliche Standards
- Kammern überwachen die Einhaltung der Berufspflichten, erlassen Berufsordnungen und sanktionieren Verstöße
- Verstöße können berufsgerichtlich geahndet werden (Verweis, Geldbuße, Ruhen oder Entzug der Approbation)
- Krankenhäuser müssen organisatorisch sicherstellen, dass ihr Personal die berufsrechtlichen Vorgaben einhält

Muster-Berufsordnung für Ärzte (MBO-Ä):

- Grundlage für alle Berufsordnungen der Landesärztekammern in Deutschland
- Weitergabe vertraulicher Daten nur mit gesetzlicher Grundlage oder wirksamer Einwilligung
- KI darf nur mit fachlicher Prüfung und Transparenz eingesetzt werden
- Stärkt Patientensicherheit, Vertrauen und Rechenschaftspflicht
- Verpflichtet Ärzt*innen zur verantwortungsvollen und fachlich begründeten Nutzung digitaler und KI-gestützter Systeme



9. Verwaltung / Staat

Gesetze zur Verwaltungsdigitalisierung und staatlichen Steuerung schaffen die rechtlichen Rahmenbedingungen für moderne, effiziente und rechtssichere Prozesse in Gesundheitseinrichtungen. Sie regeln die elektronische Kommunikation, den Zugang zu Verwaltungsleistungen, die barrierefreie Gestaltung digitaler Angebote sowie die Einbindung staatlicher Anforderungen in die digitale Infrastruktur von Krankenhäusern. Ziel ist eine nutzerfreundliche, datenschutzkonforme und sichere Verwaltung, die zugleich eine wirksame Mitbestimmung der Beschäftigten gewährleistet.

9.1 Betriebsverfassungsgesetz (BetrVG)

Das Betriebsverfassungsgesetz regelt die Mitbestimmungsrechte der Betriebsräte in privaten Unternehmen, einschließlich privater Krankenhäuser, Pflegeeinrichtungen und Rehabilitationszentren. Besonders relevant ist § 87 Abs. 1 Nr. 6 BetrVG, der die Mitbestimmung bei technischen Einrichtungen vorsieht, die geeignet sind, Verhalten oder Leistung von Beschäftigten zu überwachen. Dies betrifft insbesondere die Einführung digitaler Systeme wie Zeiterfassungssoftware, elektronische Dienstplanlösungen, Monitoring-Tools, KI-gestützte Anwendungen oder die Nutzung der elektronischen Patientenakte.

Das BetrVG stellt sicher, dass Digitalisierungsprozesse im Krankenhausbetrieb arbeitsplatzbezogen, transparent und sozialverträglich gestaltet werden. Die frühzeitige Einbindung des Betriebsrats ist verpflichtend und dient dem Schutz vor unkontrollierter Überwachung sowie technischen Belastungen.

Das BetrVG stellt sicher, dass Digitalisierungsprozesse im Krankenhausbetrieb arbeitsplatzbezogen, transparent und sozialverträglich gestaltet werden. Die frühzeitige Einbindung des Betriebsrats ist verpflichtend und dient dem Schutz vor unkontrollierter Überwachung sowie technischen Belastungen.

Tab. 14 BetrVG

Normen	Inhalte
§80 Abs.1 Nr.1 BetrVG	Allg. Aufgaben des Betriebsrats
§87 Abs.1 Nr.6 BetrVG	Mitbestimmung bei technischen Überwachungseinrichtungen
§90 BetrVG	Unterrichtungs- und Beratungsrechte bei Planung technischer Anlagen
§91 BetrVG	Abwehr von Belastungen durch technische Neuerungen
§94 BetrVG	Mitbestimmung bei Personalfragebögen oder digitalen Bewertungsinstrumenten

9.2 Onlinezugangsgesetz (OZG)

Das Onlinezugangsgesetz verpflichtet Bund, Länder und Kommunen, ihre Verwaltungsleistungen über ein einheitliches digitales Portal bereitzustellen. Öffentlich-rechtlich organisierte Krankenhäuser, kommunale Kliniken und Universitätskliniken sind betroffen, wenn sie selbst Verwaltungsleistungen erbringen oder an staatliche IT-Strukturen angebunden sind – etwa bei Personalverwaltung, Fördermitelanträgen, Abrechnungsprozessen oder Meldungen an Behörden.

Das OZG verfolgt das Ziel, Verwaltungsleistungen nutzerfreundlich, barrierefrei, interoperabel und technisch sicher anzubieten. Krankenhäuser müssen dabei datenschutzrechtliche Anforderungen, Standardisierungsvorgaben sowie IT-Sicherheitsrichtlinien berücksichtigen. Mit OZG 2.0 erfolgt eine schrittweise Vereinheitlichung der technischen Standards, um bundesweit vernetzte Verwaltungsprozesse zu ermöglichen.

Tab. 15 OZG

Normen	Inhalte
§1 OZG	Ziel und Geltungsbereich
§2 OZG	Verwaltungsleistungen
§4 OZG	Portalverbund
§5 OZG	Identifikation
§10 OZG	Zuständigkeitsverordnung und EfA-Prinzip

9.3 E-Government-Gesetze (EGovG)

Das E-Government-Gesetz des Bundes regelt die Digitalisierung staatlicher Verwaltungsprozesse und verpflichtet Behörden zur elektronischen Aktenführung (§ 6 EGovG), zur Nutzung elektronischer Identifikationsfunktionen (§ 4 EGovG), zu interoperablen IT-Verfahren (§§ 8–9 EGovG) und zur barrierefreien Gestaltung digitaler Angebote. Ergänzend gilt in Nordrhein-Westfalen das EGovG NRW für Landes- und Kommunalbehörden sowie öffentlich-rechtliche Einrichtungen wie Universitätskliniken.

Private Krankenhäuser sind betroffen, sofern sie hoheitliche Aufgaben übernehmen oder an behördliche Prozesse angebunden sind, etwa bei Förderverfahren, elektronischer Kommunikation oder digitalen Meldewegen. Besonders bedeutsam sind die Vorgaben zur digitalen Aktenführung und zum ersetzenden Scannen (§ 7 EGovG), da sie die rechtssichere Digitalisierung dokumentenbasierter Verwaltungsabläufe ermöglichen.

Tab. 16 EGovG

Normen	Inhalte
§3 EGovG	E-Mail, Onlineformulare
§4 EGovG	eID, Personalausweis
§6 und §6a EGovG	Pflicht zur elektronischen Aktenführung
§7 EGovG	Ersetzendes Scannen
§§8,9 EGovG	Interoperabilität

9.4 European Accessibility Act (EAA)

Der European Accessibility Act verpflichtet Anbieter, digitale Produkte und Dienstleistungen barrierefrei zu gestalten. Die Richtlinie wurde in Deutschland durch das Barrierefreiheitsstärkungsgesetz (BFSG) und die Barrierefreiheitsstärkungsverordnung (BFSGV) umgesetzt. Die meisten Regelungen gelten ab dem 28. Juni 2025 verbindlich, mit Übergangsfristen für Bestandslösungen bis 2030.

Für Krankenhäuser bedeutet dies, dass patienten- und personalorientierte Anwendungen – etwa Patientenportale, digitale

Aufklärungstools, Apps oder KI-gestützte Assistenzsysteme – barrierefrei nutzbar sein müssen. Dazu gehören verständliche Benutzeroberflächen, geeignete Kontraste, Kompatibilität mit Screenreadern und barrierefreie Interaktionen. Der EAA ergänzt bestehende Vorgaben zur digitalen Barrierefreiheit nach dem Behindertengleichstellungsgesetz und stärkt die gleichberechtigte Teilhabe an der digitalen Gesundheitsversorgung.

9.5 Landeshochschulgesetz NRW (HG NRW)

Das Hochschulgesetz NRW stellt den rechtlichen Rahmen für Hochschulen und Universitätskliniken dar und ist besonders relevant für datenbasierte und KI-gestützte Forschung im medizinischen Bereich. Es garantiert die Forschungsfreiheit (§ 3 HG NRW), verpflichtet jedoch gleichzeitig zur Wahrung wissenschaftlicher Integrität sowie zum Schutz der Persönlichkeitsrechte von Patient*innen und Studienteilnehmenden.

Nach §§ 31 und 32 HG NRW tragen Fakultät und Universitätsklinikum gemeinsam Verantwortung für Forschung und Lehre, insbesondere bei klinischen KI-Anwendungen.

Die Verarbeitung personenbezogener Daten ist nur auf gesetzlicher Grundlage oder mit ausdrücklicher Einwilligung zulässig (§ 73 HG NRW). Zudem ist bei Forschung am Menschen oder bei der Nutzung sensibler Gesundheitsdaten zwingend eine Ethikkommission einzubeziehen. Das HG NRW schafft damit einen verbindlichen Rahmen, der Forschungsfreiheit, Datenschutz und ethische Verantwortung ausbalanciert.

9.6 Digitalisierung von Verwaltungsprozessen im Klinikbetrieb

Die Digitalisierung der Verwaltungsprozesse in Krankenhäusern umfasst Abläufe wie Aufnahme, Abrechnung, Personalmanagement, Dokumentenverwaltung und Meldeprozesse gegenüber Behörden und Kostenträgern. Ziel ist eine effiziente, rechtssichere und medienbruchfreie Gestaltung dieser Prozesse.

Rechtlich maßgeblich sind insbesondere die Datenschutz-Grundverordnung, das Bundesdatenschutzgesetz, das Datenschutzgesetz NRW und die kirchlichen Datenschutzgesetze. Ergänzend spielen das Krankenhausrecht (z. B. § 21 KHEntgG), das Krankenhauszukunftsgesetz sowie das Onlinezugangsgesetz zentrale Rollen, da sie technische Standards und Förderbedingungen festlegen.

Weitere Anforderungen ergeben sich aus steuerrechtlichen Vorgaben zur digitalen Buchführung (GoBD) sowie arbeitsrechtlichen Mitbestimmungsrechten der Beschäftigtenvertretung, insbesondere nach § 87 BetrVG. Krankenhäuser, die als kritische Infrastrukturen gelten, müssen darüber hinaus die Vorgaben des IT-Sicherheitsgesetzes 2.0 sowie künftig der NIS2-Richtlinie einhalten.

Eine erfolgreiche Digitalisierung setzt eine enge Abstimmung zwischen Datenschutz, IT-Abteilung, Personalvertretung und Klinikleitung voraus. Nur so können digitale Systeme rechtssicher, robust, datenschutzkonform und organisatorisch tragfähig implementiert werden.



Merktafel

Betriebsverfassungsgesetz (BetrVG):

- Regelt die Mitbestimmung des Betriebsrats bei Einführung technischer Systeme (§ 87 Abs. 1 Nr. 6 BetrVG)
- Betriebsrat muss bei digitalen Tools, Zeiterfassung, ePA, KI-Systemen frühzeitig eingebunden werden
- § 90 BetrVG: Unterrichts- und Beratungsrechte bei Planung technischer Anlagen
- § 91 BetrVG: Schutz vor Überlastung durch technische Neuerungen
- § 94 BetrVG: Mitbestimmung bei Personalfragebögen oder Bewertungssoftware
- Ziel: Mitarbeiterorientierte, transparente und sozialverträgliche Digitalisierung des Klinikbetriebs

Onlinezugangsgesetz (OZG):

- Verpflichtet Bund, Länder und Kommunen zur digitalen Bereitstellung von Verwaltungsleistungen
- Krankenhäuser müssen Verwaltungsprozesse und Portale interoperabel, barrierefrei und sicher gestalten
- Relevant bei Fördermittelverwaltung, Personalprozessen, Behördenkommunikation und KHZG-Anträgen
- Einführung erfolgt schrittweise über OZG 2.0 mit stärkerer Nutzerorientierung bis 2026
- Ziel: Einheitlicher digitaler Zugang zu Verwaltungsleistungen über das Portalverbundsystem

E-Government-Gesetze (EGovG / EGovG NRW):

- Verpflichten Behörden und öffentliche Einrichtungen zur elektronischen Aktenführung (§ 6 EGovG)
- Nutzung der elektronischen Identifikation (eID) vorgeschrieben (§ 4 EGovG)
- Ersetzendes Scannen (§ 7 EGovG) erlaubt digitale Archivierung mit Originalersatz
- Pflichten zur Barrierefreiheit und Interoperabilität (§§ 8 f. EGovG)
- Betreffen Universitätskliniken und kommunale Häuser, private Träger bei hoheitlichen Aufgaben
- Ziel: Effiziente, rechtssichere und papierlose Verwaltungsprozesse

European Accessibility Act (EAA)

- EU-Richtlinie 2019/882 zur Barrierefreiheit digitaler Produkte und Dienste
- Umsetzung in Deutschland durch Barrierefreiheitsstärkungsgesetz (BFSG) und BFSG-Verordnung (BFSGV)
- Gilt ab 28. Juni 2025, mit Übergangsfrist bis 2030 für bestehende Anwendungen
- Verpflichtet zur barrierefreien Gestaltung von Websites, Apps, Patientenportalen und KI-Systemen
- Anforderungen: Screenreader-Kompatibilität, leichte Sprache, klare Struktur und Bedienbarkeit
- Ziel: Digitale Teilhabe für alle Nutzergruppen, insbesondere Menschen mit Behinderung

Landeshochschulgesetz NRW (HG NRW)

- Regelt Aufbau und Verantwortung von Hochschulen und Universitätskliniken
- §§ 31, 32 HG NRW: Gemeinsame Verantwortung von Fakultät und Klinikum für Forschung & Lehre
- § 73 HG NRW: Verarbeitung personenbezogener Daten nur mit Einwilligung oder Gesetz
- Pflicht zur Wahrung wissenschaftlicher Integrität und Persönlichkeitsrechte
- Forschung mit Gesundheitsdaten nur mit Ethikvotum und Datenschutzkonzept zulässig
- Ziel: Verbindung von Forschungsfreiheit, Datenschutz und ethischer Verantwortung

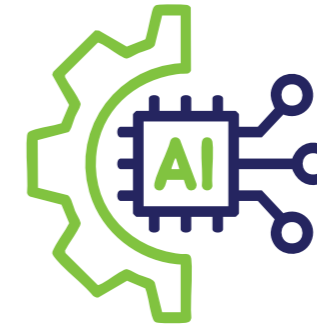
Digitalisierung von Verwaltungsprozessen im Klinikbetrieb

- Betrifft Aufnahme, Abrechnung, Personal, Dokumentenmanagement, Behördenkommunikation
- Relevante Normen: DSGVO, BDSG, DSG NRW, KHZG, OZG, GoBD
- Mitbestimmungspflicht nach § 87 BetrVG bei Einführung neuer Personal-IT-Systeme
- KRITIS-Krankenhäuser unterliegen den IT-Sicherheitsanforderungen des BSIG (inkl. IT-SiG 2.0) und künftig den europaweit harmonisierten NIS2-Pflichten
- Erfordert klare organisatorische Zuständigkeiten, Rollenmodelle und Sicherheitskonzepte
- Ziel: Rechtssichere, effiziente und technisch robuste Verwaltungsdigitalisierung



Impressum

Herausgeber: DATATREE AG, Bovermannstraße 8, 44141 Dortmund, T +49 231 54380-300 | office@datatree.ag | www.datatree.ag
Sitz der Gesellschaft: Sitz der Gesellschaft: Dortmund, Registergericht: Amtsgericht Dortmund | Registernummer: HRB 33773 |
Umsatzsteuer-Identifikationsnummer: DE279402614
Vorstand: Prof. Dr. Thomas Jäschke | Vorsitzender des Aufsichtsrates: Prof. Dr. Julius Reiter
Autorin: Enise Ba, LL.B. | Design und Umsetzung: Marina Lutsyuk
© 2025 DATATREE AG | veröffentlicht



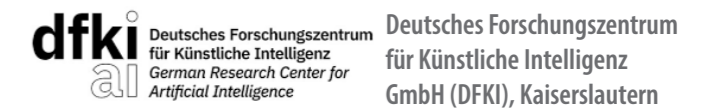
KI-AIM adressiert die datenschutzrechtlichen Hürden beim Einsatz von KI in der Medizin, indem eine Plattform zur Anonymisierung und Synthetisierung realitätsnaher Gesundheitsdaten entwickelt wird. Die erzeugten, nachweislich anonymen Datensätze ermöglichen eine rechtssichere Nutzung für Forschung und industrielle Entwicklung KI-basierter Anwendungen.

Damit leistet das Projekt einen zentralen Beitrag zur Beschleunigung medizinischer Innovationen und zur Stärkung des digitalen Gesundheitsökosystems in Deutschland und Europa.

Für Westfälische Wilhelms-Universität Münster



Projektpartner:





DATATREE
YOUR COMPLIANCE PROVIDER