Datenschutz im Gesundheitswesen

Zukünftige juristische Verpflichtungen, Haftungsrisiken und regulatorische Dynamiken

Ein Beitrag von Florian-Julian Hoffmann, Rechtsanwalt bei HFBP Rechtsanwälte und Notare.

Die tatsächliche und juristische Bedeutung des Datenschutzes im Gesundheitswesen wird in den kommenden Jahren erheblich zunehmen. Medizinische Einrichtungen, Krankenhausträger, Vertragsärztinnen und -ärzte und weitere Leistungserbringerinnen und -erbringer bewegen sich bereits heute in einem komplexen Gefüge aus Datenschutzrecht, nationalem Gesundheitsrecht, berufsrechtlichen Verschwiegenheitspflichten, spezialgesetzlichen Dokumentationsanforderungen und IT-Sicherheitsvorgaben. Mit der fortschreitenden Digitalisierung, der flächendeckenden Einführung der elektronischen Patientenakte, zunehmender telemedizinischer Anwendungen, der Nutzung von Cloud-Infrastrukturen und KI-gestützter Diagnostiksysteme wird sich dieses Regelungsumfeld naturgemäß weiter verdichten. Gleichzeitig steigen Erhebung, Umfang und Verknüpfbarkeit von Gesundheitsdaten exponentiell an.

Eine zentrale Rolle nimmt dabei die Europäischen Union ein. Besonders merklich wurde dies für die meisten Menschen mit Inkrafttreten der Datenschutz-Grundverordnung (DSGVO). Die DSGVO hat das Datenschutzrecht unionsweit vereinheitlicht, unmittelbar anwendbar ausgestaltet und mit empfindlichen Sanktionsmechanismen versehen. Für das Gesundheitswesen besonders relevant ist Art. 9 DSGVO, der Gesundheitsdaten als besondere Kategorie personenbezogener Daten qualifiziert und deren Verarbeitung grundsätzlich untersagt, es sei denn, es greift ein eng auszulegender Ausnahmetatbestand, welcher in Absatz 2 und 3 festgelegt wurde.

Datenschutz als Grundrechtsmaterie und Sanktionsmöglichkeiten

Gesundheitsdaten zählen zu den sensibelsten personenbezogenen Informationen. Sie betreffen nicht nur den physischen und psychischen Zustand einer Person, sondern erlauben Rückschlüsse auf genetische Dispositionen, Lebensführung, soziale Umstände und potenzielle zukünftige Erkrankungsrisiken. Der Schutz dieser Daten ist daher nicht lediglich einfachgesetzlich, sondern sogar grundrechtlich verankert.

Auf nationaler Ebene ist insbesondere das vom Bundesverfassungsgericht entwickelte Grundrecht auf informationelle Selbstbestimmung einschlägig, das aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz hergeleitet wird. Auf europäischer Ebene gewährleistet Art. 8 der Charta der Grundrechte der Europäischen Union ausdrücklich den Schutz personenbezogener Daten als eigenständiges Grundrecht.

Die juristische Relevanz ist erheblich: Datenschutzverstöße im Gesundheitsbereich sind nicht lediglich administrative Ordnungswidrigkeiten, sondern berühren den Kernbereich privater Lebensgestaltung. Daraus folgen eine gesteigerte Eingriffsintensität und eine strenge Verhältnismäßigkeitsprüfung bei jeder Datenverarbeitung. Für die heilberufliche Tätigkeit bedeutet dies, dass datenschutzrechtliche Verfehlungen nicht nur zivilrechtliche Schadensersatzansprüche auslösen können, sondern zugleich berufsrechtliche und im Extremfall sogar verfassungsrechtliche Implikationen haben können.

Die DSGVO bietet bei Verstößen die Möglichkeit der Verhängung einer empfindlichen Geldbuße nach Art. 83 DSGVO durch die zuständige Datenschutzaufsichtsbehörde. Zu erwähnen ist, dass die Höhe der Geldbuße einen abschreckenden Charakter haben soll, um erneute Verstöße zu verhindern.

Daneben kann die Aufsichtsbehörde gemäß Art. 58 DSGVO folgende Maßnahmen ergreifen:

- (vorsorgliche) Warnung
- Anordnung der Aussetzung der Datenübermittlung außerhalb der EU
- Anordnung, die bzw. eine bestimmte Datenverarbeitung zu beschränken
- Anordnung, bestimmte Daten zu berichtigen bzw. zu löschen
- Verbot der Verarbeitung von bestimmten Daten

Beachtlich ist, dass die datenschutzrechtlich verantwortliche Praxisinhaberin oder der datenschutzrechtlich verantwortliche Praxisinhaber auch dann von der Aufsichtsbehörde in Anspruch genommen werden kann, wenn der der Datenschutzverstoß nicht durch ihn, sondern durch eine Mitarbeiterin oder einen Mitarbeiter der Praxis verursacht wurde. Selbst Verstöße, verursacht von externen, dienstleistenden Personen, können der Praxisinhaberin oder dem Praxisinhaber zugerechnet werden.

Dynamik von Rechtsprechung und Regulierung

Die Fortentwicklung des Gesundheitsdatenschutzes wird maßgeblich auch durch die Rechtsprechung geprägt. Wenn zentrale Be-

griffe der DSGVO, wie etwa „personenbezogene Daten“ und „Verarbeitung“, regelmäßig weit bzw. der Begriff der „Einwilligung“ eng ausgelegt werden, führt dies faktisch zu einer kontinuierlichen Verschärfung der gesetzlichen Anforderungen, ohne dass es dazu formaler Gesetzesänderungen bedarf.

Nationale Konkretisierung und ärztliche Verantwortung

Auf nationaler Ebene erfolgt die Konkretisierung insbesondere durch das Bundesdatenschutzgesetz sowie durch spezialgesetzliche Regelungen im Sozial- und Gesundheitsrecht. Hinzu treten berufsrechtliche Vorschriften der Ärztekammern sowie strafrechtliche Normen, insbesondere § 203 StGB, welcher die Verletzung von Privatgeheimnissen unter Strafe stellt.

Für Ärztinnen und Ärzte lassen sich drei zentrale Pflichtenbereiche identifizieren:

1. Rechtmäßige Datenerhebung und -verarbeitung
Jede Verarbeitung bedarf einer tragfähigen Rechtsgrundlage. Im Behandlungsverhältnis stützt sie sich häufig auf Art. 9 Abs. 2 lit. h DSGVO in Verbindung mit nationalem Recht. Einwilligungen müssen freiwillig, informiert, spezifisch und widerruflich sein. Formelhafte oder pauschale Erklärungen genügen nicht.

2. Maßnahmen zur Gewährung der Datensicherheit
In einer kieferorthopädischen Praxis sind angemessene technische und organisatorische Maßnahmen zu treffen, um ein dem jeweiligen Risiko entsprechendes Schutzniveau für personenbezogene Daten sicherzustellen. Welche konkreten Maßnahmen erforderlich sind, hängt insbesondere vom Stand der Technik, dem Implementierungsaufwand sowie von Art, Umfang, Umständen und Zweck der Datenverarbeitung ab. Ebenso zu berücksichtigen sind die Eintrittswahrscheinlichkeit und die mögliche Schwere von Risiken für die Rechte und Freiheiten betroffener Personen. Folglich sind die getroffenen Maßnahmen regelmäßig zu überprüfen, neu zu bewerten und gegebenenfalls anzupassen.
Da in Praxen besonders sensible Gesundheitsdaten verarbeitet werden, ist hier ein erhöhtes Schutzniveau gegeben.
Zu den typischen Maßnahmen zur Gewährleistung der Datensicherheit zählen beispielsweise:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten,
- die dauerhafte Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der eingesetzten Systeme und Dienste,
- die Möglichkeit, personenbezogene Daten bei einem physischen oder technischen Zwischenfall zeitnah wiederherzustellen,
- sowie die regelmäßige Überprüfung und Bewertung der Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen.

Darüber hinaus sind – auch im Hinblick auf die ärztliche Schweigepflicht – geeignete organisatorische Vorkehrungen zu treffen. Dazu gehört beispielsweise, am Empfang und im Wartebereich auf ausreichende Diskretion zu achten, vertrauliche Gespräche ausschließlich in geschlossenen Räumen zu führen und Patientenakten nicht unbeaufsichtigt zugänglich zu lassen, sondern sicher und verschlossen aufzubewahren. Zudem sind Mitarbeitende regelmäßig für den vertraulichen Umgang mit Patientendaten zu sensibilisieren und entsprechend zu verpflichten.

3. Reaktionspflichten bei Datenschutzvorfällen
Bei Verletzungen des Schutzes personenbezogener Daten bestehen Meldepflichten gegenüber der zuständigen Aufsichtsbehörde binnen 72 Stunden (Art. 33 DSGVO) sowie gegebenenfalls Benachrichtigungspflichten gegenüber der betroffenen Person (Art. 34 DSGVO). Dies setzt strukturierte Incident-Response-Prozesse voraus, einschließlich Dokumentation, Ursachenanalyse und Abhilfemaßnahmen.
Zukünftig ist nicht ausgeschlossen, dass der Gesetzgeber verbindliche Zertifizierungsanforderungen für Praxissoftware, Cloud-Lösungen oder KI-Diagnostiksysteme normiert. Bereits heute existieren branchenspezifische Sicherheitsstandards, etwa im Rahmen der Telematikinfrastruktur.

> „Bei Verletzungen des Schutzes personenbezogener Daten bestehen Meldepflichten gegenüber der zuständigen Aufsichtsbehörde binnen 72 Stunden (Art. 33 DSGVO) sowie gegebenenfalls Benachrichtigungspflichten gegenüber der betroffenen Person (Art. 34 DSGVO).“

Erweiterung ärztlicher Haftungsrisiken

Die Haftungsdimension des Gesundheitsdatenschutzes ist im Wandel. Art. 82 DSGVO normiert einen eigenständigen Schadensersatzanspruch. Bereits immaterielle Schäden – etwa Kontrollverlust über persönliche Daten oder Angst vor Missbrauch – können ersatzfähig sein.

Deliktische Haftung
Bei Datenlecks, Ransomware-Angriffen oder unbefugtem Zugriff auf Patientenakten drohen Schadensersatz- und Schmerzensgeldansprüche. Die Rechtsprechung tendiert zunehmend dazu, auch geringfügige Datenschutzverstöße nicht als Bagatellen zu qualifizieren. Für größere Einrichtungen besteht zudem ein Reputationsrisiko, das mittelbar wirtschaftliche Schäden verursachen kann.

Vertragliche Haftung
Das Behandlungsverhältnis ist als Dienstvertrag mit besonderen Schutzpflichten ausgestaltet. Fehlerhafte oder unvollständige Datenschutzaufklärung könnte die Wirksamkeit einer Einwilligung beeinträchtigen und unter Umständen als Nebenpflichtverletzung gewertet werden.

Organisationshaftung
Unzureichende IT-Sicherheitsstrukturen können als Organisationsverschulden qualifiziert werden. Wird etwa keine angemessene Zugriffsbeschränkung implementiert oder werden bekannte Sicherheitslücken nicht zeitnah geschlossen, kann dies haftungsrechtlich relevant sein. In größeren Einrichtungen trifft die Leitungsebene eine eigenständige Überwachungs- und Organisationsverantwortung.

Systemische Compliance als Zukunftsmodell

Juristisch zeichnet sich ein Wandel ab: Datenschutz wird von einer punktuellen Einzelfallprüfung zu einer dauerhaften Systemverantwortung. Die DSGVO folgt dem Grundsatz der „Accountability“ (Art. 5 Abs. 2 DSGVO). Verantwortliche müssen nicht nur rechtmäßig handeln, sondern dies auch nachweisbar dokumentieren können.
Notwendig hierfür erscheint ein strukturiertes Datenschutzmanagementsystem, bestehend aus Risikoanalysen, Verzeichnissen von Verarbeitungstätigkeiten, Datenschutz-Folgenabschätzungen bei Hochrisiko-Verarbeitungen, regelmäßigen Schulungen des Personals sowie internen Kontrollmechanismen. Datenschutz wird damit Teil der Governance-Struktur medizinischer Einrichtungen und Bestandteil des Qualitätsmanagements.
Zudem wird die Wichtigkeit des Zusammenspiels von Datenschutz, IT-Sicherheit und medizinischer Behandlungsqualität zunehmen. Ein Ausfall digitaler Systeme, beispielsweise infolge eines Cyberangriffs, kann unmittelbar die Patientenversorgung beeinträchtigen. Datenschutz ist daher nicht isoliert zu betrachten, sondern als Element der Patientenversorgung und -sicherheit.

Fazit

Die zukünftige Entwicklung des Gesundheitsdatenschutzes wird durch fortschreitende Europäisierung, dynamische Rechtsprechung, sektorale Spezialregulierung und technologische Innovation geprägt sein. Für Ärztinnen und Ärzte bedeutet dies eine Verschiebung von punktueller Compliance hin zu struktureller Rechtssicherheit.
Datenschutz entwickelt sich von einer administrativen Nebenpflicht zu einem elementaren Bestandteil (zahn-)medizinischer Berufsausübung. Er beeinflusst Haftungsrisiken, Organisationsstrukturen, Investitionsentscheidungen und die Vertrauensbasis zwischen Patientinnen sowie Patienten und den sie behandelnden Fachkräften. Wer Datenschutz zukünftig noch als formale Dokumentationsaufgabe versteht, verkennt seine strategische und haftungsrechtliche Tragweite. Nachhaltige Rechtssicherheit im Gesundheitswesen wird nur durch systematische, technisch fundierte und juristisch reflektierte Datenschutzkonzepte erreichbar sein.


© HFBP Rechtsanwälte und Notare

Florian-Julian Hoffmann
HFBP Rechtsanwälte und Notare
f.hoffmann@hfbp.de

Waage: © Saidurra12 – stock.adobe.com