I Grundlagen

Daten über den Gesundheitszustand weisen einen starken Bezug zur Intimsphäre auf und geben Auskunft über seelische und körperliche Leiden, Eigenschaften und Dispositionen; sie sind mithin **äußerst sensibel**. Deshalb ist es von großer Bedeutung, dass sich Patienten vertrauensvoll in ein Krankenhaus begeben können, ohne befürchten zu müssen, dass die Informationen, die sie zum Zwecke der Behandlung über sich offenlegen, zu ihrem Schaden oder Nachteil genutzt werden.[1]

Datenschutz im Gesundheitswesen hat also das Ziel, die Patienten davor zu schützen, dass Informationen über ihren Gesundheitszustand ohne Rechtsgrundlage erhoben, verarbeitet oder weitergegeben werden und die Betreffenden so nicht mehr erfahren, wer was wann und bei welcher Gelegenheit über sie weiß.

Insbesondere die automatisierte Datenverarbeitung eröffnet heutzutage die Möglichkeit, Daten aus unterschiedlichen Datenbeständen in kürzester Zeit und in großem Umfang selbst über große Entfernungen abzurufen.

1 Das informationelle Selbstbestimmungsrecht – Historie

Im Jahre 1983 überprüfte und definierte das BVerfG[2] die verfassungsrechtlichen Rahmenbedingungen des Datenschutzes von Grund auf neu. Ursache dieser Überprüfung waren Verfassungsbeschwerden gegen das Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (**Volkszählungsgesetz**)[3] vom 25. März 1982. Das Gesetz ordnete eine umfangreiche Totalerhebung gegenüber allen volljährigen oder einen eigenen Haushalt führenden minderjährigen Personen in Deutschland an. Abgefragt wurden – unter Anordnung einer **Auskunftspflicht** – u. a.

- Angaben über die (Nicht-)Zugehörigkeit zu einer Religionsgesellschaft,
- die Quelle des überwiegenden Lebensunterhalts,

---

1 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Patientendatenschutz im Krankenhaus, www.datenschutzzentrum.de, I.1.

2 BVerfGE 65, S. 1 ff.

3 Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz) vom 25. März 1982, BGBl. I, S. 369 ff.

- die erzielten Schulabschlüsse,
- die Art der Beteiligung am Erwerbsleben,
- die Eigenschaft als Insasse einer Anstalt oder die Zugehörigkeit zum Personal der Anstalt,
- die Art, Größe, Ausstattung der Wohnung,
- detaillierte Angaben über die Arbeitsstätte,
- die Summe der Bruttolöhne und -gehälter des vorangegangenen Kalenderjahres sowie
- diverse weitere Daten.

Das Vorhaben führte zu massiven öffentlichen Diskussionen und Protesten. Da das Gesetz im Bundestag keinerlei Kontroversen ausgelöst hatte und – entgegen den von Datenschutzbeauftragten und anderen Experten erhobenen Bedenken – einstimmig verabschiedet worden war, existierte keine parlamentarische Opposition, die auf eine detaillierte verfassungsrechtliche Prüfung der Reichweite und Grenzen staatlicher Informationserhebung gedrängt hätte. Daher blieb den Betroffenen zur Durchsetzung eines kurzfristigen Stopps der Volkszählung nur, das BVerfG anzurufen.

Vorausgegangen waren dem Volkszählungsgesetz mit der »Mikrozensusentscheidung«[4] und dem »Scheidungsaktenbeschluss«[5] des BVerfG bereits grundlegende Ausführungen zum allgemeinen Persönlichkeitsrecht und zur informationellen Selbstbestimmung:

So hatte das BVerfG in der »**Mikrozensusentscheidung**« ausgeführt, dass es mit der Menschenwürde nicht zu vereinbaren sei, wenn der Staat das Recht für sich in Anspruch nehmen könne, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich sei. Eine statistische Befragung zur Person könne deshalb dort als entwürdigend und als Bedrohung des Selbstbestimmungsrechts empfunden werden, wo sie den Bereich menschlichen Eigenlebens erfasse, der von Natur aus Geheimnischarakter habe.

Im »**Scheidungsaktenbeschluss**«[6] erklärte das BVerfG die Vorlage von gerichtlichen Scheidungsakten an den Dienstvorgesetzten eines Beamten zur Durchführung eines Disziplinarverfahrens für verfassungswidrig. Dabei betonte es, dass das Grundgesetz dem einzelnen Bürger einen unantastbaren Bereich privater Lebensgestaltung gewähre, welcher der Einwirkung der öffentlichen Gewalt entzogen sei. Das verfassungskräftige Gebot einer Achtung der Intimsphäre des Einzelnen habe seine Grundlage in dem durch Artikel 2 Abs. 1 GG verbürgten Recht auf freie Entfaltung der Persönlichkeit.

Angesichts der schnellen Entwicklung der automatisierten Datenverarbeitung erwiesen sich diese Entscheidungen bald als nicht mehr ausreichend und lückenhaft.

Insofern bot das **Volkszählungsgesetz** die Möglichkeit, die gesamte bisherige Datenschutzproblematik neu zu ordnen. Mit dem Urteil vom 15. Dezember 1983[7]

4 BVerfGE 27, S. 1 ff.
5 BVerfGE 27, S. 344 ff.
6 BVerfGE 27, S. 344 ff.
7 BVerfGE 65, S. 1 ff.

hat das BVerfG diese Gelegenheit wahrgenommen und beim Volkszählungsgesetz deutlichen Korrekturbedarf angemahnt. Dabei war das sog. Recht auf informationelle Selbstbestimmung die Antwort des BVerfG auf die Frage nach der verfassungsrechtlichen Grundlage des Datenschutzes.[8] Das BVerfG stellte im Wesentlichen wie folgt fest:

> *»Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, (…). Ihrem Schutz dient (…) das in Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG gewährleistete* ***allgemeine Persönlichkeitsrecht*** *(…). Die bisherigen Konkretisierungen durch die Rechtsprechung umschreiben den Inhalt des Persönlichkeitsrechts nicht abschließend. Es umfasst (…) auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden (…)* ***Recht auf informationelle Selbstbestimmung*** *(…)*
>
> *Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem* ***Grundrecht*** *des Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. (…)« [hervorgehoben durch die Verfasser]*

Mit dieser Ableitung des informationellen Selbstbestimmungsrechts aus dem allgemeinen Persönlichkeitsrecht hat das BVerfG die verfassungsrechtlichen Grundlagen des Datenschutzes neu definiert, ohne ein neues Grundrecht zu schaffen.[9] Das BVerfG hat vielmehr aus dem Grundgesetz selbst folgende Datenverarbeitungsbarrieren abgeleitet:

- Die wichtigste Barriere folgt aus dem Erfordernis einer **bereichsspezifischen gesetzlichen Regelung**. Der Gesetzgeber hat konkrete Datenverarbeitungssituationen zu definieren, seine daran geknüpften Informationserwartungen zu präzisieren und auf diese Situationen zugeschnittene Verarbeitungsbedingungen vorzugeben. Nur eine solche, Art, Umfang und Verwendungszweck der erhobenen Daten klar beschreibende Rechtsgrundlage kann den Eingriff in das informationelle Selbstbestimmungsrecht rechtfertigen. Der Datenverarbeitungsprozess muss für die Betroffenen durchschaubar und nachvollziehbar sein. Ein Rückzug auf Generalklauseln zur Datenerhebung und -verarbeitung ist damit nicht mehr möglich.[10]
- Eine **Datensammlung »auf Vorrat«** zu unbestimmten oder noch nicht bestimmbaren Zwecken ist unzulässig.
- Das Gesetz muss dem Grundsatz der **Verhältnismäßigkeit** genügen (Übermaßverbot). Je intensiver der Eingriff elementare Bereiche der informationellen Selbstbestimmung berührt, desto gewichtiger müssen die zu seiner Rechtfertigung vorgebrachten Gründe sein.
- Das Gesetz muss **verfahrensrechtliche Vorkehrungen** beinhalten, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

---

8 Simitis, NJW 1984, 398 ff.
9 Simitis, a. a. O.
10 Simitis, a. a. O.

Zudem hat das BVerfG deutlich gemacht, dass sich die Beschränkungen für eine Datenverarbeitung nicht nur an staatliche Institutionen richten, sondern auch an **private**. Adressat der Verfassungsnormen des Grundgesetzes sind zwar unmittelbar nur **staatliche Stellen**. Jedoch fließt das Verfassungsrecht mittelbar auch in das Privatrecht ein. Insbesondere auf Gesetze, welche die Rechtsbeziehungen zwischen Privaten regeln, haben die Grundrechte eine Ausstrahlungswirkung. Insofern ist Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG der klassische Anknüpfungspunkt für eine sog. Drittwirkung von Grundrechten.[11] Für den Einzelnen ist es nämlich unerheblich, ob die Einschränkung seiner informationellen Selbstbestimmung durch eine staatliche Institution oder ein privates Unternehmen erfolgt.

2 Hintergrund und Ziele zur DS-GVO

Seit dem 25.05.2018 ist nunmehr in datenschutzrechtlicher Hinsicht eine zentrale Weichenstellung auf EU-Ebene vorgenommen worden: Am 04.05.2016 wurde die »*Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)*«, kurz: »DS-GVO«, im Amtsblatt der Europäischen Union verkündet. Die DS-GVO ist am 20. Tag nach ihrer Veröffentlichung in Kraft getreten, beansprucht jedoch erst seit dem 25.05.2018 Geltung.

Die Ziele und Grundsätze der DS-GVO sind ausweislich des Erwägungsgrundes (ErwGr.) 9, den bestehenden erheblichen Risiken für den Schutz natürlicher Personen zu begegnen, die insbesondere im Zusammenhang mit der Benutzung des Internets bestehen. So habe es die vorhergehende Datenschutz-Richtlinie 95/46/EG nicht verhindern können, dass der Datenschutz in der Union unterschiedlich gehandhabt werde. Dies habe Rechtsunsicherheiten nicht ausräumen können. Während also eine EU-Richtlinie dem habe nicht begegnen können, sei nun eine EU-Verordnung erforderlich, damit in der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen gewährleistet sei und Unterschiede, die den freien Verkehr personenbezogener Daten im Binnenmarkt behindern könnten, angeglichen würden (ErwGr. 13).

Gemäß ErwGr. 11 erfordert ein unionsweiter wirksamer Schutz personenbezogener Daten ferner die Stärkung und präzise Festlegung der Rechte der betroffenen Personen (sog. Betroffenenrechte) sowie eine Verschärfung der Verpflichtungen für diejenigen, die personenbezogene Daten verarbeiten und darüber entscheiden, ebenso wie – in den Mitgliedstaaten – gleiche Befugnisse bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten sowie gleiche Sanktionen im Falle ihrer Verletzung.

11 Simitis, a. a. O.

3 Besondere Bedeutung der Patientendaten im Krankenhaus

Die Frage, warum die Beachtung des Datenschutzes im Krankenhaus von so großer Bedeutung ist, liegt auf der Hand – im Krankenhaus werden wie in kaum einer anderen Institution sensible, persönliche Daten erhoben, gespeichert und übermittelt. Dabei handelt es sich bei den Informationen über den Patienten, seine Verhältnisse und vor allem seine Krankheiten um Daten, die besonders schützwürdig und damit geheimhaltungsbedürftig sind. Die Offenbarung von Krankheiten, Leiden oder Beschwerden kann dem Einzelnen nicht nur unangenehm und peinlich, sondern sogar seiner sozialen Geltung abträglich sein.[12] Angaben über den Gesundheitszustand eines Menschen geben Aufschluss über intimste Verhältnisse; medizinische Daten gehören somit zu den **sensibelsten Informationen** schlechthin.

Hinzu kommt, dass Krankenhäuser u. a. als Leistungserbringer nach dem SGB V auftreten, Vertragspartner der Krankenkassen und des Patienten sind und gegenüber den Krankenhausmitarbeitern Arbeitgeberfunktionen wahrnehmen. Umfangreiche Dokumentationspflichten und das komplexe System der Leistungsabrechnung bedingen die Verarbeitung einer Fülle von Daten für Verwaltungs-, Planungs-, Versorgungs- oder auch Forschungsaufgaben.

Für **Krankenhausmitarbeiter und -verwaltungen** ist es daher von höchster Wichtigkeit, die vom Gesetzgeber und der Rechtsprechung gezogenen Grenzen für den Umgang mit Patientendaten sorgfältig zu beachten. Nur wenn Patienten absolut sicher sein können, dass die intimen Informationen über sie mit größtmöglicher Vertraulichkeit behandelt werden, wird das Krankenhaus den an ein modernes Dienstleistungsunternehmen gestellten Anforderungen gerecht. Dazu gehört es, aktiv auf einen Schutz der Patientendaten hinzuwirken. Das wesentliche Problem hierbei sind nicht vorsätzliche Verstöße gegen den Datenschutz, sondern vielmehr Unachtsamkeit und mangelnde Sensibilität beim Umgang mit den Daten. Deshalb gilt es, präventiv mögliche Lücken im Datenschutz aufzudecken und konsequent zu schließen. Die beste Hilfe hierbei sind für den Datenschutz sensibilisierte Mitarbeiter, die von sich aus auf mögliche Schwachstellen aufmerksam machen und so einen Schaden vom Patienten und vom Krankenhaus abwenden.

12 Vgl. BVerfG, Beschluss vom 08.03.1972, Az.: 2 BvR 28/71 = NJW 1972, 1123 ff.

II Zentraler Grundsatz der Verarbeitung

Sofern sich Krankenhäuser / die Verantwortlichen in Krankenhäusern mit der Frage der Zulässigkeit der Erhebung, Verarbeitung oder Nutzung von Daten eines Patienten auseinandersetzen, war bereits vor dem Geltungsbeginn der DS-GVO, also dem 25.05.2018, folgender Grundsatz von zentraler Bedeutung:

> ***Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dafür eine gesetzliche Grundlage existiert oder der Betroffene eingewilligt hat.***

Dieser Grundsatz folgte z. B. aus § 4 Abs. 2 BDSG in der bis zum 24.05.2018 geltenden Fassung oder landesrechtlichen Regelungen und war – von wenigen Ausnahmen abgesehen – Grundlage für jedwede Verarbeitung von Daten.

Sollte also weder eine gesetzliche Grundlage eine Verarbeitung erlauben noch eine Einwilligung des Betroffenen vorliegen, blieb als Konsequenz nur, die Datenverarbeitung zu unterlassen.

Seit dem 25.05.2018 beansprucht nunmehr die DS-GVO unmittelbare Geltung in Deutschland. Aus diesem Grunde bedarf es seit diesem Zeitpunkt hinsichtlich jeglicher Prüfung, ob eine Verarbeitung datenschutzrechtlich zulässig ist, der Prüfung der durch die DS-GVO / das DSG-EKD[13] / das KDG[14] bedingten Anforderungen.

1 Verbot mit Erlaubnisvorbehalt gem. DS-GVO

An dem o. g. zentralen Grundsatz hat sich inhaltlich nichts geändert. Dieser findet sich seit Geltungsbeginn der DS-GVO in Form eines sog. **Verbots mit Erlaubnisvorbehalt** für die Verarbeitung sog. »besonderer Kategorien personenbezogener Daten«, mithin z. B. von Gesundheitsdaten, in Art. 6 Abs. 1 a), 9 Abs. 2 a) DS-GVO / §§ 6 Ziff. 2, 13 Abs. 2 Ziff. 1 DSG-EKD / §§ 6 Abs. 1 b), 11 Abs. 2 a) KDG wieder.

Als Grundregel verbietet diese Vorschrift die Verarbeitung von genetischen Daten, biometrischen Daten, Gesundheitsdaten usw. Es wird also ein allgemeines Verbot der Verarbeitung aufgestellt. Zu diesem Verbot existieren Ausnahmen. Eine solche

---

13 Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz – DSG-EKD); hinsichtlich weiterführender Erläuterungen vgl. III.2.2.

14 Gesetz über den kirchlichen Datenschutz (KDG); hinsichtlich weiterführender Erläuterungen vgl. III.2.2.

Ausnahme stellt die Einwilligung der betroffene Person in die Verarbeitung z. B. der Gesundheitsdaten für einen oder mehrere festgelegte Zwecke dar (sog. **besonderer Erlaubnistatbestand** (Art. 6 Abs. 1 a), 9 Abs. 2 a) DS-GVO / §§ 6 Ziff. 2, 13 Abs. 2 Ziff. 1 DSG-EKD / §§ 6 Abs. 1 b), 11 Abs. 2 a) KDG).

Anders ausgedrückt bedeutet dies: Das Verarbeitungsverbot gilt nicht, wenn die betroffene Person in die Verarbeitung z. B. der Gesundheitsdaten einwilligt. Andere Ausnahmen von dem Verbot ergeben sich im Wesentlichen aus den anderen Regelungsgegenständen von Art. 6, 9 Abs. 2, Abs. 4 DS-GVO / §§ 6, 13 Abs. 2 DSG-EKD / §§ 6, 11 Abs. 2 KDG.

Bei der Beantwortung der Frage, ob eine Verarbeitung datenschutzrechtlich zulässig ist, bedarf es also nach wie vor der Prüfung,

- ob eine Befugnisnorm die Verarbeitung legitimiert oder
- eine Einwilligung der betroffenen Person vorliegt.

Hinsichtlich der sich daran anschließenden Fragen, welche Befugnisnormen existieren und welche Anforderungen im Einzelnen an Einwilligungen zu stellen sind, vgl. vertiefend die Ausführungen unter III sowie IV.

2 »Verarbeitung« als neuer Oberbegriff

Während die deutschen Gesetze früher auf einzelne Begrifflichkeiten wie das Erheben, Verarbeiten, Nutzen usw. von Daten abgestellt haben, bildet die **Verarbeitung** seit dem 25.05.2018 den Oberbegriff. Seitdem bezeichnet der Begriff »Verarbeitung« gemäß der Legaldefinition in § 4 Ziff. 2 DS-GVO / § 4 Ziff. 3 DSG-EKD / § 4 Ziff. 3 KDG

> *»jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.«*

3 Verhältnis zwischen ärztlicher Schweigepflicht und Datenschutz

Neben den datenschutzrechtlichen Anforderungen gilt es, im Krankenhausbereich zusätzlich den Anforderungen der ärztlichen Schweigepflicht gerecht zu werden.

Während sich der Schutz sensibler Daten in datenschutzrechtlicher Hinsicht an das **Krankenhaus als Institution** bzw. durch die DS-GVO direkt an den »Verantwortlichen« richtet, bezieht sich das Gebot der ärztlichen Schweigepflicht auf das **Innenverhältnis zwischen Arzt und Patient**, adressiert also insbesondere den Arzt.[15]

Das Verhältnis zwischen ärztlicher Schweigepflicht und datenschutzrechtlichen Regelungen lässt sich wie folgt beschreiben: Datenschutzrechtliche Regelungen einerseits sowie das Gebot der ärztlichen Schweigepflicht andererseits bilden jeweils eine die unbefugte Offenbarung von Patientendaten verhindernde Schranke (Hürde). Beide Schranken stehen gleichrangig nebeneinander. Man spricht insofern von dem sog. **Zwei-Schranken-Prinzip**[16], d. h. dass bei der Frage nach der Zulässigkeit einer Verarbeitung von Patientendaten stets beide Schranken überwunden werden müssen.

Wenn jedoch ein Gesetz mit gleichem Schutzniveau die Verarbeitung von Patientendaten ausdrücklich zulässt, ist auch das Gebot der Schweigepflicht gewahrt. Der Arzt und die übrigen schweigepflichtigen Krankenhausmitarbeiter handeln befugt, soweit sie sich auf eine gesetzliche Norm stützen können, die zur Offenbarung von Patienteninformationen verpflichtet oder zumindest berechtigt. Ihr Tun ist strafrechtlich gerechtfertigt. Einer Einwilligung des Betroffenen bedarf es nicht.

Diese Auffassung wird insbesondere vor dem Hintergrund vertreten, dass es nur schwer nachvollziehbar wäre, den einzelnen Arzt bzw. die berufsmäßig tätigen Gehilfen unter Strafe zu stellen, wenn gleichzeitig die Institution Krankenhaus zur Offenbarung personenbezogener Daten im Rahmen einer zulässigen Verarbeitung legitimiert ist.

Daran ändert z. B. auch der Beschluss des Kammergerichts (KG) vom 20.08.2010[17] nichts. Dieser Beschluss hat vielmehr den speziellen Hintergrund, dass ein Rechtsanwalt unter Berufung auf seine anwaltliche Verschwiegenheitspflicht Auskünfte gegenüber dem Berliner Landesdatenschutzbeauftragten verweigerte. Das KG kam mit Beschluss vom 20.08.2010 zu dem Ergebnis, dass sich der betroffene Rechtsanwalt auf seine Verschwiegenheitspflicht berufen konnte, obwohl gemäß § 38 Abs. 3 Satz 1 BDSG (a.F.) die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen haben. Dies begründete das Gericht in erster Linie damit, dass der Auskunftspflichtige gemäß § 38 Abs. 3 Satz 2 BDSG (a.F.) die Auskunft auf solche Fragen verweigern kann, deren Beantwortung ihn der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. In dieser Fallkonstellation wird somit das Konkurrenzverhältnis zwischen datenschutzrechtlicher Übermittlungsverpflichtung und strafrechtlicher Offenbarungsbefugnis bereits durch die Vorschrift selbst, nämlich § 38 Abs. 3 Satz 2 BDSG (a.F.), geklärt. Da dies jedoch eine spezielle gesetzliche Regelung betrifft, gibt auch der Beschluss des KG keinen Aufschluss darüber, ob das Gebot der Schweigepflicht gewahrt ist, wenn

15 Vgl. hierzu vertiefend die Ausführungen zur »Ärztlichen Schweigepflicht« unter V.
16 Zum »Zwei-Schranken-Prinzip« vgl. auch Seelos, 550.
17 Az.: Ws (B) 51/07 – 2 Ss 23/07.

ein Gesetz mit gleichem Schutzniveau die Verarbeitung von Patientendaten, z. B. im Rahmen einer Auftragsverarbeitung, ausdrücklich zulässt. Der Beschluss klärt also nicht das Verhältnis zwischen datenschutzrechtlicher Verarbeitungserlaubnis und strafrechtlicher Offenbarungsbefugnis generell.

Ferner ist zu beachten, dass die **ärztliche Schweigepflicht** bei der Verarbeitung aller Patientendaten im Krankenhaus und unabhängig von der jeweiligen Trägerschaft des Krankenhauses **stets zu beachten** ist. Sie wird über das Standesrecht hinaus in § 203 StGB mit anderen Sondertatbeständen der Geheimniswahrung allgemeinverbindlich geregelt.

III Datenschutznormen/-regelungen

Wie zuvor unter II. dargestellt, ist die datenschutzrechtliche Zulässigkeit der Verarbeitung personenbezogener Daten davon abhängig, ob

- entweder eine gesetzliche Grundlage existiert, die die Verarbeitung erlaubt/legitimiert oder
- eine Einwilligung der betroffenen Person vorliegt.

Für die Beantwortung der Frage, ob Daten verarbeitet werden dürfen, bedarf es also u. a. der Prüfung des Vorliegens einer datenschutzrechtlichen Befugnisnorm.

Eine einheitliche Rechtsgrundlage bzw. ein einzelnes Gesetz für den Patientendatenschutz im Krankenhaus existiert in Deutschland bedauerlicherweise nicht. Vielmehr gibt es eine Fülle datenschutzrechtlicher Regelungen auf Landes- und Bundes- sowie EU-Ebene. Diese Regelungen sind unübersichtlich und aufgrund ihres unterschiedlichen Verhältnisses zueinander für den Anwender äußerst kompliziert.

Bei der Beurteilung der Zulässigkeit einer Verarbeitung (Erheben, Erfassen, Speichern, Verwendung, Übermittlung usw.) personenbezogener Daten kommen (neben der ärztlichen Schweigepflicht[18]) also verschiedenste Gesetze/Verordnungen zur Anwendung. Welche dies sind bzw. im Einzelfall sein können, wird nachfolgend dargestellt.

1 Übersicht über die Regelungen

Als datenschutzrechtliche Regelungen/Befugnisnormen sind folgende Gesetze/Verordnungen zu nennen:

Auf europäischer Ebene:

- EU Datenschutz-Grundverordnung (DS-GVO).

18 Vgl. ausführlich zur ärztlichen Schweigepflicht die Ausführungen unter V sowie zum Verhältnis Datenschutz zur ärztlichen Schweigepflicht die Ausführungen unter II.3.