BUNDESÄRZTEKAMMER
KASSENÄRZTLICHE BUNDESVEREINIGUNG

Bekanntmachungen

Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis[1]

1 Diese für den Bereich der ärztlichen Praxis entwickelten Hinweise und Empfehlungen (Stand: 16.02.2018) können auf den Bereich des Krankenhauses nicht ohne Weiteres übertragen werden, da der Bereich der Datenverarbeitung im Krankenhaus zum Teil durch Landesdatenschutzgesetze geregelt ist und zudem die Organisationsabläufe in Krankenhäusern Modifikationen der hier entwickelten Grundsätze erfordern.

1. Einleitung

Die ärztliche Schweigepflicht ist von grundlegender Bedeutung für das besondere Vertrauensverhältnis zwischen Arzt und Patient.[2] Ärzte haben über das, was ihnen in ihrer Eigenschaft als Arzt anvertraut oder bekannt geworden ist, zu schweigen. Die ärztliche Schweigepflicht zählt zum Kernbereich der ärztlichen Berufsethik. Die berufsrechtliche Ausgestaltung der Schweigepflicht erfolgt durch die Bestimmungen des § 9 der (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBO-Ä) sowie die entsprechenden Regelungen der Berufsordnungen der Landesärztekammern.

Neben dem Vertrauensverhältnis zwischen Arzt und Patient umfasst der Schutzzweck der ärztlichen Schweigepflicht auch die Wahrung des Patientengeheimnisses, dessen Verletzung nach dem Strafgesetzbuch mit Geld- oder Freiheitsstrafe geahndet werden kann.

Bei der Informationsverarbeitung in der Arztpraxis ist neben der ärztlichen Schweigepflicht das Recht auf informationelle Selbstbestimmung des Patienten zu beachten. Für die niedergelassenen Ärzte sind Bestimmungen der europarechtlichen Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) von Bedeutung. Daneben erlauben zahlreiche Rechtsgrundlagen aus Fachgesetzen eine Datenverarbeitung. Das Datenschutzrecht enthält zudem Rechte für die Patienten, die im Zusammenhang mit bestimmten ärztlichen Pflichten zu berücksichtigen sind. Im Kontext der ärztlichen Dokumentationspflichten und Aufbewahrungspflichten erlangen vor allem datenschutzrechtliche Auskunfts- und Löschungsrechte der Patienten Bedeutung.

Der Einsatz von EDV in der Arztpraxis kann nicht mit der privaten Nutzung von Computern verglichen werden. Deshalb sind beim beruflichen Einsatz in der Arztpraxis auch aus strafrechtlichen und haftungsrechtlichen Gründen besondere Schutzvorkehrungen erforderlich. Besondere Bedeutung kommt insoweit der Technischen Anlage zu diesen Empfehlungen zu. Diese gibt einen kompakten Überblick über die zu empfehlenden IT-Sicherheitsmaßnahmen in den Arztpraxen.

2. Die ärztliche Schweigepflichtht

2.1. Rechtsgrundlagen und Rechtsfolgengen

Die ärztliche Schweigepflicht ist in § 9 Abs. 1 MBO-Ä beziehungsweise den entsprechenden Bestimmungen der Berufsordnungen der Landesärztekammern geregelt.[3] Danach haben Ärzte über das, was ihnen in ihrer Eigenschaft als Arzt anvertraut oder bekannt geworden ist, auch nach dem Tod des Patienten, zu schweigen. Die Schweigepflicht ergibt sich zudem als Nebenpflicht aus dem zwischen Arzt und Patient geschlossenen Behandlungsvertrag, der seit dem Inkrafttreten des Patientenrechtegesetzes in den §§ 630a ff. Bürgerliches Gesetzbuch (BGB) geregelt ist.[4] Mit der ärztlichen Schweigepflicht korrespondiert das durch § 203 des Strafgesetzbuches (StGB) geschützte Patientengeheimnis, das entsprechende Verstöße des Arztes gegen die Verschwiegenheitspflicht strafrechtlich sanktioniert. Nach § 203 Abs. 1 StGB wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis, offenbart, das ihm als Arzt anvertraut worden oder sonst bekanntgeworden ist. Ein Verstoß gegen die ärztliche Schweigepflicht kann daher neben berufsrechtlichen oder berufsgerichtlichen Maßnahmen auch Schadensersatzansprüche und sogar strafrechtliche Konsequenzen zur Folge haben.

2.2. Reichweite

Die ärztliche Schweigepflicht umfasst nach den Berufsordnungen der Landesärztekammern „*das, was ihnen in ihrer Eigenschaft als Ärztin oder Arzt anvertraut oder sonst bekannt geworden ist*“ (§ 9 Abs. 1 MBO-Ä). Die berufsrechtliche Schweigepflicht ist daher umfassend zu verstehen. Die Schweigepflicht ist grundsätzlich gegenüber Dritten, aber auch gegenüber anderen Ärzten, Familienangehörigen des Patienten sowie eigenen Familienangehörigen zu beachten. Nach dem Tod des Patienten besteht die ärztliche Schweigepflicht fort.

2.3. Adressaten der Schweigepflichtcht

Die in den Berufsordnungen der Landesärztekammern geregelte ärztliche Schweigepflicht betrifft sowohl niedergelassene als auch angestellte Ärzte. Dem Straftatbestand des § 203 StGB unterliegen zudem auch die Angehörigen anderer Heilberufe und Gesundheitsfachberufe, deren Ausbildung oder Berufsbezeichnung staatlich geregelt sind (z. B. Psychotherapeuten, Physiotherapeuten, Angehörige der Pflegeberufe). Gleiches gilt für die berufsmäßig tätigen Gehilfen der Ärzte, wie Medizinische Fachangestellte sowie Auszubildende und Personen, die zur Berufsvorbereitung in der Praxis tätig sind. Schließlich werden vom Strafgesetzbuch auch die *sonstigen mitwirkenden Personen* erfasst, also insbesondere Mitarbeiter von Dienstleistungsunternehmen, die beispielsweise mit der Wartung und Instandsetzung des elektronischen Praxisverwaltungssystems beauftragt sind.

2.4. Einschränkungen der ärztlichen Schweigepflicht

Ihren Praxismitarbeitern dürfen Ärzte uneingeschränkten Zugang zu den im Praxisbetrieb anfallenden Informationen über Patienten einräumen. Sowohl die Berufsordnungen als auch das Strafgesetzbuch gehen davon aus, dass insoweit kein Verstoß gegen die Schweigepflicht gegeben ist. Das gilt auch für Personen, die zur Berufsvorbereitung in der Praxis tätig sind, also Ärzte in Weiterbildung, Auszubildende oder Praktikanten. Darüber hinaus können sich Ausnahmen von der ärztlichen Schweigepflicht ergeben, wenn eine Einwilligung des Patienten vorliegt (2.4.1.), wenn gesetzliche Vorschriften dem Arzt eine Offenbarungspflicht auferlegen (2.4.2.) oder eine Offenbarungsbefugnis einräumen (2.4.3.). Schließlich kann der Arzt durch weitere Erlaubnisgründe (2.4.4.) berechtigt sein, Informationen über Patienten weiterzugeben.

2.4.1. Schweigepflichtentbindung durch Einwilligung

Die ausdrücklich oder konkludent erteilte Einwilligung des Patienten ist nur wirksam, wenn sie auf der freien Willensbildung und Entscheidung des Patienten beruht. Hierzu muss der Patient wissen, zu welchem Zweck er den Arzt legitimiert, patientenbezogene Informationen weiterzugeben. Die Einwilligung ist nur gültig, wenn sie hinreichend konkret bestimmt ist. Nicht ausreichend ist es daher, wenn beim Abschluss eines Behandlungsvertrages pauschal für alle denkbaren Fälle der Datenweitergabe eine vorweggenommene Einwilligungserklärung des Patienten eingeholt wird. Dementsprechend bedarf die Weitergabe von Be-

2 Berufs-, Funktions- und Personenbezeichnungen wurden unter dem Aspekt der Verständlichkeit dieses Textes verwendet. Eine geschlechtsspezifische Differenzierung ist nicht beabsichtigt.

3 Im Folgenden wird auf die Vorschriften der (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBO-Ä) Bezug genommen. Rechtswirkung entfalten die entsprechenden Bestimmungen der Berufsordnungen der Landesärztekammern.

4 Gesetz zur Verbesserung der Rechte von Patientinnen und Patienten (BGBl. 2013, Teil I, Nr. 9, S. 277).

Deutsches Ärzteblatt | 09. 03. 2018 | DOI: 10.3238/arztebl.2018.ds01

handlungsdaten an privatärztliche Verrechnungsstellen zum Zweck der Abrechnung ärztlicher Leistungen einer dezidierten Einwilligung des Patienten. Gleiches gilt für die Weitergabe von Patientendaten im Rahmen einer Praxisveräußerung. Liegt keine Einwilligung der Patienten vor, kann der die Praxis veräußernde Arzt die Patientenakten dem künftigen Praxisbetreiber im Rahmen eines Verwahrungsvertrages in Obhut geben. Letzterer muss die Patientenakten unter Verschluss halten und darf sie nur mit Einwilligung des Patienten einsehen oder weitergeben (§ 10 Abs. 4 MBO-Ä). Der Arzt sollte den Patienten gegebenenfalls auch auf die Folgen der Verweigerung einer Einwilligung hinweisen.

Eine wirksame Schweigepflichtentbindung erfordert in der Regel keine Schriftform. Dennoch ist es aus Beweisgründen ratsam, eine schriftliche Einwilligungserklärung zu verlangen. Zudem ist zu berücksichtigen, dass einzelne Datenschutzbestimmungen eine schriftliche Einwilligung verlangen (Vergleiche hierzu die Darstellung unter 3.4.2.). Eine konkludente Einwilligung liegt dann vor, wenn der Patient aufgrund der Umstände üblicherweise von einer Informationsweitergabe durch den Arzt an Dritte ausgehen muss und durch schlüssiges Verhalten seine Zustimmung signalisiert (z. B. Kopfnicken). Eine Offenbarungsbefugnis kann sich darüber hinaus aus einer mutmaßlichen Einwilligung ergeben, wenn der Patient seine Einwilligung nicht erklären kann, beispielsweise weil er bewusstlos ist. Eine mutmaßliche Einwilligung kann der Arzt zugrunde legen, wenn davon auszugehen ist, dass der Patient im Fall seiner Befragung mit der Offenbarung einverstanden wäre.

> **Hinweis:** Die Weitergabe von Patientendaten an private Versicherungsunternehmen bedarf ebenfalls einer Einwilligung des Patienten und muss auf den konkreten Anlass bezogen sein. Behauptet das Versicherungsunternehmen gegenüber dem Arzt das Vorliegen einer Schweigepflichtentbindungserklärung, sollte sich der Arzt eine Kopie vorlegen lassen und deren Inhalt prüfen. In Zweifelsfällen können Ärzte die Unterlagen dem Patienten in Kopie überlassen, so dass dieser selbst entscheiden kann, welche Informationen er an das Versicherungsunternehmen weitergibt.

Exkurs: Private Krankenversicherungen bedienen sich zum Zweck von Kosten-Risiko-Prüfungen häufig externer Gutachter. Hierfür bedarf es der Übermittlung der notwendigen Information aus der Patientenakte an den Gutachter. Patienten, die von der Versicherung zu einer entsprechenden Einwilligung aufgefordert werden, wenden sich nicht selten ratsuchend an ihren Arzt. Ärzte können selbstverständlich keine rechtliche Beratung vornehmen. Denkbar ist jedoch ein Hinweis auf die Mustererklärung „Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft“, die auf den Beschluss der obersten Aufsichtsbehörden für den Datenschutz vom 17.01.2012 zurückgeht.[5] Unter Gliederungspunkt 3.1. enthält der Beschluss einen Mustertext für eine Einwilligungserklärung und Schweigepflichtentbindung bei der Datenweitergabe zur medizinischen Begutachtung.

2.4.2. Gesetzliche Offenbarungspflichten

Neben der Einwilligung eines Patienten gestatten eine Reihe von Gesetzen Ausnahmen von der ärztlichen Schweigepflicht. Ein erheblicher Teil dieser gesetzlichen Bestimmungen verpflichtet den Arzt sogar zur Meldung oder Überlassung von Patienteninformationen.

Gesetzliche Offenbarungspflichten, die u. a. dem Gesundheitsschutz der Bevölkerung dienen, ergeben sich u. a. aus den folgenden Gesetzen:

- Infektionsschutzgesetz (§§ 6 ff. IfSG),
- Krebsregistergesetze der Länder (§ 12 Abs. 2 LKRG NRW),
- Röntgenverordnung (§ 17a Abs. 4 RöV, § 28 Abs. 8 RöV),
- Bestattungsgesetze der Länder (z. B. § 7 BestattungsG NRW),
- Strahlenschutzverordnung (§ 61 StrlSchV),
- Betäubungsmittelgesetz i. V. m. § 5b BtMVV,
- SGB VII – Gesetzliche Unfallversicherung (§§ 201 ff. SGB VII),
- Personenstandsgesetz (§ 19 PStG).

Speziell für Vertragsärzte ergeben sich zahlreiche Offenbarungspflichten aus dem Sozialgesetzbuch V. Die folgenden Beispiele sollen einen Überblick geben:

- Kassenärztliche Vereinigungen, z. B.
  - zum Zweck der allgemeinen Aufgabenerfüllung (§ 294 SGB V),
  - zum Zweck der Abrechnung (§ 295 Abs. 1 Nr. 2 SGB V),
  - zum Zweck der Qualitäts- und Wirtschaftlichkeitsprüfung im Einzelfall (§ 298 SGB V),
  - zum Zweck der Qualitätssicherung (§ 299 Abs. 1 SGB V);
- Prüfungsstellen i. S. d. § 106c SGB V
  - zum Zweck der Wirtschaftlichkeitsprüfung (§ 296 Abs. 4 SGB V);
- Krankenkassen, z. B.
  - zum Zweck der allgemeinen Aufgabenerfüllung (§ 294 SGB V),
  - zum Zweck der Mitteilung von Krankheitsursachen und drittverursachten Schäden (§ 294a SGB V),
  - Arbeitsunfähigkeitsbescheinigung (§ 284 i. V. m. § 295 Abs. 1 Nr. 1 SGB V);
- Medizinischer Dienst der Krankenkassen,
  - zum Zweck gutachterlicher Stellungnahmen und Prüfungen (§§ 275, 276 Abs. 2 SGB V).

Gesetzliche Offenbarungspflichten ergeben sich auch aus dem Strafgesetzbuch. Danach macht sich jeder Bürger der Nichtanzeige geplanter Straftaten schuldig, der von dem Vorhaben oder der bevorstehenden Ausführung der dort aufgeführten, besonders schweren oder gefährlichen Straftaten erfährt und keine Anzeige erstattet, obwohl die Tat noch abgewendet werden kann (§ 138 Abs. 1 Nr. 1 bis 8 StGB). Dies gilt grundsätzlich auch für Ärzte, die im Rahmen der Patientenversorgung von solchen geplanten Straftaten erfahren. Zwar sieht das Gesetz hinsichtlich bestimmter Straftaten (z. B. Brandstiftung oder Geldfälschung) Straffreiheit vor, wenn sich der Arzt ernsthaft bemüht hat, den Patienten von dem Verbrechen abzuhalten (§ 139 Abs. 3 StGB). Diese Ausnahme gilt aber u. a. nicht für Mord und Totschlag, erpresserischen Menschenraub, Geiselnahmen sowie bestimmte Straftaten durch terroristische Vereinigungen (§ 139 Abs. 3 StGB). Insoweit besteht eine uneingeschränkte Anzeigepflicht, wenn der Arzt tatsächlich Kenntnis von der Planung oder dem Bevorstehen eines solchen Verbrechens erhält. Bloße Verdachtsmomente begründen hingegen keine Anzeigepflicht des Arztes.

[5] Abrufbar auf der Homepage des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/170120121EinwilligungVersicherungswirtschaft.html?nn=409242.

2.4.3. Gesetzliche Offenbarungsbefugnisse

Gesetzliche Bestimmungen, die Ärzten eine Offenbarungsbefugnis einräumen, ergeben sich z. B. aus § 4 Abs. 3 des Gesetzes zur Kooperation und Information im Kinderschutz (KKG) und den entsprechenden Landesgesetzen zum Schutz von Kindern und Jugendlichen (z. B. § 11 Abs. 4 Berliner KiSchuG). Danach dürfen Ärzte unter bestimmten Voraussetzungen das Jugendamt über mögliche Kindswohlgefährdungen informieren und hierbei von der Schweigepflicht abweichen. Das Gesetz geht von einem gestuften Verfahren aus. Liegen gewichtige Anhaltspunkte für die Gefährdung eines Kindes oder Jugendlichen vor, sollen die Ärzte die Situation zunächst gemeinsam mit den Eltern oder sonstigen Personensorgeberechtigten erörtern und auf die Inanspruchnahme von privater oder staatlicher Unterstützung hinwirken. Diese Vorgehensweise kommt nach dem Gesetz ausdrücklich nur in Betracht, wenn keine zusätzliche Gefährdung für die betroffenen Kinder und Jugendlichen daraus resultiert. Gewichtige Anhaltspunkte im Sinne des § 4 KKG sind konkrete Hinweise oder Informationen, wie z. B. unplausible Verletzungen, unterlassene notwendige ärztliche Versorgung, Gewalttätigkeiten in der Familie oder Suchterkrankungen der Eltern. Hinsichtlich der Einschätzung einer Kindeswohlgefährdung räumt § 4 Abs. 2 KKG Ärzten einen Beratungsanspruch gegenüber dem Träger der öffentlichen Jugendhilfe ein. Im Rahmen einer solchen Beratung dürfen Ärzte allerdings nur pseudonymisierte Daten an das Jugendamt übermitteln. Eine Befreiung von der Schweigepflicht sieht § 4 Abs. 3 KKG schließlich für den Fall vor, dass eine Kindswohlgefährdung durch Hilfsmaßnahmen nicht abgewendet werden kann und der Arzt das Tätigwerden des Jugendamtes für erforderlich hält.

> **Hinweis:** In einzelnen Bundesländern sehen die Kinder- und Jugendschutzbestimmungen nicht nur eine Offenbarungsbefugnis, sondern eine Offenbarungspflicht gegenüber dem Jugendamt vor. Eine derartige Verpflichtung enthält etwa § 14 Abs. 6 des bayerischen Gesundheitsdienst- und Verbraucherschutzgesetzes sowie § 6 Abs. 2 des Kinderschutzgesetzes Sachsen-Anhalt.

Eine wichtige Offenbarungsbefugnis im Hinblick auf die strafrechtliche Schweigepflicht regelt § 203 Abs. 3 Satz 2 StGB für den Fall, dass Ärzte externe Personen oder Unternehmen zur Unterstützung des Praxisbetriebs einsetzen. In Abgrenzung zu den Mitarbeitern, die organisatorisch in das Praxisteam eingegliedert sind, spricht das Gesetz von *sonstigen mitwirkenden Personen*. Zu diesem Personenkreis zählen insbesondere Mitarbeiter von Dienstleistungsunternehmen oder selbstständig tätige Personen, die Dienstleistungen für Ärzte erbringen, z. B. in den Bereichen Telekommunikation, Praxisverwaltungssystem, Steuerberatung oder Buchhaltung. Gegenüber diesem Personenkreis sind Ärzte zur Offenbarung von Patientengeheimnissen berechtigt, soweit bestimmte Informationen für die konkrete Tätigkeit der jeweiligen Person erforderlich sind (§ 203 Abs. 3 S. 2 StGB).

> **Hinweis:** Allerdings werden Ärzte und andere Berufsgeheimnisträger häufiger nicht einschätzen können, welche Informationen für bestimmte Dienstleistungen erforderlich sind. Beispielsweise dürfte im Vorfeld einer Instandsetzung des Praxisverwaltungssystems nicht erkennbar sein, in welchem Umfang der Mitarbeiter eines IT-Dienstleisters Zugriff auf die Patientendaten benötigt. Daher sollte in einem Vertrag über die jeweilige Dienstleistung schriftlich vereinbart werden, dass das Unternehmen und dessen ausführende Mitarbeiter sich nur insoweit Kenntnis von Informationen über Patienten verschaffen, wie dies für die Vertragserfüllung erforderlich ist. Dies kann ggf. im Rahmen eines Vertrages über eine Auftragsdatenverarbeitung erfolgen (Vergleiche die Ausführungen unter 3.6.).

Zudem hat der Arzt nach dem Strafgesetzbuch dafür zu sorgen, dass die für ihn tätigen *sonstigen mitwirkenden Personen* zur Geheimhaltung verpflichtet werden (§ 203 Abs. 4 Nr. 1 StGB). Entweder nimmt der Arzt selbst die Geheimhaltungsverpflichtung der *sonstigen mitwirkenden Personen* vor, oder er verpflichtet das von ihm beauftragte Dienstleistungsunternehmen, dass es die für den Arzt eingesetzten Unternehmensmitarbeiter seinerseits zur Geheimhaltung verpflichtet. Diese zweite Variante ist praktisch unvermeidlich, wenn die Mitarbeiter des beauftragten Unternehmens nicht in der Arztpraxis tätig werden oder häufig wechselndes Personal eingesetzt wird. Das betrifft insbesondere die in der Praxis übliche Fernwartung von IT-Systemen. Unterlässt der Arzt die Geheimhaltungsverpflichtung oder deren Übertragung auf das beauftragte Unternehmen und verraten dessen Mitarbeiter Patientengeheimnisse, macht sich auch der Arzt strafbar (§ 203 Abs. 4 Nr. 1 StGB).

> **Hinweis:** Zu Beweiszwecken sollte die Geheimhaltungsverpflichtung bzw. deren Übertragung auf das beauftragte Dienstleistungsunternehmen in schriftlicher Form erfolgen. Gegenüber Rechtsanwälten, Steuerberatern und sonstige Berufsgeheimnisträgern ist keine gesonderte Geheimhaltungsverpflichtung erforderlich (§ 203 Abs. 4 StGB).

2.4.4. Weitere Erlaubnisgründe

Liegt weder eine gesetzliche Befugnis noch eine Einwilligung zur Offenbarung patientenbezogener Informationen vor, kann dennoch ausnahmsweise eine Berechtigung zur Offenbarung gegenüber Dritten zulässig sein. Solche Ausnahmen kommen grundsätzlich dann in Betracht, wenn der Schutz bedeutender Rechtsgüter oder Rechtsinteressen eine Einschränkung der ärztlichen Schweigepflicht erfordert (§ 9 Abs. 2 MBO-Ä). Dieser Rechtsgedanke ist in den Bestimmungen zum rechtfertigenden Notstand im Strafgesetzbuch geregelt (§ 34 StGB). Ein solcher Notstand kann insbesondere gegeben sein, wenn eine gegenwärtige Gefahr für die Gesundheit oder das Leben anderer Menschen besteht und durch ein Offenbaren von schweigepflichtigen Informationen die Gefahr abgewendet werden kann. Eine solche Situation kann z. B. vorliegen, wenn ein Patient infolge einer Krankheit oder durch den Einfluss von Arzneimitteln oder Betäubungsmitteln fahruntüchtig ist und der Arzt davon ausgehen muss, dass der Patient dennoch am Straßenverkehr teilnimmt. Der Arzt hat im Einzelfall eine Abwägung vorzunehmen, ob das Risiko für Gesundheit und Leben der anderen Verkehrsteilnehmer eine Ausnahme von der Schweigepflicht rechtfertigt. In einem Grundsatzurteil hat der Bundesgerichtshof klargestellt, dass der Schutz der Verkehrsteilnehmer das Interesse des fahruntüchtigen Patienten an der Geheimhaltung seiner Fahruntüchtigkeit im Regelfall überwiegt.[6] Allerdings hat der Arzt seinen Patienten zunächst auf dessen Fahruntüchtigkeit und die Gefährdung anderer Menschen hinzuweisen, um ihn zur Einsicht zu bewegen. Auf diese Hinweise darf der Arzt nur dann verzichten, wenn dies we-

[6] BGH, 08.10.1968, Az.: VI ZR 168/67.

Deutsches Ärzteblatt | 09. 03. 2018 | DOI: 10.3238/arztebl.2018.ds01

gen der Art der Erkrankung oder wegen der Uneinsichtigkeit des Patienten von vornherein zwecklos ist.
Ein rechtfertigender Notstand kann auch vorliegen, wenn Ärzte Kenntnis davon erlangen, dass ein Patient durch rücksichtsloses Verhalten eine andere Person mit der Infektion einer schweren, möglicherweise tödlichen Krankheit gefährdet. Liegen konkrete Anhaltspunkte für ein derartiges Verhalten vor, hat der Arzt zunächst zu versuchen, seinen Patienten von dem gefährdenden Verhalten abzubringen. Ist erkennbar, dass der Patient dennoch die Ansteckung einer anderen Person, etwa seines Ehe- oder Lebenspartners in Kauf nimmt, wird der Arzt zur Abwendung der Gesundheitsgefährdung ggf. von der Schweigepflicht abweichen und die gefährdete Person informieren dürfen. In einem Einzelfall ist die Rechtsprechung sogar davon ausgegangen, dass der Arzt von der Schweigepflicht abweichen musste, um die Partnerin eines Patienten vor einer HIV-Infektion zu schützen. Hierbei war allerdings entscheidend, dass auch die Partnerin eine Patientin des Arztes war.[7]
Schließlich kann die Schweigepflicht ausnahmsweise auch dann zurücktreten, wenn Ärzte ihre eigenen berechtigten Interessen nur unter Offenbarung schweigepflichtiger Informationen wahrnehmen können. Dies kommt beispielsweise in Betracht, wenn ein Arzt gezwungen ist, seine Honorarforderung gegenüber einem Patienten anwaltlich oder gerichtlich durchzusetzen oder er sich z. B. gegen Strafverfolgungsmaßnahmen nur durch Offenbarung von Patientengeheimnissen effektiv verteidigen kann.

3. Datenschutz

Vorbemerkung: Mit Wirkung zum 25.05.2018 gilt die EU-Datenschutzgrundverordnung 2016/679 (DSGVO) allgemein und unmittelbar in allen Mitgliedstaaten der Europäischen Union. Sie dient der Angleichung des Datenschutzrechts in Europa. Es erfolgt zugleich eine Neuordnung des Datenschutzrechts in Deutschland, weil sich vor allem die Standorte der einzelnen Regelungen ändern. Einige Regelungen ergeben sich direkt aus der vorrangig zu beachtenden DSGVO, andere sind im nationalen Recht verankert. Es werden zwar einige Begriffe anders formuliert als im bisherigen Datenschutzrecht und bestimmte Pflichten für die Datenverarbeiter erweitert. Mit der neuen Rechtslage gehen aber keine gravierenden inhaltlichen Änderungen einher. Die Grundsystematik und die meisten der Grundprinzipien des Datenschutzes bleiben erhalten. Eine Verarbeitung, die bislang rechtmäßig erfolgte, wird im Wesentlichen auch weiterhin den Anforderungen des Datenschutzes genügen. Neu ist allerdings der drastisch erhöhte Sanktionsrahmen, der einer besseren Durchsetzbarkeit des Datenschutzes dienen soll. Darauf sowie auf weitere Neuerungen wird nachfolgend punktuell eingegangen.[8]

> **Empfehlung:** Für Einzelfragen wird ergänzend empfohlen, sich an die zuständigen Aufsichtsbehörden für den Datenschutz zu wenden. Ansprechpartner für Fragen zum Datenschutz sind in der Regel die Landesbeauftragten für den Datenschutz.[9]

3.1. Anwendungsbereich der DSGVO

Die DSGVO regelt nur die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten. Die nichtautomatisierte Verarbeitung ist nur erfasst, wenn personenbezogene Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Karteien zur Verwaltung von Patientenakten sind ein Dateisystem, da sie nach bestimmten Kriterien (nach Namen, Jahr oder Aktenzeichen) aufgebaute und zugängliche Sammlungen von Patientendaten sind, die ausgewertet werden können. Die rein papierbasierte Informationsverarbeitung ohne ein strukturiertes Ordnungssystem (z. B. Notizen als Gedächtnisstütze) unterfällt dem Datenschutzrecht hingegen nicht.
Der Begriff des „Verarbeitens" ist sehr weit. Er umfasst u. a. 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 von Daten.[10]
Die Verarbeitung erfolgt durch den sog. „Verantwortlichen". Das ist die Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.[11] Inhaber von Arztpraxen sind Verantwortliche in diesem Sinne.
Gegenstand des Datenschutzrechts ist nur die Verarbeitung personenbezogener Daten des Betroffenen, also die identifizierte oder identifizierbare natürliche Person (z. B. Patient), auf welche sich bestimmte Informationen beziehen.[12] Auch pseudonyme Daten (z. B. Ersetzung des Namens durch einen Identifikationscode) sind personenbezogene Daten und unterfallen dem Datenschutzrecht. Die Verarbeitung anonymer oder hinreichend anonymisierter Daten unterfällt dem Datenschutzrecht hingegen nicht. Daten gelten als anonym, wenn eine Zuordnung der Daten zu einer Person nicht ohne Weiteres möglich ist. Dabei müssen alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einem Dritten nach allgemeinem Ermessen wahrscheinlich genutzt werden, um den Patienten direkt oder indirekt zu identifizieren. Die sich hinter den Daten verbergende Person ist also nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft identifizierbar.[13] Eine absolute Anonymisierung ist schwer zu realisieren und im Praxisalltag ungeeignet, weil alle den Patienten identifizierenden Merkmale gelöscht werden müssten. Die Entfernung oder Schwärzung einzelner Angaben aus der Patientenakte genügt nicht, solange die Person für den Praxisinhaber oder einen Dritten identifizierbar bleibt.
Fazit: Die ganz oder teilweise automatisierte Verarbeitung personenbezogener, also z. B. die Erhebung, Speicherung und Übermittlung nicht anonymer Daten mittels elektronisch verwalteter Patientenakten oder durch systematisch geordnete Karteikarten und Patientenakten, unterfällt dem Datenschutzrecht, das der Praxisinhaber als „Verantwortlicher" zu wahren hat.

3.2. Rechtsgrundlagen

Für den niedergelassenen Arzt finden primär die Bestimmungen der EU-Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) in der ab dem 25.05.2018 gel-

[7] OLG Frankfurt, 05.10.1999, Az.: 8 U 67/99.
[8] Die nachfolgenden Ausführungen beziehen sich auf die ab dem 25.05.2018 geltende Rechtslage.
[9] In Bayern ist das Landesamt für Datenschutzaufsicht (LDA) zuständig. Eine Übersicht findet sich hier: https://www.datenschutz-wiki.de/Aufsichtsbeh%C3%B6rden_und_Landesdatenschutzbeauftragte
[10] Art. 4 Nr. 2 DSGVO.
[11] Art. 4 Nr. 7 DSGVO.
[12] Näher Art. 4 Nr. 1 DSGVO.
[13] Vgl. § 3 Abs. 6 BDSG a. F. Die DSGVO enthält keine Begriffsbestimmung zur Anonymisierung. S. aber Erwägungsgrund 26 der DSGVO.

tenden Fassung Anwendung. Daneben können sich spezielle datenschutzrechtliche Anforderungen aus sog. Fachgesetzen bzw. bereichsspezifischen Datenschutzgesetzen oder -regelungen ergeben. Sie ergänzen die allgemeinen Bestimmungen von DSGVO sowie BDSG und sind für den speziell geregelten Bereich vorrangig zu beachten. Sie können besondere Anforderungen (z. B. zusätzlich geforderte Schriftform der Einwilligung) enthalten. Beispiele finden sich in zahlreichen Bestimmungen des SGB V. Auch das Transfusionsgesetz (§ 11 TFG) enthält Vorschriften für die Datenverarbeitung. Zu nennen ist ferner das Infektionsschutzgesetz, das Datenübermittlungen zur Erfüllung bestimmter Meldepflichten vorsieht (§§ 9 ff. IfSG).

> **Hinweis:** Die Regelungslage im Datenschutzrecht ist sehr komplex, sodass es hilfreich sein kann, (rechtliche) Beratung in Anspruch zu nehmen. Ein Blick in das unter Umständen anzuwendende Spezialgesetz des zugrunde liegenden Sach- bzw. Aufgabenbereichs (z. B. Transfusionswesen) ist überdies oft unvermeidlich. Sofern die ärztliche Tätigkeit nicht in solchen Spezialbereichen erfolgt, sind regelmäßig die nachfolgend im Überblick behandelten allgemeinen Rechtsgrundlagen der DSGVO und des BDSG zu beachten (s. dazu den Abschnitt 3.4.1.).

Fazit: Es sind Bestimmungen der EU-Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes zu beachten.

3.3. Wichtige Grundsätze und Prinzipien im Überblick

Wegen der zunehmenden Bedeutung des Datenschutzrechts in einer von der Digitalisierung berührten Gesundheitsversorgung ist es bedeutsam, sich als Verantwortlicher für die Datenverarbeitung (z. B. Inhaber einer Arztpraxis) die Grundprinzipien des Datenschutzes zu vergegenwärtigen.[14] Allgemein ist eine Datenverarbeitung erlaubt, wenn eine gesetzliche Grundlage vorliegt oder der Betroffene eingewilligt hat (Rechtmäßigkeitsprinzip). Zu den wichtigsten Grundsätzen der Datenverarbeitung gehören die Verarbeitung für festgelegte und eindeutige Zwecke (Zweckbindung), die Beschränkung der Datenverarbeitung auf das notwendige Maß (Erforderlichkeit, Datenminimierung und Speicherbegrenzung) und die Transparenz. Ferner sind die Prinzipen der Richtigkeit sowie der Integrität und Vertraulichkeit der Verarbeitung zu nennen. Das „neue Datenschutzrecht“ entspricht in seinen wesentlichen Grundprinzipien damit dem bekannten deutschen Datenschutzrecht. Neuerdings muss der Verantwortliche aber die Einhaltung der Grundsätze nachweisen können („Rechenschaftspflicht“).

> **Empfehlung:** Ein Datenschutzmanagement und die Führung eines Verzeichnisses über die Datenverarbeitungsvorgänge (s. dazu auch noch die Abschnitte 3.7. – 3.9.) in der Arztpraxis können dazu beitragen, die neuen Rechenschafts- und Nachweispflichten zu erfüllen. Prüfungen durch externe Datenschutzprüfer, Auditierungen und Zertifizierungen kommen ebenfalls als geeignete Maßnahmen zur Wahrung des Datenschutzes in Betracht.

3.4. Besondere Vorschriften für Ärzte bei der Verarbeitung von Gesundheitsdaten

Ärzte verarbeiten im Rahmen ihrer Tätigkeit Gesundheitsdaten. Es handelt sich dabei um eine „besondere Kategorie personenbezogener Daten“ gem. Art. 9 Abs. 1 DSGVO. Diese Daten sind besonders schutzbedürftig. Gesundheitsdaten sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person (Patienten), einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.[15] Die Datenschutzgrundverordnung sieht für die Verarbeitung solcher Daten besondere Regelungen mit erhöhten Rechtmäßigkeitsanforderungen vor: Die Verarbeitung von Gesundheitsdaten ist unter den in Art. 9 Abs. 2 DSGVO genannten Voraussetzungen erlaubt. Die Bestimmung regelt die Voraussetzungen aber nicht abschließend. Zum Teil ergeben sich Erlaubnisse zur Verarbeitung von Gesundheitsdaten aus dem Bundesdatenschutzgesetz (insbesondere § 22 BDSG), in der ab dem 25.05.2018 geltenden Fassung (näher dazu im Abschnitt 3.4.1.). Überdies kann der nationale Gesetzgeber zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von Gesundheitsdaten betroffen ist.[16] Der Bereich des Gesundheitsdatenschutzrechts kann also abweichend von den Bestimmungen des Art. 9 Abs. 2 DSGVO nochmals in speziellen Vorschriften geregelt werden. Die Anpassung vieler Regelungen an die DSGVO ist noch nicht abgeschlossen. Es ist aber davon auszugehen, dass die bereichsspezifischen Regelungen in den Fachgesetzen weiterhin anwendbar bleiben. Als Beispiel für ein Gesetz, welches weitere Bedingungen und Beschränkungen bei der Verarbeitung von Gesundheitsdaten festlegt, ist das Gendiagnostikgesetz (GenDG) zu nennen.

Fazit: Weil Ärzte sensible Gesundheitsdaten verarbeiten, gelten für sie besondere Bestimmungen mit erhöhten Rechtmäßigkeitsanforderungen.

> **Hinweis:** Wegen der datenschutzrechtlichen Informationspflichten (s. u. Abschnitt 3.5.1.) sollten Ärzten die einschlägigen Rechtsgrundlagen bekannt sein, auf welche im Folgenden näher eingegangen wird.

3.4.1. Gesetzliche Erlaubnis zur Verarbeitung von Gesundheitsdaten in der Arztpraxis

In den meisten Fällen erlauben gesetzliche Bestimmungen die Verarbeitung von Gesundheitsdaten in der Arztpraxis. Das gilt insbesondere für die Informationserhebung im Rahmen der Anamnese, der Befunderhebung sowie für die Dokumentation der Diagnostik und der Therapie. Aus den einschlägigen Erlaubnisnormen[17] ergibt sich, dass die Verarbeitung von Gesundheitsdaten in folgenden Fallgruppen erlaubt ist und zwar:

- ***bei der ärztlichen Behandlung***

Die praktisch bedeutsamste gesetzliche Vorschrift für eine Verarbeitung von Gesundheitsdaten in der Arztpraxis ist Art. 9 Abs. 2 Buchst. h DSGVO i. V. m. § 22 Abs. 1 Nr. 1 Buchst. b BDSG. Im Rahmen der ärztlichen Behandlung ist die Verarbeitung von Gesundheitsdaten in den meisten Fällen aufgrund dieser Gesetzesvorschrift erlaubt. Der zusätzlichen Einholung einer Einwilligung bedarf es nicht. Etwas anderes gilt nur, wenn ein Gesetz die Einwilligung ausdrücklich vorschreibt (s. dazu im Abschnitt 3.4.2.). Die genannten Vorschriften erlauben eine Verarbeitung unter anderem, wenn sie erforderlich ist

- zum Zweck der Gesundheitsvorsorge,
- für die Beurteilung der Arbeitsfähigkeit des Beschäftigten,

[14] S. Art. 5 DSGVO.
[15] Art. 4 Nr. 15 DSGVO.
[16] Art. 9 Abs. 4 DSGVO.
[17] § 22 BDSG, der im Zusammenhang mit Art. 9 Abs. 2 DSGVO beachtet werden muss.

Deutsches Ärzteblatt | 09. 03. 2018 | DOI: 10.3238/arztebl.2018.ds01

- für die medizinische Diagnostik,
- für die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder
- für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich.

Umfasst sind damit insbesondere alle routinemäßigen Datenverarbeitungsvorgänge in der Arztpraxis im Zusammenhang mit gesundheitsbezogenen Handlungen der Prävention, Diagnostik, Therapie und Nachsorge.

Soweit diese Behandlungsmaßnahmen nicht aufgrund gesetzlicher Vorschriften erfolgen (im GKV-Bereich nach Vorschriften aus dem SGB V), ist die Verarbeitung von Gesundheitsdaten auch erlaubt, wenn sie aufgrund eines Behandlungsvertrags zwischen Patient und Arzt oder einem anderen Angehörigen eines Gesundheitsberufs erforderlich ist.[18] Das ist in der Arztpraxis im Rahmen der Behandlung (vor allem auch im privatärztlichen Bereich) regelmäßig der Fall.

Eine zusätzliche, wichtige Voraussetzung ist jeweils, dass Gesundheitsdaten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden „Geheimhaltungspflicht" unterliegen, oder unter deren Verantwortung verarbeitet werden.[19] Die Wahrung der Geheimhaltungspflicht ist eine angemessene und besondere Garantie zum Schutz der Rechte und Freiheiten des Patienten, welche von der DSGVO gefordert wird. Ärzten ist die Verarbeitung von Gesundheitsdaten zweifelsfrei erlaubt, da sie dem Berufsgeheimnis[20] unterliegen.

- ***zur Erfüllung spezieller Pflichten aus dem Sozialrecht***

Die Verarbeitung von Gesundheitsdaten ist darüber hinaus erlaubt, wenn sie zur Erfüllung vertragsärztlicher Pflichten oder Rechte gemäß sozialrechtlicher Vorschriften erforderlich ist.[21] Das betrifft sämtliche Pflichten und Rechte aus den SGB im Zusammenhang mit der gesetzlichen Krankenversicherung, der Pflegeversicherung, Unfallversicherung und der Rentenversicherung.[22] Mitteilungspflichten bestehen für Vertragsärzte gegenüber den Kassenärztlichen Vereinigungen,[23] Krankenkassen[24] oder gegenüber dem Medizinischen Dienst der Krankenversicherung[25] sowie zu Zwecken der Qualitätssicherung[26]. Ferner besteht eine Auskunftspflicht des behandelnden Arztes über Behandlung und Zustand eines Verletzten gegenüber dem Unfallversicherungsträger.[27] Zu den Übermittlungspflichten und -befugnissen in der vertragsärztlichen Versorgung siehe im Übrigen die obige Aufzählung im Abschnitt 2.4.2.

Zusätzliche Voraussetzung für die Verarbeitung von Gesundheitsdaten aufgrund dieser gesetzlichen Erlaubnisse ist, dass stets angemessene und besondere Garantien zum Schutz der Rechte und Freiheiten des Patienten eingehalten werden. Dazu können die in § 22 Abs. 2 BDSG aufgeführten Maßnahmen dienen. Exemplarisch hervorzuheben sind das Ergreifen technisch organisatorischer Maßnahmen,[28] die Nutzung von Protokollierungsverfahren,[29] die Beschränkung der Zugriffsrechte auf Gesundheitsdaten in der Arztpraxis[30] sowie die Pseudonymisierung oder Verschlüsselung[31] der verarbeiteten Gesundheitsdaten.

- ***zur Erfüllung spezieller Pflichten im öffentlichen Gesundheitsinteresse***

Die Verarbeitung von Gesundheitsdaten ist zudem erlaubt, wenn sie aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit zum Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren (z. B. Schutz vor einer Pandemie oder ähnlich schwerwiegenden Erkrankungen) oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten erforderlich ist.[32] Zusätzliche Anforderung ist auch hier, dass angemessene und spezifische Maßnahmen zur Wahrung der Rechte, Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, eingehalten werden, wozu die o. g., in § 22 Abs. 2 BDSG aufgeführten Maßnahmen ergriffen werden können.

- ***zum Schutz lebenswichtiger Interessen bei Einwilligungsunfähigkeit des Patienten***

Die Verarbeitung von Gesundheitsdaten ist ferner zulässig, wenn sie erforderlich ist zum Schutz lebenswichtiger Interessen der betroffenen Person (also des Patienten, dessen Gesundheitsdaten verarbeitet werden sollen) oder einer anderen natürlichen Person (Dritter) und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben.[33] Ist der Patient z. B. in einem Notfall nicht ansprechbar, dürfen seine Gesundheitsdaten zum Schutz seines Lebens oder des Lebens eines Dritten verarbeitet werden.

- ***zur Wahrung von Rechtsansprüchen***

Gesundheitsdaten dürfen ferner verarbeitet werden, wenn dies zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.[34] Das betrifft zum Beispiel die Durchsetzung von Honorarforderungen gegenüber dem Patienten aufgrund eines Behandlungsverhältnisses oder die Verteidigung im Fall von Behandlungsfehlervorwürfen und Aufklärungsrügen. Dabei dürfen die zur Durchsetzung notwendigen Informationen über den Patienten, z. B. an ein Zivilgericht, weitergegeben werden. In Prozessen über Behandlungsfehler dürfen die zur Verteidigung notwendigen Informationen weitergegeben werden.

> **Empfehlung:** Im Rahmen eines berufsrechtlichen oder berufs-, straf- sowie zivilgerichtlichen Verfahrens sollte mit einem Anwalt erörtert werden, welche Informationen, z. B. an das Gericht, weitergegeben werden dürfen.

Fazit: Ärzte dürfen Daten bei der ärztlichen Behandlung, zur Erfüllung spezieller Pflichten aus dem Sozialrecht, zur Erfüllung spezieller Pflichten im öffentlichen Gesundheitsinteresse, zum Schutz lebenswichtiger Interessen bei Einwilligungsunfähigkeit des Patienten oder zur Wahrung von Rechtsansprüchen verarbeiten. Hierfür stehen gesetzliche Grundlagen zur Verfügung, sodass eine Einwilligung nicht eingeholt werden muss.

---

[18] Art. 9 Abs. 2 Buchst. h DSGVO i. V. m. § 22 Abs. 1 Nr. 1 Buchst. b BDSG.
[19] Art. 9 Abs. 3 i. V. m. § 22 Abs. 1 Nr. 1 Buchst. b BDSG.
[20] § 203 StGB, § 9 MBO-Ä.
[21] Art. 9 Abs. 2 Buchst. b DSGVO i. V. m. § 22 Abs. 1 Nr. 1 Buchst. a BDSG oder einer spezialgesetzlichen Vorschrift.
[22] Vgl. z. B. § 100 SGB X i. V. m. gesetzlicher Erlaubnis oder Einwilligung.
[23] Z. B. § 295 Abs. 1 Nr. 2 SGB V.
[24] Z. B. § 295 Abs. 1, 2 a SGB V.
[25] Z. B. § 275b Abs. 2 S. 6, § 276 Abs. 2 S. 2 SGB V.
[26] § 299 SGB V.
[27] §§ 202, 203 SGB VII.
[28] Vgl. § 22 Abs. 2 Nr. 1 BDSG; s. u. Abschnitt 3.11. i. V. m. der Technischen Anlage.
[29] S. § 22 Abs. 2 Nr. 2 BDSG.
[30] S. § 22 Abs. 2 Nr. 5 BDSG.
[31] Vgl. § 22 Abs. 2 Nr. 6 u. 7 BDSG.
[32] Art. 9 Abs. 2 Buchst. i DSGVO i. V. m. § 22 Abs. 1 Nr. 1 Buchst. c BDSG oder §§ 54 ff. AMG, § 26 MPG, § 5 MBO-Ä, § 299 SGB V.
[33] Art. 9 Abs. 2 Buchst. c DSGVO.
[34] Art. 9 Abs. 2 Buchst. f DSGVO.

3.4.2. Datenschutzrechtliche Einwilligung

Im Rahmen der Behandlung kann die Datenverarbeitung in der Arztpraxis in den meisten Fällen durch eine gesetzliche Grundlage legitimiert werden. Vereinzelt ist aber eine gesetzliche Erlaubnis zur Verarbeitung von Gesundheitsdaten nicht vorhanden. In diesen Fällen kann die Verarbeitung von Gesundheitsdaten zulässig sein, wenn der Patient in die Verarbeitung für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt hat.[35]

In bestimmten Konstellationen kann die Einholung einer Einwilligung erforderlich sein: Für die Durchführung der ärztlichen Abrechnung unter Einbeziehung privater Verrechnungsstellen ist regelmäßig eine Einwilligung einzuholen. Auch in der gesetzlichen Krankenversicherung wird vereinzelt, z. B. im Rahmen der „besonderen Versorgung“[36] oder der hausarztzentrierten Versorgung,[37] eine datenschutzrechtliche Einwilligung gefordert.[38]

Eine Einwilligung im Datenschutzrecht ist „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung […], mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“.[39] Die Anforderungen an die Wirksamkeit der datenschutzrechtlichen Einwilligung sind vor allem in Art. 7 DSGVO geregelt und entsprechen im Wesentlichen denen, die bislang galten. Sie werden im Folgenden beschrieben, da in der Arztpraxis verwendete Einwilligungserklärungen spätestens jetzt an die Anforderungen angepasst werden sollten:

Informiertheit, Bestimmtheit und Verbot der Pauschaleinwilligung

Die Einwilligung muss für eine bestimmte Datenverarbeitung abgegeben werden.[40] Der Patient muss erkennen können, zu welchem Verarbeitungszweck er diese Einwilligung erteilt, welche Daten in welchem Umfang verarbeitet werden sollen und welchen Personen er die Verarbeitung seiner Gesundheitsdaten gestatten soll. Die hinreichende Informiertheit ist daher, ebenso wie die Bestimmtheit von vorformulierten Einwilligungserklärungen, weiterhin eine wichtige Voraussetzung. Es sind die bekannten Grundsätze des „informed consent“ entsprechend zu beachten. Pauschaleinwilligungen, deren Reichweite der Patient nicht zuverlässig einschätzen kann, sind unzulässig. Eine Einwilligung, die beispielsweise allgemein die „Verarbeitung von personenbezogenen Gesundheitsdaten zu Forschungszwecken“ zulassen soll, ist unwirksam. Auch die Einwilligung in die Nutzung der Anwendungen der elektronischen Gesundheitskarte kann auf einzelne Anwendungen beschränkt werden.[41]

Ausdrücklichkeit

Zu beachten ist, dass Gesundheitsdaten zu den besonderen Kategorien personenbezogener Daten zählen, bei der die Einwilligung für die Verarbeitung *ausdrücklich* erfolgen muss.[42] Das bedeutet, dass eine Einwilligung durch eine sonstige eindeutige bestätigende Handlung, z. B. durch Nicken oder durch anderes schlüssiges Verhalten (sog. konkludente Einwilligung), nicht ausreichend ist. Überdies können „Stillschweigen“ und Untätigkeit niemals eine wirksame Einwilligung darstellen.[43]

Freiwilligkeit

Zentrale Voraussetzung ist, dass die Einwilligung freiwillig erteilt wird. Das heißt, sie muss ohne Zwang, Druck oder Täuschung abgegeben worden sein. Sie darf grundsätzlich nicht von anderen Bedingungen abhängig gemacht werden, die nichts mit der Behandlung des Patienten zu tun haben („Kopplungsverbot“[44]). Die freie Willensbildung kann zwar fraglich erscheinen, wenn der Betroffene auf eine bestimmte Versorgungsleistung angewiesen ist und in die Datenverarbeitung einwilligen muss, um diese zu erlangen. Wird die datenschutzrechtliche Einwilligung zur „Vorbedingung“ einer Behandlung gemacht, ist sie aber nicht per se unfreiwillig, solange sie keine Datenverarbeitung legitimieren soll, die außerhalb des Behandlungszwecks liegt und damit über das für die Behandlung Notwendige hinausgeht. Im Rahmen einer ärztlichen Behandlung ist in der Regel eine gesetzliche Erlaubnis gegeben (s. o. 3.4.1.) und es muss mit Ausnahme der o. g. besonderen Konstellationen keine Einwilligung eingeholt werden. Auf das „Freiwilligkeitsproblem“ kommt es in diesen Fällen nicht an.

Keine Schriftform, Hervorhebung, Widerrufbarkeit

Die Einwilligung kann schriftlich, in Textform, elektronisch oder mündlich erteilt werden. Wegen der Nachweis- und Rechenschaftspflicht[45] ist es jedoch ratsam, dass die Einwilligung schriftlich eingeholt wird. Bei einer elektronischen Einwilligungserklärung ersetzt eine qualifizierte elektronische Signatur die Schriftform. Es genügt als Nachweis aber auch, wenn sie entsprechend protokolliert wird. Eine Dokumentation der mündlich erklärten Einwilligung kann ebenfalls der notwendigen Nachweisführung dienen.

Wird die Einwilligung zusammen mit anderen Erklärungen oder im Rahmen eines vorformulierten Behandlungsvertrages eingeholt, muss sie sich von anderen Sachverhalten unterscheiden lassen (z. B. durch eine Hervorhebung). Sie hat zudem bei formularmäßig verwendbaren Datenschutzerklärungen in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu erfolgen. Ankreuzlösungen („tick box“) sind zulässig, wobei der Patient aktiv ankreuzen muss („opt-in“), also das Kästchen nicht bereits vorausgefüllt sein darf („opt-out“). Die Einwilligung ist jederzeit mit Wirkung für die Zukunft widerrufbar.[46]

Einwilligung von Minderjährigen

Die Verarbeitung von Gesundheitsdaten eines Kindes ist nur rechtmäßig, wenn das Kind über die entsprechende Einsichtsfähigkeit verfügt und insoweit wirksam einwilligen kann. Das hängt im Einzelfall von der Fähigkeit des Minderjährigen ab, selbstständig und verantwortungsbewusst die Bedeutung und Tragweite seiner datenschutzrechtlichen Einwilligung einschätzen und überblicken zu können. Auf eine starre Altersgrenze kommt es nicht an, sodass z. B. auch ein fünfzehn Jahre[47] alter oder sogar jüngerer Patient unter den genannten Voraussetzungen im Einzelfall wirksam einwilligen kann.

---

[35] Vgl. Art. 9 Abs. 2 Buchst. a DSGVO.
[36] § 140a SGB V.
[37] § 73b SGB V.
[38] § 140a Abs. 5 SGB V; zur Abrechnung s. § 295a Abs. 1 SGB V.
[39] Art. 4 Nr. 11 DSGVO.
[40] Z. B. in den oben exemplarisch genannten Konstellationen: Datenübermittlung zu Abrechnungszwecken an eine bestimmte private Verrechnungsstelle.
[41] § 291a Abs. 3 S. 5 SGB V.
[42] Art. 9 Abs. 2 Buchst. a DSGVO.
[43] S. a. Erwägungsgrund 32 der DSGVO.
[44] Art. 7 Abs. 4 DSGVO; Erwägungsgrund 43 der DSGVO.
[45] Art. 5 Abs. 2 und Art. 7 Abs. 1 DSGVO.
[46] Art. 7 Abs. 3 DSGVO.
[47] Vgl. die sozialrechtliche Handlungsfähigkeit gem. § 36 SGB I: *„Wer das fünfzehnte Lebensjahr vollendet hat, kann Anträge auf Sozialleistungen stellen und verfolgen sowie Sozialleistungen entgegennehmen.“*

Besondere Bedingungen für die Einwilligung von Minderjährigen enthält aber Art. 8 DSGVO; jedoch nur für „Dienste der Informationsgesellschaft“[48] (z. B. rechtlich zulässige Fernbehandlungen). Aus der Vorschrift lässt sich die allgemeine Vermutung ableiten, dass die Einsichtsfähigkeit jedenfalls gegeben ist, wenn das Kind das sechzehnte Lebensjahr vollendet hat. Ist der Minderjährige nicht einsichtsfähig und/oder hat er noch nicht das sechzehnte Lebensjahr vollendet, ist die Einwilligung nur zulässig mit der Einwilligung des Trägers der elterlichen Verantwortung für das Kind oder wenn dieser der Einwilligung des Kindes zustimmt. Träger der elterlichen Verantwortung für das Kind sind die Personen, welche nach deutschem Recht das Sorgerecht innehaben, in der Regel die Eltern,[49] ein Vormund[50] oder ein Pfleger[51].

Einige Gesetze schreiben die (schriftliche) Einwilligung vor (Einwilligungsvorbehalte)

Einige Fachgesetze schreiben eine Einwilligung vor. So ist im Rahmen der vertragsärztlich geregelten „besonderen Versorgung“[52] die Erhebung, Verarbeitung und Nutzung der für die Durchführung der Verträge über die besondere Versorgung erforderlichen personenbezogenen Daten durch die Vertragspartner nur mit Einwilligung und nach vorheriger Information der Versicherten zulässig. Auch der Einsatz bestimmter freiwilliger Anwendungen der elektronischen Gesundheitskarte setzt eine Einwilligung des Versicherten voraus.[53] Vereinzelt verlangen die Regelungen überdies eine besondere Form der Einwilligung: So ist beispielsweise für die Teilnahme an strukturierten Behandlungsprogrammen die schriftliche Einwilligung des Versicherten für die Erhebung, Verarbeitung und Nutzung von Daten einzuhalten.[54] Gleiches gilt im Rahmen der vertragsärztlichen Versorgung für den Austausch von Behandlungsdaten zwischen Hausarzt, Facharzt und sonstigen Leistungserbringern.[55] Soweit eine Mit- oder Weiterbehandlung durch den Hausarzt initiiert wurde, wird zum Teil vertreten, dass das Einverständnis des Patienten zur Rückmeldung der Patientendaten an den Hausarzt anzunehmen ist.[56] Eine schriftliche Einwilligung ist aber in jedem Fall rechts- und beweissicherer.

Fazit: In besonderen Fällen kann die Einholung einer Einwilligung zur Datenverarbeitung erforderlich sein. Es ist wichtig, dass diese Einwilligungserklärung entsprechend dem „informed consent“ eingeholt wird. Sie muss insbesondere freiwillig und ausdrücklich erteilt worden und darf nicht pauschal abgefasst sein. Ansonsten ist die Erklärung unwirksam und die Datenverarbeitung rechtswidrig, was ein Bußgeld zur Folge haben kann.[57] Eine Schriftform ist zwar nicht vorgeschrieben, aus Nachweis- und Beweisgründen aber sinnvoll.

3.5. Rechte des Patienten (Betroffenenrechte)

Mit der DSGVO sollten ganz erheblich die Betroffenenrechte gestärkt werden. Die folgenden wichtigsten Rechte von Patienten, deren Daten verarbeitet werden, sind zu beachten.

3.5.1. Transparenz- und Informationspflichten

Die DSGVO sieht umfangreiche Informationspflichten für den Verantwortlichen vor, der Gesundheitsdaten verarbeitet. Diese dienen der Transparenz. Werden Daten direkt bei dem Patienten erhoben (Direkterhebung), gelten die Anforderungen von Art. 13 DSGVO. Erfolgt eine Erhebung der Patientendaten bei einem Dritten, z. B. bei einem ärztlichen Kollegen oder einem Familienangehörigen (Dritterhebung), ist Art. 14 DSGVO zu beachten. Im Fall der Direkterhebung ist der Patient zum Zeitpunkt der Erhebung, im Fall der Dritterhebung nachträglich in angemessener Zeit (längstens nach einem Monat), zu informieren. In beiden Fällen sind dem Patienten bestimmte Informationen zu geben: Z. B. Name und Kontaktdaten des Verantwortlichen und die Zwecke sowie die Rechtsgrundlage für die Verarbeitung der Gesundheitsdaten.[58]

Ein Katalog, der die schriftlich oder in anderer Form bereitzustellenden Informationen aufführt, ist in Art. 13 bzw. 14 DSGVO zu finden. Es wird differenziert zwischen Informationen, die dem Patienten „mitgeteilt“ werden müssen[59] und solchen, die lediglich „zur Verfügung gestellt“ werden müssen.[60] Die Informationspflicht kann im Fall der Mitteilung z. B. mündlich oder durch Aushändigung eines vorgefertigten standardisierten Formulars und im Fall der Zurverfügungstellung z. B. durch einen deutlich sichtbaren Aushang in der Praxis erfüllt werden. Auch Verweise auf entsprechende Informationen auf einer Praxiswebsite sind möglich, wenn es sich nicht um eine Information eines anwesenden Patienten handelt und die Informationen leicht auffindbar sind. In jedem Fall müssen die Informationen einfach verständlich, in klarer Sprache und leicht zugänglich sein.

Wenn und soweit die betroffene Person bereits über die Informationen verfügt, besteht eine Informationspflicht nicht.[61] Weitere Ausnahmen sieht das BDSG vor: Eine Informationspflicht besteht im Fall der Dritterhebung insbesondere nicht, wenn Informationen anderer Personen (z. B. Familienangehöriger) betroffen sind und diese aus Gründen der ärztlichen Schweigepflicht vertraulich behandelt werden müssen.[62] Sie besteht im Fall der Direkterhebung nicht, wenn sie die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen.[63]

Informationspflichten bestehen nur, wenn eine Datenverarbeitung im Sinne von Art. 4 Nr. 2 DSGVO erfolgt. Das ist zum Beispiel nicht der Fall, wenn einem Arzt Daten unverlangt zugesendet werden und dieser diese sogleich löscht. In diesem Fall erfolgt keine Erhebung (im Sinne eines Beschaffens von Daten) und keine Speicherung der Daten, sodass von einer Datenverarbeitung nach der Löschung nicht ausgegangen werden kann.

Fazit: Das Datenschutzrecht sieht gegenüber dem bisherigen Recht ausgeweitete Informationspflichten vor, wenn Daten beim Patienten oder bei Dritten über den Patienten erhoben werden. Eine Ausnahme von der Pflicht besteht beispielsweise, wenn die Patienten bereits über alle notwendigen Informationen verfügen, die in Art. 13 Abs. 1 und 2 bzw. Art. 14 Abs. 1 und 2 DSGVO aufgelistet sind.

---

[48] S. Art. 4 Nr. 25 DSGVO i. V. m. Art. 1 Abs. 1 Buchst. b Richtlinie (EU) 2015/1535: Eine gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung.
[49] §§ 1626 ff. BGB.
[50] §§ 1773 ff. BGB.
[51] § 1630 Abs. 1 und Abs. 2 BGB.
[52] § 140a Abs. 5 SGB V.
[53] § 291a Abs. 3 S. 4 und Abs. 5 S. 1 SGB V.
[54] § 137f Abs. 3 S. 2 SGB V.
[55] § 73 Abs. 1b SGB V.
[56] Vgl. für die ärztliche Schweigepflicht im Berufsrecht § 9 Abs. 4 MBO-Ä.
[57] Art. 83 Abs. 5 Buchst. a DSGVO.
[58] S. Abschnitt 3.4.1.
[59] Art. 13 Abs. 1 und Art. 14 Abs. 1 DSGVO.
[60] Art. 13 Abs. 2 und Art. 14 Abs. 2 DSGVO.
[61] Art. 13 Abs. 4 und Art. 14 Abs. 5 Buchst. a DSGVO.
[62] Art. 14 Abs. 5 Buchst. d DSGVO i. V. m. § 29 Abs. 1 S. 1 BDSG.
[63] § 32 Abs. 1 Nr. 4 BDSG.

Hinweis: Entsprechende Vordrucke zur Umsetzung der Informationspflichten werden gegenwärtig erarbeitet und sollen Ärzten zur Verfügung gestellt werden.[64]

3.5.2. Auskunftsrecht des Patienten

Artikel 15 DSGVO enthält das Recht des Patienten auf Auskunft über alle (!) ihn betreffenden personenbezogenen Daten. Der Arzt hat diese Auskunft unverzüglich[65] in schriftlicher, elektronischer oder – auf Wunsch des Patienten – mündlicher Form sowie unentgeltlich zu erteilen. Wichtige Ausnahmen sind im BDSG geregelt.[66] Diese betreffen zum Beispiel Situationen, in denen Aufbewahrungspflichten oder besondere Geheimhaltungspflichten bestehen oder die Datenverarbeitung zu wissenschaftlichen Forschungszwecken erfolgt. Das Auskunftsrecht besteht demnach nicht, wenn die Daten nur deshalb gespeichert sind, weil sie aufgrund von Aufbewahrungsvorschriften nicht gelöscht werden dürfen und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.[67] Das Auskunftsrecht besteht auch nicht, soweit durch die Auskunft Informationen offenbart würden, die insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten geheim gehalten werden müssen.[68]

Besteht das Auskunftsrecht, sind dem Patienten darüber hinaus die in Art. 15 Abs. 1 DSGVO aufgeführten Informationen zu geben, z. B. Verarbeitungszwecke, Empfänger (einschließlich Auftragsverarbeiter), geplante Speicherdauer und das Bestehen von Betroffenenrechten (z. B. das Recht auf Löschung).

Hinweis: Das datenschutzrechtliche Auskunftsrecht ist zu unterscheiden vom Recht des Patienten zur Einsichtnahme in seine Patientenakte gemäß § 630g BGB, welches eigenen Maßstäben unterliegt (s. u. Abschnitt 5.).

3.5.3. Berichtigung, Löschung und Einschränkung der Verarbeitung von Daten

Patienten haben das Recht, vom Arzt die Berichtigung sie betreffender, unrichtiger personenbezogener Daten zu verlangen,[69] die in die Patientendokumentation gelangt sind. Es kann, je nach Verarbeitungszweck, als Unterfall der Berichtigung auch die Vervollständigung unvollständiger personenbezogener Daten durch ein Hinzufügen fehlender Daten verlangt werden.[70] Die Berichtigung erfolgt unentgeltlich[71] und „unverzüglich“,[72] d. h. sie darf nach der Überprüfung der Unrichtigkeit bzw. Unvollständigkeit nicht weiter hinausgezögert werden. Eine Ablehnung ist zu begründen.[73] Der Berichtigungsanspruch bezieht sich nur auf Tatsachenangaben, also Angaben, die einem empirischen Beweis zugänglich sind, z. B. Daten, die anlässlich einer Behandlung erhoben worden sind (z. B. Körpergewicht, Größe des Patienten) und ggf. fehlerhaft dokumentiert wurden. Auf das Verschulden und die Ursache des Fehlers kommt es nicht an. Unrichtig sind Daten, wenn z. B. getätigte Feststellungen zur körperlichen Befindlichkeit oder zur Behandlung nach objektiven Maßstäben nicht der Realität entsprechen. Werturteile sind von dem Berichtigungsanspruch nicht erfasst. Ärztliche Bewertungen (z. B. Diagnosen) können demnach nicht berichtigt werden,[74] soweit sie einem Beweis nicht zugänglich sind. Den Beurteilungen zugrundeliegende Gesundheitsdaten als Tatsachenbestandteile können demgegenüber zu berichtigen sein. Eine Tatsachenangabe wird nicht unrichtig, weil sich die Tatsache zwischenzeitlich verändert hat (z. B. Gewichtsreduktion). Fehlen die aktuellen Angaben, kann die Patientendokumentation aber unter Umständen unvollständig sein, sodass eine Vervollständigung verlangt werden kann, wenn der Verarbeitungszweck (Dokumentation des Körpergewichts über einen bestimmten Zeitraum) dies gebietet. Die nachträgliche Berichtigung bzw. Vervollständigung ist unter Beibehaltung der alten Angabe zu vermerken. Zu beachten sind dementsprechend Pflichten, die sich aus der ärztlichen Dokumentationspflicht gem. § 630f BGB ergeben: Von dem Anspruch auf Berichtigung unberührt bleibt die Pflicht des Arztes, die Patientenakte so zu führen, dass der ursprüngliche Inhalt der Dokumentation erkennbar bleibt (vgl. Abschnitt 4.1.).[75]

Ein Anspruch der Patienten auf unverzügliche Löschung[76] ihrer Daten besteht insbesondere, wenn diese Patientendaten nicht mehr benötigt werden, die Einwilligung in die Verarbeitung widerrufen wurde, ein Widerspruch gegen die Verarbeitung erklärt wurde oder die Speicherung unzulässig ist.[77] Ein Anspruch des Patienten auf Löschung der patientenbezogenen Daten kommt gemäß § 35 Abs. 3 BDSG aber nicht in Betracht, wenn dem eine vertragliche oder satzungsgemäße Aufbewahrungspflicht entgegensteht.[78] Für den Bereich der ärztlichen Dokumentation gilt grundsätzlich eine 10-jährige Aufbewahrungspflicht[79] (vgl. Abschnitt 4.3.). In diesem Fall tritt an die Stelle einer Löschung die Einschränkung der Verarbeitung („Sperrung“).[80] Eine „Einschränkung der Verarbeitung“ ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.[81]

Die weitere Speicherung der Patientendaten bleibt auch erlaubt, wenn sie zur Erfüllung sonstiger rechtlicher Verpflichtungen (z. B. im Rahmen der vertragsärztlichen Abrechnung) erfolgt.[82] Weitere Ausnahmen von der Löschungspflicht bestehen aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit[83] (z. B. zum Zweck der Meldung an Krebsregister oder im Rahmen des Infektionsschutzes) oder im Interesse wissenschaftlicher Forschung.[84] Ferner müssen Patientendaten nicht gelöscht werden, wenn sie in einem konkreten Fall zur Geltendmachung oder Ausübung von Rechtsansprüchen (z. B. Honorarforderungen) oder zur eigenen Verteidigung (z. B. Behandlungsfehlervorwürfe) erforderlich sind.[85]

---

[64] Siehe zur Zeit das von der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. erstellte Muster „GDD-Praxishilfe DS-GVO VII“, S. 8 ff., abrufbar unter: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_7.pdf

[65] D. h. „ohne schuldhaftes Zögern“ (vgl. § 121 Abs. 1 BGB), jedenfalls aber innerhalb eines Monats (Art. 12 Abs. 3 DSGVO).

[66] Siehe die Ausnahmen in § 27 Abs. 2, § 29 Abs. 1 und 34 BDSG.

[67] § 34 Abs. 1 Nr. 1, Buchst. a BDSG.

[68] § 29 Abs. 1 S. 1 BDSG.

[69] Art. 16 S. 1 DSGVO, s.a. Art. 5 Abs. 1 Buchst. d DSGVO und Art. 8 Abs. 2 S. 2 EU-Grundrechtecharta.

[70] Art. 16 S. 2 DSGVO.

[71] Art. 12 Abs. 5 DSGVO.

[72] § 121 Abs. 1 S. 1 BGB: „ohne schuldhaftes Zögern“.

[73] Art. 12 Abs. 4 DSGVO.

[74] Vgl. BGH NJW 1989, 774 f.

[75] § 630f Abs. 1 S. 2 u. 3 BGB: „Berichtigungen und Änderungen von Eintragungen in der Patientenakte sind nur zulässig, wenn neben dem ursprünglichen Inhalt erkennbar bleibt, wann sie vorgenommen worden sind.“

[76] Art. 17 DSGVO.

[77] Erwägungsgrund 65 der DSGVO.

[78] S.a. Art. 17 Abs. 3 Buchst. b DSGVO (Rechtspflicht).

[79] § 630f Abs. 3 BGB.

[80] § 35 Abs. 3 i. V. m. § 35 Abs. 1 S. 2 BDSG.

[81] Art. 4 Nr. 3 DSGVO.

[82] Art. 17 Abs. 3 Buchst. b DSGVO.

[83] Art. 17 Abs. 3 Buchst. c DSGVO i. V. m. Art. 9 Abs. 2 lit. i DSGVO (s. o. Abschnitt 3.4.1.).

[84] § 27 Abs. 2 BDSG.

[85] Art. 17 Abs. 3 Buchst. e DSGVO.

Deutsches Ärzteblatt | 09. 03. 2018 | DOI: 10.3238/arztebl.2018.ds01

Bis geprüft werden konnte, ob Berichtigungs- oder Löschungsansprüche bestehen, kann die Verarbeitung übergangsweise einzuschränken sein.[86] Die Einschränkung der Verarbeitung erfolgt zudem, wenn die Daten für den Verarbeitungszweck zwar nicht mehr gebraucht werden, der Patient die Daten aber benötigt, um Rechtsansprüche (z. B. gegenüber seiner Krankenversicherung) geltend machen zu können.[87] Im Falle der Einschränkung der Verarbeitung dürfen die Patientendaten nur mit der Einwilligung des Patienten weiterverarbeitet werden.[88]

Hinweis: Jede Berichtigung, Löschung von Daten oder Einschränkung der Verarbeitung ist dem Patienten im Nachhinein mitzuteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.[89]

Fazit: Im Zusammenhang mit Berichtigungs- und Löschungsansprüchen von Patienten müssen Dokumentationspflichten und Aufbewahrungsfristen berücksichtigt werden, welche die Ansprüche des Patienten begrenzen können.

3.5.4. Recht des Patienten auf Datenübertragbarkeit

Art. 20 DSGVO enthält das neue Recht für Patienten, ihre Daten unentgeltlich in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, also „mitnehmen“ zu können (sog. Datenportabilität). Es dient der Erleichterung des elektronischen Informationstransfers. Das Recht betrifft nur Daten, die von den Patienten auf Basis einer Einwilligung selbst zur Verfügung gestellt wurden[90] (z. B. aus Fitness-Apps) und automatisiert, also nicht papierbasiert, verarbeitet werden. Es reicht damit nicht so weit wie das sog. Einsichtsrecht gem. § 630g BGB, wonach Patienten auf Verlangen unverzüglich Einsicht in die vollständige, ihn betreffende Patientenakte zu gewähren ist, soweit der Einsichtnahme nicht erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen.

Darüber hinaus besteht ein Recht der Patienten, dass diese Daten an einen anderen Verantwortlichen (z. B. einem anderen Arzt) übermittelt werden, sofern die Datenverarbeitung auf einer Einwilligung beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt. Der Patient hat das Recht, dass die Daten direkt von einem Arzt an einen anderen Verantwortlichen (z. B. einen nachbehandelnden Arzt) übermittelt werden, soweit dies technisch machbar ist.

Fazit: Das neue Recht auf Datenportabilität betrifft nur Daten, die von den Patienten auf Basis einer Einwilligung selbst zur Verfügung gestellt wurden und nicht papierbasiert, sondern elektronisch verarbeitet werden. Im Übrigen sind die weitergehenden Auskunfts- und Einsichtsrechte der Patienten zu beachten.

3.6. Auftragsverarbeitung

In Einzelfällen kann es erforderlich sein, dass Ärzte für bestimmte Aufgaben externen Sachverstand bei der Datenverwaltung einbeziehen, z. B. für die (Fern-)Wartung ihrer IT-Systeme oder die Vernichtung von Patientenakten oder Datenträgern. Soweit die herangezogenen Dienstleister (Auftragsverarbeiter[91]) aus diesem Anlass auf Patientendaten zugreifen können, ist neben der strafrechtlichen Befugnis[92] eine datenschutzrechtliche Legitimation erforderlich. Diese besteht in der Möglichkeit, eine Auftragsverarbeitung zu vereinbaren mit der Folge, dass die Datenverarbeitung als „Verarbeitung durch eine Stelle“ angesehen wird (Privilegierung) und eine weitere Erlaubnis des Arztes für die Datenübertragung an den Dienstleister in diesem „Innenverhältnis“ nicht erforderlich ist.

Hinweis: Einer datenschutzrechtlichen Erlaubnis aus dem Gesetz oder durch eine Einwilligung bedarf es bei der Auftragsverarbeitung zwar nicht mehr. Die Auftragsverarbeitung stellt aber keine Befugnis im Sinne von § 203 StGB dar. Es ist hierbei die Neuregelung des § 203 Abs. 3 S. 2 StGB n. F. zu beachten (s. o. Abschnitt 2.4.3.).

Die Art. 28 ff. DSGVO sehen für die Auftragsverarbeitung bestimmte Anforderungen vor: Der Auftragsverarbeiter (z. B. Auftragnehmer einer externen IT-Dienstleistung) ist bspw. unter besonderer Berücksichtigung seiner Eignung sorgfältig auszuwählen.[93] Er darf personenbezogene Daten nur im Rahmen der Weisungen des Verantwortlichen (Auftraggeber einer externen IT-Dienstleistung) verarbeiten.[94] Der Auftragsverarbeiter haftet künftig gemeinsam mit dem Auftraggeber[95] und hat neben diesem zahlreiche selbstständige datenschutzrechtliche Pflichten zu erfüllen.[96] Die Gesamtverantwortung bleibt aber beim Verantwortlichen. Der Auftragsverarbeiter muss den Verantwortlichen darin unterstützen, die Einhaltung der Pflichten nach der DSGVO nachweisen und Überprüfungen durchführen zu können.[97] Der Auftraggeber kann seinen Kontrollpflichten durch eine Zertifizierung nachkommen.[98]

Hinweis: Es bestehen im Fall der Auftragsverarbeitung bestimmte Informationspflichten (s. o. Abschnitt 3.5.1.): Da in diesem Zusammenhang alle Empfänger mitzuteilen sind,[99] muss über die mögliche Einbeziehung von Auftragsverarbeitern bzw. „sonstigen mitwirkenden Personen“[100] (z. B. zur Wartung der Praxis-EDV) informiert werden. Über diese Empfänger muss ggf. Auskunft erteilt werden (s. dazu Abschnitt 3.5.2.) und sie müssen zudem im Verzeichnis der Verarbeitungstätigkeiten (s. dazu Abschnitt 3.7.) aufgeführt werden.

Empfehlung: Die Auftragsverarbeitung setzt in der Regel den Abschluss eines Vertrages voraus. Ärzte sollten sich daher juristisch beraten lassen. Sie können aber zumindest auf Muster-Vorlagen für Verträge über die Auftragsverarbeitung zurückgreifen.[101]

3.7. Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten

Praxisinhaber haben als „Verantwortliche“ für die Verarbeitung von Gesundheitsdaten ein Verzeichnis von Verarbeitungstätigkeiten zu führen.[102] Dieses betrifft alle automatisierten Verarbeitungsvorgänge sowie die nichtautomatisierte Verarbeitung, wenn beabsichtigt ist, die Daten in einem Dateisystem zu speichern.

---

[86] Art. 18 Abs. 1 Buchst. a DSGVO.
[87] Art. 18 Abs. 1 Buchst. c DSGVO.
[88] Art. 18 Abs. 2 DSGVO.
[89] Art. 19 DSGVO.
[90] S. dazu Abschnitt 3.4.2.
[91] Art. 4 Nr. 8 DSGVO. Er ist nicht Dritter i. S. v. Art. 4 Nr. 10 DSGVO.
[92] § 203 Abs. 3 S. 2 StGB n. F.; s. dazu Abschnitt 2.4.3.
[93] Vgl. Art. 28 Abs. 1 DSGVO.
[94] Art. 28 Abs. 3 S. 2 Buchst. a und Art. 29 DSGVO.
[95] Vgl. Art. 82 Abs. 1, 2 u. 4 DSGVO.
[96] Z. B. Art. 30 Abs. 2 DSGVO.
[97] Art. 28 Abs. 3 Buchst. h DSGVO.
[98] Art. 28 Abs. 5 i. V. m. Art. 42 Abs. 1 DSGVO.
[99] S. Art. 13 Abs. 1 Buchst. e und Art. 14 Abs. 1 Buchst. e DSGVO.
[100] Vgl. § 203 Abs. 3 S. 2 StGB, s. dazu o. 2.4.2.
[101] Siehe derzeit den vom Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V., der DKG u. a. ausgearbeiteten „Muster-Auftragsverarbeitungs-Vertrag für das Gesundheitswesen“, abrufbar unter: https://www.bvdnet.de/wp-content/uploads/2017/07/Muster-AV-Vertrag.pdf
[102] Art. 30 DSGVO.

Bei mehreren Einzelverarbeitungsschritten kann eine Zusammenfassung erfolgen, sofern mehrere Verarbeitungsschritte zu einem gemeinsamen Zweck erfolgen.
Da in Arztpraxen regelmäßig Daten besonderer Kategorien verarbeitet werden, zu denen gem. Art. 9 Abs. 1 DSGVO Gesundheitsdaten[103] zählen, sind die Verantwortlichen ausnahmslos zur Führung des Verzeichnisses verpflichtet.[104] Die Führung dieses Verzeichnisses ist ein Teil der neuen Rechenschafts- und Nachweispflicht der Verantwortlichen. Zwar müssen Ärzte das Verzeichnis nicht initiativ bei der zuständigen Datenschutzaufsichtsbehörde vorlegen; es besteht also keine Meldepflicht. Das Verzeichnis von Verarbeitungstätigkeiten ist aber vorzuhalten, da es den Aufsichtsbehörden jederzeit auf Anfrage zur Verfügung zu stellen ist.[105] Das schriftlich oder elektronisch zu führende Verzeichnis hat sämtliche in Art. 30 Abs. 1 S. 2 DSGVO aufgeführten Angaben zu enthalten, z. B. die Zwecke der Verarbeitung, die Kategorien von Empfängern, gegenüber denen Gesundheitsdaten offengelegt werden und, wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung.

> **Hinweis:** Ärzte müssen die wesentlichen Informationen einer Verarbeitung von Gesundheitsdaten schriftlich dokumentieren. Die deutschen Aufsichtsbehörden für den Datenschutz wollen dafür eine Muster-Vorlage sowie weitere Hinweise bereitstellen.[106]

Verstöße gegen die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten können mit einer Geldbuße von bis zu 10.000.000 EUR oder von bis zu 2 % seines gesamten erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs sanktioniert werden.[107]
Fazit: Alle Praxisinhaber haben für die Verarbeitung von Gesundheitsdaten ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Das Verzeichnis dient vorrangig der eigenen Datenschutzorganisation in der Arztpraxis sowie als Grundlage zur Erfüllung anderer Pflichten (z. B. der Rechenschaftspflicht oder der Datenschutzfolgenabschätzung).

3.8. Pflicht zur Vornahme einer Datenschutz-Folgenabschätzung

Der Einhaltung der Vorgaben der DSGVO soll auch die Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO dienen. Eine solche Abschätzung der Folgen eines Datenverarbeitungsvorgangs ist immer dann vorzunehmen, wenn die Form der Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten von Patienten zur Folge hat, deren Gesundheitsdaten verarbeitet werden sollen. Die DSGVO nimmt das bei der Verwendung neuer Technologien[108] (z. B. Cloud Dienste) und in drei gesetzlich aufgeführten Fällen an, u. a. bei systematischer umfangreicher Überwachung öffentlich zugänglicher Bereiche[109] (z. B. Videoüberwachung in der Arztpraxis) sowie bei der „umfangreichen Verarbeitung“ von Gesundheitsdaten als besondere Kategorien von personenbezogenen Daten.[110] In diesen Fällen ist die Datenschutz-Folgenabschätzung obligatorisch.
Eine „umfangreiche Verarbeitung“ von Gesundheitsdaten erfolgt bei einer Vielzahl automatisiert bearbeiteter Datensätze einer größeren Anzahl von Patienten in der Arztpraxis. Kriterien zur Bestimmung sind:

- die Zahl der Betroffenen (Patienten),
- die verarbeitete Datenmenge,
- die Dauer der Verarbeitung und
- ein geografischer Aspekt (regionale, nationale oder supranationale Reichweite).

Nach Erwägungsgrund 91 der DSGVO ist eine Verarbeitung aber nicht als umfangreich einzuordnen, wenn die Verarbeitung „personenbezogene Daten von Patienten“ betrifft und durch einen „einzelnen Arzt“ erfolgt. Unabhängig von der Organisationsform (Einzelarztpraxis, Berufsausübungs- oder Praxisgemeinschaft) ist eine Datenschutz-Folgenabschätzung damit nicht vorzunehmen, wenn in Orientierung am durchschnittlich betroffenen einzelnen Arzt als Referenzpunkt eine umfangreiche Verarbeitung nicht stattfindet. Da bislang keine konkreten Schwellenwerte benannt wurden, ist es jeweils eine Prüfung im Einzelfall (s. zu dem Aspekt der „umfangreichen Verarbeitung“ auch 3.9.).
Die „umfangreiche Verarbeitung von Gesundheitsdaten“ ist jedoch nur ein Kriterium zur Einschätzung, ob „hohe Risiken“ für die Rechte der Patienten bestehen, welche die Vornahme einer Datenschutz-Folgenabschätzung erforderlich machen. Unabhängig davon ist eine Datenschutz-Folgenabschätzung in einer Arztpraxis durchzuführen, wenn ansonsten ein „hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ besteht, das u. a. „zu einem physischen, materiellen oder immateriellen Schaden“ führen könnte. Nach einem Kriterienkatalog soll das der Fall sein, wenn die Verarbeitung insbesondere[111]

- zu einer Diskriminierung,
- zu einem finanziellen Verlust,
- zu einer Rufschädigung,
- zu einem Verlust der Vertraulichkeit des Patientengeheimnisses (Gefahr des Bruchs der ärztlichen Schweigepflicht),
- zur Hinderung der Kontrolle über die eigenen Daten oder
- zur Erstellung von Profilen durch Analysen und Prognosen (z. B. genetische Analysen) führen könnte, ferner
- wenn personenbezogene Daten schutzbedürftiger natürlicher Personen (insbesondere von Kindern oder psychisch Erkrankten) verarbeitet werden oder
- wenn sensible Daten betroffen sind (z. B. genetische Daten, Gesundheitsdaten oder Daten über das Sexualleben),
- wenn die Verarbeitung einer großen Menge von Patientendaten erfolgt und eine große Anzahl von Patienten betrifft (s. dazu oben zur „umfangreichen Verarbeitung).

Nach Auffassung der Artikel-29-Datenschutzruppe und der Aufsichtsbehörden für den Datenschutz ist eine Datenschutz-Folgenabschätzung durchzuführen, wenn mindestens zwei dieser Kriterien erfüllt sind. Demnach ist die Datenschutz-Folgenabschätzung in einem Krankenhaus durchzuführen,

---

[103] Art. 4 Nr. 15 DSGVO.
[104] Vgl. Art. 30 Abs. 5 DSGVO.
[105] Art. 30 Abs. 4 DSGVO.
[106] Siehe zurzeit das vom Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. zur Verfügung gestellte Muster, abrufbar unter: https://www.bvdnet.de/wp-content/uploads/2017/06/Muster_Verz_der_Verarbeitungst%C3%A4tigkeiten_Verantwortlicher.pdf; siehe ferner die Hinweise zum Verzeichnis der Verarbeitungstätigkeiten der Datenschutzkonferenz, abrufbar unter: https://datenschutz.sachsen-anhalt.de/informationen/internationales/datenschutz-grundverordnung/verzeichnis-der-verarbeitungstaetigkeiten-nach-artikel-30-ds-gvo/
[107] Art. 83 Abs. 4 Buchst. a DSGVO.
[108] Art. 35 Abs. 1 DSGVO.
[109] Art. 35 Abs. 3 Buchst. c DSGVO.
[110] Art. 35 Abs. 3 Buchst. b DSGVO.
[111] Vgl. zum Ganzen Erwägungsgrund 75 der DSGVO.

Deutsches Ärzteblatt | 09. 03. 2018 | DOI: 10.3238/arztebl.2018.ds01

wenn dort genetische oder medizinische Daten in einem Krankenhausinformationssystem verarbeitet werden. Hingegen soll die Verarbeitung von Patientendaten durch einen einzelnen Arzt nicht dazu führen, dass eine Datenschutz-Folgenabschätzung durchzuführen ist.

Eine Datenschutz-Folgenabschätzung ist aber auch in einer Praxis eines einzelnen Arztes durchzuführen, wenn die Beurteilung ergibt, dass ein hohes Risiko nach den aufgeführten Kriterien dennoch anzunehmen ist. Das kann z. B. Praxen betreffen, die gendiagnostische Verfahren anwenden oder die besonders schutzbedürftige Patientengruppen behandeln (z. B. Kinder). Diese Aspekte, wie auch das Kriterium der umfangreichen Verarbeitung, sind bei der Gesamtwürdigung, ob ein hohes Risiko besteht, jedoch jeweils nur ein Faktor.

Risikoreiche Verfahren der Datenverarbeitung, die eine Datenschutz-Folgenabschätzung erforderlich machen, können im Rahmen der hausarztzentrierten Versorgung oder der integrierten Versorgung auftreten, wenn eine große Zahl von Patientendaten durch verschiedene Ärzte verwendet, übertragen und auf andere Weise verarbeitet werden und Risiken für das Patientengeheimnis bestehen. Das gilt umso mehr, wenn eine Beteiligung von Ärzten an elektronischen Gesundheitsakten[112] erfolgt. Ein Verlust der Vertraulichkeit des Patientengeheimnisses ist hierbei möglich.

Ergibt die Vorprüfung (sog. Schwellwertanalyse) jedoch, dass bereits durch technisch-organisatorische Vorkehrungen hinreichende Abwehrmaßnahmen ergriffen worden sind, welche das Risiko wirksam eindämmen und damit deren Eintrittswahrscheinlichkeit gering ist, muss eine Datenschutz-Folgenabschätzung nicht durchgeführt werden. Dieses Ergebnis ist wegen der datenschutzrechtlichen Nachweispflicht[113] aber zu dokumentieren.

> **Hinweis:** Vertiefende Hinweise über die Kriterien zur Bestimmung der Risiken hat die europäische Artikel-29-Datenschutzgruppe in Leitlinien zur Datenschutz-Folgenabschätzung erarbeitet.[114] Abschließende Rechtsmeinungen haben sich noch nicht herausgebildet. Ob eine Datenschutz-Folgenabschätzung im Einzelfall durchzuführen ist, sollte im Zweifel bei der zuständigen Aufsichtsbehörde für den Datenschutz erfragt werden. Die zuständige Aufsichtsbehörde erstellt und veröffentlicht zudem eine Liste zu Vorgängen, bei denen eine Datenschutz-Folgenabschätzung erforderlich ist und kann eine Liste zu Vorgängen erstellen, in denen eine solche entbehrlich ist.[115]

Inhaltlich richtet sich die Folgenabschätzung nach den Vorgaben von Art. 35 Abs. 7 DSGVO, was unter anderem eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck, eine Bewertung der Risiken für die Patienten sowie die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen umfasst.

Ergibt die Datenschutz-Folgenabschätzung, dass wegen der Verarbeitung ein hohes Risiko für die Rechte von Patienten besteht, muss der Arzt die zuständige Aufsichtsbehörde konsultieren bevor mit der Verarbeitung begonnen wird, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.[116] Ansonsten bestehen nach der DSGVO wegen des damit verbundenen bürokratischen und finanziellen Aufwandes keine Meldepflichten für Verarbeitungsvorgänge mehr.[117] Das Ergebnis der Datenschutz-Folgenabschätzung ist zu dokumentieren.[118]

> **Hinweis:** Auf Basis des Verzeichnisses der Verarbeitungstätigkeiten lässt sich eine Datenschutz-Folgenabschätzung vornehmen, die überdies bei Einrichtung neuer Verarbeitungsverfahren durchgeführt werden sollte. Bestehen möglicherweise hohe Risiken bei der Datenverarbeitung, ist eine externe Datenschutzprüfung zu empfehlen.

3.9. Pflicht zur Benennung eines Datenschutzbeauftragten

Verantwortliche müssen grundsätzlich einen Datenschutzbeauftragten (DSB) benennen. Dieser dient der internen Kontrolle, um den Datenschutz einzuhalten. Die Pflicht zur Benennung eines DSB in der Arztpraxis wird gegenwärtig unterschiedlich beurteilt. Nach der neuen Gesetzeslage gibt es drei zu unterscheidende gesetzliche Fälle, nach denen ein DSB zu benennen ist:

1. Fall: Soweit in einer Arztpraxis „*in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten*“ beschäftigt werden, ist in jedem Fall ein DSB zu benennen.[119] Es sind die Mitarbeiter zu berücksichtigen, die regelhaft und nicht nur gelegentlich mit der Datenverarbeitung beschäftigt sind. Dies sind typischerweise die Mitarbeiter, die beispielsweise mit der Datenerfassung am Empfang oder der Datenverarbeitung im Rahmen der Abrechnung betraut sind. Erfasst werden auch angestellte Ärzte, Auszubildende sowie freie Mitarbeiter, jedoch nicht der Praxisinhaber selbst. „In der Regel“ beschäftigt ist eine Person, wenn sie für diese Aufgabe, die nicht ihre Hauptaufgabe sein muss, zumindest auf längere Zeit vorgesehen ist und sie entsprechend wahrnimmt.

2. Fall: Unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen ist ein DSB zu benennen, wenn unter den oben bereits erläuterten Voraussetzungen (s. o. bei 3.8.) eine Datenschutz-Folgenabschätzung[120] vorzunehmen ist.[121] Das ist, wie gezeigt, in der Einzelarztpraxis nicht stets der Fall, sondern nur, wenn ein „hohes Risiko“ besteht. Ein DSB ist zu benennen, wenn eine „umfangreiche Verarbeitung“ von Gesundheitsdaten (z. B. durch eine große Anzahl von Patientendatensätzen)[122] erfolgt, die über das übliche Maß der in einer Einzelarztpraxis verarbeiteten Daten hinausgeht, oder wenn ansonsten ein „hohes Risiko“ für die Rechte und Freiheiten der Patienten durch die Datenverarbeitung (z. B. bei der Verarbeitung genetischer Daten) anzunehmen ist.[123]

---

[112] § 68 SGB V.
[113] Art. 5 Abs. 2 DSGVO.
[114] Datenschutzgruppe nach Artikel 29, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, WP 248 Rev.01, S. 10 ff., abrufbar hier: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
[115] Art. 35 Abs. 4, Abs. 5 DSGVO.
[116] Art. 36 Abs. 1 DSGVO.
[117] Erwägungsgrund 89 der DSGVO.
[118] Art. 5 Abs. 2 DSGVO.
[119] § 38 Abs. 1 BDSG.
[120] Art. 35 DSGVO.
[121] § 38 Abs. 1 S. 2 BDSG.
[122] Art. 35 Abs. 3 Buchst. c DSGVO.
[123] Art. 35 Abs. 1 DSGVO.

3. Fall: Im Übrigen sind Arztpraxen nach Art. 37 Abs. 1 DSGVO verpflichtet, einen DSB zu benennen, wenn die „*Kerntätigkeit*“ des Verantwortlichen in der „*umfangreichen Verarbeitung*“ von Gesundheitsdaten besteht. Auf die Anzahl der Beschäftigten kommt es hiernach nicht an. Die „Kerntätigkeit“ von Ärzten ist die Behandlung von Patienten und nicht die Datenverwaltung. Zwar gehört dazu auch die Verarbeitung von Daten zum Zweck der Dokumentation. Dies ist aber nicht der eigentliche Geschäftszweck des ärztlichen Handelns. Ob es sich in der Arztpraxis um eine „umfangreiche Verarbeitung“ von Gesundheitsdaten handelt, hängt vom Einzelfall ab. Ebenso wie bei der Datenschutz-Folgenabschätzung ist eine „umfangreiche Verarbeitung“ nicht gegeben, wenn die Verarbeitung der Gesundheitsdaten durch einen „einzelnen Arzt“ erfolgt. Dieser wird von Erwägungsgrund 91 der DSGVO privilegiert (s. schon im Abschnitt 3.8.).

Praxen von „einzelnen Ärzten“ müssen damit grundsätzlich keinen DSB benennen, es sei denn, sie sind ausnahmsweise in einem Ausmaß mit einer Datenverarbeitung von Patientendaten befasst, welche die des durchschnittlichen „einzelnen Arztes“ erheblich übersteigt. Die Aufsichtsbehörden für den Datenschutz vertreten in einem Kurzpapier offenbar,[124] dass auch in Einzelarztpraxen ein DSB zu benennen sein kann, wenn ein „erheblich“ vom „durchschnittlichen privilegierten Einzelarzt“ abweichender Umfang einer Datenverarbeitung erfolgt, der an der Betroffenenanzahl zu bemessen sein soll. Was darunter konkret zu verstehen ist, wird offen gelassen. Da für einzelne Facharztbereiche Behandlungsfallzahlen von bis zu 1.500 Patienten pro Quartal durchschnittlich sind, kann eine Orientierung am Wert von ca. 6.000 Datensätzen über einen Zeitraum von einem Jahr erfolgen, wobei die aufgrund von Aufbewahrungsfristen ohnehin schon dokumentierten Patientendatensätze hinzuzurechnen sind.

Für Organisationsgemeinschaften, wie Praxisgemeinschaften, gilt nichts anderes als für Einzelarztpraxen, da dort eine getrennte Datenhaltung erfolgen muss und insoweit – abgesehen von der Kostenteilung für Geräte und Personal – eine Behandlung durch einen „einzelnen Arzt“ im Sinne von Erwägungsgrund 91 der DSGVO stattfindet. Für sie ist die Benennung eines DSB nicht verpflichtend.

Dieses Ergebnis kann auch auf Berufsausübungsgemeinschaften übertragen werden, soweit dort die Behandlung durch einen „einzelnen Arzt“ erfolgt und dieser die Dokumentation verantwortet. In vielen Berufsausübungsgemeinschaften findet im Vergleich zum durchschnittlichen Einzelarzt keine umfangreiche Verarbeitung statt, wenn keine signifikant höhere Anzahl an Patientendatensätzen verarbeitet wird. In diesen Fällen ist die Benennung eines DSB auch in Berufsausübungsgemeinschaften nicht verpflichtend.

> **Beispiel:** Findet in einer Berufsausübungsgemeinschaft von drei Psychotherapeuten im Quartal eine Behandlung von z. B. ca. 150 Patienten statt, kann im Vergleich z. B. zu einer augenheilkundlichen Einzelpraxis mit einer Behandlungsfallzahl von 1.200 Patienten im Quartal keine „umfangreiche Verarbeitung“ angenommen werden.

Ist dagegen zum Beispiel in Berufsausübungsgemeinschaften (z. B. Gemeinschaftspraxen mit mehr als zehn mit der Datenverarbeitung befassten Mitarbeitern), in der eine im Vergleich zum einzelnen Arzt überdurchschnittliche Verarbeitungstätigkeit erfolgt, ein DSB zu benennen, ist darauf zu achten, dass die Person fachlich qualifiziert ist, um die in Art. 39 DSGVO aufgeführten Aufgaben zu erfüllen.[125] Das Maß der erforderlichen Fachkunde bestimmt sich nach dem Umfang der Datenverarbeitung und dem Schutzbedarf der personenbezogenen Daten. Zur erforderlichen Fachkunde gehören neben guten Kenntnissen über die technischen Gegebenheiten zudem gute Kenntnisse über die rechtlichen Regelungen. Auch ein Mitarbeiter der Arztpraxis, der über entsprechende Kenntnisse verfügt, kann als betrieblicher DSB benannt werden. Der Praxisinhaber als Verantwortlicher im Sinne des Datenschutzrechts kann diese Aufgabe nicht übernehmen. Die notwendigen Fachkenntnisse können über Schulungen erworben werden. Mit der Wahrnehmung der Funktion des DSB kann auch ein externer Dienstleister beauftragt werden.[126] Diesem steht, ebenso wie dem Arzt, ein Zeugnisverweigerungsrecht zu und er ist nach dem Datenschutzrecht zur Verschwiegenheit verpflichtet.[127] Im Übrigen wird dem DSB gemäß § 203 Abs. 4 S. 1 StGB n. F. eine strafbewehrte Schweigepflicht auferlegt.

Die Kontaktdaten des DSB sind zu veröffentlichen und der zuständigen Aufsichtsbehörde mitzuteilen.[128] Der DSB ist durch die Praxisinhaber (Verantwortlicher im Sinne des Datenschutzrechts) frühzeitig in Datenverarbeitungsprozesse einzubinden und bei der Erfüllung seiner Aufgaben zu unterstützen.[129] Ihm dürfen indes hinsichtlich der Erfüllung seiner Aufgaben keine Weisungen erteilt werden und er darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden.[130]

Verstöße gegen die Vorschriften über die Benennung, Stellung und Aufgaben des DSB können mit einer Geldbuße von bis zu 10.000.000 EUR oder von bis zu 2 % seines gesamten erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs sanktioniert werden.[131]

Fazit: Arztpraxen müssen prüfen, ob sie einen (externen) DSB zu benennen haben. Einzelarztpraxen und Organisationsgemeinschaften dürften in der Regel keinen DSB zu benennen haben. Bei größeren Berufsausübungsgemeinschaften ist eine Prüfung im Einzelfall vorzunehmen. In jedem Fall ist ein DSB zu benennen, wenn mindestens zehn Mitarbeiter mit der automatisierten Datenverarbeitung befasst sind. Insbesondere ist der Zusammenhang mit der Datenschutz-Folgenabschätzung zu beachten: Ist diese verpflichtend durchzuführen, ist die Benennung eines (externen) DSB obligatorisch. Auf die Frage der „Kerntätigkeit“ kommt es dann nicht mehr an.

> **Hinweis:** Wegen der derzeit unterschiedlichen juristischen Auffassungen ist es aus Gründen der Vorsicht und wegen der möglichen Bußgelder in jedem Fall sinnvoll, sich mit der Frage ernsthaft auseinanderzusetzen und ggf. professionellen Rat einzuholen. Die Benennung eines (externen) DSB ist in jedem Fall zu empfehlen, damit Ärzte einen Ansprechpartner für Datenschutzfragen haben und durch Einhaltung des Da-

[124] Datenschutzkonferenz (DSK), Kurzpapier 12: „Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern“, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Kurzpapier_Datenschutzbeauftragte.pdf?__blob=publicationFile&v=3
[125] Art. 37 Abs. 5 DSGVO.
[126] Art. 37 Abs. 6 DSGVO.
[127] § 38 Abs. 2 i. V. m. § 6 Abs. 6 u. Abs. 5 S. 2 BDSG n. F.
[128] Art. 37 Abs. 7 DSGVO.
[129] Art. 38 Abs. 1 und 2 DSGVO.
[130] Art. 38 Abs. 3 DSGVO.
[131] Art. 83 Abs. 4 Buchst. a DSGVO.

tenschutzes aufsichtsbehördliche Maßnahmen vermeiden können. Zu beachten ist dabei stets, einen externen DSB zur Geheimhaltung zu verpflichten, da sich Berufsgeheimnisträger ansonsten strafbar machen können.[132]

3.10. Melde- und Benachrichtigungspflichten bei Datenschutzverstößen

Sofern Verletzungen des Datenschutzes auftreten („Datenpannen"), haben Praxisinhaber innerhalb von 72 Stunden diesen Vorfall an die zuständige Aufsichtsbehörde zu melden.[133] Meldepflichtige Vorfälle sind z. B. Angriffe von außen („Hacking-Angriffe"), der versehentliche Verlust von Datenträgern oder die Missachtung von Datenschutzvorgaben durch Mitarbeiter. Kann die Meldung nicht innerhalb dieser Zeitspanne erfolgen (z. B. am Wochenende) ist sie nachzuholen und eine entsprechende Begründung für die Verzögerung beizufügen. Die Inhalte der Meldung können Art. 33 Abs. 3 DSGVO entnommen werden. Die Datenpanne ist zudem zu dokumentieren.[134]

Eine Meldepflicht wird indes nicht ausgelöst, wenn voraussichtlich kein Risiko für die Rechte und Freiheiten der betroffenen Patienten besteht, weil Maßnahmen zur Schadenseindämmung nachweisbar[135] ergriffen worden sind. Mögliche Risiken sind der Verlust der Kontrolle über die eigenen Gesundheitsdaten, der Verlust der Vertraulichkeit des Berufsgeheimnisses, Diskriminierungen, eine Rufschädigung oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile.[136]

Sofern eine meldepflichtige „Datenpanne" vorliegt, muss auch der betroffene Patient unverzüglich in klarer und einfacher Sprache benachrichtigt werden, wenn ein Risiko für die persönlichen Rechte und Freiheiten des Patienten wahrscheinlich erscheint.[137] Eine Benachrichtigung ist entbehrlich, wenn geeignete technisch-organisatorische Maßnahmen (z. B. eine Verschlüsselung) ausschließen, dass ein Schaden für den Patienten eintreten kann oder wenn wirksame Maßnahmen zur Schadensbegrenzung ergriffen wurden.

> **Hinweis:** Die Pflichten sind problematisch, sofern der Verantwortliche sich selbst belasten würde, einen Verstoß gegen eine bußgeldbewehrte Pflicht oder gegen die ärztliche Schweigepflicht begangen zu haben. In diesem Fall ist die Meldung zwar vorzunehmen, es besteht aber ein „Verwertungsverbot": Meldungen und Benachrichtigungen bei „Datenpannen" dürfen im Strafverfahren oder im Ordnungswidrigkeitenverfahren nur mit Zustimmung des Arztes verwendet werden.[138]
>
> **Empfehlung:** Es sollten in der Arztpraxis Verfahren und Zuständigkeiten festgelegt werden, wie Datenschutzvorfälle gemeldet werden sollen.

Fazit: Bei Datenpannen ist grundsätzlich die zuständige Aufsichtsbehörde für den Datenschutz zu informieren und der betroffene Patient zu benachrichtigten. Ausnahmen bestehen, wenn wirksame Gegenmaßnahmen getroffen wurden.

3.11. Technische und organisatorische Maßnahmen

Die DSGVO verpflichtet den Arzt, im Interesse des Datenschutzes in seiner Praxis technische und organisatorische Maßnahmen zu treffen.[139] Sie müssen unter Berücksichtigung der bezweckten Verarbeitung von Gesundheitsdaten und der möglichen Risiken für die Rechte von Patienten geeignet sein, den Datenschutz gemäß der DSGVO und eine hinreichende Datensicherheit sicherzustellen.[140]

> **Empfehlung:** Auf Basis des Verzeichnisses der Verarbeitungstätigkeiten lässt sich eine Bewertung der Risiken vornehmen.

Zu berücksichtigende Schutzziele der Informationssicherheit (IT-Sicherheit) werden in Art. 32 DSGVO benannt: Dazu zählt z. B. die Vertraulichkeit, Integrität und Verfügbarkeit der Daten. Eine nähere Konkretisierung erfolgt jedoch nicht.

> **Hinweis:** Weitere Informationen sind in der Technischen Anlage zu diesem Papier[141] sowie im Addendum zur Technischen Anlage[142] enthalten. Die Anlagen befinden sich gegenwärtig in der Überarbeitung und sollen im Laufe des Jahres 2018 veröffentlicht werden. Bis dahin kann auf die bisherigen Dokumente zurückgegriffen werden.

3.12. Sanktionen bei Verstößen

Eine konsequente Berücksichtigung der datenschutzrechtlichen Vorschriften ist zu gewährleisten, da deren Verletzung als bußgeldbewährte Ordnungswidrigkeit geahndet werden kann. Datenschutz soll künftig besser durchgesetzt werden. Dazu steht den Aufsichtsbehörden ein umfassendes Instrumentarium zur Verfügung, z. B. die Erteilung von Warnungen, Verwarnungen, Weisungen oder die Verhängung eines Verbots der Datenverarbeitung.[143] Anstelle oder neben diesen Maßnahmen können Geldbußen verhängt werden.

Mit Geltung der Datenschutzgrundverordnung wird der Rahmen möglicher Geldbußen drastisch erhöht. Es können bei bestimmten Verstößen Geldbußen von bis zu 10.000.000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden.[144] Das betrifft etwa Verstöße gegen die Vorschriften zur Datenschutz-Folgenabschätzung oder zur Führung eines Verarbeitungsverzeichnisses. Bei Verstößen gegen besonders wichtige Datenschutzbestimmungen, die vor allem für Ärzte in Bezug auf ihre Berufstätigkeit einschlägig sind, können die Geldbußen nochmals höher ausfallen: Bei bestimmten Verstößen, z. B. bei einer Verarbeitung von Gesundheitsdaten ohne Rechtsgrundlage, können Geldbußen von bis zu 20.000.000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden; und zwar je nach dem, welcher der Beträge höher ist.[145] In Betracht kommt eine solche Geldbuße ferner bei Verstößen im Hinblick auf die Einwilligung[146], gegen die anderen Anforderungen bei der Verarbeitung von Gesundheitsdaten[147] oder die Missachtung von Betroffenenrechten. Daneben können Patienten materielle und neuerdings auch immaterielle Schadensersatzansprüche geltend machen.[148] Immate-

---

[132] § 203 Abs. 4 S. 2 Nr. 1 StGB, s. o. Anschnitt 2.4.3.
[133] Art. 33 DSGVO.
[134] Art. 33 Abs. 5 DSGVO.
[135] Art. 5 Abs. 2 DSGVO.
[136] Erwägungsgrund 85 der DGSVO.
[137] Art. 34 DSGVO.
[138] §§ 42 Abs. 4, 43 Abs. 4 BDSG n. F.
[139] Art. 24 DSGVO.
[140] Vgl. Art. 24 und Art. 32 DSGVO.
[141] DÄBl. 19/2008, S. 1 ff.
[142] DÄBl. 21/2014, A-969 ff.
[143] Art. 58 Abs. 2 DSGVO.
[144] Art. 83 Abs. 4 DSGVO.
[145] Art. 83 Abs. 5 DSGVO.
[146] Art. 7 DSGVO; s. o. Abschnitt 3.4.1.
[147] Art. 9 DSGVO; s. o. Abschnitt 3.4.2.
[148] Art. 82 Abs. 1 DSGVO.

rielle Schäden resultieren unter Umständen aus schweren Persönlichkeitsrechtsverletzungen.
Fazit: Mit der neuen DSGVO bestehen ab dem 25.05.2018 verschärfte Sanktionsmöglichkeiten und Datenschutzverstöße können härter geahndet werden.

3.13. Beschränkte Befugnisse der Aufsichtsbehörden bei Berufsgeheimnisträgern

Den Aufsichtsbehörden für den Datenschutz stehen grundsätzlich umfassende Untersuchungsbefugnisse zur Überprüfung der Einhaltung des Datenschutzes zu[149] und die Verantwortlichen treffen Mitwirkungspflichten. Zu beachten ist aber, dass bestimmte Untersuchungsbefugnisse[150] gegenüber Berufsgeheimnisträgern nicht bestehen, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten führen würde.[151] Ärzte als Berufsgeheimnisträger müssen den Aufsichtsbehörden für den Datenschutz daher keinen Zugang zu personenbezogenen Daten und Informationen gewähren, die dem Patientengeheimnis unterfallen (z. B. zu Patientenakten). Sie müssen zudem keinen Zugang zu den Geschäftsräumen während der Sprechzeiten oder einen vollständigen Zugang zu allen Datenverarbeitungsanlagen gewähren, wenn zu erwarten ist, dass dadurch die ärztliche Schweigepflicht nicht gewahrt werden kann.

> **Beispiel:** Die Überprüfung der Einhaltung geeigneter technisch-organisatorischer Maßnahmen im Praxis-EDV-System oder einer Videoüberwachungsanlage in der Arztpraxis während der Öffnungszeiten ist grundsätzlich legitim. Wenn aber zu erwarten ist, dass die Aufsichtsbehörde dadurch Kenntnis von der Tatsache der Behandlung einer Person erlangt, handelt es sich schon um eine Informationen, die dem Patientengeheimnisschutz gem. § 203 StGB unterfällt. Eine Zugangsbefugnis der Behörde besteht dann nicht. Kündigt die Aufsichtsbehörde dagegen eine Überprüfung außerhalb der Praxisöffnungszeiten an und sind die in den zu untersuchenden Datenverarbeitungsanlagen enthaltenden Patientendaten hinreichend vor einer Kenntnisnahme gesichert (z. B. durch eine Verschlüsselung) sollte den Aufsichtsbehörden der Zugang nicht verwehrt werden. Dasselbe gilt, soweit es um die Überprüfung der Einhaltung des Beschäftigtendatenschutzes geht, weil hierbei nicht die Gefahr besteht, dass Patientengeheimnisse zur Kenntnis der Aufsichtsbehörden gelangen.

Fazit: Hinsichtlich der Befugnisse der Aufsichtsbehörden ist auf die Wahrung der ärztlichen Schweigepflicht zu achten. Die Aufsichtsbehörden sollten keinen Zugang zu personenbezogenen Daten und Informationen erhalten, wenn damit die Verletzung des Patientengeheimnisses verbunden wäre.

> **Hinweis**: Bei einer Androhung von Bußgeldern[152] sollten Ärzte im Zweifel rechtlichen Beistand zu Rate ziehen.

4. Ärztliche Dokumentation

4.1. Rechtsgrundlagen und Rechtsfolgen

Die Verpflichtung zur ärztlichen Dokumentation wird durch unterschiedliche Rechtsvorschriften unabhängig voneinander geregelt. Sie ergibt sich in berufsrechtlicher Hinsicht aus § 10 Abs. 1 MBO-Ä, in zivilrechtlicher Hinsicht aus § 630f Abs. 1 BGB sowie aus spezialgesetzlichen Bestimmungen, wie der Röntgenverordnung (RöV). Für Vertragsärzte ergibt sie sich zudem aus § 57 Abs. 1 Bundesmantelvertrag-Ärzte (BMV-Ä).

Gemäß § 10 Abs. 1 MBO-Ä haben Ärzte über die in Ausübung ihres Berufs gemachten Feststellungen und getroffenen Maßnahmen die erforderlichen Aufzeichnungen anzufertigen.
Die zivilrechtlichen Bestimmungen zum Behandlungsvertrag fallen etwas ausführlicher aus. Nach § 630f BGB haben Ärzte zum Zweck der Dokumentation in unmittelbarem zeitlichen Zusammenhang mit der Behandlung eine Patientenakte in Papierform oder elektronisch zu führen. Ärzte sind verpflichtet, in der Patientenakte sämtliche aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlichen Maßnahmen und deren Ergebnisse aufzuzeichnen, insbesondere die Anamnese, Diagnosen, Untersuchungen, Untersuchungsergebnisse, Befunde, Therapien und ihre Wirkungen, Eingriffe und ihre Wirkungen sowie Einwilligungen und Aufklärungen. Arztbriefe sind in die Patientenakte aufzunehmen. Dies gilt gleichermaßen für papiergebundene Arztbriefe wie auch für solche in elektronischem Format. Wenn die Patientenakte in Papierform geführt wird, sind Arztbriefe in Gestalt elektronischer Dokumente in geeigneter Weise aufzunehmen.
Der unmittelbare zeitliche Zusammenhang mit der Behandlung dürfte in der Regel gegeben sein, wenn die Dokumentation während oder unmittelbar im Anschluss an die Behandlung vorgenommen wird. Wenn dies aufgrund besonderer Umstände der ärztlichen Tätigkeit im Einzelfall nicht möglich ist, hat der Arzt die Dokumentation zum nächstmöglichen Zeitpunkt nachzuholen.
Nachträgliche Berichtigungen und Änderungen von Eintragungen in der Patientenakte sind nur unter der Voraussetzung zulässig, dass sowohl der ursprüngliche Inhalt als auch der Zeitpunkt der Änderung erkennbar ist. Löschungen früherer Aufzeichnungen vor Ablauf der Aufbewahrungsfrist sind danach sowohl für die papiergebundene als auch für die elektronisch geführte Patientenakte ausgeschlossen (vgl. zu den Anforderungen an die elektronisch geführte Patientenakte 4.4.1.).
Die umfassende ärztliche Dokumentationspflicht dient primär dem Ziel der optimalen Behandlung des Patienten. Aus der Perspektive des Arztes ergibt sich jedoch noch ein weiterer Gesichtspunkt. Hat der Arzt eine wesentliche Maßnahme und ihr Ergebnis nicht in der Patientenakte dokumentiert, wird nach § 630h Abs. 3 BGB zulasten des Arztes davon ausgegangen, dass er eine solche Maßnahme nicht durchgeführt hat. In einem eventuellen Arzthaftungsprozess müsste der Arzt dann beweisen, dass er die Maßnahme dennoch durchgeführt hat. Gelingt ihm das nicht, könnte er den Haftungsprozess gegebenenfalls allein aufgrund unvollständiger Dokumentation verlieren, ohne tatsächlich einen Behandlungsfehler begangen zu haben.

4.2. Elektronische Dokumentation

4.2.1. Eigene Dokumentation

§ 630f Abs. 1 BGB stellt in zivilrechtlicher Hinsicht ausdrücklich klar, dass der Arzt die Patientenakte auch elektronisch führen kann. Wie für die Patientenakte in Papierform gilt auch für die elektronische Patientenakte, dass nachträgliche Berichtigungen und Änderungen nur zulässig sind, wenn neben dem ursprünglichen Inhalt erkennbar bleibt, wann sie vorgenommen wurden. Im

[149] S. Art. 58 DSGVO.
[150] Art. 58 Abs. 1 Buchst. e und f DSGVO.
[151] Art. 90 i. V. m. § 29 Abs. 3 BDSG.
[152] Art. 83 Abs. 5 Buchst. e DSGVO.

Deutsches Ärzteblatt | 09. 03. 2018 | DOI: 10.3238/arztebl.2018.ds01

Fall der elektronisch geführten Patientenakte ist dies durch den Einsatz einer Software sicherzustellen, die nachträgliche Änderungen automatisch kenntlich macht. Dies ergibt sich insbesondere aus der Gesetzesbegründung zum Patientenrechtegesetz, wonach sich der Arzt bei der Führung einer elektronischen Patientenakte einer Softwarekonstruktion zu bedienen hat, die gewährleistet, dass nachträgliche Änderungen erkennbar sind.
Zum Zeitpunkt des Inkrafttretens des Patientenrechtegesetzes dürften allenfalls einzelne Praxisverwaltungssysteme (PVS) über diese Funktionalität verfügt haben. Ein Übergangszeitraum wurde durch das Gesetz nicht eingeräumt. Da ein Wechsel des PVS-Anbieters häufig mit hohem Aufwand verbunden ist, wird sich der Arzt möglicherweise gezwungen sehen, abzuwarten, bis der PVS-Hersteller die entsprechende Funktionalität nachrüstet. Diese Vorgehensweise birgt jedoch das Risiko, dass der Arzt in einem späteren Arzthaftungsprozess in Beweisnot geraten könnte, wenn der Kläger die Dokumentation in Zweifel zieht.
Aus Sicht des Arztes ist es daher dringend geboten, so schnell wie möglich ein PVS einzusetzen, das über die zuvor beschriebene Funktionalität verfügt. In jedem Fall sollte sich der Arzt beim Erwerb einer entsprechenden Software von dem betreffenden PVS-Hersteller schriftlich bestätigen lassen, dass die Software die Anforderungen des § 630f BGB erfüllt.
Zwangsläufig stellt sich die Frage, wie der Arzt in der Zwischenzeit verfahren soll. Rechtssichere und gleichermaßen praktikable Alternativen zur Verwendung einer manipulationsgesicherten Software sind nicht ersichtlich. Die im Addendum zur Technischen Anlage dargestellten Maßnahmen können daher nur unverbindliche Anhaltspunkte bieten[153]. Ob sich diese Maßnahmen als hinreichend geeignet erweisen, die Position des Arztes in einer gerichtlichen Auseinandersetzung zu verbessern, bleibt abzuwarten. Im Ergebnis ist festzuhalten, dass elektronisch geführte Patientenakten den Einsatz einer Software im Sinne des § 630f Abs. 1 S. 2 BGB erfordern.

4.2.2. Externe Dokumente

§ 630f Abs. 2 S. 2 BGB legt fest, dass Arztbriefe in die Patientenakte aufzunehmen sind. Arztbriefe liegen in der Regel als Brief, Telefax oder in elektronischer Form vor. Nicht geregelt ist, wie die unterschiedlichen Formate in die elektronisch geführte Patientenakte aufzunehmen sind. Im Fall eines elektronisch übermittelten Arztbriefes ist dieser in der Patientenakte abzuspeichern. In Papierform übermittelte Arztbriefe (z. B. Brief, Telefax) können durch Scannen in die Patientenakte aufgenommen werden. Umstritten ist jedoch weiterhin, ob Arztbriefe in Papierform nach dem Scannen vernichtet werden können oder in Papierform aufbewahrt werden müssen[154]. Unstreitig ist, dass ein vom Ersteller unterzeichneter Arztbrief die Qualität einer Urkunde besitzt und vor Gericht den vollen Beweiswert erreicht. Das Scannen mit anschließender Vernichtung eines solchen Arztbriefes geht stets mit einer Verringerung des Beweiswertes einher, da dieser in einem Prozess allenfalls als Augenscheinsbeweis gewertet werden kann. Der Arzt hat daher im Einzelfall abzuwägen, ob er Arztbriefe in Papierform nach dem Scannen vernichtet oder aufbewahrt.
Für nichtärztliche Dokumente sieht das Gesetz keine Pflicht zur Aufnahme in die Patientenakte vor. Dessen ungeachtet besteht auch insofern die Pflicht zur Aufzeichnung fachlich wesentlicher Maßnahmen und Ergebnisse. Der Arzt hat die Wahl, die Originaldokumente in die Patientenakte aufzunehmen oder nur die fachlich wesentlichen Informationen in der Patientenakte zu dokumentieren. Unter Abwägung möglicher Haftungsrisiken kann es sachgerecht sein, auch die nichtärztlichen Originaldokumente aufzubewahren.

4.2.3. Anforderungen an die Dokumentation bei unterschiedlichen Tätigkeitsfeldern

Besondere Anforderungen im Hinblick auf Schweigepflicht und Datenschutz können sich ergeben, wenn der Arzt in mehreren Bereichen ärztlich tätig ist.
Bei der gemeinschaftlichen Berufsausübung mit anderen Ärzten muss zwischen Zusammenschlüssen zur gemeinsamen Berufsausübung auf der einen Seite und Organisationsgemeinschaften auf der anderen Seite unterschieden werden. Bei den Berufsausübungsgemeinschaften (z. B. Gemeinschaftspraxis) kommt der Behandlungsvertrag zwischen dem Patienten und der Berufsausübungsgemeinschaft zustande. Die Pflicht zur Erbringung der Behandlungsleistung erstreckt sich jedoch auch auf die ärztlichen Gesellschafter. In dieser Konstellation entfaltet die Schweigepflicht unter den Gesellschaftern keine Wirkung. Etwas anderes gilt nur dann, wenn dies bei Vertragsschluss ausdrücklich vereinbart wird. Eine Besonderheit besteht bei den sog. Teilberufsausübungsgemeinschaften. Hier ist darauf zu achten, dass eine strikte Trennung zwischen den Daten der Patienten der Teilberufsausübungsgemeinschaft einerseits und den Daten der Patienten der eigenen Praxis erfolgt. Von der Schweigepflicht entbunden sind die beteiligten Ärzte untereinander nur im Rahmen der vertraglich vereinbarten gemeinsamen Berufsausübung.
Bei Organisationsgemeinschaften (z. B. Praxisgemeinschaft, Laborgemeinschaft) handelt es sich nicht um Formen der gemeinsamen Berufsausübung. Hier gilt die ärztliche Schweigepflicht unter den Partnern der Gemeinschaft uneingeschränkt. Die EDV-Anlagen müssen so aufgebaut sein, dass der Zugriff auf die Daten der Patienten des jeweils anderen Gemeinschaftspartners ausgeschlossen ist.
Ist der niedergelassene Arzt nebenberuflich als Betriebsarzt tätig, hat er darauf zu achten, dass die betriebsärztliche Dokumentation getrennt von den Patientenakten der Praxis zu führen ist. Für die betriebsärztliche Tätigkeit darf er sich eigener angestellter Hilfskräfte (z. B. MFA) nur aufgrund entsprechender vertraglicher Regelung bedienen. Andernfalls läge in der Einsichtnahme der betriebsärztlichen Unterlagen durch das Praxispersonal bereits ein Verstoß gegen die ärztliche Schweigepflicht.
Übt der (Chef-)Arzt eines Krankenhauses eine ambulante Tätigkeit auf der Grundlage einer Nebentätigkeitsgenehmigung (z. B. privates Liquidationsrecht, Ermächtigung) aus, kommt der Behandlungsvertrag nicht mit dem Krankenhaus, sondern unmittelbar mit dem Arzt zustande. Der Arzt hat darauf zu achten, dass die Dokumentation im Rahmen der ambulanten Nebentätigkeit getrennt von der Krankenhausdokumentation geführt wird. Insbesondere ist sicherzustellen, dass eine Einsichtnahme durch nicht an der Behandlung beteiligte Mitarbeiter des Krankenhauses ausgeschlossen ist.
Sofern der Arzt in den aufgeführten Konstellationen eine Durchbrechung der Schweigepflicht, etwa im Interesse des Patienten,

[153] Vgl. Addendum zur Technischen Anlage – 1. Elektronische Dokumentation.
[154] Zur Frage der Anwendbarkeit der Technischen Richtlinie RESISCAN vgl. das Addendum zur Technischen Anlage – 2. Ersetzendes Scannen.

als erforderlich ansieht, bedarf es der rechtfertigenden Einwilligung des Patienten (vgl. 2.4.). Im Übrigen ist bereits bei der Planung der Praxis-EDV-Anlage auf die getrennte Führung der Patientenakten der unterschiedlichen Tätigkeitsbereiche und deren Schutz vor der Einsichtnahme Unbefugter zu achten.

4.3. Aufbewahrungspflicht

Ärztliche Aufzeichnungen sind für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach gesetzlichen Vorschriften eine längere Aufbewahrungspflicht besteht (vgl. § 10 Abs. 3 MBO-Ä, § 630f Abs. 3 BGB sowie für den vertragsärztlichen Bereich § 57 Abs. 2 BMV-Ä). Längere Aufbewahrungsfristen ergeben sich beispielsweise für Aufzeichnungen über eine Röntgenbehandlung gemäß § 28 Abs. 3 S. 1 RöV oder für die Anwendung von Blutprodukten nach § 14 Abs. 3 Transfusionsgesetz. Bewahrt der Arzt die Patientenakte nicht bis zum Ende der Aufbewahrungsfrist auf, trifft ihn in einem möglichen Arzthaftungsprozess gegebenenfalls die Pflicht zu beweisen, die medizinisch gebotenen Maßnahmen tatsächlich getroffen zu haben (vgl. 4.1. a. E.).

Zu beachten sind zudem die zivilrechtlichen Verjährungsfristen, die etwa für einen Schadensersatzanspruch eines Patienten wegen eines Behandlungsfehlers des Arztes gelten. Die regelmäßige Verjährungsfrist nach § 195 BGB beträgt drei Jahre. Sie beginnt jedoch erst mit dem Ende des Jahres, in dem der Patient von den anspruchsbegründenden Umständen der fehlerhaften Behandlung Kenntnis erlangt oder die Kenntnisnahme grob fahrlässig versäumt hat. Erlangt der Patient beispielsweise erst 20 Jahre nach der Behandlung Kenntnis von einem ärztlichen Behandlungsfehler, kann er einen etwaigen Schadensersatzanspruch gegenüber dem Arzt auch noch nach diesem Zeitraum geltend machen, es sein denn, er hat die späte Kenntniserlangung grob fahrlässig verschuldet. Erst wenn seit der fehlerhaften Behandlung 30 Jahre vergangen sind, verjähren mögliche Schadensersatzansprüche endgültig (§ 199 Abs. 2 BGB). Es sind daher Konstellationen denkbar, in denen es aus Sicht des Arztes erforderlich sein kann, einzelne Aufzeichnungen über die jeweils vorgeschriebene Aufbewahrungsfrist hinaus aufzubewahren.

5. Einsichtnahme in Patientenakten

Das Einsichtnahmerecht des Patienten wird unabhängig voneinander sowohl in den ärztlichen Berufsordnungen (vgl. § 10 Abs. 2 MBO-Ä) als auch in den zivilrechtlichen Bestimmungen zum Behandlungsvertrag geregelt (§ 630g BGB).

Nach § 630g Abs. 1 BGB hat der Arzt dem Patienten auf Verlangen unverzüglich Einsicht in die vollständige, ihn betreffende Patientenakte zu gewähren. § 630g Abs. 2 BGB stellt klar, dass der Patient neben papiergebundenen Kopien oder Ausdrucken „auch elektronische Abschriften“ der Patientenakte – also in Dateiform – verlangen kann, wenn eine elektronische Patientenakte geführt wird. Der Arzt kann bei Aushändigung der Kopien der Patientenakte bzw. bei elektronischer Übermittlung entsprechender Dateien die angefallenen Kosten erstattet verlangen. Der Patient kann auch eine Einsichtnahme seiner Patientenakte in den Praxisräumen verlangen. Im Fall der Einsichtnahme in eine elektronisch geführte Patientenakte ist sicherzustellen, dass der Patient keine Informationen über andere Patienten erhält. Eine postalische Zusendung der Abschriften können Arzt und Patient individuell vereinbaren.

Soweit der Einsichtnahme erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen, hat der Arzt die Einsichtnahme im erforderlichen Umfang zu verweigern. Erhebliche therapeutische Gründe können entgegenstehen, wenn die uneingeschränkte Einsichtnahme in die Dokumentation mit der Gefahr einer erheblichen gesundheitlichen (Selbst-)Schädigung des Patienten verbunden sein kann. Bestehen Zweifel, ob durch die Einsichtnahme eine erhebliche gesundheitliche Gefährdung des Patienten zu befürchten ist, darf der Arzt die Einsichtnahme nicht per se verweigern. Erforderlich ist stets eine Entscheidung im Einzelfall unter Abwägung sämtlicher für und gegen die Einsichtnahme sprechender Umstände im Hinblick auf die Gesundheit des Patienten.

Enthalten die Aufzeichnungen Informationen über die Persönlichkeit dritter Personen, die ihrerseits schutzwürdig sind („erhebliche Rechte Dritter“), hat der Arzt die betreffenden Textpassagen unkenntlich zu machen. Denkbar ist dies beispielsweise im Zusammenhang mit der Behandlung minderjähriger Patienten. Aufzeichnungen des Arztes, beispielsweise über das Eltern-Kind-Verhältnis, sind vom Einsichtsrecht ausgenommen, sofern eine Offenbarung das Persönlichkeitsrecht der Eltern verletzen würde. Auch Geheimnisse, die Familienangehörige des Patienten dem Arzt anvertraut haben, wie z. B. unbekannte Vorerkrankungen naher Angehöriger, sind ihrerseits schutzwürdig und gegebenenfalls der Einsichtnahme des Patienten zu entziehen.

Aufzeichnungen des Arztes über persönliche Eindrücke oder subjektive Wahrnehmungen hinsichtlich des Patienten sind nach neuer Rechtslage im Regelfall offenzulegen. Nach der Begründung des Gesetzgebers sind jedoch Einzelfälle denkbar, die eine Ablehnung rechtfertigen. Dem Einsichtnahmerecht des Patienten kann beispielsweise im Bereich der Psychiatrie und Psychotherapie im Einzelfall das Persönlichkeitsrecht des Arztes entgegenstehen.

In jedem Fall hat der Arzt eine Ablehnung oder Einschränkung der Einsichtnahme gegenüber dem Patienten zu begründen.

Soweit weder eine gesetzliche Übermittlungsbefugnis besteht noch darüber hinaus ein besonderer Rechtfertigungsgrund vorliegt, darf eine Übermittlung personenbezogener Patientendaten nur erfolgen, wenn eine ausdrückliche oder stillschweigende Einwilligung des Patienten vorliegt. Die Einwilligungserklärung muss sich auf den konkreten Übermittlungsvorgang beziehen.

6. Anforderungen an die IT- und Datensicherheit in der Arztpraxis

6.1. Allgemeine Hinweise und Empfehlungen

Neben der Beachtung der aufgezeigten rechtlichen Rahmenbedingungen erfordert der Einsatz von Informations- und Kommunikations-Technologie in der Arztpraxis, dass der technische und organisatorische Ablauf den auftretenden Besonderheiten Rechnung trägt.[155] Unter anderem mit Blick auf die Anforderungen des § 10 Abs. 5 MBO-Ä sind folgende Hinweise zu beachten:

- Zur Sicherung der Patientendaten sind täglich Sicherungskopien auf geeigneten externen Medien zu erstellen.
- Die externe Speicherung von Patientendaten zum Zweck einer zusätzlichen Datensicherung außerhalb der Praxis ist nur unter bestimmten Voraussetzungen zulässig. Dabei sind die für die Auftragsverarbeitung geltenden Grundsätze zu beach-

[155] Vgl. o. Abschnitt 2.11.

Deutsches Ärzteblatt | 09. 03. 2018 | DOI: 10.3238/arztebl.2018.ds01

ten (vgl. Abschnitt 3.6.). Eine externe Datenspeicherung kann nur zum Zweck einer zusätzlichen Datensicherung (Sicherungskopien) empfohlen werden (vgl. Abschnitt 6 der Technischen Anlage).

- Der Arzt muss während der gesetzlichen Aufbewahrungsfristen (vgl. Abschnitt 4.3.) in der Lage sein, nach einem Wechsel des EDV-Systems oder der Programme innerhalb angemessener Zeit die elektronisch dokumentierten Informationen lesbar und verfügbar zu machen.
- Die (Fern-) Wartung von EDV-Systemen in Arztpraxen ist eine Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch Externe. Dabei sind die für die Auftragsverarbeitung geltenden Grundsätze zu beachten (vgl. Abschnitt 3.6.). Zu den im Rahmen der (Fern-) Wartung durchgeführten Maßnahmen s. Abschnitt 10 der Technischen Anlage.
- Auszumusternde Datenträger müssen unter Beachtung des Datenschutzes (z. B. durch mehrfaches Überschreiben mittels geeigneter Software) fachgerecht unbrauchbar gemacht werden.
- Der Arzt sollte beim Abschluss von EDV-Verträgen und in jedem einzelnen Wartungs- oder Reparaturfall darauf achten, dass die gesetzlichen Vorschriften eingehalten werden.
- Drahtlose Verbindungen in der Arztpraxis können ein Sicherheitsrisiko darstellen. Daher sollten die in der Technischen Anlage beschriebenen Vorgaben beachtet werden (vgl. Abschnitt 4.).

6.2. Schutz vor Einsichtnahme und Zugriff

Beim Umgang mit Patientendaten in der Arztpraxis ist das Allgemeine Persönlichkeitsrecht des Patienten zu beachten. Diesem Gedanken muss der Arzt dadurch Rechnung tragen, dass er sowohl bei konventionellen Patientenakten als auch beim Einsatz von Datenverarbeitungstechniken gewährleistet, dass unbefugte Dritte weder im Empfangsbereich noch in den Behandlungsräumen Einblick oder gar Zugriff auf die Patientendaten erhalten. So dürfen papiergebundene Patientenakten in keinem Fall so bereitgelegt werden, dass etwa Patienten Daten anderer Patienten zur Kenntnis nehmen können. Dementsprechend sind Bildschirme so aufzustellen, dass sie nur vom Arzt und dem Praxispersonal eingesehen werden können. Gegebenenfalls muss der EDV-Arbeitsplatz gesperrt werden, so dass wartende Patienten keine Möglichkeit haben, Patientendaten zur Kenntnis zu nehmen.

6.3. Sicherheitsvorkehrungen bei externer elektronischer Kommunikation

Die externe elektronische Kommunikation erfordert Sicherheitsvorkehrungen. Eine bedeutende Sicherheitsvorkehrung kann darin bestehen, den Computer mit Patientendaten von dem Rechner zu trennen, über den die Internetverbindung hergestellt wird. Soweit eine Verbindung mit dem Praxisrechner erfolgt, sollten die Patientendaten auf dem Praxiscomputer verschlüsselt gespeichert und eine leistungsfähige, regelmäßig gewartete und aktualisierte Firewall verwendet werden. Auf diese Weise kann verhindert werden, dass unbefugte Dritte unbemerkt eine Verbindung zu dem Praxiscomputer aufbauen, Schaden verursachende Programme auf dem Praxiscomputer installieren oder den Datenbestand ausspähen, verändern oder löschen. Auf die in Abschnitt 3 der Technischen Anlage dargestellten technischen Vorgaben wird verwiesen.

Übermittelt der Arzt patientenbezogene Daten über ein öffentliches Datennetz (Internet), so ist sicherzustellen, dass der Zugriff Unbefugter auf die Dokumente ausgeschlossen ist. Die zu übermittelnden Daten sollten daher durch ein hinreichend sicheres Verfahren verschlüsselt werden (vgl. Abschnitt 5 der Technischen Anlage). Zur Sicherung der Authentizität ist insbesondere die Verwendung einer qualifizierten elektronischen Signatur geeignet. Ein höheres Sicherheitsniveau wird durch die Nutzung eines gesicherten Datennetzes erreicht, in dem die Datenpakete nochmals verschlüsselt werden. Dies kann insbesondere für die Kommunikation innerhalb von Praxisverbünden/Praxisnetzen relevant sein.

Bei einer Übertragung per Fax ist darauf zu achten, dass im Rahmen einer Abgangskontrolle die richtige Faxnummer und der richtige Adressat angewählt werden. Bei der Übersendung ist sicherzustellen, dass bei dem jeweiligen Adressaten nur Berechtigte von den Daten Kenntnis nehmen können. Vor Absendung des Faxes kann gegebenenfalls eine telefonische Rücksprache mit dem Empfänger erforderlich sein.

Bei der telefonischen Kommunikation findet die sogenannte Internet-Telefonie (Voice over IP, VoIP) zunehmende Verbreitung. Viele Anbieter bieten nur noch VoIP-Telefonanschlüsse an, ohne dass dies für die Kunden erkennbar ist. In diesem Fall haben die Anbieter Maßnahmen zum Schutz der ausgetauschten personenbezogenen Daten auf dem aktuellen Stand der Technik zu treffen (§ 109 Telekommunikationsgesetz). Bestehen Zweifel an der Umsetzung der deutschen Rechtslage, sollte sich der Arzt verbindlich zusichern lassen, dass die Vertraulichkeit der Kommunikation nach dem Stand der Technik gewährleistet ist. Wird (Internet-)Telefonie in der Arztpraxis über drahtlose Funknetzwerke („WLAN“) praktiziert, ist nach Einschätzung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eine zusätzliche Absicherung, z. B. über Verschlüsselung, geboten.