I. Rechtliche Grundlagen

Die beständig fortschreitende Digitalisierung unserer Gesellschaft ist Fluch und Segen zugleich. Der schnelle Zugriff auf Daten – egal zu welcher Zeit und an welchem Ort – ist ein unschätzbarer Vorteil. Aber damit wächst auch die Gefahr, dass Unberechtigte Zugriff auf sensible Daten erlangen. Deshalb tragen all jene, die Daten sammeln, verarbeiten oder an andere weiterleiten, und dazu gehören auch Therapeuten und Rezeptionsfachkräfte in Heilmittelpraxen, eine große Verantwortung. Nachfolgend soll deshalb versucht werden, eine für Nichtjuristen „trockene Materie" möglichst verständlich und „praxisnah" zu vermitteln.

1. Anwendungsbereich der EU-Datenschutz-Grundverordnung und des Bundesdatenschutzgesetzes

In Deutschland basiert der Datenschutz auf diversen rechtlichen Regelungen, die dem Bürger den selbstbestimmten Umgang mit seinen Daten garantieren und die datenverarbeitenden Stellen (Behörden, Unternehmen etc.) zum gewissenhaften Umgang mit diesen Daten anhalten sollen.

Im Folgenden wird das Hauptaugenmerk auf den Regelungen des Bundesdatenschutzgesetzes (BDSG) und der EU-Datenschutz-Grundverordnung (DSGVO) liegen. Stichtag für die Anwendbarkeit der DSGVO und des neuen BDSG ist der 25.5.2018. An diesem Tag ersetzen die DSGVO und das neue BDSG das bisherige BDSG. Daneben gibt es noch weitere relevante Regelungen. Für Heilmittelpraxen gilt vor allem noch die Schweigepflicht für Angehörige der Heilberufe nach § 203 StGB zu beachten.

Anwendung finden die DSGVO und das BDSG insbesondere, wenn in Deutschland und/oder einem EU-Staat personenbezogene Daten automatisiert verarbeitet oder bei nicht automatisierter Verarbeitung in einem Dateisystem gespeichert werden oder gespeichert werden sollen[1].

Für Therapeuten und Heilmittelerbringer heißt das also, dass jede elektronische Verarbeitung (auch wenn sie nur in der Verwendung von Praxissoftware oder E-Mail-Programmen besteht) und jede strukturierte Ablage von Daten (z. B. auch in sortierten Karteikästen) unweigerlich den Anwendungsbereich des BSDG und der DSGVO eröffnet.

[1] Vgl. Art. 2 Abs. 1 und Art. 3 DSGVO.

Dabei hat die DSGVO grundsätzlich Vorrang vor dem BDSG. Das BDSG stellt nur ergänzende Regelungen auf. Die notwendigen Datenschutz-Grundsätze sowie erforderlichen Maßnahmen, die im Folgenden geschildert werden, sind demnach primär der DSGVO zu entnehmen.

Begriffsbestimmung

Personenbezogene Daten sind all jene Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („Betroffener") beziehen. Identifizierbar wird die Person, wenn sie mittels Name, Wohnort, Versicherungsnummer etc. ermittelt werden kann.

Zur **Datenverarbeitung** gehört der Umgang mit personenbezogenen Daten, wie z. B. das Erheben, das Erfassen, das Ordnen, die Speicherung, das Auslesen, die Offenlegung, die Löschung oder die Vernichtung.

Ein **Dateisystem** ist die strukturierte Sammlung von personenbezogenen Daten, unabhängig davon, ob die Sammlung zentral (z. B. auf dem Praxisrechner) oder dezentral (z. B. in einer Cloud) geführt wird.

Als **Unternehmen** sind alle natürlichen oder juristischen Personen zu verstehen, die einer wirtschaftlichen Tätigkeit nachgehen, unabhängig von der Rechtsform (Einzelpraxen, Gesellschaften bürgerlichen Rechts, Gesellschaften mit beschränkter Haftung etc.).

2. Grundsätze für die Verarbeitung personenbezogener Daten

2.1. Rechtmäßigkeit der Datenverarbeitung

Grundsätzlich ist es untersagt, personenbezogene Daten zu verarbeiten. Ausnahmen von diesem Verbot werden nur ermöglicht, wenn der Verarbeiter sich auf eine Rechtsgrundlage berufen kann, die ihm die Verarbeitung erlaubt oder diese gar anordnet.

10. Ich habe zwei Praxen mit insgesamt über zehn Mitarbeitern. Zählen die Mitarbeiter insgesamt oder je Praxis?

Dies kommt darauf an, ob die Praxen nicht nur räumlich, sondern auch rechtlich voneinander getrennt und daher selbstständig sind. Liegen aus gesellschaftsrechtlicher Sicht zwei selbstständige Praxen vor, so werden auch die Mitarbeiter getrennt voneinander addiert. Aber werden besonders schutzwürdige Daten, zu denen auch die Gesundheitsdaten zählen, umfangreich verarbeitet, so ist die Bestellung eines Datenschutzbeauftragten auch unabhängig von der Anzahl der Mitarbeiter verpflichtend; ausgenommen ist die Verarbeitung durch einen einzelnen Angehörigen eines Gesundheitsberufes[48].

11. Wenn ich einen eigenen Server habe, wo nur ich drauf zu greifen kann, bin ich dann sicherer als wenn es über eine Cloud läuft?

Der eigene Server bietet insoweit ein „Mehr" an Sicherheit, als dass man nicht auf Dritte angewiesen ist und man die Daten nicht an diese oder auf deren Server übertragen muss. Ein größerer Schutz vor dem Zugriff durch Unberechtigte entsteht aber nicht automatisch durch die Verwendung eigener Server. Vielmehr hat man lediglich die Sicherheitseinstellungen für den Server in der eigenen Hand und kann selbst entsprechend geeignete technische Maßnahmen zum Schutz der Daten ergreifen.

12. Meine Angestellten müssen bei Arbeitsvertragsunterzeichnung ein Merkblatt (Verpflichtung auf das Datengeheimnis nach § 5 Bundesdatenschutzgesetz (BDSG alte Fassung) unterschreiben. Reicht das (neben Schulung) rechtlich aus?

Um Patientendaten unter Zuhilfenahme von Angestellten verarbeiten zu dürfen, genügt eine Verpflichtung auf das Datengeheimnis. Diese sollte auch auf die Verschwiegenheitspflicht nach § 203 StGB hinweisen und über die datenschutzrechtlichen, strafrechtlichen und arbeitsrechtlichen Konsequenzen informieren. Dadurch wird aber lediglich eine wirksame Rechtsgrundlage für die Hinzuziehung der Mitarbeiter geschaffen.

Den Anforderungen an die Schaffung und Einhaltung von organisatorischen Maßnahmen zur Verhinderung von Datenverletzungen wird dadurch noch nicht genüge getan. Erforderlich ist vielmehr ein internes Konzept/interne Datenschutzrichtlinien. Dort können alle Verarbeitungsvorgänge beschrieben und mit expliziten Handlungsanweisungen an die Mitarbeiter hinterlegt werden. Zudem ist selbstverständlich eine regelmäßige Überprüfung der Einhaltung des Konzeptes notwendig.

13. Darf eine Praxis Geld für Auskunft der Daten verlangen?

Die Auskunft hat unentgeltlich zu erfolgen. Verlangt der Betroffene jedoch weitere Kopien, so können hierfür die entsprechenden Verwaltungskosten verlangt werden.

14. Wo muss der Datenschutzbeauftragte gemeldet werden?

Die Kontaktdaten des Datenschutzbeauftragten müssen veröffentlicht (z. B. auf der Homepage oder in einer Datenschutzerklärung) und der zuständigen Aufsichtsbehörde mitgeteilt werden. Die Aufsichtsbehörden stellen auf ihren Internetseiten rechtzeitig vor dem 25.5.2018 Meldeformulare zur Verfügung.

15. Reicht es aus, dass ich die Patienten z. B. in einem Aushang im Wartezimmer darauf aufmerksam mache, dass ich mit einem Abrechnungszentrum abrechne oder muss ich mir das von jedem Patienten unterschreiben lassen. Wenn ja, was ist mit den Patienten, von denen ich die Unterschrift nicht habe?

Eine Einwilligung in die Datenverarbeitung muss nicht zwingend schriftlich erfolgen. Ein Aushang in der Praxis genügt allerdings nicht, da dadurch nicht gewährleistet werden kann, dass jeder Patient von der Datenweitergabe Kenntnis erlangt hat und mit der Datenweitergabe tatsächlich einverstanden ist. Zum Zwecke des Nachweises ist daher die Schriftform empfehlenswert. Hat die Praxis (noch) keine schriftliche Einwilligung, so darf das Abrechnungszentrum dennoch beauftragt werden, wenn mindestens die mündliche Einwilligung vorliegt.

[48] Erwägungsgrund 91 der DSGVO.

II. Umsetzung der Anforderungen des Datenschutzes in der Praxis

1. Das Verzeichnis von Verarbeitungstätigkeiten (Verarbeitungsverzeichnis)

Das Verzeichnis von Verarbeitungstätigkeiten, auch genannt Verarbeitungsverzeichnis, ist ein zentrales Element in der europäischen Datenschutzgrundverordnung. Auch das bisher gültige Bundesdatenschutzgesetz forderte solch ein Register bereits. Einige kennen es eventuell unter dem früher verwendeten Begriff des Verfahrensverzeichnisses. Um was es sich bei diesem Verzeichnis konkret handelt und wer zur Führung einer solchen Übersicht gesetzlich verpflichtet ist, wird im Folgenden für Sie erörtert.

Was ist ein Verarbeitungsverzeichnis?

Art. 30 Abs. 1 DSGVO verpflichtet den Verantwortlichen (hier: den Praxisinhaber) zur Erstellung und laufenden Pflege eines Verzeichnisses von Verarbeitungstätigkeiten.

Eine Verarbeitung im Sinne der DSGVO ist z. B. der Umgang mit Bewerberdaten oder das Führen einer Personalakte oder einer Patientenakte. Ebenso ist eine Verarbeitung im Sinne der DSGVO die Buchführung der Praxis, die Abrechnung mithilfe einer Verrechnungsstelle oder das Führen einer Liste von Lieferanten für den Praxisbedarf.

Auch eher technische Sachverhalte können Verarbeitungen sein, so z. B. die Telefonanlage, die Rufnummern und aufgebaute Verbindungen speichert, oder die Firewall, die die Internetnutzung der Mitarbeiter der Praxis protokolliert. In allen Fällen werden personenbezogene Daten zu einem bestimmten Zweck verarbeitet.

Ziel und Zweck des Verarbeitungsverzeichnisses

Das Verarbeitungsverzeichnis soll Transparenz über alle Vorgänge in einer Praxis schaffen, die mit der Verarbeitung personenbezogener Daten zu tun haben. Diese klare Auflistung hilft sowohl dem betrieblichen Datenschutzbeauftragten sowie der zuständigen Datenschutzbehörde bei der Erfüllung ihrer Aufgaben. Mit diesem Verarbeitungsregister belegen Sie gegenüber den Behörden, dass Sie und Ihre Praxis die Vorgaben der europäischen Datenschutzgrundverordnung einhalten. Die jeweils zuständige Datenschutzbehörde kann gemäß Art 30 Abs. 4 DSGVO die Aushändigung eines Verarbeitungsverzeichnisses bei Ihnen anfordern.

In Erwägungsgrund 82 der DSGVO heißt es hierzu: „Zum Nachweis der Einhaltung dieser Verordnung sollte der Verantwortliche oder der Auftragsverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen. Jeder Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage das entsprechende Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrolliert werden können.“ Das Verarbeitungsverzeichnis soll demnach eine erste, zumindest grobe Prüfung der Rechtmäßigkeit der Verarbeitungen auf dem Papier durch die Aufsichtsbehörde ermöglichen. Zugleich schafft das Verarbeitungsverzeichnis Bewusstsein für die vorgenommenen Verarbeitungen. Ferner erleichtert es die interne Selbstkontrolle durch die Praxis und die Organisation der Verarbeitungen. Das Verarbeitungsverzeichnis ist damit ein wesentliches Element der Aufbereitung und der Prüfung des Themas Datenschutz.

Wer ist dafür verantwortlich?

Doch wer ist nun konkret in der Praxis dafür zuständig, solch ein Verarbeitungsverzeichnis zu führen? Rein formal ist der Praxisinhaber bzw. die Geschäftsführung verantwortlich, solch ein Verzeichnis zu führen (vgl. Art 30 Abs. 1 DSGVO). Wen die Praxisführung letztendlich mit der konkreten Ausführung dieser Aufgabe betraut, obliegt aber ihr. Zu bedenken ist jedoch, dass ein vorhandener betrieblicher Datenschutzbeauftragter rechtzeitig eingebunden werden muss. Soweit ein Datenschutzbeauftragter bestellt ist, wird dieser oftmals diese Aufgabe übernehmen oder zumindest Zuarbeit leisten. Bei der Erstellung ist er aber auf das Wissen der einzelnen, die Verarbeitungen durchführenden Mitarbeiter angewiesen. Rechtlich ist und bleibt jedoch der Praxisinhaber verantwortlich, vgl. Art. 30 Abs. 1 DSGVO.

Wird kein Verarbeitungsverzeichnis erstellt und laufend auf dem aktuellen Stand gehalten, so kann dies nach Art. 83 Abs. 4 lit. a DSGVO von der Aufsichtsbehörde mit einer Geldbuße von bis zu 10.000.000 EUR oder im Fall eines Unternehmens von bis zu 2 Prozent des Jahresumsatzes des vorangegangenen Geschäftsjahrs sanktioniert werden.

2.1. Ablauforganisation

1.1. Empfangsbereich/Anmeldung/Rezeption

Vor allem im Empfangsbereich ist mit viel Patientenverkehr zu rechnen. Hier gilt es die Patienten und ihre sensiblen Daten vor fremden Augen und Ohren zu schützen. Aber auch sonst muss darauf geachtet werden, dass Unbefugte keinen Zugang zu Praxisräumen haben.

Zu überprüfender Bereich	Ja	Nein	Trifft nicht zu
a) Ist sichergestellt, dass Besucher/Patienten/Unbefugte die Praxis nicht unbemerkt betreten können?	☐	☐	○
b) Können Besucher/Patienten ihre Anliegen schildern, ohne dass neugierige Ohren mithören (Diskretionszone, Einzelabfertigung, Verwendung von Anamnesebögen, ...)?	☐	☐	○
c) Wird dem Patienten erklärt, wofür zusätzliche Daten, die über die eigentlichen Stammdaten hinausgehen (z. B. Telefonnummer oder die E-Mail-Adresse) benötigt werden, und dass diese Angaben in der Regel freiwillig sind? Und werden die Patienten darüber informiert, dass sie ihre Einwilligung zur Verarbeitung und Speicherung von zusätzlichen Daten auch jederzeit widerrufen können?[3]	☐	☐	○
d) Können Telefongespräche mit sensiblen personenbezogenen Inhalten geführt werden, ohne dass Unbefugte zuhören?	☐	☐	○
e) Sind Patientenunterlagen wie Karteikarten und Terminkalender vor dem Zugriff und der Einsicht durch Unbefugte geschützt?	☐	☐	○
f) Sind Faxgeräte und Bildschirme so aufgestellt, dass sie nicht von Unbefugten eingesehen werden können?	☐	☐	○
g) Ist der Empfang deutlich vom Wartebereich getrennt?	☐	☐	○

[3] Hinweis: Stammdaten wie Name, Anschrift, Krankenkasse und Verordnungsdaten sind notwendig, wenn der Patient eine Behandlung wünscht.

Musterlösungen Empfangsbereich/Anmeldung/Rezeption

1.1. a) Ist sichergestellt, dass Besucher/Patienten/Unbefugte die Praxis nicht unbemerkt betreten können?

	Maßnahmen	Das wollen wir umsetzen
1	Tür ist verschlossen, Patienten klingeln und erhalten dann Eintritt	☐
2	Rezeption dauerhaft besetzen	☐
3	Automatischer Summer, der darüber informiert, dass Besucher die Praxis betreten haben. Ein Mitarbeiter geht dann sofort in den Empfangsbereich und empfängt den Besucher.	☐
4	Unbeaufsichtigte Neben- und Hintereingänge müssen immer verschlossen sein.	☐
5	Zum Schutz vor ungewollten Besuchern die Fenster im Erdgeschoss in Räumen, die nicht benutzt und eingesehen werden können, geschlossen halten.	☐
6	Zum Feierabend sollten noch einmal alle Türen und Fenster kontrolliert werden.	☐
7	Um einen Überblick darüber zu haben, welche Personen sich erlaubten Zutritt zur verschlossenen Praxis verschaffen können, sollte die Schlüsselvergabe immer protokolliert werden. Dies gilt sowohl für die Schlüsselausgabe, als auch für die Schlüsselrückgabe.	☐
8	Achten Sie darauf, dass ausscheidende Mitarbeiter und Hilfskräfte wie etwa Reinigungskräfte ihren Schlüssel unmittelbar bei Vertragsende abgeben	☐
9	Verwenden Sie nur Schlüssel, die von einem Schlüsseldienst nicht ohne Erlaubnis des Inhabers nachgemacht werden.	☐
10	Ist die Praxis über eine Schließanlage mit Pin-Code verschlossen, muss dieser Code geändert werden, wenn ein Mitarbeiter aus der Praxis ausscheidet. Bedenken Sie das auch, wenn sie Kurzzeitpraktikanten betreuen oder Personen zur Probearbeit bei Ihnen sind.	☐
11	Während der Schließzeiten die Praxis über eine Alarmanlage sichern.	☐

Widerruf der Einwilligung in die Verarbeitung und Speicherung von Daten

Widerruf der Einwilligung in die Verarbeitung und Speicherung von Daten

Hiermit widerrufe ich

Name, Vorname

gemäß Artikel 7 Absatz 3 EU-DSGVO meine Einwilligung in die Verarbeitung und Speicherung meiner personenbezogenen Daten vom

Datum

zum Zwecke _____

_____

_____

und fordere Sie auf, die entsprechenden Daten unverzüglich zu löschen.

Sollte eine Löschung aus rechtlichen Gründen nicht möglich sein, fordere ich Sie auf, die Daten in einer Form zu kennzeichnen, dass Sie von Ihrer Praxis zu keiner weiteren Verarbeitung genutzt werden.

Ort / Datum

Unterschrift

„Der Letzte macht das Licht aus“

Die Anforderungen in den Heilmittelpraxen sind sehr unterschiedlich. Deshalb dient diese Checkliste nur als Ideensammlung und kann beliebig ergänzt oder gekürzt werden.

Was ist zu tun?	erledigt
5 Minuten durchlüften	☐
Lichter in allen Räumen ausschalten	☐
Fenster in allen Räumen schließen	☐
Aktenschränke verschließen	☐
Praxiscomputer herunterfahren	☐
Kontrollgang durch Umkleidekabinen und Sanitäranlagen, ob sich noch irgendwo ein Patient aufhält	☐
Praxistür verschließen	☐
Alarmanlage aktivieren	☐
	☐
	☐
	☐
	☐
	☐
	☐