BPtK
Bundes
Psychotherapeuten
Kammer

Praxis-Info

DATENSCHUTZ 2018

www.bptk.de

Impressum

HERAUSGEBER
Bundespsychotherapeutenkammer (BPtK)
Klosterstraße 64
10179 Berlin
Tel.: 030. 278 785 – 0
Fax: 030. 278 785 – 44
info@bptk.de
www.bptk.de

Satz und Layout: PROFORMA GmbH & Co. KG
1. Auflage, Juli 2018

Inhaltsverzeichnis

Alle Geschlechter sollen sich von dem Inhalt dieser Praxis-Info gleichermaßen angesprochen fühlen. Aus Gründen der Lesbarkeit erwähnen wir beide Geschlechter beziehungsweise nur die männliche Form, gemeint sind dann alle Geschlechter. In der Reihe Praxis-Info verwenden wir in diesem Sinne in den einzelnen Ausgaben abwechselnd entweder die weibliche oder die männliche Form.

Editorial

Liebe Kolleginnen und Kollegen,

Ende Mai 2018 trat die EU-Datenschutzgrundverordnung in Kraft. Sie ist damit auch in Deutschland unmittelbar gültig. Viele der Regelungen waren bei uns auch schon vorher geltendes Recht. Dennoch bringen die EU-Vorgaben zusätzliche Pflichten für die psychotherapeutische Praxis. Insbesondere drohen bei Verstößen empfindliche Geldbußen.

Wir haben diese Änderungen zum Anlass genommen, die wesentlichen Anforderungen in Sachen Datenschutz und Schweigepflicht in einer Praxis-Info zusammenzufassen.

Herzlichst

Ihr Dietrich Munz

Gesetzliche Vorschriften

Für Psychotherapeutinnen und Psychotherapeuten in Praxen ist insbesondere die EU-Datenschutzgrundverordnung und das Bundesdatenschutzgesetz in der seit dem 25. Mai 2018 geltenden Fassung wichtig. Weitere Anforderungen können sich aus weiteren Gesetzen wie dem Fünften Buch Sozialgesetzbuch ergeben.

Die EU-Datenschutzgrundverordnung (DSGVO) gilt für die Verarbeitung personenbezogener Daten. Verarbeiten umfasst praktisch jede Art der Datenverwendung, zum Beispiel das Erheben, Ordnen, Speichern, Ändern, Anpassen, Nutzen, Weiterleiten, Verknüpfen, Löschen oder Vernichten von Daten. Dabei spielt es keine Rolle, ob die Daten in elektronischer Form oder auf Papier vorliegen. Personenbezogene Daten sind dabei alle Informationen, die eindeutig einer bestimmten oder bestimmbaren Person zugeordnet werden können. Solche Daten sind zum Beispiel Name, Adresse, E-Mail-Adresse oder Sozialversicherungsnummer.

Als besonders schutzbedürftig gelten Gesundheitsdaten. In der psychotherapeutischen Praxis geht es insbesondere um den Schutz von Gesundheitsdaten, also Daten der Patienten, die für die Behandlung benötigt werden. Die Datenverarbeitung beginnt bereits bei der Terminvereinbarung am Telefon, da Name und gegebenenfalls Telefonnummer des Patienten aufgenommen werden. Sollte in der Praxis zum Beispiel ein Psychotherapeut oder eine Sprechstundenhilfe angestellt sein, sind auch die Daten der Beschäftigten zu schützen.

Praxisorganisation

Verzeichnis von Verarbeitungstätigkeiten

Als Praxisinhaber sind Sie verpflichtet, ein Verzeichnis von „Verarbeitungstätigkeiten" zu erstellen. Das Verzeichnis ist über alle Tätigkeiten eines Unternehmens zu führen, bei denen personenbezogene Daten verarbeitet werden (Artikel 30 DSGVO). Die Pflicht zur Führung des Verzeichnisses trifft nicht nur Unternehmen, die mindestens 250 Mitarbeiter haben, sondern auch psychotherapeutische Praxen, da sie Gesundheitsdaten (Artikel 9 Absatz 1 DSGVO) verarbeiten.

Das Verzeichnis muss mindestens folgende Inhalte haben:

- Name und Kontaktdaten des Verantwortlichen,
- gegebenenfalls Datenschutzbeauftragter,
- Zweck der Verarbeitung,
- Kategorien betroffener Personen,
- Kategorien personenbezogener Daten,
- Kategorien von Empfängern und
- vorgesehene Fristen zur Löschung.

Änderungen müssen immer sofort in das Verfahrensverzeichnis aufgenommen werden. Für jede Verarbeitungstätigkeit sollte ein Verzeichnis erstellt werden, zum Beispiel ein Verzeichnis für die psychotherapeutische Dokumentation in der Patientenakte. Wie konkret die Angaben sein müssen, wird erst die Auslegung durch die Aufsichtsbehörden genauer zeigen.

Es bietet sich an, verschiedene Tätigkeiten, die demselben Zweck dienen, in einem Verzeichnis zusammenzufassen. Die Datenschutzkonferenz hat ein Muster für das Verzeichnis von Verarbeitungstätigkeiten erstellt. Dieses können Sie unter folgendem Link herunterladen und ausfüllen: *https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/Muster_Verzeichnis_Verarbeitungstaetigkeiten.html.*

Früher hieß dieses Verzeichnis „Verfahrensverzeichnis" und musste öffentlich zugänglich sein. Das neue Verzeichnis der Verarbeitungstätigkeiten muss zwar nicht mehr öffentlich zugänglich sein. Es muss aber auf Verlangen der Aufsichtsbehörde vorgelegt werden können, damit Sie nachweisen können, dass Sie sich datenschutzkonform verhalten.

To-do:
Erstellen Sie ein Verzeichnis von Verarbeitungstätigkeiten.

Praxishomepage

Eine Praxishomepage muss ein Impressum und eine Datenschutzerklärung enthalten.

Impressumspflicht

Psychotherapeuten, die ihre Dienste auch über das Internet anbieten und über das Internet werben, haben nach § 5 Telemediengesetz die Pflicht, ein Impressum auf ihrer Homepage einzustellen. Die Impressumspflicht gilt unabhängig von den Regelungen der DSGVO weiter.

Im Impressum sind anzugeben:

- der Name und die Anschrift der Praxis,
- die Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit dem Anbieter ermöglichen, zum Beispiel E-Mail-Adresse,
- die Angaben zur Aufsichtsbehörde (Landespsychotherapeutenkammer),
- die gesetzliche Berufsbezeichnung und der Staat, der die Berufsbezeichnung verliehen hat,
- die Bezeichnung der Berufsordnung und wie diese zugänglich ist,
- eine Umsatzsteuer-Identifikationsnummer (wenn umsatzsteuerpflichtige Leistungen erbracht werden).

Datenschutzerklärung

Auf einer Praxishomepage muss eine Datenschutzerklärung eingestellt sein, die die Nutzer über die Verarbeitung personenbezogener Daten auf der Homepage sowie ihre Rechte informiert (Artikel 13 DSGVO). Dabei sind unter anderem anzugeben:

1. der Verantwortliche der Homepage,
2. gegebenenfalls der Datenschutzbeauftragte,
3. die Art, der Umfang, der Zweck, ggf. die Empfänger der verarbeiteten Daten,
4. die Rechtsgrundlage für die Datenverarbeitung,
5. die Dauer der Speicherung,
6. die Widerrufsmöglichkeiten der Zustimmung zur Datenverarbeitung sowie
7. die Betroffenenrechte.

Diese Informationen müssen den Homepage-Nutzern präzise, verständlich, leicht zugänglich und in einer klaren und einfachen Sprache zur Verfügung gestellt werden. Die Datenschutzerklärung sollte auf jeder Seite Ihrer Homepage direkt und klar erkennbar zugänglich sein, zum Beispiel am Seitenende.

Die Bundespsychotherapeutenkammer hat eine Muster-Datenschutzerklärung erstellt, die Sie hier abrufen können: *https://www.bptk.de/uploads/media/20180518_muster-datenschutzerklaerung.pdf.*

TSL-Verschlüsselung des Kontaktformulars

Wenn Sie zum Beispiel über ein Kontaktformular oder eine Online-Terminvergabe personenbezogene Daten wie Name oder E-Mail-Adresse erheben, empfehlen wir dringend, diese Kommunikation zu verschlüsseln. Auch die Namen von Patientinnen und Patienten sind Gesundheitsdaten, die besonders geschützt werden müssen. Dafür sollten Sie eine TSL-Verschlüsselung (Transport Layer Security) verwenden, die häufig noch unter ihrer Vorgängerbezeichnung SSL-Verschlüsselung (Secure Socket Layer) bekannt ist.

Die Datenschutzbehörden der Länder haben unterschiedliche Anforderungen an Verschlüsselungen von Kontaktformular und Online-Terminvergabe. Einige fordern zusätzlich zur TSL-Verschlüsselung eine Ende-zu-Ende-Verschlüsselung. Falls Ihre zuständige Aufsichtsbehörde keine öffentlichen Informationsmaterialien zu diesen Fragen zur Verfügung gestellt hat, können Sie dort auch direkt anfragen.

To-do:

Versehen Sie Ihre Praxishomepage mit Impressum und Datenschutzerklärung. Verschlüsseln Sie Kontaktformular und Online-Terminvergabe.

Dokumentation der Maßnahmen zur Datensicherheit

Datenschutz ist nicht lückenlos. Hacker nutzen immer wieder Lücken von Datenschutz-Software. Damit Sie nachweisen können, dass Sie für den erforderlichen Datenschutz gesorgt haben, sollten Sie ihre technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten dokumentieren. Die EU-Datenschutzgrundverordnung macht keine konkreten Vorgaben, welche Vorkehrungen zu treffen und zu dokumentieren sind.

Was ist zu tun?

Stellen Sie fest, wo Ihre Praxis personenbezogene Daten erhebt oder nutzt. Überlegen Sie, welche Patientendaten Sie haben und wo sich diese befinden. Auf der Hand liegt die Patientenakte. Denken Sie aber auch an die Kommunikation mit Patienten (handschriftlich ausgefüllte Formulare, Homepage). Das Gleiche gilt für Abrechnungsdaten, aber auch Kontaktdaten Ihres beruflichen Netzwerkes (kooperierende Praxen, Intervisionsgruppe). Falls Sie Beschäftigte haben, gehören auch die Beschäftigtendaten dazu.

Zentrales Schutzziel ist die Vertraulichkeit und die Integrität der Daten (Artikel 32 DSGVO). Um Vertraulichkeit zu sichern, sind die Informationen vor Unbefugten zu verbergen. Die Integrität der Daten zu sichern bedeutet, diese nicht beabsichtigt oder unbeabsichtigt zu verändern.

In der psychotherapeutischen Praxis sind zum Beispiel folgende Maßnahmen erforderlich:

- Telefonische Auskünfte nicht im Beisein von Dritten geben, insbesondere keine Namen und Diagnosen nennen.
- Patientendaten nur verschlüsselt über das Internet versenden (zum Beispiel E-Mails, Chats, Videotelefonate). Standard ist eine TSL-Verschlüsselung. Manche Aufsichtsbehörden verlangen auch eine Ende-zu-Ende-Verschlüsselung. Das gilt auch für die Online-Terminvergabe.
- Keine SMS-Kommunikation mit Patienten.
- PCs mit einem ausreichend langen Passwort schützen.[1]
- Betriebssystem und Virenscanner ständig aktualisieren.
- Das Praxisverwaltungssystem sollte nur auf einem PC verwendet werden, der nicht mit dem Internet verbunden ist. Ist dies nicht möglich, sollten die Patientendaten besonders verschlüsselt und eine leistungsstarke Firewall verwendet werden.
- Das WLAN mit einem ausreichend hohen Sicherheitsstandard (zurzeit WPA2) einrichten und mit einem ausreichend langem Passwort schützen. Voreingestellte Passwörter des WLAN-Routers sollten geändert werden.
- Bildschirme in der Praxis so aufstellen, dass sie von Patienten nicht eingesehen werden können.
- Keine Bearbeitung von Patientendaten oder Patientenakten in Anwesenheit Dritter, die mitlesen könnten.
- Patientenakten in Papier- und/oder elektronischer Form sicher verwahren und nach Ablauf der Aufbewahrungsfrist vernichten oder löschen. Beim Vernichten und Löschen sind DIN-Normen zu beachten, die je nach Bundesland unterschiedlich sind (siehe „Dokumentation und Aufbewahrung“, Seite 10).
- Die psychotherapeutische Behandlung findet grundsätzlich im geschlossenen Raum statt, sodass Dritte nicht mithören können. Müssen die Therapieräume verlassen werden, beispielsweise bei einer Expositionstherapie, muss der Datenschutz gewahrt bleiben, zum Beispiel sollte der Patient gegebenenfalls nicht namentlich angesprochen werden.
- Mitarbeiter und Dienstleister im Datenschutz unterrichten und zur Einhaltung der Datenschutzregelungen und der Schweigepflicht verpflichten.
- Ein Datenschutzkonzept für die Praxis aufstellen, das festlegt, wer auf welche Unterlagen zugreifen kann, wann und durch wen personenbezogene Daten gelöscht werden und wie mit Datenpannen und Datenschutzverstößen umgegangen wird.

To-do:

- Fragen Sie zur notwendigen Verschlüsselung von E-Mails, Kontaktformular und Online-Terminvergabe die zuständige Aufsichtsbehörde für Datenschutz an.
- Verwenden Sie das Praxisverwaltungssystem möglichst nur auf einem PC, der nicht mit dem Internet verbunden ist.
- Erstellen Sie eine Aufstellung der technischen und organisatorischen Maßnahmen zur Datensicherheit.

1 *Tipps für gute Passwörter vom Bundesamt für Sicherheit in der Informationstechnik finden Sie hier: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html.*

Datenschutz-Folgenabschätzung

Eine Datenschutz-Folgenabschätzung ist ein spezielles Instrument, um vorab besondere Risiken bei der Verarbeitung von Daten einzuschätzen. Sie ist jedoch nur dann durchzuführen, wenn die Verarbeitung personenbezogener Daten ein hohes Risiko für die Patienten darstellt. Dies wird bei einer umfangreichen Verarbeitung von Gesundheitsdaten angenommen. In einer psychotherapeutischen Einzelpraxis ist das in der Regel nicht der Fall.

Regelmäßige Updates

Rechtsgrundlagen und Sicherheitsstandards können sich ändern. Aus diesem Grund sollte die Aktualität von Nutzerinformationen und Software regelmäßig überprüft werden.

Datenschutzbeauftragter

In der Psychotherapeutenpraxis ist in der Regel kein Datenschutzbeauftragter notwendig. Ein Datenschutzbeauftragter muss zum Beispiel bestellt werden, wenn entweder mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind oder wenn eine umfangreiche Verarbeitung von Gesundheitsdaten erfolgt (Artikel 37 DSGVO). Bei einer Einzelpraxis liegt jedoch keine umfangreiche Verarbeitung vor. In größeren Praxisgemeinschaften sollte aber davon ausgegangen werden. Sie können einen Datenschutzbeauftragten auch freiwillig benennen.

Falls ein Datenschutzbeauftragter bestellt werden muss, ist dieser der Aufsichtsbehörde zu melden. Er kann in der Praxis arbeiten oder als externer Datenschutzbeauftragter bestellt werden. Er hat unter anderem die Aufgabe, den Verantwortlichen und die Beschäftigten einer Praxis zu beraten und die Einhaltung der gesetzlichen Datenschutzvorschriften zu überwachen.

Praxispersonal

Beschäftigte einer Praxis sind über die datenschutzrechtlichen Vorgaben beim Umgang mit personenbezogenen Daten zu unterrichten und auf die Einhaltung zu verpflichten. Zu der Belehrung gehört zum Beispiel, dass personenbezogene Daten nur zu einem bestimmten Zweck verarbeitet werden dürfen und nicht darüber hinaus. Die Unterrichtung und Verpflichtung auf den Datenschutz sollte am ersten Arbeitstag geschehen.

Ein Muster für die Verpflichtung von Beschäftigten finden Sie hier: *https://www.lda.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf.*

Um Praxispersonal für das Thema Datenschutz und Datenschutzrisiken zu sensibilisieren, bietet es sich an, eine praxisinterne Richtlinie zum Datenschutz zu erstellen, in der konkrete Handlungsanweisungen zum Umgang mit Patientendaten gegeben werden.

To-do:

Unterrichten Sie Ihre Beschäftigten über den erforderlichen Datenschutz und lassen Sie sich dies schriftlich und mit Unterschrift bestätigen.

Verträge mit Dienstleistern

Auftragsverarbeitung

Manche Praxen beauftragen für die Wartung der IT-Systeme oder die Buchhaltung einen Dienstleister. Wenn dabei personenbezogene Daten, zum Beispiel Patientendaten, verarbeitet werden, spricht man von einer Auftragsverarbeitung (Artikel 28 DSGVO). Dafür muss ein schriftlicher Vertrag, eine „Vereinbarung zur Auftragsverarbeitung", geschlossen werden. Im Vertrag muss der Dienstleister insbesondere zur Geheimhaltung verpflichtet werden (§ 203 Absatz 4 Nummer 1 Strafgesetzbuch [StGB]).

Der Auftragsverarbeiter ist vom Praxisinhaber sorgfältig auszuwählen und ist an dessen Weisungen gebunden. Er haftet gemeinsam mit dem Aufraggeber und hat selbstständige datenschutzrechtliche Pflichten zu erfüllen. Dennoch trägt der verantwortliche Praxisinhaber weiterhin die Gesamtverantwortung.

Reinigungsfirmen und andere Dienstleister

Die Verpflichtung zur Geheimhaltung gilt auch für andere Personen, die Dienstleistungen für die Praxis erbringen, zum Beispiel müssen Reinigungsfirmen zur Geheimhaltung verpflichtet werden. Wenn der Vertrag nicht mit einer Einzelperson geschlossen wird, sondern mit einem Unternehmen, sollte dieses wiederum seine Mitarbeiter, die in der Praxis tätig sind, zur Geheimhaltung verpflichten. Dies sollte im Vertrag ausdrücklich festgehalten werden.

To-do:

- Schließen Sie Verträge zur Auftragsverarbeitung ab.
- Verpflichten Sie Ihren IT-Service oder Ihren Reinigungsdienst zur Geheimhaltung.

Verhältnis zum Patienten

Grundsätzliche Rechte des Patienten

Patienten haben nach der EU-Datenschutzgrundverordnung grundlegende Rechte zum Schutz ihrer Daten erhalten. Ihre „Betroffenenrechte" umfassen unter anderem das Recht auf Auskunft, auf Berichtigung unrichtiger Daten, Löschung von Daten, Einschränkung der Verarbeitung und das Recht auf Datenübertragbarkeit (Artikel 15 bis 21 DSGVO). Außerdem können sich Betroffene bei der Aufsichtsbehörde beschweren. Darüber müssen die Patienten informiert werden (siehe „Informationspflichten", Seite 10).

Datenverarbeitung bei Diagnostik und Behandlung

Grundsätzlich ist die Verarbeitung von Gesundheitsdaten zur Diagnostik, Behandlung und Dokumentation zulässig (Artikel 9 Absatz 2 Buchstabe h DSGVO i. V. m. § 22 Absatz 1 Nummer 1 Buchstabe b Bundesdatenschutzgesetz). Eine besondere Einwilligung des Patienten ist hierfür nicht notwendig. Auch die Datenverarbeitung bei Prävention und Nachsorge ist damit zulässig. Dies gilt sowohl für Behandlungen in GKV-Praxen als auch in Privatpraxen.

Die Verarbeitung von Gesundheitsdaten ist auch zur Erfüllung vertragspsychotherapeutischer Pflichten oder aufgrund sozialrechtlicher Regelungen zulässig (Artikel 9 Absatz 3 DSGVO). Das betrifft die Auskunftspflicht gegenüber Leistungsträgern wie der Krankenversicherung, Unfallversicherung oder Rentenversicherung (§ 100 Fünftes Buch Sozialgesetzbuch [SGB V]), gegenüber der Kassenärztlichen Vereinigung und Krankenkasse (§ 295 SGB V) oder dem Medizinischen Dienst der Krankenversicherung (§ 276 SGB V). Auch um Rechtsansprüche geltend zu machen, zum Beispiel zur Durchsetzung von Honoraransprüchen gegenüber dem Patienten, dürfen Gesundheitsdaten verarbeitet werden.

Weitere Datenverarbeitung

Ohne Rechtsgrundlage ist die Verarbeitung von Gesundheitsdaten darüber hinaus nicht zulässig. Dafür ist dann eine ausdrückliche und zweckgebundene Einwilligung des Patienten notwendig. Eine pauschale Einwilligung für alle nicht einzeln aufgeführten Zwecke ist unzulässig. Sie ist vielmehr für ausdrücklich genannte Zwecke einzuholen und ist beispielsweise erforderlich, wenn mit der neuen

elektronischen Gesundheitskarte der Krankenversicherungen freiwillige digitale Anwendung wie die Patientenakte oder das Patientenfach der Telematikinfrastruktur genutzt werden sollen. Der Patient muss auch einwilligen, wenn eine private Verrechnungsstelle genutzt werden soll.

Einwilligung der Patienten in die Datenverarbeitung

Ist eine Einwilligung notwendig, muss der Patient diese für eine ganz bestimmte Datenverarbeitung abgeben. Dazu muss der Patient ausreichend informiert sein, für welchen Zweck welche Daten verarbeitet werden sollen und welche Personen die Daten empfangen. Eine pauschale Einwilligung für alle möglichen Zwecke ist unzulässig. Die Einwilligung muss ausdrücklich erfolgen: Sie ist mündlich, schriftlich oder elektronisch wirksam. Um die Einwilligung des Patienten auch belegen zu können, ist es jedoch ratsam, sie schriftlich oder mit qualifizierter elektronischer Signatur einzuholen.

Bei der Einwilligung in die Verarbeitung von Gesundheitsdaten von Minderjährigen hängt die Wirksamkeit davon ab, ob dieser fähig ist, die Bedeutung und Auswirkung der Einwilligung einschätzen zu können. Eine feste Altersgrenze gibt es dafür nicht. Es kann aber angenommen werden, dass in der Regel mit der Vollendung des 16. Lebensjahres die notwendige Einsichtsfähigkeit gegeben ist. Wenn die Einsichtsfähigkeit nicht gegeben ist, müssen die Sorgeberechtigten, wie Eltern oder der Vormund, einwilligen.

To-do:

Benennen Sie die Rechtsgrundlage, aufgrund derer Sie Patientendaten verarbeiten:

- in dem Verzeichnis der Verarbeitungstätigkeiten,
- in der Datenschutzerklärung auf der Homepage sowie
- in der Patienteninformation der Praxis.

Informationspflichten – Patienteninformation der Praxis

Bevor Patientendaten verarbeitet werden, müssen die Patienten darüber informiert werden, was mit ihren Daten geschieht. Dazu können Sie zum Beispiel ein Informationsblatt in Ihrer Praxis gut sichtbar auslegen oder aushängen. Patienten sollen wissen, wer welche Informationen über sie zu welchem Zweck speichert und wie er diese Daten nutzt.

Die Patienteninformation muss beinhalten:

- den Namen und die Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten,
- den Zweck der Datenverarbeitung,
- die Empfänger der Daten, falls die Daten weitergegeben werden,
- die Dauer der Speicherung der Daten,
- die Rechtsgrundlage,
- die Betroffenenrechte (Artikel 15 bis 21 DSGVO).

Die Kassenärztliche Bundesvereinigung hat ein Muster für die Patienteninformation zum Datenschutz in der Praxis erarbeitet. Dieses Muster finden Sie hier: *www.kbv.de/media/sp/Praxisinformation_Datenschutz_Patienteninformation_Muster.docx.*

Dokumentation und Aufbewahrung

Bei der Dokumentation muss sichergestellt sein, dass ein unbefugter Zugriff ausgeschlossen ist. Die Dokumentation muss deshalb verschlossen aufbewahrt werden, wenn der Psychotherapeut den Raum verlässt. Die Dokumentation kann auch außerhalb der Praxis aufbewahrt werden, solange der Ort für die Lagerung von Dokumentationen geeignet ist. Die Akte muss nicht nur vor dem Zugriff unbefugter Dritter geschützt werden, sondern auch vor anderen Einflüssen, die die Akte beschädigen oder gar zerstören können. Die Dokumentation ist mindestens zehn Jahre aufzubewahren.

Die Dokumentation kann auch elektronisch geführt werden (§ 630f Bürgerliches Gesetzbuch). Für diese gelten grundsätzlich die gleichen Datenschutz- und Aufbewahrungspflichten. Der Computer, auf dem Patientenunterlagen gespeichert sind, muss passwortgeschützt sein. Außerdem sollte eine automatische Bildschirmsperre mit geringer Zeitspanne aktiviert werden, um den Inhalt vor Blicken Dritter zu schützen.

weiter Seite 12

Exkurs: Schweigepflicht

Psychotherapeuten sind zur Verschwiegenheit über das verpflichtet, was ihnen im Zusammenhang mit ihrer beruflichen Tätigkeit von Patienten oder von Dritten anvertraut und bekannt geworden ist. Im Rahmen von kollegialer Beratung, Intervision, Supervision oder zum Zwecke der wissenschaftlichen Forschung und Lehre dürfen Informationen über Patienten und Dritte anonymisiert verwendet werden.

Die Schweigepflicht ist einerseits in § 8 der Musterberufsordnung für die Psychologischen Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten (*https://www.bptk.de/fileadmin/user_upload/Recht/Satzungen_und_Ordnungen/musterberufsordnung.PDF*) sowie in den Berufsordnungen der Landespsychotherapeutenkammern geregelt. Sie ist aber auch eine Nebenpflicht aus dem Behandlungsvertrag nach § 603a Bürgerliches Gesetzbuch.

Das Strafgesetzbuch stellt unter Strafe, wer ein Geheimnis verrät, das ihm als Psychotherapeut anvertraut wurde oder sonst bekannt geworden ist (§ 203 StGB). Strafbar macht sich nicht nur der Psychotherapeut, sondern auch berufsmäßige Gehilfen, zum Beispiel Auszubildende. Seit einer Änderung des § 203 StGB im November 2017 gehören dazu auch „sonstige mitwirkende Personen", das heißt IT-Dienstleister, die von der Praxis mit der Wartung des Praxisverwaltungssystems beauftragt werden. Mitarbeiter und Gehilfen sowie die sonstigen mitwirkenden Personen sind vom Psychotherapeuten zur Geheimhaltung zu verpflichten. Auch ein Verstoß gegen diese Pflicht ist strafbar. Andere Berufsgeheimnisträger müssen nicht extra zur Geheimhaltung verpflichtet werden.

Entbindung von der Schweigepflicht

Eine Ausnahme von der Schweigepflicht ist möglich, wenn der Patient den Psychotherapeuten von der Schweigepflicht entbindet. Dies setzt eine wirksame Einwilligung des Patienten voraus. Diese muss konkret und ausreichend informiert erteilt werden. Um die Entbindung von der Schweigepflicht belegen zu können, sollte sie immer schriftlich erfolgen.

Gesetzliche Offenbarungspflichten und -befugnisse

Die Schweigepflicht besteht zum Beispiel nicht gegenüber der Kassenärztlichen Vereinigung, Krankenkasse und dem Medizinischen Dienst der Krankenversicherung. Gegenüber diesen Organisationen hat der Psychotherapeut gesetzliche Offenbarungspflichten.

Außerdem bestehen gesetzliche Offenbarungsbefugnisse bei Kindeswohlgefährdung. Wenn konkrete Hinweise einer Kindeswohlgefährdung vorliegen, können Jugendämter informiert werden (§ 4 Absatz 3 des Gesetzes zur Kooperation und Information im Kinderschutz sowie entsprechende Landesgesetze zur Information der Jugendämter bei Kindeswohlgefährdungen). Hierbei ist abzuwägen, was am besten für das Kindeswohl ist.

Eine Offenbarungsbefugnis besteht ferner, wenn ein Psychotherapeut Dritte, wie IT-Wartungsdienste, mit Dienstleistungen in der Praxis beauftragt (§ 203 Absatz 3 Satz 2 StGB).

Ausnahmen können sich auch aus dem Strafgesetzbuch ergeben. Psychotherapeuten sind von der Schweigepflicht entbunden, wenn sie von geplanten, besonders schweren oder gefährlichen Straftaten erfahren. In diesen Fällen müssen sie die Strafverfolgungsbehörden (Polizei, Staatsanwaltschaft) informieren. Wer dann keine Anzeige erstattet, macht sich strafbar (§ 138 StGB).

Letztlich kann ausnahmsweise die Schweigepflicht gebrochen werden, wenn es sich darum handelt, eine gegenwärtige Gefahr für die Gesundheit oder das Leben anderer Menschen abzuwenden (Rechtfertigender Notstand, § 34 StGB).

Schweigepflicht gegenüber der Aufsichtsbehörde

Um die Einhaltung des Datenschutzes zu überprüfen, haben Aufsichtsbehörden das Recht, die Räumlichkeiten des Verantwortlichen einschließlich der Datenverarbeitungsanlagen zu betreten und Zugang zu allen personenbezogenen Daten zu erlangen. Diese Befugnisse sind jedoch für Berufsgeheimnisträger wie Psychotherapeuten beschränkt, soweit diese dadurch gegen Geheimhaltungspflichten verstoßen würden (§ 29 Bundesdatenschutzgesetz). Das heißt, Aufsichtsbehörden können zum Beispiel keine Einsichtnahme in Patientenakten verlangen.

Die Bearbeitung von Patientenunterlagen sollte so geschehen, dass Dritte keinen Einblick nehmen können. Patientenakten dürfen nicht in der Öffentlichkeit, beispielsweise im Zug, bearbeitet werden.

Nach Ablauf der Aufbewahrungsfristen sind die Akten zu vernichten, soweit sie nicht mehr benötigt werden. Die Akten dürfen jedoch nicht einfach in einem Papierkorb entsorgt, sondern müssen zuvor in einem Aktenvernichter zerkleinert werden. Damit kann auch ein Unternehmen beauftragt werden, das professionell Akten vernichtet. Für das Vernichten der Akten gibt es DIN-Vorschriften, die in Sicherheitsstufen vorgeben, wie groß die zerkleinerten Partikel sein dürfen.

Auch bei einer elektronischen Dokumentation sind besondere DIN-Vorschriften für eine ordnungsgemäße Vernichtung zu beachten. Von den Datenschutzbeauftragten der Länder werden unterschiedliche Angaben zur Höhe der Sicherheitsstufe gemacht. Es empfiehlt sich daher, vor der Vernichtung Informationen im eigenen Bundesland einzuholen oder die Akten nach der höchsten Sicherheitsstufe zu vernichten.

To-do:
Vernichten Sie Patientenakten nach Ablauf der Aufbewahrungsfristen.

Regeln bei Datenpannen

Trotz Sicherheitsvorkehrungen sind Datenpannen nicht immer zu vermeiden, zum Beispiel wenn ein Arztbrief falsch adressiert, in die Praxis eingebrochen oder ein Computer per Virus oder Wurm nach Daten durchsucht wurde. Ein solcher Verstoß gegen den Datenschutz muss in der Regel innerhalb von 72 Stunden der Aufsichtsbehörde, die für den Datenschutz zuständig ist, gemeldet werden. Eine Meldung an die Personen, zu deren Daten Dritte unbefugt Zugang erlangt haben, hat dann zu erfolgen, wenn ein „hohes Risiko" für deren Rechte und Freiheiten besteht. In der Begründung der Vorschrift sind als hohes Risiko Rufschädigung, Diskriminierung oder erhebliche wirtschaftliche Nachteile genannt. Ihre zuständige Aufsichtsbehörde finden Sie hier: *https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html* (Aufsichtsbehörden der Länder für den nicht-öffentlichen Bereich).

To-do:
Melden Sie Datenschutzverstöße Ihrer Aufsichtsbehörde für Datenschutz.

Sanktionen und Haftung

Bei Verstößen gegen den Datenschutz kann die Aufsichtsbehörde mit Verwarnungen oder empfindlichen Geldbußen reagieren. Daneben können Patienten, deren Daten nicht ausreichend geschützt wurden, Schadensersatz geltend machen. Neu ist, dass nicht nur ein materieller, sondern auch ein immaterieller Schaden, zum Beispiel wegen schwerer Persönlichkeitsverletzungen, zum Schadensersatz verpflichtet.

Zurzeit ist unter Juristen strittig, ob Verstöße gegen die Datenschutzgrundverordnung auch abgemahnt werden können. Abmahnungen können grundsätzlich nur von Wettbewerbern geltend gemacht werden. Denkbar ist, dass abgemahnte Verstöße gar nicht wettbewerbsrechtlich relevant sind. Geben Sie bei der noch unklaren Rechtslage nicht ungeprüft eine Unterlassungserklärung ab. Wenden Sie sich im Zweifel an einen Rechtsanwalt.

Abmahnfähig ist jedoch der Verstoß gegen die Impressumspflicht nach dem Telemediengesetz.

Verstöße gegen die Schweigepflicht können strafrechtlich verfolgt werden (§ 203 StGB) und daneben zivilrechtliche Ansprüche, zum Beispiel wegen der Verletzung von Nebenpflichten aus dem Behandlungsvertrag, zur Folge haben.

Weitere Informationen

Die Datenschutz-Aufsichtsbehörden der Länder stimmen ihre Auffassung zur Auslegung der DSGVO untereinander ab. Diese Informationen werden durch die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in Kurzpapieren zur Verfügung gestellt. Diese finden Sie hier: *https://www.bfdi.bund.de/DE/Home/Kurzmeldungen/DSGVO_Kurzpapiere1-3.html*. Lassen Sie sich von Ihrer Aufsichtsbehörde für Datenschutz oder Ihrem Datenschutzexperten beraten!

www.bptk.de