Deutscher Bundesverband für Logopädie e.V.

Datenschutz in der Logopädie 2018

Schritt-für-Schritt-Anleitung samt Checkliste

Wir haben Ihnen in der nachfolgenden Liste einige wichtige Punkte für den Datenschutz zusammengetragen, welche leicht umsetzbar sind und in jeder Praxis unbedingt beachtet werden sollten. Die anschließende Checkliste gibt einen allgemeinen Überblick und kann eine individualisierte Datenschutzbetreuung oder Prüfung nicht ersetzen kann.

Unser Tipp:
Gehen Sie zunächst die einzelnen, ausführlich formulierten Schritte durch. Die Checkliste dient dann zur Überprüfung der einzelnen Bereiche.

Schritt 1: Sicherung der Patientendaten allgemein

Stellen Sie sicher, dass ein Zugriff auf Patientendaten durch unbefugte Dritte soweit wie möglich ausgeschlossen ist. Dies erreichen Sie zum einen dadurch, dass Sie den physischen Zugriff etwa durch das Verschließen von Aktenschränken verhindern und PCs mittels Passwörtern sperren.

Schritt 2: Patientendaten und Computer

Vergewissern Sie sich, dass die ggfs. in der Praxis vorhandenen Monitore der Praxis-EDV für Patienten nicht einsehbar sind. Insbesondere wenn der Anmeldetresen nicht sehr hoch ist kann es sein, dass das Monitorbild eingesehen werden kann und so durch flüchtige, neugierige Blicke personenbezogene Daten von Patienten ausgespäht werden könnten.

Unser Tipp: Abhilfe kann hier ggfs. auch schon dadurch geschaffen werden, den Monitor anders zu stellen oder auf diesem eine Sichtschutzfolie anzubringen.

Unser Tipp für Passwörter: Stellen Sie sicher, dass ausschließlich Passwörter mit einer Schlüssellänge von mindestens acht Zeichen (bestehend aus Buchstaben, Zahlen und Sonderzeichen) verwendet werden.

Schritt 3: Patientenakten

Vergewissern Sie sich, dass durch die in Ihrer Praxis etablierten Arbeitsabläufe keine Patientendateien/Patientenakten für Patienten frei herumliegen. In vielen Praxen werden Patientenakten noch papierhaft geführt und häufig in die Behandlungszimmer mitgenommen oder auf Anmeldetresen für die nächste Behandlung zurechtgelegt.

Unser Tipp: Weisen Sie alle Ihre Mitarbeiterinnen und Mitarbeiter ganz generell dazu an, Patientenakten nicht in Bereichen liegen zu lassen, wo diese von nicht befugten Personen eingesehen werden können.

Schritt 4: Patientendaten im kollegialen Austausch

Halten Sie Ihre Mitarbeiterinnen und Mitarbeiter dazu an, auch untereinander Diskretion zu wahren. Grundsätzlich ist es natürlich erlaubt, sich im beruflichen Alltag unter Kolleginnen und Kollegen über Behandlungen auszutauschen. Aber machen Sie sich bewusst: Das Patientengeheimnis gilt für jeden Therapeuten auch gegenüber den Kolleginnen und Kollegen.

Schritt 5: Datenschutzbeauftragter

Prüfen Sie, ob Sie zur Benennung eines Datenschutzbeauftragten ggfs. verpflichtet sind. Eine wesentliche Neuerung der EU-Datenschutzgrundverordnung besteht in dem sogenannten risikobasierten Ansatz. Dies bedeutet, dass alle Verantwortlichen nun selbst Entscheidungen über den Datenschutz treffen und dokumentieren müssen. Eine Praxis ab 10 regelmäßig mit der Verarbeitung von personenbezogenen Daten beschäftigten Personen ist gemäß § 38 Abs. 2 BDSG neu ein Datenschutzbeauftragter zwingend zu benennen.

Checkliste

Nachdem Sie die obigen fünf Schritte bearbeitet haben, gehen Sie nachfolgende Checkliste durch. Sollten Sie eine Frage mit „Nein“ beantworten, besteht Handlungsbedarf. Wir haben versucht, die Liste so ausführlich wie möglich zu gestalten, bitten jedoch um Berücksichtigung, dass stets Besonderheiten des Einzelfalls beachtet werden müssen. Die Checkliste haben wir nach den üblichen Einteilungen des Datenschutzrechts erstellt.

I. Zutrittskontrolle

Der Datenschutz beginnt bereits auf der physischen Ebene. Der oder die Verantwortliche hat durch angemessene technische und organisatorische Maßnahmen dafür zu sorgen, dass Unbefugten bereits der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird.

Verfügt die Praxis über eine Sicherheitsschließanlage?
❑ JA ❑ NEIN

Sind die Praxisräume und alle Räume, in denen sich Patientendaten befinden, ausreichend gegen Einbruch geschützt?
❑ JA ❑ NEIN

Ist sichergestellt, dass niemand die Praxis unbemerkt betreten kann?
❑ JA ❑ NEIN

Sind alle Computer mit einem PC-Schloss fest angeschlossen?
❑ JA ❑ NEIN

Befindet sich der Server in einem abgeschlossenen Raum?
❑ JA ❑ NEIN

Befinden sich Patientendaten in einem Schrank, welcher abgeschlossen werden kann?
❑ JA ❑ NEIN

Befinden sich Patientendaten in einem Computer, welcher über ein Passwort geschützt ist?
❑ JA ❑ NEIN

Ist sichergestellt, dass wartende Personen nicht mithören können, was am Empfang besprochen wird (Diskretionszone)?
❑ JA ❑ NEIN

Besteht eine räumliche Trennung zwischen dem Wartebereich und dem Behandlungsbereich?
❑ JA ❑ NEIN

Sind Behandlungsräume so gestaltet, dass ein vertrauliches Gespräch zwischen Therapeut und Patient stattfinden kann, bei dem kein Dritter mithört?

❑ JA ❑ NEIN

Wird darauf geachtet, dass während der Behandlung oder während eines Gesprächs mit dem Patienten Türen geschlossen bleiben?

❑ JA ❑ NEIN

Werden in einem Schlüsselbuch alle ausgegebenen Schlüssel (an Mitarbeiter, Putzpersonal, andere Praxisnutzer etc.) samt Nummer aufgeführt?

❑ JA ❑ NEIN

Ist die Schlüsselausgabe mit einer Quittung protokolliert?

❑ JA ❑ NEIN

II. Zugangskontrolle

Die Datenverarbeitungssysteme und Anlagen müssen so beschaffen sein, dass nur diejenigen Personen sie nutzen können, die dazu befugt sind.

Ist sichergestellt, dass die Verarbeitung von Patientendaten nur mit Hardware stattfindet, welche von der Praxis gestellt wird?

❑ JA ❑ NEIN

Werden das Betriebssystem und die Software regelmäßig upgedatet?

❑ JA ❑ NEIN

Wird aktuelle Anti-Viren-Software genutzt?

❑ JA ❑ NEIN

Wird eine aktuelle Firewall genutzt?

❑ JA ❑ NEIN

Sind an Computern äußere Schnittstellen gesperrt?

❑ JA ❑ NEIN

Erfolgt eine Verschlüsselung des W-LAN mittels WPA2-Standard?

❑ JA ❑ NEIN

Ist sichergestellt, dass private Geräte keinen Zugriff auf das Netzwerk der Praxis-EDV haben?

❑ JA ❑ NEIN

Werden mobile Geräte mit einem Code gesperrt?
❑ JA ❑ NEIN

Sind Monitore und Telefaxgeräte so aufgestellt, dass unbefugte weder Zugriff noch Einsicht nehmen können?
❑ JA ❑ NEIN

Wird ein Computer nach einem gewissen Zeitablauf automatisch gesperrt?
❑ JA ❑ NEIN

Ist es möglich Telefonate mit Patienten zu führen, ohne dass Dritte zuhören?
❑ JA ❑ NEIN

Ist sichergestellt, dass bei einem Telefonat mit einem Patienten genau dieser Patient auch am Hörer ist?
❑ JA ❑ NEIN

Können Patienten Informationen mitteilen, ohne dass jemand anders außer dem Therapeuten hört?
❑ JA ❑ NEIN

Sind Behandlungsräume ausreichend schallisoliert, dass Unbefugten ein Mithören nicht möglich ist?
❑ JA ❑ NEIN

Ist sichergestellt, dass Angehörige von Patienten nur Auskunft erhalten, wenn der Patient sich hiermit schriftlich einverstanden erklärt hat?
❑ JA ❑ NEIN

Ist sichergestellt, dass Dritte keinen Zugriff auf Patientenunterlagen oder den Terminkalender haben?
❑ JA ❑ NEIN

Ist sichergestellt, dass Reinigungspersonal keinen Zugang zu Patientendaten hat?
❑ JA ❑ NEIN

Werden alte Patientenunterlagen derart sicher gelagert, dass unbefugte Dritte keinen Zugriff darauf haben?
❑ JA ❑ NEIN

III. Zugriffskontrolle

Es muss gewährleistet sein, dass die zur Benutzung von Datenverarbeitungsanlagen berechtigten Nutzer ausschließlich auf Inhalte zugreifen können, für welche sie berechtigt sind und dass personenbezogene Daten bei der Verarbeitung und Nutzung und nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können.

Sind Patientendaten davor geschützt, dass diese nicht vor Unberechtigten eingesehen werden können?

❑ JA ❑ NEIN

Werden für die Vernichtung von Patientenunterlagen Shredder mit einem Partikelschnitt verwendet? (Aktenvernichter der Sicherheitsstufe 4 oder 5 nach DIN 66399)

❑ JA ❑ NEIN

Werden elektronische Datenträger und Filme vor der Entsorgung gelöscht und physikalisch zerstört?

❑ JA ❑ NEIN

Besteht eine Ordnung am Arbeitsplatz, sodass vor allem Datenträger und Patientendaten nicht offen herumliegen?

❑ JA ❑ NEIN

Werden Datenträger in abgeschlossenen Behältern aufbewahrt?

❑ JA ❑ NEIN

Besteht eine Liste betrieblicher Datenträger?

❑ JA ❑ NEIN

Ist die Anzahl der Administratoren auf das notwendigste reduziert?

❑ JA ❑ NEIN

Ist sichergestellt, dass Praxismitarbeiter nur Zugriff auf die Daten haben und nur die Rechte eingeräumt bekommen haben, welche zur Abarbeitung der entsprechenden Tätigkeit berechtigen?

❑ JA ❑ NEIN

Bestehen Regeln für die private Internetnutzung?

❑ JA ❑ NEIN

Bestehen Regeln für die private E-Mail-Nutzung?

❑ JA ❑ NEIN

IV. Weitergabekontrolle

Es muss verhindert werden, dass personenbezogenen Daten bei der elektronischen Übertragung oder beim Transport oder bei der Speicherung auf Datenträgern unbefugt gelesen, kopiert, verändert oder gelöscht werden können und das festgestellt werden kann, an welchen Stellen eine Übermittlung solcher Daten im Datenverarbeitungssystem vorgesehen ist.

Sind Praxismitarbeiter über ihre Befugnisse und gesetzlichen Pflichten bei der Wahrung der Schweigepflicht ausreichend informiert und wurden diese schriftlich auf das Datengeheimnis verpflichtet?

❑ JA ❑ NEIN

Werden E-Mails verschlüsselt?

❑ JA ❑ NEIN

Besteht eine Dokumentation der Empfänger von Daten wie beispielsweise Ärzten, Abrechnungszentren und Steuerberater?

❑ JA ❑ NEIN

Wird bei der Nutzung von Cloud-Diensten sichergestellt, dass sich die Server in Deutschland befinden?

❑ JA ❑ NEIN

Ist sichergestellt, dass Daten immer sicher übermittelt werden, also unverschlüsselte E-Mails nicht geschickt werden, und soziale Netzwerke oder WhatsApp für den Austausch mit Patienten nicht genutzt werden?

❑ JA ❑ NEIN

Wird bei der Herausgabe von Daten an Dritte sichergestellt, dass der Patient mit der Herausgabe einverstanden ist?

❑ JA ❑ NEIN

Wird darauf geachtet, dass bei der Übermittlung von Patientendaten der Empfänger nicht mehr Informationen erhält, als er zur Erfüllung seiner Aufgaben benötigt?

❑ JA ❑ NEIN

Ist sichergestellt, dass Patienten nicht unbefugt Fotos fertigen?

❑ JA ❑ NEIN

Werden Patienten in einem Behandlungsvertrag darüber aufgeklärt und wird deren Einwilligung eingeholt, dass man Daten an externe Abrechnungsdienstleister weitergibt?

❑ JA ❑ NEIN

V. Eingabekontrolle

Im Rahmen der Eingabekontrolle soll die nachträgliche Überprüfbarkeit und Feststellung gewährleistet werden, ob und von wem personenbezogene Daten in Dateiverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Werden Daten nach einem Datenlöschkonzept (gesetzliche Vorschriften beachten) gelöscht?
❑ JA ❑ NEIN

Bestehen Löschungspläne (Datensätze löschen, Datenträger zerstören, Papierunterlagen mit personenbezogenen Daten shreddern) für Daten?
❑ JA ❑ NEIN

Werden alle Vorgänge wie beispielsweise auch Terminabsagen in der Patientenakte vermerkt?
❑ JA ❑ NEIN

Werden Änderungen an den Patientendaten protokolliert?
❑ JA ❑ NEIN

VI. Auftragskontrolle

Die Verantwortlichen müssen gewährleisten können, dass alle Stellen, welche personenbezogene Daten im Auftrag verarbeiten (Auftragsdatenverarbeitung), ausreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen auch auf deren Seite im Einklang mit der Datenschutz-Grundverordnung bestehen. Datenverarbeitung im Auftrag führen typischerweise zum Beispiel Steuerberater oder Abrechnungszentren durch.

Werden Verarbeitungsaufträge nur an sorgfältig ausgewählte Auftragnehmer vergeben?
❑ JA ❑ NEIN

Wird geprüft, ob sich der Auftragnehmer an den Datenschutz hält?
❑ JA ❑ NEIN

Ist mit jedem Dienstleister, welcher Daten für die Praxis verarbeitet ein Vertrag zur Auftragsdatenverarbeitung geschlossen worden?
❑ JA ❑ NEIN

Ist gewährleistet, dass der Auftragnehmer nach Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten löscht und zurückgibt, sofern keine Verpflichtung zur Speicherung besteht?
❑ JA ❑ NEIN

Sind der Praxis Kontrollrechte gegenüber dem Auftragsdatenverarbeiter eingeräumt worden?
❑ JA ❑ NEIN

Wird die Einhaltung des Datenschutzes bei der Auftragsdatenverarbeitung überprüft?
❑ JA ❑ NEIN

VII. Verfügbarkeitskontrolle

Die oder der Verantwortliche muss sicherstellen können, dass sämtliche personenbezogenen Daten, gegen zufällige Zerstörung oder Verlust geschützt sind. Hierzu gehören technische Maßnahmen zum Beispiel am Gebäude und auch EDV-Maßnahmen.

Existiert ein Überspannungsschutz im Stromverteiler (sämtliche wichtigen IT-Komponenten sind an eine unterbrechungsfreie Stromversorgung mit Überspannungsschutz angeschlossen)?
❑ JA ❑ NEIN

Existiert ein Feuerlöscher in der Praxis?
❑ JA ❑ NEIN

Ist sichergestellt, dass Patienten binnen zehn Jahren die Behandlungsdokumentation ausgehändigt bekommen können?
❑ JA ❑ NEIN

Werden regelmäßig verschlüsselte Sicherheitskopien der Daten der Praxis gefertigt (Empfohlen: 3-Generationen-Prinzip: Abend des Praxistages, Ende der Woche und am Ende des Monats)?
❑ JA ❑ NEIN

Werden Sicherungskopien der Daten der Praxis ausreichend gegen Diebstahl und Brand geschützt?
❑ JA ❑ NEIN

Besteht ein Notfallplan, falls es zu Sicherheitslecks in der EDV kommt (Aufbau eines Risiko- und Fehlermanagements)?
❑ JA ❑ NEIN

Datenschutzverletzungen

Haben Sie sichergestellt, dass die Meldung von Verletzungen des Schutzes personenbezogener Daten innerhalb von 72 Stunden an die Aufsichtsbehörde möglich ist (z.B. nach Hackerangriff)?
❑ JA ❑ NEIN

Stellen Sie sicher, dass Datenschutzverletzungen erkannt werden (sensibilisieren der Mitarbeiter; aktuelles Antivirenprogramm, etc.)?

❑ JA ❑ NEIN

Haben Sie festgelegt, wer, wann und wie mit der Datenschutzbehörde im Schadensfall kommuniziert?

❑ JA ❑ NEIN

Info: Die Meldung muss bei der nach § 38 BDSG zuständigen Aufsichtsbehörde erfolgen, in deren Aufsichtsbezirk die meldepflichtige Stelle ihren Sitz hat.

Schritt 7:

Erstellen Sie abschließend ein Verzeichnis von Verarbeitungstätigkeiten. Gemäß Artikel 30 der EU-Datenschutzgrundverordnung sind alle Vertreter der Heilberufe verpflichtet, ein Verzeichnis darüber zu führen, welche personenbezogenen Daten von Verarbeitungstätigkeiten in der Praxis erfasst sind. Der Begriff der Verarbeitung wird dabei vom Gesetz äußerst weit verstanden: Praktisch immer, wenn Sie mit Daten „irgendwie umgehen", stellt dies eine Verarbeitung im Sinne des Gesetzes dar.

Das Verzeichnis muss mindestens enthalten:

Den Namen und die Kontaktdaten des Verantwortlichen, d.h. der Praxisinhaberin/des Praxisinhabers, und ggfs. die Anschrift und Kontaktinformationen des Datenschutzbeauftragten.

Weiter müssen Sie in dem Verzeichnis die Zwecke der Verarbeitung offenlegen; d.h.:

Abgabe von Heilbehandlungen, Organisation von Terminen etc.

Das Verzeichnis muss weiter eine Beschreibung der Kategorien der betroffenen, personenbezogenen Daten enthalten. Außerdem muss in dem Verzeichnis ausgewiesen sein, welche Empfänger personenbezogene Daten von der Praxis erhalten.

Unser Tipp: Fügen Sie dem Verzeichnis von Verarbeitungstätigkeiten auch noch eine Übersicht, der von Ihnen in der Praxis umgesetzten, technischen und organisatorischen Maßnahmen (gem. 25 DSGVO) zur Schaffung eines angemessenen Datenschutzniveaus bei. Dabei hilft Ihnen schon die obige Checkliste.

Wer hilft bei konkreten Fragen zur Umsetzung in Praxen oder zu bestimmten Verfahrensweisen weiter?

- Datenschutzaufsichtsbehörden der Länder
- Virtuelle Datenschutzbüro
- IHK bietet auch Checklisten für Klein- und Mittelständische Unternehmen an
- Artikel-29-Gruppe
- www.dsgvo-gesetz.de

(dbl-Geschäftsstelle / Mai 2018)