Datenschutz in der Praxis

Für Heilpraktiker und Heilpraktiker für Psychotherapie

Keiner von uns möchte, dass seine Daten von irgendjemand in irgendeiner Form missbraucht oder zweckentfremdet werden. Wir wollen selbst bestimmen, wem wir unsere Daten geben und was derjenige, dem wir sie gegeben haben, damit tun. Das ist unser Recht. Wir dürfen unsere Person schützen und selbst bestimmen. Das nennt man auch Recht auf „informelle Selbstbestimmung". Es ist zwar nicht als solches direkt im Grundgesetz formuliert, leitet sich aber aus diesem in Verbindung mit einem wegweisenden Urteil, dem „Volkszählungs-Urteil" vom 15. Dezember 1983, ab.

Daten, Daten, Daten … Oft ist es uns nicht bewusst, mit welcher Fülle von Daten wir im Rahmen unserer Arbeit im Praxisalltag umgehen. Aber in der Heilpraktikerpraxis haben wir es tagtäglich mit „personenbezogenen Daten" und auch mit besonders „sensiblen Daten" zu tun. Diese müssen nach Vorgabe der EU-Datenschutzgrundverordnung (EU-DSGVO) auch besonders geschützt werden. Seit dem 25.05.2018 ist die Verordnung in allen EU-Ländern verbindlich anzuwenden.

Was sind personenbezogene Daten?

Das sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. „Bestimmbar" bedeutet: Ich kann mir die Person aus verschiedenen Einzelangaben, die ich habe, ableiten.

Das zählt zu den „persönlichen Verhältnissen":

Personendaten
- Name
- Titel
- Alter
- Geburtsort
- Geburtsdatum
- Anschrift
- Telefonnummer
- E-Mail-Adresse
- Familienstand
- Konfession
- Staatsangehörigkeit
- …

Kennnummern
- Sozialversicherungsnummer
- Steueridentifikationsnummer
- Krankenversicherungsnummer
- Ausweisnummer
- Matrikelnummer
- …

Bankdaten
- Kontonummer
- Kreditkartennummer
- …

Online-Daten
- IP-Adresse
- Standortdaten
- …

Kundendaten
- Bestellungen
- Adressdaten
- …

Was gehört zu den „sachlichen Verhältnissen"?

Dabei geht es um Angaben, die Auskunft über die Besitz- und Eigentumsverhältnisse des „Betroffenen" geben:
- Einkommen
- Vermögen
- Eigentum
- Grundbesitz
- Schulden
- …

Was sind „sensible Daten"? Das sind personenbezogene Daten „besonderer Art" (§ 3 Abs. 9 BDSG), z. B.:

- Ethnische Herkunft
- Politische Meinung
- Religiöse und weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Angaben zur Gesundheit
- Angaben zur Sexualität
- …

Merke: Gesundheitsdaten sind personenbezogene Daten besonderer Art (§ 3 Abs. 9 BDSG). Sicherlich achten Sie schon jetzt sorgsam auf diese Daten. Gesundheitsdaten müssen aber auch formell besonders gut geschützt werden. Ist Ihre Praxis schon fit?

Das ist jetzt wichtig Stellen Sie sicher, dass die Daten Ihrer Patienten nicht in falsche Hände geraten können. Unsere Hilfe: „Checkliste Datenschutz in der Heilpraktikerpraxis".

Die Daten, die Sie über Ihre Patienten speichern, müssen transparent sein. Das bedeutet, Sie sollten jederzeit in der Lage sein, Ihren Patienten darüber Auskunft zu geben. Unsere Hilfen: „Informationspflichten für Therapeuten"/„Datenschutzinformation und Einwilligungserklärung in die Datenverarbeitung"/„Verzeichnis von Verarbeitungstätigkeiten"/„Ausfüllhinweise Verzeichnis von Verarbeitungstätigkeiten"/„Datenschutzerklärung Praxishomepage"/„Ergänzung Impressum".

Alle Datenschutzmaßnahmen müssen erfasst und dokumentiert werden. Unsere Hilfen: „Technische und organisatorische Maßnahmen der Datensicherheit"/„Fragenkatalog zu technischen und organisatorischen Maßnahmen zur Datensicherheit".

Ein Verstoß gegen die DSGVO kann teuer werden: Es drohen hohe Geldbußen bis 4 % des Jahresumsatzes oder bis 20 Millionen Euro.

Ihr DSGVO-Masterplan

1. Datenschutzbeauftragter: Ja oder Nein? Je nach Praxisgröße benötigen Sie einen „Datenschutzbeauftragten". Das ist ab 10 Mitarbeitern zwingend notwendig. Dieser muss von Ihnen benannt und geschult und der zuständigen Aufsichtsbehörde für Datenschutz gemeldet werden.

Führen Sie eine Einzelpraxis, sind Sie selbst für den Datenschutz in Ihrer Praxis verantwortlich und müssen sich von nun an in Sachen Datenschutz ständig auf dem Laufenden halten. Oder Sie bestellen einen „externen Datenschutzbeauftragten". Die Kosten für einen externen Datenschutzbeauftragten können jedoch für den Inhaber einer Einzelpraxis unverhältnismäßig hoch sein.

2. „Verzeichnis von Verarbeitungstätigkeiten" erstellen Listen Sie darin auf, wo und wie personenbezogene Daten in Ihrer Praxis verarbeitet werden. Frage ist, was sind eigentlich „Verarbeitungstätigkeiten"?

„Verarbeitung" meint jeden Vorgang, bei dem mit oder ohne Hilfe automatisierter Verfahren (damit ist also auch handschriftliche Verarbeitung von Daten gemeint) personenbezogene Daten bearbeitet werden (Art. 4, Nr. 2 DSGVO). Darunter fallen:

- Erheben
- Erfassen
- Organisation
- Ordnen
- Speichern
- Anpassen/Verändern
- Auslesen
- Abfragen
- Verwenden
- Offenlegen durch Übermittlung, Verbreitung oder andere Form der Bereitstellung
- Abgleich/Verknüpfung
- Einschränkung
- Löschen/Vernichtung
- …

Diese Fragen sollten Sie sich bei der Erstellung des Verzeichnisses stellen:

Welche personenbezogenen Daten erfasse ich in der Praxis? Von wem?

- Patienten
- Klienten
- Mitarbeitern
- Bewerbern
- Kooperationspartnern
- Lieferanten
- …

Für welche Prozesse in meiner Praxis nutze ich diese Daten?

- Behandlung
- Beratung
- Coaching
- Patientendatenbank
- Abrechnung
- E-Mail-Verkehr
- Praxis-Newsletter
- …

Benutze ich dabei IT-Systeme? Wenn ja, welche?

- Gebe ich meine Daten an „externe Dienstleister" weiter?
- Haben Sie Abrechnungs- oder Buchhaltungsleistungen abgegeben?
- Nutzen Sie ein professionelles Call-Center zwecks Terminvergabe?
- Haben Sie jemanden, der Ihr IT-System wartet?
- Lassen Sie Ihre Weihnachtspost verschicken und geben dafür Ihre Patientendaten weiter?
- Lassen Sie Patientendaten extern archivieren oder vielleicht vernichten?
- …

Wichtig: Auch Prozesse, die über „externe Dienstleister" laufen, müssen in Ihrem „Verzeichnis von Verarbeitungstätigkeiten" erfasst werden.

Wie ein Verarbeitungsverzeichnis aussehen sollte, sehen Sie auf der nächsten Seite.

3. Organisatorische Maßnahmen zu Datenschutz und Datensicherheit dokumentieren Was sind Ihre TOM = Technische und/oder Organisatorische Maßnahmen? Schaffen Sie geeignete organisatorische und technische Vorkehrungen, um die Daten Ihrer Patienten und anderer Betroffener (z.B. Mitarbeiter) zu schützen. Das ist für Nicht-IT'ler gar nicht so einfach. Deswegen stellen wir eine Checkliste „Technische und organisatorische Maßnahmen der Datensicherheit" und einen „Fragenkatalog zu technischen und organisatorischen Maßnahmen zur Datensicherheit" zur Verfügung. (Mit freundlicher Genehmigung von Stephan Hansen-Oest, Rechtsanwalt/Fachanwalt für IT-Recht, www.datenschutz-guru.de).

Mit der Checkliste und dem Fragenkatalog können Sie überprüfen, welche Maßnahmen in Ihrer Praxis bereits laufen und welche Sie zur Optimierung Ihrer Datensicherheit noch ergreifen können.

Diese Fragen sollten Sie sich bei der Erstellung Ihrer Dokumentation stellen:

- Ist meine Software auf dem neuesten Stand?
- Besitze ich eine aktive Firewall und Virenschutz?
- Welche Produkte werden eingesetzt?
- Wer soll außer mir Zugangs- bzw. Zugriffsberechtigungen auf die Daten meiner Patienten haben?
- Verwende ich ausreichend sichere Passwörter?
- Erfolgt eine automatische Sperrung meines Bildschirms mit Passwortschutz bei Pausen?

Das Verarbeitungsverzeichnis gibt klare Vorgaben für den Inhalt, nicht aber für die Art seiner Darstellung.

Das gehört in ein Verarbeitungsverzeichnis

- Angaben zum Verantwortlichen (i.d.R. also des Heilpraktikers)
- Name
- Anschrift
- Kontaktdaten (Telefon, E-Mail)
- Internetadresse

Angaben zum Datenschutzbeauftragten (soweit vorhanden)

- Zuständige Person für den Datenschutz bzw. Datenschutzbeauftragter, ggf. sein Vertreter
- Name und Kontaktdaten des Verantwortlichen, ggf. Vertreter
- Verarbeitungstätigkeit(en)

Tipp: Bündeln Sie Verarbeitungen nach dem Zweck!

Das sind Verarbeitungstätigkeiten in der Heilpraktikerpraxis

- Verarbeitung von Patientendaten zur Behandlung
- Verarbeitung von Patientendaten zur Abrechnung mit dem Patienten/mit privaten Krankenversicherungen/der Beihilfe/der Heilpraktikerzusatzversicherung
- Verarbeitung von Patientendaten zur Praxisverwaltung (ggf. mit Einsatz und Nutzung einer Praxissoftware)
- Betrieb einer Webseite mit Möglichkeit der Online-Terminbuchung
- Führen von Personalakten
- …

Merke: Auch das „Datum der Anlegung" der Verarbeitungstätigkeit und das „Datum der letzten Änderung" der Verarbeitungstätigkeit müssen im Verarbeitungsverzeichnis dokumentiert werden.

Zweck(e) der Verarbeitung Je nach Beschreibung einer Verarbeitungstätigkeit ist der Verarbeitungszweck zu dokumentieren:

- Patientenbehandlung
- Abrechnung von Leistungen
- Behandlungs-Dokumentation, Qualitätssicherung, Terminvergabe, Tagesplanung, Wochenplanung
- Betrieb einer Webseite/Terminbuchung
- Durchführung von Beschäftigungsverhältnissen
- …

Kategorien betroffener Personen:

- Patienten, Klienten
- Mitarbeiter, Bewerber, Assistenten, Praktikanten, Schüler …
- Webseitenbesucher
- Seminarteilnehmer/Selbsthilfegruppenteilnehmer
- Lieferanten/Geschäftspartner, die zur Erfüllung von Verarbeitungszwecken notwendig sind
- …

Kategorien personenbezogener Daten:

- Daten zur Person des Patienten
- Name
- Anschrift
- Geburtsdatum
- Religion
- …

Daten zur Patientenbehandlung

- Anamnestische Daten
- Diagnosedaten
- Therapiedaten
- …

Daten zur Personalverwaltung

- Daten zur Person
- Name
- Anschrift
- Geburtsdatum
- Religion
- Familienstand/ Kinder
- Bankverbindung
- …

Daten zur Lohn- und Gehaltsabrechnung

- Personalstammdaten
- Zeiterfassungsdaten
- …

Daten von Bewerbern

Daten von Lieferanten

Kategorien von Empfängern

Hier geht es um Empfänger, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden.

Interne Empfänger

- Übermittlung an alle Mitarbeiter der Heilpraktikerpraxis

Externe Empfänger

- Übermittlung an Mitbehandler/ den weiterbehandelnden Arzt
- Übermittlung an private Versicherungsgesellschaften/Beihilfe/Zusatzversicherungen
- Übermittlung an das Gesundheitsamt
- Infektionsschutzgesetz
- Übermittlung an Angehörige/Erben
- Übermittlung an die Berufsgenossenschaft
- Übermittlung bei Praxisverkauf
- …

Wichtig: Auch Ihre Mitarbeiter müssen zur Verschwiegenheit (bezieht sich auf das „Patientengeheimnis") und zum Datenschutz (d.h. Datenschutz im Allgemeinen) verpflichtet werden (siehe Muster „Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung").

Bevor Sie Daten extern weitergeben, müssen Sie sich individuell von Ihrer Patientin/Ihrem Patienten von der Schweigepflicht entbinden lassen (siehe Muster „Entbindung von Frau/ Herrn Heilpraktiker/in … und Praxisteam von der Schweigepflicht").

Ggf. Übermittlungen an ein Drittland oder an eine internationale Organisation.

Beim Heilpraktiker/Heilpraktiker für Psychotherapie in der Regel: Keine.

Fristen für die Löschung

- Patientendaten: 10 Jahre nach dem letzten Kontakt
- Personaldaten: 10 Jahre nach Ausscheiden des Mitarbeiters
- Finanzwirksame Daten: 10 Jahre nach Ablauf des letzten Geschäftsjahrs

- Sind meine Datenträger ausreichend verschlüsselt?
- Ist sichergestellt, dass unbefugte Personen nicht auf meinen Computer zugreifen können?
- …

Technische und organisatorische Maßnahmen:

- Alarmanlage
- Sicherheitsschloss
- Sichere Aufbewahrung von Datenträgern
- Verschlüsselung von (mobilen) Datenträgern
- Festlegung von Berichtigungen in das IT-System
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Einsatz von Verschlüsselungs-Technologie (SSL-Verschlüsselung von E-Mails)
- Einsatz von Anti-Viren-Software
- Erstellung eines Backup- und Recovery-Konzepts
- Testen von Datenwiederherstellung
- …

4. „Auftragsverarbeitungs-Verträge" schließen: Wenn nötig

Wenn personenbezogenen Daten in Ihrem Auftrag von einem anderen Unternehmen (also weisungsabhängig) verarbeitet werden, müssen Sie nach EU-Datenschutzgrundverordnung einen „Auftragsverarbeitungs-Vertrag (AV-Vertrag)" schließen. Deshalb stellen wir Ihnen in unserem Mitgliederbereich, mit freundlicher Genehmigung des Bayrischen Landesamts für Datenschutzaufsicht, eine „Formulierungshilfe für einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO" zur Verfügung.

Beispiele für AV-Dienstleister sind:

- Wartungsdienste für die Praxis EDV
- Nutzung von Cloud-Diensten
- Datenträgerentsorger
- …

Wichtig: Auch diese Unternehmen sind dazu verpflichtet, ihrerseits Datenschutzmaßnahmen zu protokollieren und umzusetzen. Wovon Sie sich wiederum überzeugen sollten.

5. Datenschutz-Folgenabschätzung: Nein!

Nach unseren bisherigen Informationen (Stand 05/2018) haben Einzelpraxen mit Blick auf „einen geringen Umfang der Datenverarbeitung" keine Datenschutz-Folgenabschätzung durchführen. Wenn wir zukünftig abweichende Informationen hierzu erhalten sollten, teilen wir Ihnen diese umgehend mit und helfen Ihnen auch hier, die entsprechenden Maßnahmen zum Datenschutz einzuleiten.

Was tun bei „Datenpannen"?

- Meldepflicht nach Art. 33 DSGVO
- Auch, wenn es unangenehm ist: Melden Sie Zwischenfälle innerhalb von 72 Stunden nach Bekanntwerden an Ihre zuständige Datenschutzbehörde.

Datenpannen sind:

- Fehlversendungen von Post oder E-Mails
- Verlust von Datenträgern
- Verlust von Aktenordnern
- Unmöglichkeit, ein Backup wiederherzustellen
- Löschung von Daten durch eine nicht autorisierte Person
- Datendiebstahl („Hacking")
- Abhandenkommen eines Schlüssels zur Entschlüsselung von Daten
- Verlust eines mobilen, unverschlüsselten Datenträgers

Hinweis: Bei einer eventuell auftretenden Datenpanne wenden Sie sich bitte an den Vorstand des VUH bzw. VFP, wir stellen Ihnen dann entsprechende Hilfen zur Verfügung.

Anfangen! Schritt für Schritt zum Datenschutz

Auch wenn Datenschutz vielleicht bisher nicht das Hauptaugenmerk in Ihrer Praxis hatte, trauen Sie sich Schritt für Schritt an die verschiedenen Maßnahmen heran! Wir haben uns bemüht, unsere Hilfen (zu finden im internen Downloadbereich unserer Verbands-Webseiten) für jeden verständlich zu machen und auf das Wesentliche zu reduzieren. Wir wünschen Ihnen gutes Gelingen!

Ihr VUH- und Ihr VFP-Team

Sonja Kohn
Heilpraktikerin, freie Redakteurin, Dozentin an den Paracelsus Schulen

kontakt@naturheilpraxis-kohn.de

Ergänzend zum Artikel finden Sie im Magazin „Freie Psychotherapie" 03.18 ein Interview mit dem IT-Experten Hajo Nolte zum Thema „Praxis-Homepage und DSGVO".

Das sind Ihre Informationspflichten nach Art. 13 und 14 EU-DSGVO

- Name des Praxisinhabers bzw. Namen der Praxisinhaber und Kontaktdaten (kann entfallen, wenn dem Patienten dies bereits bekannt ist)
- Kontaktdaten des Datenschutzbeauftragten (soweit erforderlich)
- Zweck der Datenerhebung (normalerweise „Behandlung von Erkrankungen") sowie deren Rechtsgrundlage
- Empfänger bei Übermittlung von personenbezogenen Daten (Abrechnungsfirmen, Labore usw.)
- Übermittlung von personenbezogenen Daten ins Ausland (wenn dies erfolgt)
- Kategorien von personenbezogenen Daten, die in der Praxis verarbeitet werden (Gesundheitsdaten sind eine „besondere Kategorie personenbezogener Daten" nach Art. 9 Abs. 1 EU-DSGVO; dies ist nur anzugeben, wenn die Daten nicht beim Patienten erhoben werden)
- Dauer der Speicherung (im Regelfall 10 Jahre nach dem letzten Kontakt)
- Rechte des Patienten nach Art. 15-18 EU-DSGVO (Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung) oder Widerspruch gegen die Verarbeitung nach Art. 21 EU-DSGVO
- Recht des Patienten, sich beim Datenschutzbeauftragten des Bundeslandes als Aufsichtsbehörde im Bereich des Datenschutzes zu beschweren, sowie
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für den Vertragsschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte.

Wann müssen Sie diese Informationen Ihren Patienten mitteilen?

- Bei der erstmaligen Erhebung der personenbezogenen Daten (Erstbesuch).

Diese Rechte haben Betroffene nach EU-DSGVO

- Informationsrecht
- Auskunftsrecht
- Recht auf Datenübertragbarkeit
- Recht auf Berichtigung
- Recht auf Löschung/Vergessenwerden
- Recht auf Einschränkung der Verarbeitung
- Widerspruchsrecht