Checkliste Datenschutz in der Heilpraktikerpraxis für Psychotherapie / Psychologischen Beratungspraxis

Leitfaden zum Umgang mit Patientendaten

Schützen Sie die Daten Ihrer Patienten / Klienten (stets beide gemeint)! Beim Datenschutz in der Heilpraktikerpraxis / Psychologischen Beratungspraxis (stets beide gemeint) sind nicht nur die Datengrundschutz-Grundverordnung (DS-GVO) und das neue Bundesdatenschutzgesetz (BDSG-N) zu beachten, sondern auch die Anforderungen, die an Sie als Therapeut /Berater gestellt werden, da Sie nach § 630a BGB und der Berufsordnung des VFP der „Verschwiegenheitspflicht“ unterliegen. (https://www.vfp.de/images/stories/psy-vfp/downloads/berufsordnung-1-und-2.pdf)

Wichtig: Auch Ihre Mitarbeiterinnen und Mitarbeiter müssen in puncto Datenschutz fit sein. Vergessen Sie daher bitte nicht, diese zur Verschwiegenheit und zum Datenschutz zu verpflichten.

Diese Checkliste soll Sie dabei unterstützen Datenschutzmängel aufzudecken und zu beseitigen.

Wird eine Frage mit NEIN beantwortet besteht Handlungsbedarf.

Checkpoint 1: Empfang/ Anmeldung

Schützen Sie die Daten Ihrer Patienten vor neugierigen Blicken, spitzen Ohren und flinken Fingern…	**ja**	**nein**
Haben Sie sichergestellt, dass niemand (Besucher, Lieferanten etc.) Ihre Praxis unbemerkt betreten kann? *Stichwort: Zutrittskontrolle*	☐	☐
Wenn Sie einen Empfang in Ihrer Praxis haben, ist dieser während der Öffnungszeiten auch ununterbrochen besetzt?	☐	☐
Haben Sie einen Bereich eingerichtet, in dem Ihre Patienten Ihr Anliegen schildern können, ohne dass jemand mithören kann? *Stichwort: Diskretionszone*	☐	☐
Werden die Anmelde- und Patientendaten in Ihrer Praxis diskret erhoben (Verwendung von Anamnesebögen…)?	☐	☐
Erklären Sie Ihren Patienten, wofür Sie Ihre Daten (Telefonnummer, E-Mail…) benötigen und dass ihre Angaben grundsätzlich freiwillig sind?	☐	☐
Weisen Sie auch darauf hin, dass das Ausfüllen des Anamneseformulars freiwillig ist?	☐	☐
Sind die Akten Ihrer Patienten vor unbefugten Zugriff geschützt (abschließbarer Karteischrank etc.)?	☐	☐
Ist auch Ihr Terminkalender vor Einsicht und Zugriff von nicht befugten Personen geschützt?	☐	☐
Sind Bildschirme, Fax, Telefone usw. so aufgestellt, dass sie nicht von Unbefugten eingesehen werden können?	☐	☐

Checkpoint 2: Wartezimmer/ Wartebereich

Schützen Sie die Daten Ihrer Patienten vor neugierigen Blicken, spitzen Ohren und flinken Fingern…	**ja**	**nein**
Ist das Wartezimmer/ der Wartebereich so gelegen, dass keine Gespräche am Empfang mitgehört werden können (keine Wartestühle am Empfang…)?	☐	☐
Ist das Wartezimmer/ der Wartebereich so gestaltet, dass wartende Patienten nicht hören können, was im Behandlungszimmer besprochen wird (keine Wartestühle vor Behandlungsräumen, Warte- und Behandlungszimmertür normalerweise geschlossen…)?	☐	☐

Checkpoint 3: Behandlungszimmer

Achten Sie bei der Behandlung Ihrer Patienten auf Diskretion und tragen Sie dafür Sorge, dass es keine ungewollten Zuhörer oder Zuschauer gibt. Wichtig: Schützen Sie auch im Behandlungszimmer die Unterlagen Ihrer Patienten vor unbefugten Zugriffen.	**ja**	**nein**
Sind Ihre Behandlungsräume so gestaltet, dass bei Gesprächen, Untersuchungen und Behandlungen keine unbefugten Personen teilhaben können?	☐	☐
Achten Sie darauf, dass während eines Gesprächs oder einer Behandlung die Tür geschlossen bleibt?	☐	☐
Sind Ihre Behandlungsräume ausreichend „schallisoliert“, sodass niemand vor der Tür unberechtigt mithören kann?	☐	☐
Achten Ihre Mitarbeiter beim Betreten oder Verlassen der Räume darauf, dass niemand sonst „Einblick“ in das Behandlungszimmer und die Vorgänge dort haben kann?	☐	☐
Tragen Sie dafür Sorge, dass keine vertraulichen Telefonate von Unbefugten mitgehört werden können?	☐	☐
Sind Karteikarten und Patientenakten sowie andere schriftliche Patientenunterlagen vor Einsicht und Zugriff unbefugter Personen auch in Ihrer Abwesenheit geschützt?	☐	☐
Sind die Unterlagen Ihrer Patienten vor zufällige Blicken geschützt? *Hinweis: Denn schon ein kurzer Blick genügt für die meisten, um wesentliche Informationen zu lesen!*	☐	☐
Haben Sie abschließbare Akten-/ Karteischränke in Ihrem Behandlungsraum und werden diese nach der Sprechstunde auch abgeschlossen?	☐	☐
Haben Sie sichergestellt, dass Ihre Patienten keinen Zugang zu (ungesicherten) Praxisrechnern haben?	☐	☐

Checkpoint 4: Praxisverwaltung

Tragen Sie auch im hektischen Praxisalltag dafür Sorge, dass die sensiblen Daten Ihrer Patienten sicher und geschützt sind.	**ja**	**nein**
Sind Sie und Ihre Mitarbeiter über Ihre Befugnisse und Pflichten bei der Wahrung Ihrer gesetzlichen Verschwiegenheitspflicht informiert? *Stichwort: Patientengeheimnis*	☐	☐
Haben Sie Ihre Mitarbeiterinnen und Mitarbeiter, möglichst schriftlich, auf das Datengeheimnis verpflichtet (§ 5 Bundesdatenschutzgesetz)?	☐	☐
Ist die Einsicht jedes einzelnen Mitarbeiters in die Daten an deren jeweilige Berechtigung zur Einsicht angepasst (eingeschränktes Benutzerprofil)?		
Sind schriftliche Patientenunterlagen vor Einsicht und Zugriff durch unbefugte Personen geschützt?	☐	☐
Sind abschließbare Aktenschränke vorhanden und werden diese nach der Sprechstunde auch abgeschlossen?	☐	☐
Haben Sie sichergestellt, dass auch Ihr Reinigungspersonal keinen Zugang zu Ihren Patientendaten hat?	☐	☐
Sind die Praxisräume in denen sich die Patientendaten befinden ausreichend gegen Einbruch geschützt?	☐	☐
Tragen Sie dafür Sorge, dass auch alte Akten sicher vor Einsicht und Zugriff unbefugter Personen geschützt sind (nicht im „offenen Keller“/ Abstellraum…)?	☐	☐
Verwenden Sie in Ihrer Praxis Shredder für die Aktenvernichtung nach DIN 66399-1/2 der Partikelgröße P-5?	☐	☐

Checkpoint 5: Datensicherheit

Moderne Informationstechnik ist auch in der Heilpraktikerpraxis nicht mehr wegzudenken. Sorgen Sie dafür, dass Ihre IT sicher funktioniert und regelmäßig auf Risiken überprüft wird. ***Wenn Sie einen Dienstleister für Systembetreuung und Wartung beauftragt haben, schließen Sie bitte einen Vertrag nach § 11 Bundesdatenschutzgesetz.***	**ja**	**nein**
Haben Sie Ihren Computer „physisch“ geschützt (Computer nicht unbeaufsichtigt, beschränkter Zugang zur IT etc.)?	☐	☐
Sind auch Ihre Drucker und Faxgeräte vor unbefugtem Zugriff geschützt?	☐	☐
Sind Ihre Bildschirme so aufgestellt, dass Sie nicht durch Unbefugte eingesehen werden können?	☐	☐
Ist der Zugang zu Ihrem Computer z.B. durch ein Passwort geschützt?	☐	☐
Entspricht das Passwort dem aktuellen Sicherheitsstandard (mindestens 8 Stellen, bestehend aus Buchstaben, Zahlen und Sonderzeichen)?		
Werden die Passwörter auch regelmäßig gewechselt?	☐	☐
Haben Sie auch, falls vorhanden, Ihren WLAN-Router ausreichend geschützt (z.B. durch ein Passwort)?	☐	☐
Ist Ihr Computer, falls er unbeaufsichtigt ist, stets gesperrt (inkl. Passwortschutz)?	☐	☐
Haben Sie auf Ihren Bildschirmen, v.a. in Behandlungsräumen, passwortgeschützte Bildschirmschoner aktiviert?	☐	☐

Haben Sie Virenschutzprogramme und Firewalls installiert und sind diese auch auf dem neuesten Stand?	☐	☐
Erstellen Sie regelmäßig eine Sicherung der Daten (externe Festplatte)?	☐	☐
Schützen Sie diese Sicherungen auch ausreichend gegen Diebstahl, Brand und andere physische Einflüsse?	☐	☐
Verwenden Sie für die Verarbeitung Ihrer Patientendaten keine privaten Notebooks oder Handys?	☐	☐
Wenden Sie bei der Verarbeitung Ihrer Patientendaten nur Programme etc. an, die Sie in Ihrem Verarbeitungsverzeichnis erfasst haben?	☐	☐
Verwenden Sie eine Software, die Ihre Patientendaten verschlüsselt speichert, soweit dies möglich ist?	☐	☐
Haben Sie einen Notfallplan, falls eine Datenpanne auftritt (z.B. Computervirus)?	☐	☐
Nutzen Sie für die Speicherung Ihrer Patientendaten Verfahren, die auch die Möglichkeit einer Löschung der Daten vorsehen?	☐	☐
Werden nicht mehr benötigte Informationen und Datenträger gemäß Datenschutzbestimmungen korrekt entsorgt?	☐	☐

Checkpoint 6: Datenübermittlung/ Datenaustausch

Auch als Heilpraktiker übertragen Sie u.U. Patientendaten an Dritte (z. B. Mitbehandler). Das ist allerdings nur erlaubt, wenn eine Einwilligung Ihres Patienten vorliegt („Verschwiegenheitentbindungserklärung“)	**ja**	**nein**
Ist eine sichere Übertragung (auch physisch) von Daten gewährleistet (verschlüsselte E-Mails, kein Facebook, kein WhatsApp, kein Instagram)? *Wichtig: Auch wenn Ihr Patient einen unsicheren Übermittlungsweg wünscht oder wählt, tragen Sie die datenschutzrechtliche Verantwortung!*	☐	☐
Verwenden Sie Mustererklärungen zur Entbindung von der Verschwiegenheitspflicht, in denen Sie Ihren Patienten ausreichend erklären, welche Daten Sie für welche Zwecke an welchen Empfänger weitergeben?	☐	☐
Dokumentieren Sie jede Datenübermittlung in der Patientenkartei und welcher Empfänger die Daten erhalten hat?	☐	☐
Achten Sie darauf, dass Sie wirklich nur die Daten und Informationen weitergeben, die der Empfänger tatsächlich zu der Erfüllung seiner spezifischen Aufgabe benötigt?	☐	☐
Vergewissern Sie sich, wenn Sie Daten telefonisch oder per Fax weitergeben, dass diese wirklich nur an den vorgesehenen Empfänger gehen?	☐	☐
Wenn Sie einen externen Dienstleister mit Ihrer Abrechnung beauftragen, haben Sie dafür auch eine schriftliche Einwilligung ihres Patienten erfragt?	☐	☐
Falls Sie nicht allein behandeln, informieren Sie Ihre Patienten über Mitbehandler oder ggf. Nachbehandler und vergewissern Sie sich, dass Ihre Patienten keine Einwände dagegen, insbesondere den	☐	☐

Datenaustausch, haben?		
Wenn Sie Anfragen von privaten Versicherern haben, prüfen Sie, ob Sie die geforderten Auskünfte/ Berichte dem Patienten zur Weiterleitung aushändigen dürfen?	☐	☐
Geben Sie Angehörigen von Patienten grundsätzlich nur dann Auskunft, wenn sich Ihr Patient damit auch einverstanden erklärt hat? *Hinweis: Möglichst schriftlich!*	☐	☐
Tragen Sie dafür Sorge, wenn Zweifel daran bestehen, dass eine Übermittlung von Patientendaten nicht zulässig ist, eine rechtliche Klärung herbeizuführen?	☐	☐

Checkpoint 7: Betrieblicher Datenschutzbeauftragter

Sollten Sie in Ihrer Praxis 10 oder mehr Mitarbeiter haben, die ständig automatisiert bearbeiten, benötigen Sie einen Datenschutzbeauftragten.	**ja**	**nein**
Besitzt der Datenschutzbeauftragte zur Erfüllung seiner Aufgaben auch die erforderliche Fachkunde und Zuverlässigkeit (§ 4f Abs. 2 BDSG)?	☐	☐
Ist der Praxisinhaber *nicht* gleich der Datenschutzbeauftragte?	☐	☐

Checkpoint 8: Informationspflicht bei Datenpannen

Auch wenn es unangenehm ist: Sie sind gesetzlich verpflichtet Datenpannen zu melden (§ 42a BDSG).	**ja**	**nein**
Ist Ihnen bekannt, wann und wie Datenpannen an die zuständige Aufsichtsbehörde und unter Umständen die Betroffenen zu melden sind?	☐	☐

Meine Datenschutzaufsichtsbehörde:

_____

Checkpoint 9: Patientenrechte

Ihre Patienten haben Rechte: Sie können Akteneinsicht und Auskunft verlangen und haben u. U. einen Anspruch auf Korrektur und Löschung von Daten.	**ja**	**nein**
Haben Sie sichergestellt, dass Ihre Patienten ihre Rechte auch tatsächlich geltend machen können (Auskunft, Akteneinsicht, Aushändigung von Kopien, Korrektur unrichtiger Daten, Löschung von Daten sofern möglich da 10jährige Dokumentationspflicht, sonst Sperrung)? *Bearbeitungszeit: „unverzüglich“ bis maximal zwei Wochen*	☐	☐
Werden von Ihnen die Fristen für die Aufbewahrung und Löschung von Gesundheitsdaten eingehalten?	☐	☐
Ist Ihnen bekannt, dass unter bestimmten Voraussetzungen (§ 630g Bürgerliches Gesetzbuch, BGB) auch Erben und Angehörige von verstorbenen Patienten ein Recht auf Akteneinsicht haben? *Stichwort: Geltendmachung von Vermögensinteressen, insbesondere bei Schadenersatzansprüchen aufgrund von Behandlungsfehlern*	☐	☐
Ist Ihnen bekannt, dass Sie Ihre Patienten darüber unterrichten müssen, welche Daten zu welchem Zweck erhoben und gespeichert werden, wenn es Ihr Patient wünscht?	☐	☐
Wissen Sie, dass Sie Ihre Patienten darüber unterrichten müssen, an welche Empfänger Sie welche Daten zu welchem Zweck übermittelt haben, wenn es Ihr Patient wünscht?	☐	☐
Ist Ihnen bekannt, wann Sie unter ganz bestimmten Voraussetzungen eine Akteneinsicht oder Auskunft verweigern dürfen? *Stichwort: „soweit nicht erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen“* *Hinweis: Durchsetzung, zu unserem jetzigen Wissensstand, jedoch eher unwahrscheinlich.*	☐	☐

Checkpoint 10: Externe Dienstleister

Wenn Sie einen externen Dienstleister (Auftragnehmer), z.B. für die Verwaltung Ihrer IT oder die Aktenvernichtung beauftragen, kann leider nicht zu 100% ausgeschlossen werden, dass Einsicht und Zugriff auf Patientendaten aus bleibt.	**ja**	**nein**
Ist Ihnen bekannt, dass Sie als Auftraggeber die Verantwortung dafür tragen, dass der Auftragnehmer datenschutzrechtliche Vorschriften einhält?	☐	☐
Stellen Sie sicher, dass in Ihrem Auftragsverarbeitungs-Vertrag (AV-Vertrag) Umfang, Art und Zweck der vorgesehenen Datenverarbeitung sowie Sicherheitsvorkehrungen, Kontroll-und Weisungsrechte festgelegt sind? *Sicherheitsvorkehrungen nach § 11 Abs. 2 BDSG):* *Berichtigung, Löschung, Sperrung/ Rückgabe von Daten*	☐	☐
Wählen Sie Ihre externen Dienstleister mit Bedacht aus, insbesondere im Hinblick auf Ihre Eignung aus und ob sie geeignete technische und organisatorische Maßnahmen zur Datensicherheit treffen?	☐	☐

Wissen Sie, dass es Ihre Aufgabe ist, sich vor Beginn und während der Arbeit Ihres Dienstleisters, sich von der Einhaltung der vereinbarten Sicherheitsvorkehrungen zu überzeugen?	□	□

Was tun bei Datenpannen?

Die DSGVO regelt in den Artikeln 33 und 34 den Umgang bei Datenpannen.

Die Meldung der Datenpanne muss innerhalb von 72 Stunden bei der zuständigen Aufsichtsbehörde stattfinden.

Eine Meldung hat nur dann nicht zu erfolgen, wenn die Datenpanne „voraussichtlich nicht zu einem Risiko“ für den Betroffenen führt.

Die betroffene Person selbst muss nur erfolgen, wenn ein „hohes Risiko für deren Rechte und Freiheiten“ besteht.

Das müssen Sie melden:

- die Art der Datenpanne
- die Kategorien von betroffenen Daten
- die Anzahl der Betroffenen
- die Anzahl der betroffenen Datensätze
- eine Einschätzung der Folgen für den Betroffenen
- Ihre Maßnahmen zur Ursachenbeseitigung/ Schadenminimierung beim Betroffenen

Wir wünschen Ihnen eine erfolgreiche Umsetzung Ihrer Datenschutzmaßnahmen!

Ihr VFP-Team