Häufige Fragen und Antworten für Therapeut*innen zum REVIDIERTEN DATENSCHUTZRECHT

1. Bearbeitungsverzeichnis

Müssen alle KomplementärTherapeut*innen ein Bearbeitungsverzeichnis führen?

Da Gesundheitsdaten als besonders schützenswert gelten, ist es Therapeut*innen sehr zu empfehlen, ein Verzeichnis zu führen.

Was gehört alles in ein Bearbeitungsverzeichnis?

Für eine übliche Praxis reicht eine Liste darüber, welche Daten durch welche Person und für welchen Zweck gesammelt und ob die Daten weiteren Personen weitergegeben werden. Normalerweise dürfte es sich hierbei um das Patient*innendossier, die Agenda (v. a. wenn online) und die Fakturierung handeln (siehe dazu die Vorlage auf der Webseite der OdA KT). Bei allen Daten, die nicht schriftlich oder auf der eigenen Festplatte gespeichert sind, sondern in der Cloud eines Anbieters (Tarif 590 etc.) muss die Therapeut*in sicherstellen, dass die DSG-Richtlinien eingehalten werden.

2. Datenschutzverantwortliche Person

Ist eine datenschutzverantwortliche Person zwingend?

Im Gesetz ist immer wieder die Rede vom «Datenverantwortlichen». Daher muss eine solche Person für alle Datensammlungen existieren, welche die (Mit-)Verantwortung trägt und als Ansprechperson dient (auch für Behörden und Gerichte). Als Therapeut*in in einer Einzelpraxis sind Sie selbst der/die Datenschutzverantwortliche.

Was bedeutet «notwendige Fachkenntnisse»?

Es bestehen keine gesetzlichen Vorgaben. Aus den Umständen ergibt sich, dass die Person über das revidierte Datenschutzrecht sowie die nötigen Massnahmen informiert ist, und sich damit auseinandergesetzt hat.

3. Technische und organisatorische Massnahmen für die Datensicherheit

Was muss an der eigenen Website geändert werden?

Es sollte eine Datenschutzerklärung (DSE) auf der Website aufgeschaltet werden, welche einfach zu finden ist. Auf der Webseite der OdA KT ist eine einfache Vorlage einer DSE für Therapeut*innen zu finden, ausführlichere Varianten sind im Internet zahlreich und häufig kostenlos verfügbar. Jede*r Therapeut*in ist selber verantwortlich, eine auf die eigenen Bedingungen passende Datenschutzerklärung zu formulieren.

In unserer Gruppenpraxis haben wir Zugriff auf die Daten aller Klient*innen der bei uns tätigen Therapeut*innen und Fachpersonen, müssen wir dies anpassen?

Auch in einer Gruppenpraxis sind die Zugangsrechte auf die Daten der selber betreuten Klient*innen zu beschränken.

Was ist bei elektronisch abgelegten Daten zu beachten?

Die Datensicherheit muss z.B. durch Firewalls und Zugangsbeschränkungen (Passwortschutz für PC/Laptop) gewährleistet sein. Alternativen für den Transfer von Daten in unsichere Drittstaaten sind zu prüfen, d.h. nach Möglichkeit andere Anbieter für Software oder Applikationen wählen, Standort Server/Cloud wechseln (Datenablage im Ausland durch Speicher-Anbieter in die Schweiz wechseln).

Darf ich Personendaten per E-Mail versenden?

Falls Personendaten per E-Mail versendet werden, ist ein System zu verwenden, welches die Verschlüsselung vornimmt (z. B. HIN) oder das Einverständnis der betroffenen Person einzuholen, dass die Übermittlung unverschlüsselt stattfinden darf.

Können die Krankengeschichten weiterhin auf Papier geführt werden?

Werden Krankengeschichten physisch abgelegt, sind diese in einem sicheren Aufbewahrungsort zu lagern, der vor unbefugtem Zugriff, Diebstahl oder physischen Schäden schützt (z.B. in einem abschliessbaren Schrank, Tresor oder in einem abschliessbaren Raum). Sollten mehrere Personen in der Praxis arbeiten, müssen die Zugriffe auf die Krankengeschichten beschränkt werden, indem nur gewisse Personen einen Schlüssel zum Aufbewahrungsort haben.

Wie informiere ich meine Mitarbeiter*innen?

Bei Angestellten sind Schulungen/Weiterbildungen durchzuführen, um auf den Datenschutz zu sensibilisieren. Aber auch Weisungen/Reglemente zum Datenschutz können eingeführt werden, allenfalls mit Beizug von externen Anbietern (z.B. Hosting-Anbieter, Webmaster, etc.). Für die Anstellung von Mitarbeiter*innen ist etwa im Arbeitsvertrag oder im Personalreglement auf eine entsprechende Datenschutzerklärung zu verweisen.

4. Recht auf Auskunft/Informationspflicht

Wie müssen Therapeut*innen ihre Klient*innen informieren?

Das nDSG gibt nicht vor, wie betroffene Personen informiert werden müssen. In der Praxis ist eine Datenschutzerklärung üblich, aber auch eine Information in den AGB, ein Einwilligungsformular oder eine mündliche Information (z. B. Tonbandansage) genügt. Ungenügend ist dagegen die blosse Angabe einer Kontaktperson für weitere Fragen.
Ob die betroffenen Personen die Datenschutzerklärung tatsächlich anschauen, spielt keine Rolle.

Wer keine Website hat, muss die Datenschutzerklärung abgeben (z.B. mit der Patienteninformation) oder an einem gut sichtbaren Ort in der Praxis aufhängen oder auflegen.

Wann ist eine Übermittlung an Dritte erlaubt?

Sofern die Datenbearbeitung rechtmässig ist, den datenschutzrechtlichen Grundsätzen entspricht und die betroffenen Personen über die Weiterleitung informiert sind (siehe Datenschutzerklärung).

Dürfen Rechnungen, Berichte usw. per E-Mail an Klienten/Krankenversicherungen versendet werden?

Hier sind technische Massnahmen zu ergreifen, damit keine unberechtigten Dritte die Daten einsehen können. Dies kann z.B. durch eine Verschlüsselung erreicht werden (z.B. mit HIN-Mail). Bei sensiblen persönlichen Daten sollte immer das explizite Einverständnis der betroffenen Person vorliegen oder noch besser der Transfer via betroffene Person erfolgen.

Wann müssen Verletzungen der Datensicherheit dem EDÖB gemeldet werden?

Eine Verletzung liegt dann vor, wenn die Vertraulichkeit, Integrität oder Verfügbarkeit von Personendaten beeinträchtigt wird, also Personendaten gelöscht, verloren, verändert oder Unbefugten offengelegt oder zugänglich gemacht werden. Gemeldet werden müssen aber nur solche Verletzungen, die ein hohes Risiko für negative Folgen für die betroffene Personen aufweisen. Ein solcher Fall liegt vor, wenn z.B. Patientenakten auf einem unverschlüsselten Memorystick gespeichert sind und der Stick verloren geht.

Was muss ich tun, wenn ich eine Mail an den falschen Adressaten sende oder einen Stick mit Daten verliere?

Es ist eine Einzelfallbeurteilung nötig, ob eine Meldung an den EDÖB nötig ist. Wird z.B. eine E-Mail mit Personendaten falsch an eine Person versendet, die vertrauenswürdig und dem/der Sender*in bekannt ist, besteht kein hohes Risiko. Geht dagegen ein Stick mit Mitarbeiterdaten und deren Gehaltsangaben verloren, ist eine Meldung erforderlich.

5. Datenportabilität

Ich führe meine KG auf Papier, wie kann ich die Anforderung an eine Herausgabe in elektronischem Format erfüllen?

Falls die Dokumente nicht elektronisch abgelegt und nur physisch vorhanden sind, sind die Unterlagen einzuscannen und als PDF herauszugeben. Daher ist es wichtig, alle Dokumente, welche eine*n Klient*in betreffen, beisammen und geordnet zu haben.

6. Datenlöschung

Wie lange dürfen Klient*innen-Daten aufbewahrt werden.
Entsprechend den Verjährungsfristen des Obligationenrechts und den Bestimmungen einzelner Kantone kann in der Regel von einer Aufbewahrungsfrist von 20 Jahren ausgegangen werden.

Müssen nur elektronische Daten gelöscht werden?
Nein, dies gilt auch für Patientendaten wie z.B. Krankengeschichten, die auf Papier geführt werden.

Dieses Merkblatt und seine Beilagen wurden nach dem aktuellen Wissensstand so genau und vollständig wie möglich erstellt. Trotzdem kann dafür rechtlich keine Gewähr geleistet werden.

Solothurn, 28.06.2023