Organisation der Arbeitswelt Komplementär Therapie

Merkblatt für Therapeut*innen zum REVIDIERTEN DATENSCHUTZRECHT

Ausgangslage

Das totalrevidierte Datenschutzgesetz (nDSG) tritt am 1. September 2023 in Kraft. Ziel der Revision war es, das Datenschutzrecht an das europäische Recht anzugleichen und die Rechte der betroffenen Personen hinsichtlich der Selbstbestimmung und Transparenz zu stärken. Dieses Merkblatt zeigt die wichtigsten Neuerungen und den Handlungsbedarf auf.

Übersicht der grundlegendsten Änderungen per 1. September 2023

1. Wer Daten bearbeitet, muss ein **Bearbeitungsverzeichnis** führen.
2. Für jede Datensammlung muss es eine **datenschutzrechtlich verantwortliche Person** geben.
3. Datenschutz muss durch **Technik** sichergestellt sein.
4. Wer Daten bearbeitet, muss **Betroffene informieren** und auf Anfrage Auskunft erteilen.
5. Daten müssen so abgelegt sein, dass sie brauchbar reproduziert und auch versandt werden können **(«Datenportabilität»).**
6. Neu ist die **Datenlöschung** ausdrücklich geregelt: wer Daten bearbeitet, muss sie auch rechtzeitig wieder löschen.
7. Androhung bei absichtlichen Verstössen: **Busse** bis zu CHF 250'000.00 möglich.

Erläuterungen

Das revidierte Datenschutz auferlegt neue Pflichten, welche in diesem Merkblatt beschrieben sind. Häufig gestellte Fragen (FAQ) werden in einem separaten Dokument beantwortet. Die gesetzlichen Grundlagen sind im Bundesgesetz über den Datenschutz (DSG) und in der Verordnung über den Datenschutz (DSV) zu finden und entsprechend verlinkt.

1. Pflicht zur Führung eines Bearbeitungsverzeichnis (Art. 12 nDSG)

Neu verlangt das Gesetz, dass ein **Verzeichnis** über jede Bearbeitungstätigkeit geführt und laufend aktualisiert werden muss. Gemäss Art. 24 nDSV sind Betriebe mit weniger als 250 Mitarbeitenden von dieser Pflicht befreit, ausser wenn *besonders schützenswerte Personendaten im grösseren Umfang* bearbeitet werden. Da Gesundheitsdaten als besonders schützenswert gelten, ist es für Therapeut*innen sehr zu empfehlen, ein solches Verzeichnis zu führen, unabhängig von einer gesetzlichen Pflicht.

2. Datenschutzrechtlich verantwortliche Person

Die Praxis (das Unternehmen) gilt als datenschutzrechtlich Verantwortliche und die Therapeutin / der Therapeut ist dafür verantwortlich den Datenschutz im Unternehmen umzusetzen.
Die Bearbeitung von Personendaten kann einem Auftragsbearbeiter (z.B. Cloud-Services für Datenspeicherung, ausgelagerte Finanzbuchhaltung, Softwareanbieter Tarif 590) übertragen werden. Wird ein Auftragsbearbeiter beigezogen, bleibt der datenschutzrechtlich Verantwortliche (die Praxis) weiterhin verantwortlich für die Daten und muss kontrollieren und sicherstellen, dass der Auftragsbearbeiter die Daten nur nach seinen Vorgaben und Weisungen bearbeitet. . Eine **Auftragsbearbeitung** muss zwingend vertraglich geregelt sein und die entsprechenden Datenschutzerklärungen beinhalten (Art. 9 nDSG).

3. Technische und organisatorische Massnahmen für die Datensicherheit (Art. 8 nDSG)

Bei den technischen Massnahmen handelt es sich um die internen Zugriffsrechte (wer hat Einsicht in welche Daten) und den Schutz gegen aussen (z.B. Firewalls, Passwörter). Zweck dieser Massnahmen ist,

dass in Personendaten nur diejenigen Personen Einsicht haben, welche den Zugriff für die Erfüllung ihrer Arbeit benötigen.

Wenn *Personendaten verloren gehen, gelöscht, verändert oder Drittpersonen (Unbefugten) zugänglich gemacht werden (z. B. durch Diebstahl)* und durch die Verletzung ein hohes Risiko für negative Folgen der betroffenen Person besteht, muss dies dem Eidgenössischen Datenschutzbeauftragten EDÖB gemeldet werden.

Versand von besonders schützenswerten Daten: Beim Versenden sind Massnahmen zu ergreifen, damit keine unberechtigten Dritte sie einsehen können, namentlich der verschlüsselte Versand.

4. Recht auf Auskunft/Informationspflicht (Art. 25 nDSG)

Wo Daten gesammelt werden, muss eine **Datenschutzerklärung** existieren. Die Datenschutzerklärung muss mindestens die Kontaktdaten der verantwortlichen Person, den Bearbeitungszweck und gegebenenfalls die Empfänger*innen der Daten beinhalten. Ein Hinweis auf der Website oder in schriftlichen Unterlagen muss die Information enthalten, wo die Datenschutzerklärung eingesehen/abgeholt werden kann. Ob die betroffene Person diese tatsächlich anschaut, spielt keine Rolle.

Personendaten sind Betroffenen auf Anfrage innert 30 Tagen herauszugeben. Es ist sicherzustellen, dass die Daten innert Frist gefunden und in elektronischer Form der betroffenen Person herausgegeben werden können (siehe 5. Datenportabilität).

5. Datenportabilität (Art. 28 nDSG)

Die Betroffenen haben neu das Recht, ihre Personendaten in einem gängigen elektronischen Format zu verlangen oder an Dritte übertragen zu lassen. Die Herausgabe bzw. Übermittlung muss in der Regel kostenlos erfolgen, falls dies keinen übermässigen Aufwand verursacht. Gängig ist ein «elektronisches Format», welches das automatische Einlesen der Daten in ein Computersystem in strukturierter Form ermöglicht (z. B. als PDF, EXCEL, XML-File usw.). Falls die Dokumente nicht elektronisch abgelegt und nur physisch vorhanden sind, sind die Unterlagen einzuscannen und als PDF herauszugeben.

6. Datenlöschung (Art. 6 Abs. 4 nDSG)

Aufgrund der Verhältnismässigkeit dürfen Datenbearbeitungen nur so weit gehen, wie sie für den verfolgten Zweck **erforderlich sind.** Anschliessend sind die Daten zu löschen oder anonymisieren. Eine zu lange Aufbewahrung von Daten stellt eine Datenschutzverletzung dar.
Es gelten die gesetzlichen Aufbewahrungsfristen. **Patientendossiers** sind in der Regel 20 Jahre aufzubewahren. Ältere Daten von Patient*innen, welche sich nicht mehr in Behandlung befinden, sind zu löschen.
Arbeitsrechtliche Unterlagen sind spätestens 10 Jahre nach Austritt zu löschen, nicht mehr Benötigtes, wie Bewerbungsunterlagen, direkt nach Beendigung des Arbeitsverhältnisses.
Falls gesetzliche Aufbewahrungspflichten vorhanden sind, kann dem Löschungsbegehren nicht entsprochen werden.

7. Verstösse / Sanktionen

Bei vorsätzlichem (absichtlichem) Handeln bzw. Unterlassen droht eine Busse von bis zu CHF 250'000.--, und zwar als Privatperson. Fahrlässigkeit wird dagegen nicht bestraft. Sanktioniert werden also nur jene, die nicht die minimalen Massnahmen zur Datensicherheit treffen.
Nur auf Antrag bestraft werden die Missachtung von Informations-, Auskunfts- und Meldepflichten sowie die Verletzung von Sorgfaltspflichten und der beruflichen Schweigepflicht.

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, 14.02.2024