

Infoblatt zum Datenschutz

Bern, 13.04.2023



Illustration: © strichfiguren – AdobeStock (bearbeitet von Physioswiss)

Die Grundlage für dieses Merkblatt wurde Physioswiss freundlicherweise zur Verfügung gestellt von der Verbindung der Schweizer Ärztinnen und Ärzte (FMH).

Datenschutz in der Physiotherapiepraxis

Das Bundesgesetz über den Datenschutz sowie die dazugehörige Verordnung bezwecken den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, deren Personendaten bearbeitet werden. Physiotherapeut:innen sowie deren Mitarbeitende haben Personendaten nach diesen gesetzlichen Anforderungen zu bearbeiten.

In diesem Informationsblatt wird aufgezeigt, was Datenschutz ist, was das für eine Tierphysiotherapiepraxis bedeutet und was es dabei zu beachten gilt. Zur Unterstützung der Tierphysiotherapiepraxen sind zu den jeweiligen Themen Hilfestellungen wie Vorlagen, Prozesse und Checklisten verlinkt. Zusätzlich zu diesem Dokument sind FAQ zum Datenschutz in Tierphysiotherapiepraxen abrufbar.

Ziel und Zweck des Datenschutzes

Der Datenschutz befasst sich mit der informationellen Selbstbestimmung sowie dem Schutz vor missbräuchlicher Datenbearbeitung, welche natürliche Personen in ihrer Persönlichkeit oder ihren Grundrechten einschränkt.

Das Datenschutzgesetz hat zum Zweck, diese Rechte zu schützen, indem es Vorgaben zum Umgang und zur Bearbeitung mit Personendaten definiert.

Änderungen mit dem neuen Datenschutzgesetz

Das revidierte Datenschutzgesetz (DSG), welches am 1. September 2023 in Kraft tritt, stärkt insbesondere die Selbstbestimmung über die eigenen Daten der betroffenen Personen, indem Verantwortliche zu erhöhter Transparenz verpflichtet werden und die Rechte der betroffenen Personen erweitert werden. Für Tierphysiotherapiepraxen sind in erster Linie nachfolgende Änderungen relevant:

- Die Definition der besonders schützenswerten Personendaten wird erweitert um genetische und biometrische Daten, sofern diese eine natürliche Person eindeutig identifizieren. Die strengeren Bedingungen an die Bearbeitung besonders schützenswerter Personendaten gelten zukünftig auch für diese Arten von Daten.
- Das heute geltende Register der Datensammlungen wird abgelöst durch ein Verzeichnis der Bearbeitungstätigkeiten. Damit stehen nicht mehr die Datensammlungen im Fokus, sondern die Art und Weise sowie der Zweck einer Bearbeitung von Personendaten.
- Neu sieht das Gesetz die Durchführung einer Datenschutz-Folgenabschätzung (DSFA) vor, wenn eine Bearbeitung geplant ist, welche voraussichtlich ein hohes Risiko für die Persönlichkeits- oder Grundrechte der betroffenen Person mit sich bringt. Ein solches Risiko kann beispielsweise vorliegen, wenn besonders schützenswerte Personendaten wie Gesundheitsdaten bearbeitet werden oder wenn neue Technologien (z.B. Cloud-Produkte, Künstliche Intelligenz) bei der Bearbeitung der Personendaten zum Einsatz kommen. Von einer Datenschutz-Folgenabschätzung kann abgesehen werden, wenn die Bearbeitung aufgrund einer gesetzlichen Vorgabe erfolgt, wenn die eingesetzten Systeme, Produkte oder Dienstleistungen für die vorgesehene Bearbeitung zertifiziert sind oder wenn ein dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) vorgelegter Verhaltenskodex eingehalten wird.

- Das revidierte Gesetz sieht eine Meldepflicht für Verletzungen der Datensicherheit vor (vgl. Abschnitt «[Meldepflicht Datensicherheitsverletzung](#)»).
- Die Strafbestimmungen im DSG werden verschärft (vgl. Abschnitt «[Datenschutzrechtliche Strafbestimmungen](#)»).

Personendaten

Als Personendaten oder auch personenbezogene Daten gelten alle Daten, die sich auf eine Person beziehen und diese identifizieren oder zur Identifizierung der Person beitragen. Der Begriff der Personendaten ist daher weit zu fassen.

Das Datenschutzgesetz unterscheidet dabei zwischen Personendaten und besonders schützenswerten Personendaten. Schützenswert sind dabei grundsätzlich alle Personendaten. Im Zusammenhang mit der Bearbeitung von besonders schützenswerten Personendaten sieht das Gesetz jedoch zusätzliche Anforderungen vor. Als besonders schützenswerte Personendaten nennt das Gesetz unter anderem Daten über die Gesundheit, die Intimsphäre sowie Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten.

Zu den Personendaten, die in Tierphysiotherapiepraxen bearbeitet werden, gehören beispielsweise:

- Stamm- und Kontaktdaten von Besitzer:innen, Mitarbeitenden, Ansprechpersonen von Dienstleistern oder anderen Gesundheitseinrichtungen (z.B. Namen, Telefonnummer, Anschrift, E-Mail-Adresse oder auch das Geburtsdatum)
- Aufzeichnungen über den Verlauf einer Tier - Behandlung, Symptombeschreibungen, Diagnosen, Verordnungen, Reaktionen, Röntgenbilder
- Daten zu Mitarbeitenden und dem Anstellungsverhältnis inklusive Leistungsbeurteilungen und Lohnabrechnungen

Grundsätze der Bearbeitung

Bearbeiten nach dem DSG umfasst jeden Umgang mit Personendaten wie etwa Beschaffung, Aufbewahrung, Verwendung, Umarbeitung, Bekanntgabe, Archivierung und Vernichtung von Daten, unabhängig von angewandten Mitteln und Verfahren. Bei der Bearbeitung von Personendaten gelten folgende Grundsätze:

- Die Bearbeitung von Personendaten ist grundsätzlich rechtmässig, wenn die geltende Rechtsordnung und die Datenschutzvorgaben eingehalten werden.
- Im Zusammenhang mit der Bearbeitung von Personendaten haben Tierphysiotherapeut:innen gegenüber betroffenen Personen (unter anderem Besitzer:innen) eine Informations- und Aufklärungspflicht. Die Tierphysiotherapeut:innen haben die Besitzer:innen über die Datenbearbeitung in verständlicher Art und Weise darüber zu informieren, zu welchem Zweck die Personendaten erhoben und bearbeitet werden und an welche Kategorien von Empfängern eine Weitergabe der Daten erfolgt.
- Die Tierphysiotherapeut:innen setzen für eine ausreichende Besitzerinformation entsprechende Aufklärungsformulare ein, welche nach erfolgtem Aufklärungsgespräch

durch die Besitzer unterzeichnet werden und damit bestätigen, dass sie die Besitzerinformation verstanden haben und sie dem jeweiligen Behandlungsschritt zustimmen.

- Die Erhebung sowie der Zweck der Bearbeitung haben transparent und nach Treu und Glauben zu erfolgen. Sofern die Datenbeschaffung und der Zweck der Bearbeitung für die betroffene Person nicht ersichtlich sind, muss sie darüber informiert werden. Treu und Glauben bedeutet auch, dass die Daten nur so bearbeitet werden, wie es die betroffene Person erwarten kann.

Tierphysiotherapiepraxen können zur Schaffung von Transparenz beispielsweise eine Besitzerinformation/Einwilligungserklärung oder eine Datenschutzerklärung bereitstellen, in welcher über die Bearbeitung aufgeklärt wird.

Hilfsmittel

Eine Vorlage zur Einwilligungserklärung kann auf der HP abgerufen werden.
Eine Vorlage zu deiner Datenschutzerklärung kann auf der HP abgerufen werden.

- Die Bearbeitung der Personendaten hat verhältnismässig zu erfolgen. Die Verhältnismässigkeit ist gegeben, wenn die Bearbeitung auf die Daten beschränkt wird, die für die Erfüllung der Aufgabe oder die Erreichung des angegebenen Zwecks geeignet und notwendig sind. Weiter bedeutet die Verhältnismässigkeit, dass Personendaten nur so lange aufbewahrt werden sollen, wie sie auch tatsächlich für die Aufgabenerfüllung benötigt werden oder eine gesetzliche Aufbewahrungspflicht dies erfordert. Werden Personendaten nicht mehr benötigt und steht einer Löschung keine gesetzliche Aufbewahrungspflicht entgegen, sind sie unwiderruflich zu löschen.

Hilfsmittel

Ein Leitfaden für die Aufbewahrung und Archivierung von Personendaten kann auf der HP abgerufen werden.

- Die Bearbeitung muss zweckmässig sein. Die Zweckmässigkeit ist gegeben, wenn die Bearbeitung von Personendaten nur zu dem Zweck erfolgt, welcher definiert und bei der Beschaffung der Daten angegeben wurde.
- Sind die Personendaten nicht korrekt, sind diese zu berichtigen oder zu löschen.

Beispielsweise wenn Besitzer:innen umziehen.

Verantwortlichkeit innerhalb der Tierphysiotherapiepraxis

Der Verantwortliche im Sinne des Datenschutzgesetzes ist grundsätzlich die Tierphysiotherapiepraxis. Sie ist dafür verantwortlich, den Datenschutz einzuhalten und hat insbesondere dafür zu sorgen, dass die Persönlichkeits- und Grundrechte ihrer Besitzer:innen sowie der Mitarbeitenden geschützt sind.

Wünscht oder benötigt eine Tierphysiotherapiepraxis Unterstützung bei der Umsetzung der Datenschutzerfordernungen, hat sie die Möglichkeit, eine:n interne:n oder externe:n

Datenschutzberater:in beizuziehen. Ein:e Datenschutzberater:in ist für privatrechtlich geführte Tierphysiotherapiepraxen freiwillig und keine gesetzliche Pflicht.

Datenschutzberater stehen betroffenen Personen als Anlaufstelle bei Fragen zum Datenschutz zur Verfügung und sind Ansprechperson des EDÖB bzw. der kantonalen Datenschutzbehörden. Sie unterstützen, beraten und schulen die Mitarbeitenden des jeweiligen Unternehmens in Fragen rund um den Datenschutz und wirkt bei der Umsetzung von Datenschutzerfordernissen mit (z.B. bei der Bearbeitung von Betroffenenersuchen [Informationspflicht, Auskunftsrecht, Datenherausgabe etc.], der Ausarbeitung von internen Regelungen zum Datenschutz etc.).

Datensicherheit

Damit die Persönlichkeits- und Grundrechte von Besitzer:innen sowie von Mitarbeitenden gewahrt werden, müssen die Personendaten vor unberechtigten Zugriffen, Veränderungen sowie vor Verlust geschützt werden. Die Tierphysiotherapiepraxis hat entsprechend technische und organisatorische Massnahmen für die Datensicherheit zu treffen. Die zu wählenden technischen und organisatorischen Massnahmen richten sich grundsätzlich nach dem Risiko. Es sind entsprechend die Vorgaben zur Datensicherheit in der Verordnung über den Datenschutz (DSV) zu beachten.

Beispiele für technische und organisatorische Massnahmen sind Zugriffsbeschränkungen auf Systeme und physische Daten (z.B. Papierakten), Datensicherungen (Back-ups), Schulungen von Mitarbeitenden etc.

Meldepflicht Datensicherheitsverletzung

Eine Verletzung der Datensicherheit liegt vor, wenn die Vertraulichkeit, die Integrität oder die Verfügbarkeit der Personendaten verletzt wird. Dies ist beispielsweise der Fall, wenn Daten

- verloren gehen,
- versehentlich oder unerlaubt gelöscht, vernichtet oder verändert werden oder
- für nicht berechnigte Personen zugänglich werden oder diese Einsicht in die Daten erhalten.

Eine Verletzung der Datensicherheit könnte beispielsweise verursacht werden durch:

- menschliches Versagen,
- kriminelle Handlungen (Hacking),
- Malware (Einschleusen von Schadsoftware),
- Verlust oder Diebstahl von Geräten (z.B. Laptops), Datenträgern (z.B. USB-Sticks, Festplatten, CD/DVD) oder Papierunterlagen.

Eine Verletzung der Datensicherheit, welche zu einem hohen Risiko für die Persönlichkeitsrechte oder die Grundrechte der betroffenen Personen führt, ist gemäss dem revidierten Bundesgesetz über den Datenschutz sowie der zugehörigen Verordnung so rasch als möglich dem EDÖB zu melden. Sofern die Datensicherheitsverletzung keine oder nur geringe Auswirkungen auf die betroffenen Personen hat, kann von einer Meldung abgesehen werden.

Die Meldung enthält mindestens folgende Angaben:

- Art der Verletzung der Datensicherheit (z. B. Zerstörung der Daten, Diebstahl der Daten etc.);
- sofern bekannt Zeitpunkt und Dauer der Verletzung;
- soweit möglich die Kategorien der Personendaten und die ungefähre Anzahl der betroffenen Personendaten;
- soweit möglich die Kategorien der betroffenen Personen und die ungefähre Anzahl der betroffenen Personen;
- Folgen der Verletzung der Datensicherheit, einschliesslich der allfälligen Risiken für die betroffenen Personen (z. B. kein Zugriff auf Patientendokumentationen, folglich Nachvollziehbarkeit der Behandlung nur noch teilweise möglich und folglich mögliche Gefährdung der Gesundheit der betroffenen Person; Publikation der Patientendokumentation im Darknet, folglich Gefährdung der Persönlichkeit der betroffenen Person);
- ergriffene oder vorgesehene Massnahmen, um den Mangel zu beheben oder die Folgen zu mindern (z. B. Wiederherstellung des Back-ups bei digitalen Daten);
- Namen und Kontaktdaten einer Ansprechperson.

Ist es nicht möglich, alle Informationen zur gleichen Zeit mitzuteilen, können die weiteren Informationen dem EDÖB in einem angemessenen Zeitrahmen schrittweise zur Verfügung gestellt werden.

Hilfsmittel

Eine Checkliste und ein Prozessablauf bei Datenschutzverletzungen kann auf der HP abgerufen werden.

Auskunftsrecht der Betroffenen

Die Patient:innen haben das Recht, ohne Angabe von Gründen kostenlos Auskunft über die sie betreffenden Daten und deren Bearbeitung zu erhalten. Vorausgesetzt, es liegen keine Gründe vor, unter welchen eine Auskunft verweigert, eingeschränkt oder aufgeschoben werden kann. Die Auskunft, ob und wie Daten über die betroffene Person bearbeitet werden, ist der gesuchstellenden Person innerhalb einer 30-tägigen Frist mitzuteilen.

Hilfsmittel

Eine Anleitung zur Auskunft- und Herausgabe über Personendaten kann auf der HP abgerufen werden.

Datenbearbeitung durch Auftragsbearbeiter

Artikel 9 des revidierten Datenschutzgesetzes regelt die Datenbearbeitung durch Auftragsbearbeiter. Eine Auftragsbearbeitung liegt beispielsweise bei einer Auslagerung von IT-Systemen in ein externes Rechenzentrum oder der Auslagerung der Lohn- und Gehaltsabrechnung vor.

Datenschutzrechtliche Strafbestimmungen

Nach dem revidierten Datenschutzgesetz kann in bestimmten Fällen die Verletzung von verpflichtenden Datenschutzanforderungen zu einer persönlichen Strafbarkeit führen. Die Busse von bis zu CHF 250'000.– wird dabei der fehlbaren natürlichen Person auferlegt. Voraussetzung ist, dass die Datenschutzverletzung vorsätzlich begangen wird, das heisst, dass mit Wissen und Willen Mitwirkungs- und Sorgfaltspflichten verletzt werden.