Leitfaden Verzeichnis der Bearbeitungs-tätigkeiten

Version 03/2023

FMH · Verbindung der Schweizer Ärztinnen und Ärzte- Fédération des médecins suisses
Elfenstrasse 18 · Postfach 3000 · CH-3000 Bern 15 · Telefon +41 31 359 11 11 · Fax +41 31 359 11 12 · info@fmh.ch · www.fmh.ch

Vorwort

Das neue Bundesgesetz über den Datenschutz (DSG) sowie die dazugehörige Verordnung (DSV) verfolgen den Zweck, die Persönlichkeit und die Grundrechte von natürlichen Personen zu schützen. Um dieses Ziel zu erreichen, sind im Gesetz sowie in der Verordnung Anforderungen zur Bearbeitung von Personendaten definiert.

Arztpraxen bzw. Ärztinnen, Ärzte sowie ihre Hilfspersonen bearbeiten im Rahmen ihrer Tätigkeit zahlreiche Personendaten. Infolgedessen haben sie unter anderem die Vorgaben des DSG zu beachten und umzusetzen.

Zur Umsetzung und Einhaltung von datenschutzrechtlichen Vorgaben soll dieses Dokument neben weiteren Dokumenten eine Hilfestellung bieten.

Inhaltsverzeichnis

1 Begriffsdefinitionen 4

2 Leitfaden zur Vorlage des Verzeichnisses der Bearbeitungstätigkeiten 5

2.1 Allgemeines 5

2.2 Anleitung zum Ausfüllen des Verzeichnisses 5

3 Rechtliche Anforderungen zur Aufbewahrung und Archivierung 7

3.1 Gesetzliche Aufbewahrungsfristen (Stand 31.10.2022) 7

3.2 Übersicht gesetzliche Aufbewahrungsfristen 8

3.3 Checkliste zur Aufbewahrung und Archivierung von Personendaten 12

1 Begriffsdefinitionen

Begriff	Beschreibung
Automatisierte Bearbeitung	Als automatisierte Bearbeitung gilt die Bearbeitung (vgl. Begriff «Bearbeitung») von Personendaten mittels automatisierter Verfahren. **Automatisiert** ist eine Bearbeitung, wenn diese in einer strukturierten Form in der Regel mittels Datenbearbeitungsanlagen erfolgt (z. B. Server, Kommunikationsdienste, Computer, Computersysteme bzw. -programme). Nicht unter den Begriff der automatisierten Bearbeitung fallen analoge Datenablagen wie beispielsweise unstrukturierte Papierablagen oder schriftliche Aufzeichnungen.
Bearbeitung	Die **Bearbeitung** von Daten umfasst jeden Umgang mit Personendaten, unabhängig von angewandten Mitteln und Verfahren. Als Bearbeitung wird daher unter anderem Beschaffung, Speicherung, Aufbewahrung, Verwendung, Veränderung, Bekanntgabe, Archivierung, Löschung oder Vernichtung von Personendaten verstanden.
Datenträger	Die Definition Datenträger wird verwendet, wenn sowohl physische als auch digitale Datenträger eingesetzt werden.
Digitale (Wechsel-) Datenträger	Als digitale (Wechsel-)Datenträger gelten unter anderem CD/DVD, USB-Stick, externe Festplatte, Tape, Laptop, Server etc.
Personendaten/ besonders schützenswerte Personendaten	Als **Personendaten** gelten alle Daten, die sich auf eine bestimmte oder bestimmbare Person beziehen. Ob eine Person direkt oder indirekt bestimmbar bzw. identifizierbar ist, hängt dabei insbesondere auch vom Kontext ab, in dem sich die Daten befinden bzw. in dem sie bearbeitet werden. Personendaten sind unter anderem Personalien, Kontaktdaten, Geschlecht, Geburtsdatum, berufliche Tätigkeit etc. **Besonders schützenswerte Personendaten** umfassen gemäss dem DSG Daten, die Auskunft geben über — die Gesundheit (z. B. Zustand, Diagnosen, Behandlungen etc.) und die Intimsphäre (z. B. Sexualität), — die Rassenzugehörigkeit und die Ethnie, — religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, — Massnahmen der sozialen Hilfe sowie — administrative oder strafrechtliche Verfolgungen und Sanktionen. Ebenfalls zu den besonders schützenswerten Personendaten gehören genetische Daten sowie biometrische Daten, die eine Person eindeutig identifizieren.
Physische Datenträger	Als physische Datenträger gelten z. B. Papierdokumente.
Profiling	Als Profiling gilt jede automatisierte Bearbeitung von Personendaten, die dazu dient, persönliche Aspekte einer natürlichen Person zu bewerten, zu analysieren oder vorherzusagen. Für das Profiling werden gemäss DSG insbesondere folgende persönliche Aspekte zur Analyse oder zur Vorhersage genutzt: Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel.

2 Leitfaden zur Vorlage des Verzeichnisses der Bearbeitungstätigkeiten

2.1 Allgemeines

Mit Inkrafttreten des neuen Bundesgesetzes über den Datenschutz (DSG) werden Verantwortliche unter bestimmten Voraussetzungen verpflichtet, ein Verzeichnis der Bearbeitungstätigkeiten zu führen. Diese Pflicht trifft Verantwortliche mit mehr als 250 Mitarbeitenden sowie Verantwortliche, welche eine umfangreiche Bearbeitung von besonders schützenswerten Personendaten vornehmen (siehe Kapitel 1 Definitionen). Aufgrund der Sensitivität der Gesundheitsdaten wird Ärztinnen und Ärzten beziehungsweise den Praxen empfohlen, zumindest diejenigen Bearbeitungstätigkeiten in das Verzeichnis aufzunehmen, bei welchen die Bearbeitung von besonders schützenswerten Personendaten im Fokus steht (z. B. Führung und Verwaltung der Krankengeschichten, Verwaltung der Patientendaten zur Abrechnung der Sozialversicherungen, Personalverwaltung etc.). Grundsätzlich haben sowohl die Verantwortlichen (bspw. Arztpraxis) als auch bestimmte Auftragsbearbeiterinnen und Auftragsbearbeiter (bspw. Abrechnungscenter) je ein Verzeichnis zu führen.

2.2 Anleitung zum Ausfüllen des Verzeichnisses

Die nachfolgenden Erläuterungen zu den jeweiligen Spalten des Verzeichnisses sollen die Verantwortlichen beim Ausfüllen der Vorlage unterstützen. Bei den aufgeführten Spalten handelt es sich um die gesetzlichen Mindestangaben, welche im Verzeichnis aufgeführt sein müssen. Die Vorlage enthält einige Beispiele (rot markiert), welche weiter angepasst, ergänzt oder gelöscht werden können, falls die vorgeschlagenen Bearbeitungstätigkeiten nicht zutreffen.

Physische Vernichtung	Hier soll die spezifische Bearbeitungstätigkeit angegeben werden, in welcher Personendaten bearbeitet werden. Zusammenhängende oder ähnliche Bearbeitungstätigkeiten können, wo sinnvoll, auch zu einer einzelnen Bearbeitungstätigkeit zusammengefasst werden. Die Bezeichnung der Tätigkeit sollte so eindeutig wie möglich sein und Auskunft darüber geben, wie und in welchem Zusammenhang die Personendaten bearbeitet werden.
Zweck	In dieser Spalte ist der Zweck anzugeben, für den die Personendaten bearbeitet werden. Es können auch mehrere Zwecke aufgeführt werden.
Verantwortliche	Hier ist jeweils die Person anzugeben, welche für die Bearbeitungstätigkeit und die bearbeiteten Daten verantwortlich ist. Verantwortlich ist dabei die Person, welche darüber entscheidet, wie und womit die Daten bearbeitet werden (z. B. die Ärztin/der Arzt). Sind für eine Bearbeitungstätigkeit (z. B. die Führung der Krankengeschichte in einer Gemeinschaftspraxis) mehrere Personen verantwortlich, wird empfohlen, den Namen der Arztpraxis sowie die Funktionen der Verantwortlichen aufzuführen (z. B. behandelnde/r Ärztin/Arzt). Mehrere Verantwortliche sind insbesondere auch dann möglich, wenn mehrere Personen über die eingesetzten Mittel und Verfahren für die Bearbeitung entscheiden (z. B. die Geschäftsleitung).
Kategorien betroffener Personen	Hier sind die Kategorien der betroffenen Personen zu nennen, über welche Daten bearbeitet werden. Mit Kategorien betroffener Personen sind typisierte Gruppen gemeint, die bestimmte gemeinsame Merkmale haben (z. B. Interessenten, Patientinnen und Patienten, Mitarbeitende, Dienstleistende etc.).
Kategorien der Personendaten	Hier können die bearbeiteten Personendaten in Kategorien zusammengefasst werden (z. B. Personalien, Stammdaten, Kontaktdaten, Lohndaten, [Sozial-]Versicherungsdaten, Bankverbindungsdaten, Behandlungsdaten, Gesundheitsdaten etc.). Die Kategorisierung kann dabei unterschiedlich detailliert ausfallen.

Kategorie der Empfänger	Auch die Empfänger, welche im Rahmen einer Tätigkeit Einsicht in oder Zugang auf die Personendaten erhalten, können in Kategorien zusammengefasst werden. Bei den Empfängern spielt es keine Rolle, ob eine aktive Übertragung an diese stattfindet oder ob sie direkten Zugriff auf die Daten haben. Empfänger können Personen, Unternehmen, Behörden etc. sein. Es wird empfohlen, eine aussagekräftige Bezeichnung für die jeweilige Kategorie der Empfänger zu wählen (z. B. Krankenkassen, Invalidenversicherungen, Buchhaltung, Steuerverwaltung, Aufsichtsbehörden, [IT-]Dienstleister etc.).
Aufbewahrungsdauer/ Aufbewahrungskriterium	Sofern bekannt, sollten die konkreten Fristen für die Aufbewahrung der Daten aufgeführt werden (z. B. Anzahl Tage oder Jahre). Dabei sind insbesondere gesetzliche bzw. standesrechtliche Aufbewahrungspflichten zu berücksichtigen. Bestehen keine gesetzlich bzw. standesrechtlich festgelegten Aufbewahrungsfristen, sollte festgehalten werden, nach welchen Kriterien die Personendaten aufbewahrt werden (z. B. bis zur Erfüllung des Zwecks, bis Austritt der/des Mitarbeitenden).
Massnahmen zur Datensicherheit	Hier ist festzuhalten, ob und welche technischen und organisatorischen Massnahmen bereits umgesetzt werden, um die Daten vor Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit zu schützen (z. B. abgeschlossene Schränke bei physischen Krankengeschichten, verschlüsselter E-Mail-Verkehr, Zugriffsbeschränkung auf digitale Ablagen, Schulung der Mitarbeitenden etc.). Hier besteht grundsätzlich auch die Möglichkeit, auf bestehende Sicherheitskonzepte zu verweisen.
Bekanntgabe ins Ausland	In dieser Spalte kann mit «Ja» oder «Nein» angegeben werden, ob Personendaten im Rahmen einer Bearbeitungstätigkeit ins Ausland bekannt gegeben werden. Eine Bekanntgabe liegt unter anderem vor, wenn die Personendaten an eine/n andere/n Ärztin/Arzt oder ein Labor im Ausland übermittelt werden oder wenn ein System für die Bearbeitungstätigkeit eingesetzt wird, dessen Anbieter seinen Sitz im Ausland hat und damit potenziell auf die Daten zugreifen kann (z. B. Einsatz von Cloud-basierten Systemen, sofern der Provider Zugriff auf die Daten im Klartext hat oder haben könnte).
Angabe Staat und Garantien/ Instrumente	Sofern bei der Frage nach der Bekanntmachung von Personendaten ins Ausland «Ja» angegeben wurde, ist der jeweilige Staat zu nennen. Zusätzlich ist festzuhalten, auf welche Art und Weise ein angemessener Schutz der Personendaten und dadurch der Persönlichkeitsrechte der Betroffenen gewährleistet wird. Es wird aufgrund der Komplexität von IT-Vorgängen empfohlen, beim jeweiligen IT-Dienstleister abzuklären, ob Personendaten ins Ausland bekannt gegeben werden. Im Falle einer Bekanntgabe ins Ausland sollte zusätzlich abgeklärt werden, durch welche Massnahmen die rechtlichen Vorgaben eingehalten werden. Der Datenschutz gilt als gewährleistet, wenn der Bundesrat einen entsprechenden Angemessenheitsbeschluss für das jeweilige Land bzw. die Regierung erlassen hat. Ob ein solcher Angemessenheitsbeschluss vorliegt, ist der Staatenliste [1] zu entnehmen. Fehlt eine solche Gesetzgebung, so regelt das Gesetz weitere Voraussetzungen, welche für die Bekanntgabe ins Ausland gegeben sein müssen (siehe Art. 16 ff. Bundesgesetz über den Datenschutz). Bei Fehlen eines Angemessenheitsbeschlusses und unzureichender Gesetzesgrundlage im Empfängerland empfiehlt sich insbesondere bei hohem Risiko für die Persönlichkeit oder die Grundrechte einer betroffenen Person, auf die Bekanntgabe von Personendaten ins Ausland zu verzichten. In jedem Fall ist sicherzustellen, dass der Datenschutz und insbesondere die Sicherheit der Daten gewährleistet sind. Bei Gesundheitsdaten handelt es sich zudem um besonders schützenswerte Personendaten. Dem erhöhten Schutzbedarf ist mit entsprechenden technischen und organisatorischen Massnahmen Rechnung zu tragen. Die Mindestanforderungen an die Datensicherheit sind in der Verordnung zum Bundesgesetz über den Datenschutz (DSV) geregelt. Eine weitere Hilfestellung für die Datensicherheit bieten zudem die Minimalanforderungen aus dem IT-Grundschutz [2].

[1] Anhang 1 Datenschutzverordnung (DSV)
[2] https://www.fmh.ch/ Dienstleistungen / E -Health / Minimalanforderungen IT-Grundschutz

3 Rechtliche Anforderungen zur Aufbewahrung und Archivierung

3.1 Gesetzliche Aufbewahrungsfristen (Stand 31.10.2022)

In Gesundheitseinrichtungen fallen täglich Dokumentationen an, welche unter anderem auch Angaben (Personendaten) über Patientinnen und Patienten sowie Mitarbeitende der Gesundheitseinrichtung selbst oder von Dienstleistenden beinhalten. Die Aufbewahrung dieser Dokumentationen ergeben sich aufgrund des Prinzips der Verhältnismässigkeit. Personendaten dürfen deshalb so lange aufbewahrt werden, wie sie geeignet und erforderlich sind für die Aufgabenerfüllung. Bundesgesetze und kantonale Erlasse legen zudem konkrete Aufbewahrungsfristen fest. Neben diesen kann ein Zweck zur Aufbewahrung auch darin bestehen, die Nachvollziehbarkeit einer Behandlung, einer Leistungsbeurteilung oder eines Sachverhaltes zu Beweiszwecken zu gewährleisten.

Geschäftsdaten, welche keine Personendaten enthalten, können grundsätzlich unbegrenzt aufbewahrt werden. Mindestens sind sie aber solange aufzubewahren, wie es gesetzliche Aufbewahrungsfristen vorsehen.

Zur Orientierung enthalten die nachfolgenden Tabellen eine Zusammenstellung der gesetzlich vorgesehenen Anforderungen an die Art und Dauer der Aufbewahrung. Bestehen keine gesetzlichen Regelungen zur Aufbewahrung, verlangt das Datenschutzgesetz, dass mindestens die Kriterien für die Aufbewahrung festgelegt werden (Art. 12 DSG).

Da während der gesamten Aufbewahrungsdauer sicherzustellen ist, dass der Datenschutz und insbesondere die Datensicherheit gewährleistet bleiben, ist in einem letzten Abschnitt dieses Dokumentes zudem eine Checkliste enthalten, welche mögliche technische und organisatorische Massnahmen zur Aufrechterhaltung der Datensicherheit aufzeigt.

Exkurs: Übergabe/Aufgabe der Geschäftstätigkeit – Aufbewahrungspflicht Krankengeschichten

Grundsätzlich bleibt bei Aufgabe oder Übergabe der Geschäftstätigkeit die Aufbewahrungspflicht der Krankengeschichte bestehen. Hierbei wird unterschieden, mit wem die Patientinnen und Patienten jeweils den Behandlungsvertrag abgeschlossen haben. Das heisst, wenn der Behandlungsvertrag mit einer Gemeinschaftspraxis (AG oder GmbH) geschlossen wurde, verbleibt die Aufbewahrungspflicht bei der Gemeinschaftspraxis selbst. Wurde hingegen der Behandlungsvertrag mit dem Arzt/der Ärztin geschlossen, hat er/sie für eine angemessene Aufbewahrung der Krankengeschichten zu sorgen.

Übernimmt ein/e Nachfolger/in (eine natürliche oder juristische Person) die Arztpraxis bzw. die weitere Behandlung der Patientinnen und Patienten, bedeutet dies nicht automatisch, dass die Krankengeschichten ihm/ihr übergeben werden dürfen resp. er/sie Einsicht erhält. Die Einsicht darf dem/der Nachfolger/in nur gewährt werden, wenn eine vorgängige Einwilligung seitens des/der Patienten/in vorliegt. Liegt (noch) keine Einwilligung seitens des/der Patienten/in vor, kann das sogenannte Zwei-Schränke-Prinzip angewendet werden. Dies bedeutet, in einen Schrank kommen die Krankengeschichten, bei welchen die Patientinnen und Patienten in die Behandlung durch den/die Nachfolger/in zugestimmt haben. In den zweiten Schrank kommen die Krankengeschichten, für welche (noch) keine Einwilligung für die Einsicht vorliegt. Bei der elektronischen Führung von Krankengeschichten kommt grundsätzlich die gleiche Regelung zur Anwendung.

Bei Aufgabe der Tätigkeit stehen Ärztinnen und Ärzte weiterhin in der Pflicht, innert der gesetzlichen Frist Patientinnen und Patienten Auskunft über die Krankengeschichte zu geben. Folglich hat die Ärztin/der Arzt dafür zu sorgen, dass die Krankengeschichten auf eine angemessene Art und Weise aufbewahrt werden und vor unberechtigten Zugriffen geschützt sind. Beispielsweise lagert sie/er diese privat oder delegiert die Aufbewahrung an einen Dritten.

Hinweis: *Zusätzlich sind die allfällig geltenden kantonalen Bestimmungen (kantonale Gesundheits- oder Patientengesetze) zu konsultieren, da diese längere Aufbewahrungsfristen oder besondere Formen der Aufbewahrung vorsehen könnten.*

3.2 Übersicht gesetzliche Aufbewahrungsfristen

Gesundheitsdaten/Patientendokumentation		
Art der Unterlagen	**Aufbewahrungsdauer/-art**	**Rechtliche Grundlage**
Krankengeschichte	Aufgrund der Verjährungsfrist im Haftungsrecht ist die Krankengeschichte **20 Jahre** nach Abschluss der jeweiligen Behandlung aufzubewahren. Darüber hinaus darf sie nur mit der Zustimmung der betroffenen Person aufbewahrt bleiben.	Art. 60 Abs. 1bis und 2 Obligationenrecht (OR)/ Art. 128a OR Art. 12 Standesordnung der FMH
	Hinweis: *Für die geltenden Aufbewahrungspflichten betreffend Dauer und Art sind jeweils die für den Standort der Arztpraxis geltenden kantonalen Gesundheitsgesetze zu konsultieren. Für Krankengeschichten sehen die kantonalen Bestimmungen mindestens eine Aufbewahrungspflicht von **10 Jahren** vor. Einige Kantone erlassen allerdings für spezifische Fälle eine Aufbewahrungspflicht von **20 Jahren**. Weiter wird von wenigen kantonalen Erlassen eine Vernichtung der Unterlagen nach 20 Jahren vorgesehen, wenn dem kein überwiegendes Interesse entgegensteht.*	Kantonale Gesundheitsgesetze (abhängig vom Standort der Arztpraxis)
Dokumentation von Strahlenanwendung und Betriebsauslastung	Die Daten sind gemäss den für die Krankengeschichte geltenden Bestimmungen aufzubewahren.	Art. 20 Abs. 5 lit. a Röntgenverordnung (RöV)
	Allerdings gilt **20 Jahre** für Daten betreffend die Expositionsparameter für Röntgentherapieanlagen sowie Daten, welche im Zusammenhang mit Röntgensystemen zur Positionskontrolle, Planung und Simulation in der Strahlentherapie erhoben werden.	
	Daten, die im Rahmen von Anwendungen im mittleren und im Hochdosisbereich sowie bei der Mammografie festgehalten werden, sind für **10 Jahre** aufzubewahren.	Art. 20 Abs. 5 lit. b RöV
Dokumentation des Umgangs mit Blut oder Blutprodukten	Erwächst aufgrund des Heilmittelgesetzes eine Aufzeichnungspflicht im Zusammenhang mit dem Umgang mit Blut oder Blutprodukten (z. B. bei Blutentnahme), so ist die Dokumentation während 30 Jahren aufzubewahren.	Art. 39 und 40 Bundesgesetz über Arzneimittel und Medizinprodukte (Heilmittelgesetz, HMG)
	Hinweis: *Besondere Bestimmungen sind vorgesehen, wenn die Beendigung der Geschäftstätigkeit vor dem Ablauf der Aufbewahrungsfrist erfolgt.*	
Dokumentation des Umgangs mit Organen, Geweben oder Zellen	Erwächst aufgrund des Transplantationsgesetzes eine Aufzeichnungspflicht im Zusammenhang mit dem Umgang mit Organen, Gewebe oder Zellen, so muss die Dokumentation während **20 Jahren** aufbewahrt werden.	Art. 34 und 35 Bundesgesetz über die Transplantation von Organen, Geweben und Zellen (Transplantationsgesetz)
Arbeitsmedizinische Dokumente	**40 Jahre** für arbeitsmedizinische Dokumente.	Art. 8 Anhang 4 zur Standesordnung der FMH

Ergebnisse von präsymptomatischen genetischen Untersuchungen	Die/der beauftragte Ärztin/Arzt darf die Untersuchungsergebnisse aus präsymptomatischen genetischen Untersuchungen nur aufbewahren, wenn diese für den Vertragsabschluss relevant sind. Die Untersuchungsergebnisse dürfen ausschliesslich für den Zweck verwendet werden, für den sie bei der antragstellenden Person erhoben worden sind.	Art. 28 Bundesgesetz über genetische Untersuchungen beim Menschen (GUMG)
Dokumentation der Information der Lebendspenderinnen und -spender von Organen, Geweben oder Zellen	Ärztinnen oder Ärzte, die Organe, Gewebe oder Zellen entnehmen, müssen die für eine Spende infrage kommende Person vor der Entnahme in mündlicher und schriftlicher Form umfassend und verständlich informieren. Die Dokumentation der Information an den/die Lebendspender/in muss während **10 Jahren getrennt** von der Krankengeschichte aufbewahrt werden.	Art. 9 Abs. 4 und 10 Abs. 2 Verordnung über die Transplantation von menschlichen Organen, Geweben und Zellen (Transplantations-verordnung)
Belegpflicht für kontrollierte Substanzen nach der Betäubungsmittelkontrollverordnung	Die Belege, Daten und Dateiträger über die Verschreibung und den Verkehr mit kontrollierten Substanzen nach der Betäubungsmittelkontrollverordnung sind **10 Jahre** lang aufzubewahren.	Art. 62 Verordnung über die Betäubungsmittelkontrolle (Betäubungsmittelkontrollverordnung, BetmKV)

Mitarbeiterdokumentation		
Art der Unterlagen	**Aufbewahrungsdauer/-art**	**Rechtliche Grundlage**
Personaldossier (Arbeitsverträge, Mitarbeiterdossier inkl. Beurteilungen, Arbeitszeugnissen, Bestätigungen, Aktennotizen, Verwahrungen, Kündigung usw.)	**5 Jahre** ab Austritt des/der Mitarbeitenden, auf Papier (analog) oder elektronisch (digital), sodass der Sachverhalt nachgewiesen und jederzeit wieder lesbar gemacht werden kann.	Art. 330a OR i.V. Art. 128 OR/ Art. 46 Arbeitsgesetz (ArG) und 73 Verordnung 1 zum Arbeitsgesetz (ArGV 1)
Lohnwesen (Lohnausweise, Abrechnungen, Sozialversicherungen und Pensionskasse)	**5 Jahre** ab Austritt des/der Mitarbeitenden, auf Papier (analog) oder elektronisch (digital), sodass der Sachverhalt nachgewiesen und jederzeit wieder lesbar gemacht werden kann.	Art. 128 Abs. 3 OR
Arbeitszeiterfassung (Erfasste Arbeitszeiten in einem Zeiterfassungssystem)	**5 Jahre** ab Austritt des/der Mitarbeitenden, auf Papier (analog) oder elektronisch (digital), sodass der Sachverhalt nachgewiesen und jederzeit wieder lesbar gemacht werden kann.	Art. 46 Arbeitsgesetz (ArG) und 73 Verordnung 1 zum Arbeitsgesetz (ArGV 1)

Geschäftsunterlagen		
Art der Unterlagen	**Aufbewahrungsdauer/-art**	**Rechtliche Grundlage**
Rechnungen (Debitoren, Kreditoren, Jahresabschlüsse inkl. Revisionsberichten)	**10 Jahre** ab Beendigung des Geschäftsjahres, auf Papier (analog), elektronisch (digital) oder in vergleichbarer Weise, sodass der Sachverhalt gewährleistet ist und jederzeit wieder lesbar gemacht werden kann.	Art. 958 und 958f OR
Steuerunterlagen (sämtliche Unterlagen im Zusammenhang mit Steuern)		
Spesen (Spesenbelege sowie sämtliche Unterlagen im Zusammenhang mit Spesen)		

Sonstige Dokumentationen		
Art der Unterlagen	**Aufbewahrungsdauer/-art**	**Rechtliche Grundlage**
Protokolle bei automatisierter Bearbeitung von besonders schützenswerten Personendaten/ Profiling	Sofern die Arztpraxis besonders schützenswerte Personendaten automatisiert bzw. digitalisiert bearbeitet und die eingesetzten Massnahmen keinen genügenden Datenschutz bieten, hat sie die Bearbeitung zu protokollieren. Die Protokolle sind während **einem Jahr** revisionsgerecht aufzubewahren.	Art. 4 Verordnung zum Bundesgesetz über den Datenschutz (DSV)
Datenschutz-Folgenabschätzung (DSFA) (sämtliche relevanten Unterlagen im Rahmen einer Datenschutz-Folgenabschätzung)	Mindestens **2 Jahre** ab Beendigung der Datenbearbeitung. ***Hinweis:*** *Eine Pflicht zur Erstellung einer DSFA besteht, wenn Personendaten bearbeitet werden, welche bei einer allfälligen Verletzung der Vertraulichkeit, der Integrität oder bei einem Missbrauch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person haben könnten.* *Ausgenommen von der Pflicht zur Erstellung einer DSFA sind private Verantwortliche, welche gesetzlich zur Bearbeitung der Daten verpflichtet sind. Das bedeutet, dass privatrechtliche Gesundheitseinrichtungen aufgrund der gesetzlichen Verpflichtung zur Führung einer Krankengeschichte grundsätzlich keine DSFA vornehmen müssen. Dies gilt nur für die Führung der Krankengeschichte gemäss Gesetz. Sollen in Gesundheitseinrichtungen beispielsweise Cloud-Produkte eingesetzt werden, könnte eine DSFA notwendig werden, da der Einsatz einer Cloud nicht gesetzlich vorgeschrieben ist.*	Art. 14 DSV
Dokumentation Verletzung der Datensicherheit (sämtliche relevanten Unterlagen im Zusammenhang mit der Meldung zu einer Verletzung der Datensicherheit)	Mindestens **2 Jahre** ab dem Zeitpunkt der Meldung einer Verletzung der Datensicherheit.	Art. 15 DSV

3.3 Checkliste zur Aufbewahrung und Archivierung von Personendaten

Sind die Daten aufgrund von einem oder mehreren der oben genannten oder aus anderen Gründen aufzubewahren, so ist sicherzustellen, dass die Datensicherheit auch während der Aufbewahrung gegeben ist. Die nachfolgenden Checklisten können als Hilfestellung zur Gewährung der Datensicherheit bei der Aufbewahrung beigezogen werden.

Hinweis: *Im Zusammenhang mit der Frage, ob und wie Personendaten gelöscht werden dürfen, bietet die Checkliste Löschung eine Hilfestellung.*

Weitere Empfehlungen zu Sicherheitsanforderungen in Praxen sind im Dokument Minimalanforderungen IT-Grundschutz für Praxisärztinnen und Praxisärzte auffindbar.

Ort		
Massnahme	**Erläuterung/Hinweise**	**Check**
Zugangsverwaltung	Datenträger mit Personendaten sind an einem Ort aufzubewahren, zu dem nur ein ausgewählter Personenkreis Zugang hat. Beispielsweise in verschliessbaren Aktenschränken, Archiven, Räumen mit Schlüssel- oder Badge-System etc., wobei nur die berechtigten Personen im Besitz der Schlüssel oder eines Badge sind.	☐
Schutz vor umweltbedingten Ereignissen	Die Datenträger sind so aufzubewahren, dass diese nicht durch Wasser, Feuer oder andere umweltbedingte Ereignisse zerstört werden können.	☐

Format		
Massnahme	**Erläuterung/Hinweise**	**Check**
Schutz vor Korrosion/ Papierzerfall	Datenträger sind auf eine Art und Weise aufzubewahren, dass diese nicht durch Korrosion (digitale Datenträger) oder Papierzerfall (physische Datenträger) zerstört werden können.	☐
Aktuelle Formate	Digitale Daten sind in einem Format aufzubewahren, welches langfristig gelesen werden kann. Ist dies nicht möglich, ist sicherzustellen, dass die Daten rechtzeitig in ein aktuelles Format übertragen werden. Nachfolgend aufgeführte Formate sind archivtauglich:	☐

Anwendungsbereich	**Archivtaugliche Formate**
Dokumente von Office (Word, Excel, Powerpoint, Outlook)	PDF/A
Text (unformatiert)	TXT
Tabellen	CSV
Datenbanken	SIARD
Digitale Bilder	TIFF oder PDF/A
Audio	WAVE
Video	MPEG-4

Hinweis: *Die Übertragung von Daten in ein anderes Format kann die Daten verändern oder andere Beeinträchtigungen hervorrufen.*

Zugriff		
Massnahme	**Erläuterung/Hinweise**	**Check**
Zugriffs-berechtigungen	Es wird nur denjenigen Personen Zugriff auf die Daten gewährt, welche die Daten wirklich benötigen (z. B. zu Beweiszwecken im Rahmen eines Haftungsanspruches, zur Sicherstellung der Lesbarkeit etc.). Berechtigungen für den Zugriff auf Daten sind auf ein notwendiges Minimum zu beschränken (z. B. Beschränkung auf ein bis zwei Personen). Es ist sicherzustellen, dass die Berechtigungen den Gegebenheiten angepasst werden können (z. B. Mutation, Stellvertretung etc.).	☐
Schutz von Authentisierungs-mitteln	Es ist sicherzustellen, dass die Authentisierungsmittel (z. B. Benutzername/Passwort, Schlüssel, Badge) während der gesamten Aufbewahrungsdauer verfügbar, aber vor dem Zugriff durch unberechtigte Personen geschützt sind.	☐
Aktuelle Verschlüsselungs-technologien	Es ist sicherzustellen, dass Verschlüsselungstechnologien zum Einsatz kommen, welche eine Entschlüsselung während der gesamten Aufbewahrungsdauer ermöglichen. Sofern die Technologien während der Aufbewahrungszeit eine Änderung erfahren, sind die Daten rechtzeitig mit einer neuen Technologie zu verschlüsseln.	☐
Back-up	Werden die Daten in Form eines digitalen Back-ups aufbewahrt, ist die Wiederherstellung des Back-ups regelmässig (Empfehlung einmal jährlich) zu testen. ***Hinweis:*** *Die Empfehlung 8 der Minimalanforderungen IT-Grundschutz FMH bietet weitere Hinweise zu Massnahmen, welche im Zusammenhang mit der Erstellung von Back-ups beachtet werden sollten.*	☐

Nachvollziehbarkeit		
Massnahme	**Erläuterung/Hinweise**	**Check**
Schutz vor unberechtigter Veränderung	Es ist sicherzustellen, dass Veränderungen an aufbewahrten Daten ersichtlich und nachvollziehbar sind. — Papierdokumente und Wechseldatenträger: z.B. Liste mit manuell eingetragener Protokollierung — Digitale Datenträger: z.B. Protokollierung von Änderungen (Logging), auch während der Aufbewahrung	☐
Schutz der Protokollierung	Systeme zur Protokollierung sowie Protokolle sind vor unbefugtem Zugriff und vor Manipulation zu schützen.	☐

Zusammenarbeit mit Dritten		
Massnahme	**Erläuterung/Hinweise**	**Check**
Vertragliche Bestimmungen	Werden Dritte in die Aufbewahrung involviert, ist sicherzustellen, dass vertragliche Vorgaben zur Aufbewahrung vereinbart sind und die Einhaltung dokumentiert wird. ***Hinweis:*** *Beim Beizug von Dienstleistenden für die Aufbewahrung ist sicherzustellen, dass die Dienstleistenden sorgfältig ausgewählt, über ihre Pflichten instruiert und regelmässig überprüft werden. Es wird empfohlen, eine Geheimhaltungserklärung durch die Dienstleistenden unterzeichnen zu lassen. Eine Vorlage kann hier heruntergeladen werden.*	☐
Behandlung bei Verletzung der Datensicherheit	Werden Dritte in die Aufbewahrung involviert, ist sicherzustellen, dass das Vorgehen bei Verletzung der Datensicherheit definiert ist. ***Hinweis:*** *Eine Hilfestellung bietet die Empfehlung 10 aus dem IT-Grundschutz FMH (Vorkehrung für die Behandlung von Sicherheitsvorfällen).*	☐
Vertraglich vereinbarte Herausgabe	Werden Dritte in die Aufbewahrung involviert, ist sicherzustellen, dass eine Herausgabe der Daten bei Beendigung der Zusammenarbeit erfolgt.	☐

Erfüllung der Vorgaben		
Massnahme	**Erläuterung/Hinweise**	**Check**
Kontrolle der Aufbewahrungsfristen	Die Fristen zur Aufbewahrung sind sichergestellt und Personendaten werden nach Ablauf der Frist unverzüglich und unwiderruflich gelöscht oder vernichtet. ***Hinweis:*** *Betreffend die Löschung/Vernichtung von Personendaten kann die Checkliste Löschung als Hilfestellung beigezogen werden.*	☐
Dokumentation	Die Fristen zur Aufbewahrung und die anschliessende Löschung/Vernichtung sind zu dokumentieren.	☐

Impressum
Herausgeberin: FMH – Verbindung der Schweizer Ärztinnen und Ärzte, Bern
Text: Redguard AG, Bern
Gestaltung: Hahn + Zimmermann, Bern
Publikation: März 2023
www.fmh.ch