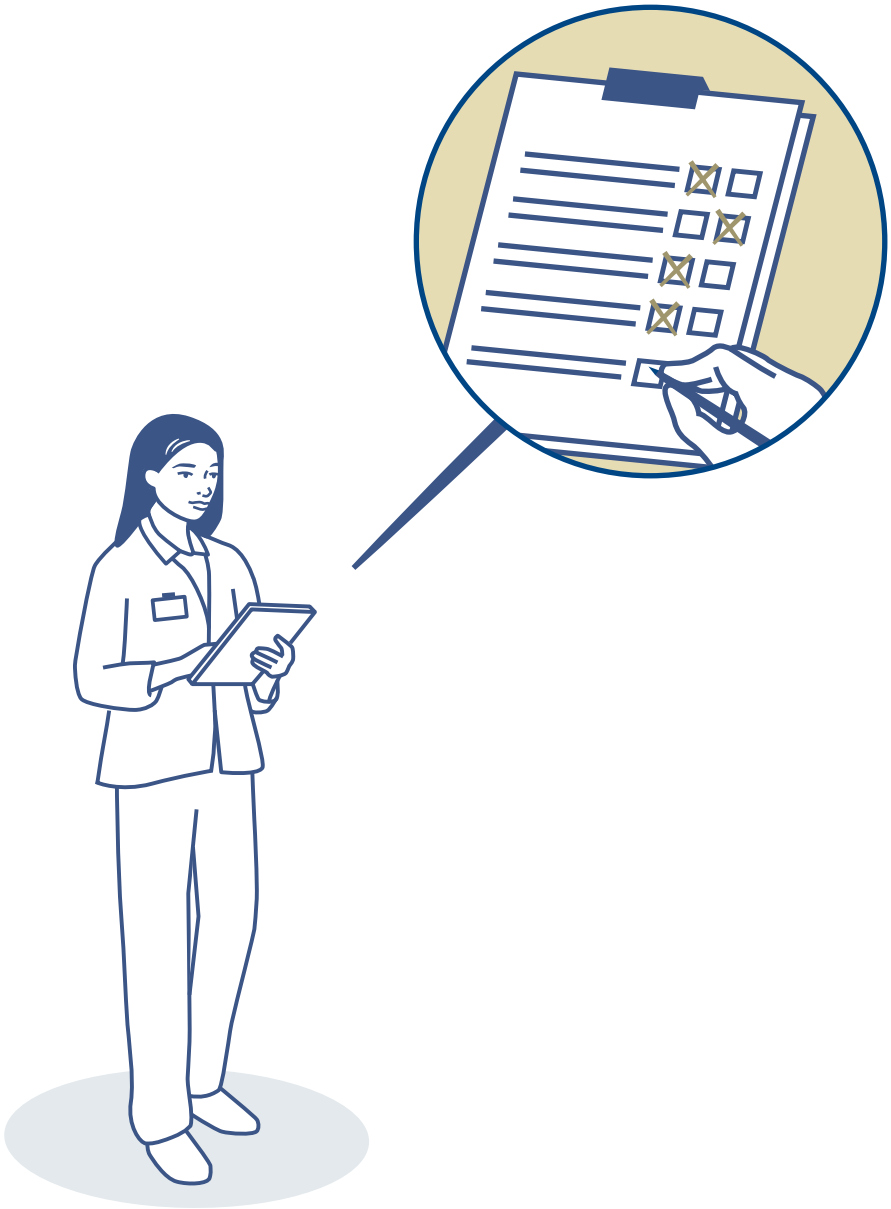
Leitfaden Verzeichnis der Bearbeitungs-tätigkeiten



Version 03/2023

FMH · Verbindung der Schweizer Ärztinnen und Ärzte · Fédération des médecins suisses
Postfach · CH-3000 Bern 16 · Telefon +41 31 359 11 11 · info@fmh.ch · www.fmh.ch

Vorwort

Das neue Bundesgesetz über den Datenschutz (DSG) sowie die Verordnung über den Datenschutz (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

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.

Bearbeitungstätigkeit	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 oder 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 Ärztin oder behandelnder 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 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 andere Ärztin 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. DSG). 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 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

Impressum
Herausgeberin: FMH – Verbindung der Schweizer Ärztinnen und Ärzte, Bern
Publikation: März 2023
www.fmh.ch