**Datenschutzkonzept (Muster)**

Version 01/2023

Name Arztpraxis

Adresse

PLZ/ORT

Tel.: +41 XX XXX XX XX

gültig ab XX.XX.XXXX

Inhaltsverzeichnis

[1 Allgemeines 3](#_Toc135057319)

[1.1 Ziel und Zweck des Datenschutzkonzepts 3](#_Toc135057320)

[1.2 Weitere Dokumente 3](#_Toc135057321)

[2 Grundlagen 4](#_Toc135057322)

[2.1 Begriffe 4](#_Toc135057323)

[2.1.1 Informationen 4](#_Toc135057324)

[2.1.2 Personendaten 4](#_Toc135057325)

[2.1.3 Betroffene Personen 4](#_Toc135057326)

[2.1.4 Bearbeiten 4](#_Toc135057327)

[2.1.5 Bekanntgeben 4](#_Toc135057328)

[2.1.6 Datenschutz 4](#_Toc135057329)

[2.1.7 Datensicherheit (Informationssicherheit) 4](#_Toc135057330)

[3 Verantwortlichkeiten 5](#_Toc135057331)

[3.1 Geheimhaltungspflichten 5](#_Toc135057332)

[4 Grundsätze der Datenbearbeitung 6](#_Toc135057333)

[4.1 Bearbeiten von Personendaten 6](#_Toc135057334)

[4.1.1 Rechtmässigkeit 6](#_Toc135057335)

[4.1.2 Verhältnismässigkeit 6](#_Toc135057336)

[4.1.3 Zweckbindung 6](#_Toc135057337)

[4.1.4 Transparenz 6](#_Toc135057338)

[4.1.5 Informationssicherheit 6](#_Toc135057339)

[4.2 Weitergabe von Personendaten an Dritte 6](#_Toc135057340)

[4.2.1 Grundsatz 6](#_Toc135057341)

[5 Rechte betroffener Personen 7](#_Toc135057342)

[5.1 Auskunftsrecht 7](#_Toc135057343)

[5.2 Weitere Rechte 7](#_Toc135057344)

[6 Informationssicherheit 8](#_Toc135057345)

[6.1 Technische und organisatorische Massnahmen (TOM) 8](#_Toc135057346)

[6.1.1 Organisatorische Massnahmen 8](#_Toc135057347)

[6.1.2 Technische Massnahmen 8](#_Toc135057348)

[6.1.3 Benutzerverwaltung und -berechtigungen 8](#_Toc135057349)

[6.1.4 Protokollierung 8](#_Toc135057350)

[6.1.5 Meldung von Datenschutzverletzungen 8](#_Toc135057351)

[7 Beauftragte Dritte («Outsourcing») 9](#_Toc135057352)

[8 Sensibilisierung der Mitarbeitenden 9](#_Toc135057353)

[9 Aufbewahrungsfristen, Archivierung und Löschung 9](#_Toc135057354)

# Allgemeines

## Ziel und Zweck des Datenschutzkonzepts

Das Ziel des Datenschutzkonzepts ist es, die internen Rahmenbedingungen für die Datenbearbeitungen festzulegen. Sie sollen die korrekte und einheitliche Umsetzung der datenschutzrechtlichen Vorgaben erlauben und die Risiken für die Sicherheit der Datenbearbeitungen minimieren.

Das Datenschutzkonzept bezweckt dabei

* Transparenz über die Datenbearbeitungen zu schaffen,
* Rahmenbedingungen und konkrete Handlungsanleitungen festzulegen,
* einen sicheren Einsatz der Informations- und Kommunikationstechnologie (IKT) zu gewährleisten.

Gleichzeitig wird mit dem Datenschutzkonzept der Nachweis für das Einhalten der Datenschutzvorvorgaben erbracht.

## Weitere Dokumente

Integrierter Bestandteil des Datenschutzkonzepts sind die folgenden Dokumente:

* [Leitfaden Verzeichnis der Bearbeitungstätigkeiten](https://www.fmh.ch/files/pdf28/leitfaden-verzeichnis-der-bearbeitungstaetigkeiten.pdf)
* [Datenschutzerklärung](https://www.fmh.ch/files/doc3/datenschutzerklaerung.docx)
* [Einwilligungserklärung](https://www.fmh.ch/files/doc3/einwilligungserklaerung-patientenformular.docx)
* [Geheimhaltungsvereinbarung](https://www.fmh.ch/files/doc3/geheimhaltungsvereinbarung.docx)

# Grundlagen

## Begriffe

Die Definitionen der Begriffe sind der aktuellen Gesetzgebung (Datenschutzgesetz, DSG) entnommen oder angelehnt. Sie dienen im vorliegenden Zusammenhang dem gemeinsamen Verständnis für alle Beteiligten.

### **Informationen**

Informationen sind alle Aufzeichnungen, unabhängig von ihrer Darstellungsform und ihrem Informationsträger.

### **Personendaten**

Personendaten sind Informationen, die sich auf eine bestimmte oder bestimmbare Person beziehen (Identifizierbarkeit). *Besonders schützenswerte Personendaten* sind eine Teilmenge von Personendaten. Dabei handelt es sich um «sensitive» Daten wie Gesundheitsdaten, genetische oder biometrische Daten.

### **Betroffene Personen**

Betroffene Personen sind natürliche Personen, über die Daten (Personendaten) bearbeitet werden.

### **Bearbeiten**

Bearbeiten ist jeder Umgang mit Personendaten wie das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben oder Vernichten.

### **Bekanntgeben**

Bekanntgeben ist das Zugänglichmachen von Personendaten wie das Einsicht gewähren, Weitergeben oder Veröffentlichen.

### Datenschutz

Der Datenschutz umfasst den Umgang mit Personendaten. Das Ziel des Datenschutzes ist der Schutz der Persönlichkeitsrechte und der Grundrechte von Personen, über die Daten bearbeitet werden.

### Datensicherheit (Informationssicherheit)

Die Datensicherheit oder Informationssicherheit umfasst alle Massnahmen zum Schutz der Informationen und Daten durch organisatorische und technische Massnahmen. Das Ziel der Datensicherheit ist es, die Risiken der Datenbearbeitung zu minimieren (Verlust, unbefugte Veränderung oder Kenntnisnahme, etc.).

# Verantwortlichkeiten

Alle Mitarbeitenden der Arztpraxis sowie alle beauftragte Personen sind persönlich verantwortlich für die Datenbearbeitungen in ihren Aufgabenbereichen. Sie werden zur Einhaltung der Datenschutz- und Informationssicherheitsvorgaben entsprechend verpflichtet (Anstellungsvertrag, Mandatsverhältnis und/oder Dienstleistungsvertrag).

## Geheimhaltungspflichten

Alle Mitarbeitenden und beauftragte Personen sind zur Verschwiegenheit über alle Angelegenheiten verpflichtet. Als Arzt oder Ärztin und als Hilfspersonen unterstehen sie dem Berufsgeheimnis (Art. 321 StGB). Eine Verletzung des Berufsgeheimnisses ist strafbar.

Die Geheimhaltungspflicht wird in die vertraglichen Vereinbarungen der Arbeits- oder Mandatsverhältnisse sowie Dienstleistungsverträge aufgenommen. Die Geheimhaltungspflicht gilt nach Beendigung des Arbeits- oder Mandatsverhältnisses weiter.

# Grundsätze der Datenbearbeitung

## Bearbeiten von Personendaten

Die nachfolgenden gesetzlichen Grundsätze sind für das Bearbeiten von Personendaten zu beachten.

### Rechtmässigkeit

Das Bearbeiten von Personendaten ist rechtmässig, wenn die Rahmenbedingungen des Datenschutzgesetzes (DSG) eingehalten werden (siehe Ziff. 4.1.2 – 4.1.5 nachfolgend) oder ein Rechtfertigungsgrund vorliegt (z.B. Einwilligung der betroffenen Personen).

### Verhältnismässigkeit

Einzelne Personendaten dürfen bearbeitet werden, soweit sie für die Aufgabenerfüllung geeignet und erforderlich sind.

### Zweckbindung

Die Personendaten dürfen nur für den ursprünglich festgelegten Zweck verwendet werden. Eine andere Verwendung braucht die Einwilligung der betroffenen Person oder eine Rechtsgrundlage.

### Transparenz

Die Datenbearbeitungsprozesse müssen transparent und nachvollziehbar sein. Dies betrifft insbesondere die Datenbeschaffung, die in der Regel bei der betroffenen Person zu erfolgen hat. Die betroffene Person hat ein Auskunftsrecht über ihre Daten (siehe Ziff. 5.1 nachfolgend).

### Informationssicherheit

Mit geeigneten technischen und organisatorischen Massnahmen ist eine der Sensitivität der bearbeiteten Informationen und Personendaten angemessene Datensicherheit zu gewährleisten.

## Weitergabe von Personendaten an Dritte

### Grundsatz

Personendaten dürfen an Dritte weitergeben, soweit eine gesetzliche Grundlage hierzu ermächtigt (z.B. KVG) oder die betroffene Person eingewilligt hat.

# Rechte betroffener Personen

## Auskunftsrecht

Alle Personen, deren Daten durch die Arztpraxis bearbeitet werden, haben einen Anspruch auf Auskunft über ihre Daten (Art. 25 DSG). Diese Auskunft erfolgt auf schriftliches Gesuch hin schriftlich (z.B. Kopien), sie kann aber auch mündlich erfolgen. In beiden Fällen ist die Identität der betroffenen Person festzustellen.

Die Auskunft über Gesundheitsdaten können der betroffenen Person über eine von ihr bezeichnete Gesundheitsfachperson mitgeteilt werden.

Bei überwiegenden privaten oder öffentlichen Interessen kann die Auskunft eingeschränkt oder aufgeschoben werden.

Die Auskunft oder der begründete Entscheid über die Beschränkung des Auskunftsrechts wird innert 30 Tagen seit dem Eingang des Auskunftsbegehrens erteilt.

Vergleiche im Einzelnen das Dokument „Anleitung Auskunft- und Herausgabegesuche über Personendaten“[[1]](#footnote-2)

## Weitere Rechte

Den betroffenen Personen stehen weitere Rechte zu wie das Recht auf Berichtigung unrichtiger Daten oder das Recht auf Löschung von Daten, die unrechtmässig bearbeitet werden.

# Informationssicherheit

## Technische und organisatorische Massnahmen (TOM)

Die Massnahmenplanung im Bereich Datenschutz und Informationssicherheit erfolgt unter Berücksichtigung anerkannter Standards und Best Practices.

### Organisatorische Massnahmen

Die für die Mitarbeitenden zu beachtenden Einzelheiten im Umgang mit IKT-Mitteln sind in den IKT Dokumenten geregelt.

### Technische Massnahmen

Technische Massnahmen werden nach dem Stand der Technik umgesetzt (siehe Empfehlungen der FMH „Minimalanforderungen IT-Grundschutz für Praxisärztinnen und Praxisärzte“[[2]](#footnote-3)).

### Benutzerverwaltung und -berechtigungen

Die Benutzerverwaltung und die Benutzerberechtigungen sowie die entsprechenden Prozesse und Verantwortlichkeiten werden in einem Berechtigungs- und Rollenkonzept festgehalten.

### Protokollierung

Die Ausübung der Zugriffsberechtigungen als auch die Bearbeitung der Daten in den Systemen der Arztpraxis wird bezüglich der Einhaltung der Datenschutzvorgaben sowie aus Sicherheitsgründen protokolliert.

### Meldung von Datenschutzverletzungen

Datenschutzverletzungen sind umgehend dem Verantwortlichen der Arztpraxis zu melden. Er entscheidet über die zu treffenden Massnahmen (z.B. Beizug einer externen Unterstützung). Er beurteilt, ob eine Information der betroffenen Personen und/oder der zuständigen Datenschutzbehörde (EDÖB) notwendig ist (bei hohem Risiko für die Persönlichkeitsrechte der betroffenen Personen) (Art. 24 DSG).

Vergleich im Einzelnen das Dokument „Checkliste und Prozessablauf bei Datenschutzverletzungen“[[3]](#footnote-4).

# Beauftragte Dritte («Outsourcing»)

Wird die Bearbeitung von Information und Personendaten an einen Dritten übertragen (z.B. Mandatsnehmer, IT-Dienstleister, usw.), ist sicherzustellen, dass die folgenden Voraussetzungen erfüllt sind:

• die Daten werden nur so bearbeitet, wie die Arztpraxis selbst es tun dürfte; und

• der Übertragung an den Dritten steht keine gesetzliche oder vertragliche Geheimhaltungspflicht entgegen.

Insbesondere müssen bei externen Dienstleistern im IT-Bereich und deren Mitarbeitenden (z.B. Datenbank- oder Netzwerkadministratoren) mindestens folgende Massnahmen ergriffen werden:

* + vertragliche Vereinbarung, welche die Geheimhaltungsverpflichtungen sowie die Weisungs- und Kontrollrechte der Arztpraxis gegenüber dem Dienstleister und seinen Mitarbeitenden festhält;
  + gültig unterzeichnete Geheimhaltungserklärungen der Mitarbeitenden des externen Dienstleisters;
  + klare Regelung des Umfangs der Zugriffsberechtigungen auf die Systeme und Daten;
  + die Nachvollziehbarkeit der Aktivitäten der externen Mitarbeitenden auf den Systemen muss mittels angemessener organisatorischer und technischer Massnahmen sichergestellt werden (z.B. Vier-Augen-Prinzip, Protokollierungen, u.a.).

# Sensibilisierung der Mitarbeitenden

Das Datenschutzkonzept sowie der Umgang mit den sensitiven Daten und dem Berufsgeheimnis wird im Rahmen der Einarbeitung von neuen Mitarbeitenden stufengerecht und angemessen erläutert.

Mit der Unterzeichnung des Anstellungsvertrags bestätigen die Mitarbeitenden, diese Bestimmungen gelesen und verstanden zu haben sowie diese zu befolgen.

Eine Sensibilisierung der Mitarbeitenden für den Datenschutz und die Sicherheit findet regelmässig statt.

# Aufbewahrungsfristen, Archivierung und Löschung

Grundlagen der Aufbewahrungsdauer, Archivierung und Löschung bzw. Vernichtung von Personendaten und Informationen bilden die relevanten gesetzlichen Bestimmungen.

Vergleiche im Einzelnen das Dokument «Leitfaden für die Aufbewahrung und Archivierung»[[4]](#footnote-5).

1. https://www.fmh.ch/files/pdf29/anleitung-auskunft-und-herausgabegesuche.pdf [↑](#footnote-ref-2)
2. https://www.fmh.ch/dienstleistungen/e-health/it-grundschutz.cfm [↑](#footnote-ref-3)
3. https://www.fmh.ch/files/pdf28/checkliste-und-prozessablauf-bei-datenschutzverletzungen.pdf [↑](#footnote-ref-4)
4. https://www.fmh.ch/files/pdf28/leitfaden-fuer-die-aufbewahrung-und-archivierung.pdf [↑](#footnote-ref-5)