

Leitfaden zur Verwendung der Geheimhaltungs- vereinbarung und der Vereinbarung für eine Auftrags- bearbeitung

*Kann dieser Titel
gekürzt werden?*

Inhaltsverzeichnis

1	Inhalt des Leitfadens	3
2	Wer unterliegt dem Berufsgeheimnis?	3
3	Wann ist eine Vereinbarung für eine Auftragsbearbeitung oder eine Geheimhaltungsvereinbarung abzuschliessen?	3
4	Was ist der Inhalt einer Geheimhaltungsvereinbarung?	3
5	Was ist eine Auftragsbearbeitung?	3
6	Was muss ich beim Einholen einer Datenbearbeitungsvereinbarung beachten?	3
7	Wann muss der Auftragsbearbeiter ein Bearbeitungsreglement haben?	4
8	Wann muss der Auftragsbearbeiter ein Bearbeitungsverzeichnis führen?	4
9	Wann ist der Auftragsbearbeiter protokollierungspflichtig?	4
10	Muss ich den Patienten über eine Auftragsdatenbearbeitung informieren?	4

1 Inhalt des Leitfadens

In diesem Leitfaden werden die Vorlagen für den Abschluss einer Geheimhaltungsvereinbarung und einer Vereinbarung für eine Auftragsbearbeitung erläutert.

2 Wer unterliegt dem Berufsgeheimnis?

Ärztinnen und Ärzte sowie deren Hilfspersonen unterliegen dem Berufsgeheimnis gemäss Art. 321 StGB. Der Begriff der Hilfsperson ist dabei weit gefasst und umfasst alle Personen, die den Arzt oder die Ärztin in ihrer beruflichen Tätigkeit direkt oder indirekt unterstützen.

3 Wann ist eine Vereinbarung für eine Auftragsbearbeitung oder eine Geheimhaltungsvereinbarung abzuschliessen?

Sobald ein Dritter mit einer Datenbearbeitung beauftragt wird, ist die Vereinbarung für eine Auftragsbearbeitung und die Geheimhaltungsvereinbarung abzuschliessen.

4 Was ist der Inhalt einer Geheimhaltungsvereinbarung?

Die Geheimhaltungsvereinbarung regelt das Bearbeiten von vertraulichen Informationen, die nicht dem Berufsgeheimnis unterliegen.

5 Was ist eine Auftragsbearbeitung?

Im Rahmen einer Auftragsverarbeitung bearbeitet der Auftragnehmer weisungsgemäss Personendaten. Eine Auftragsbearbeitung liegt typischerweise in folgenden Situationen vor:

- **Cloud-Dienstleistungen:** Cloud-Computing-Anbieter/Auslagerung von IT-Systemen und/oder Daten in ein externes Rechenzentrum (Outsourcing);
- **IT-Dienstleistungen:** Datenerfassung/Datenkonvertierung/Backup-Auslagerung und Archivierung/Analyse und Tracking Dienstleistungen (z.B. Google Analytics);
- **Datenvernichtung und -aufbewahrung:** Papier- und Aktenvernichtung/Vernichtung von Datenträgern/Archivierungsdienstleistungen;
- **Marketing/kommerzielle Kommunikation:** Extern beauftragtes Call-Center/Web- und E-Mail-Hoster/Newsletter-Dienstleister/Werbeadressenverarbeitung/Marketing-Agentur die Kundendaten verarbeitet/Marketing-Analyse-Anbieter;
- **Buchhaltung:** Buchhaltungen in Cloud/Auslagerung der Lohn- und Gehaltsabrechnung.

6 Was muss ich beim Einholen einer Datenbearbeitungsvereinbarung beachten?

Die eigentlich zu erbringende Dienstleistung ist in einem gesonderten Vertrag (sog. «Hauptvertrag») geregelt. Die ABV enthält nur die bei Erfüllung des Hauptvertrages zu beachtenden datenschutzrechtlichen Bestimmungen. Der Hauptvertrag muss deshalb in der ABV genau spezifiziert werden. Weiter darf der Hauptvertrag keinen Vorrang hinsichtlich den Bestimmungen der ABV vorsehen. Solche Klauseln wären aus dem Hauptvertrag zu streichen. Weiter müssen die betroffenen Personendaten und die Art der Datenbearbeitung in der ABV definiert werden (siehe Vorlage). Schliesslich sind die technischen und organisatorischen Massnahmen festzulegen, die der Auftragnehmer zur Sicherstellung der Datensicherheit umsetzen muss. Diese Massnahmen hängen von Art und Umfang der bearbeiteten Daten sowie dem damit einhergehenden datenschutzrechtlichen Risiko ab. Es können entsprechend abstrakt nur Bereiche definiert werden, in denen konkrete Massnahmen umgesetzt werden müssen (siehe Vorlage).

7 Wann muss der Auftragsbearbeiter ein Bearbeitungsreglement haben?

Ein Bearbeitungsreglement muss nur bei erhöhtem Risiko vorliegen bzw. wenn (a) besonders schützenswerte Personendaten in grossem Umfang bearbeitet werden oder (b) ein Profiling mit hohem Risiko durchgeführt wird. Ausgeschlossen werden damit Fälle, in denen besonders schützenswerte Personen nur vereinzelt bearbeitet werden. Viele Unternehmen, insbesondere «traditionelle» KMU, nehmen keine solche Bearbeitungen vor. Sie sind somit von dieser Verpflichtung nicht betroffen.

8 Wann muss der Auftragsbearbeiter ein Bearbeitungsverzeichnis führen?

Datenbearbeiter mit mehr als 250 Mitarbeitenden müssen ein Bearbeitungsverzeichnis führen, in dem alle Datenbearbeitungen übersichtlich dargestellt werden. Wer am 1. Januar eines Jahres weniger als 250 Mitarbeitende beschäftigte, muss nur dann ein Bearbeitungsverzeichnis führen, wenn (a) besonders schützenswerte Personendaten in grossem Umfang bearbeitet werden oder (b) ein Profiling mit hohem Risiko durchgeführt wird.

9 Wann ist der Auftragsbearbeiter protokollierungspflichtig?

Bei der Bearbeitung besonders schützenswerter Daten in grossem Umfang und beim Profiling mit hohem Risiko muss eine Protokollierung der Bearbeitungen erfolgen, wenn ansonsten nicht nachträglich festgestellt werden kann, ob die Daten für die vorgesehenen Zwecke bearbeitet wurden. Protokolliert werden müssen zumindest die Vorgänge des Speicherns, Veränderns, Lesens, Bekanntgebens, Löschens und Vernichtens von Daten.

10 Muss ich den Patienten über eine Auftragsdatenbearbeitung informieren?

Das Gesetz sieht bei einer Auftragsdatenbearbeitung keine Information der betroffenen Personen vor.