

Merkblatt betreffend Sicherheit der Datenübermittlung im elektronischen Datenverkehr

Die Sicherheit der elektronischen Datenübermittlung¹ ist allseits zu gewährleisten. Die Gewährleistung ist Sache des Softwareanbieters, z.B. bei der Übermittlung elektronischer Rechnungsdaten.

Es liegt in der Verantwortung des Anwenders², beim Softwareanbieter zu klären und sicherzustellen, dass dieser die Gewährleistung übernimmt, und dies auch vertraglich festzuhalten. Die Gewährleistung hinsichtlich Sicherheit der Datenübermittlung betrifft den gesamten Transportweg, also ab Absender (z.B. beim Physiotherapeuten) bis hin zum Empfänger (z.B. bei einer Versicherung, bei einem Arzt oder bei der physiotrust ag).

Kann der Softwareanbieter dies nicht sicherstellen, so muss der Anwender² zusammen mit seinem Softwareanbieter entsprechende Lösungen (eventuell Zusatzprogramme) finden.

Kommt eine Lösung zum Einsatz, bei welcher andere, ausser dem Anwender² selber, Einsicht in die Daten nehmen könnten (z.B. bei einer Weblösung/Internetlösung oder durch einen Supporter, welcher das EDV-System wartet usw.), so ist auch hier durch den Anwender² sicherzustellen, dass seine Daten nicht missbräuchlich verwendet werden können. In der Regel wird dieser Punkt mit einer sogenannten **Geheimhaltungsvereinbarung** sichergestellt.

Bietet Ihnen Ihr Softwareanbieter bereits eine Vereinbarung an, in welcher die nachstehenden Punkte geregelt sind, ist ein zusätzlicher Vertrag grundsätzlich hinfällig.

Ein entsprechender Vertrag zwischen Softwareanbieter (nachstehend Firma XY genannt) und Anwender² (nachstehend Physiotherapie Z genannt) könnte in etwa wie folgt aussehen

Beispiel einer Geheimhaltungsvereinbarung: ³:

„Die Firma XY verpflichtet sich gegenüber der Physiotherapie Z, sämtliche ihr zugänglichen Daten vertraulich zu behandeln. Sie verpflichtet sich insbesondere zur Einhaltung des Datenschutzgesetzes (DSG), ihre Mitarbeiter sowie beauftragte Dritte über die einschlägigen Bestimmungen zur Schweigepflicht gemäss Art 33 ATSG und zur Wahrung des ärztlichen Berufsgeheimnisses gemäss Art 321 StGB zu informieren und deren Einhaltung uneingeschränkt sicher zu stellen. Sie stellt insbesondere sicher, dass Daten oder andere Informationen unter keinen Umständen ohne ausdrückliche schriftliche Ermächtigung durch Physiotherapie Z an Dritte weiter gegeben werden.

Die Firma XY verpflichtet sich im Weiteren, die Sicherheit der ihr im Rahmen des Betriebes übergebenen Daten zu gewährleisten. Sie trifft insbesondere die gemäss dem eidgenössischen Datenschutzbeauftragten notwendigen organisatorischen und technischen Massnahmen zur Regelung der nachstehenden Aspekte in ihrem Zuständigkeitsbereich:

- Zugangs-, Benutzer- und Zugriffskontrolle,
- Datensicherung,
- Datenträger- und Transportkontrolle,
- Empfänger-Identifikationskontrolle (beim elektronischen Übermitteln der Daten),
- Speicherkontrolle und Virenschutz.

Die Datenschutzbestimmungen und Geheimhaltungsverpflichtungen bleiben auch nach Beendigung des Vertrages weiterhin bestehen.“

¹ Patientendaten, E-Mail mit Patienteninformationen, elektronische Rechnungsstellung usw.

² In diesem Fall des Physiotherapeuten

³ Dies ist ein Formulierungsvorschlag; physioswiss übernimmt keine Haftung für denselbigen