SLKK

vernünftig versichert: die ehemalige Schweizerische Lehrerkrankenkasse

Datenschutz-Bestimmungen für die App *SLKKconnect*

Zugang zur App *SLKKconnect*

Der Zugang zur App ist beschränkt auf den registrierten Benutzer, deren Identität geprüft wurde. Eine Registrierung erfolgt:

- eine gültige E-Mail-Adresse und ein persönliches frei wählbares Passwort
- Vorname/Name/gültige Telefonnummer (Handy)
- die Versichertennummer

Sorgfaltspflicht des Kunden

Die Benutzerinnen und Benutzer haben sicherzustellen, dass sämtliche Legitimations-mittel vor Dritten geheim gehalten werden und gegen missbräuchliche Verwendung durch Unbefugte geschützt sind. Insbesondere dürfen Passwörter nicht aufgeschrieben oder ungeschützt auf dem Endgerät abgelegt werden. Der Benutzer oder die Benutzerin trägt sämtliche Risiken, die sich aus der Preisgabe der Legitimationsmittel ergeben.

Besteht Anlass zur Befürchtung, dass eine unberechtigte Drittperson Kenntnis vom Passwort hat, muss der Umstand der SLKK gemeldet werden und das Passwort umgehend geändert werden.

Dateneinsicht bei einer Familie

Die SLKK stellt je Partnernummer einen Zugang aus. Die Rechnungen können via einem LogIn an die SLKK (analog Papierversand) eingereicht werden. Wichtig ist der Vermerk der Versichertennummer auf der Rechnung, damit die SLKK die Rechnung dem Versicherten zugeordnet werden kann

Sichere Kommunikation

Die Übermittlung erfolgt über eine sichere Verbindung. Die Benutzerinnen und Benutzer sind sich jedoch dessen bewusst und damit einverstanden, dass die versendeten Nachrichten von Mitarbeitenden der SLKK eingesehen werden können. Die Mitarbeitenden der SLKK unterstehen der Schweigepflicht und dürfen keine Daten an Dritte weitergeben.

Sicherheit im Portal

Auch bei modernen Systemen mit gängigen Sicherheitsvorkehrungen kann eine absolute Sicherheit weder auf SLKK- noch auf Kundenseite garantiert werden. Das Endgerät auf Kundenseite ist Teil des Systems, befindet sich aber ausserhalb der Kontrolle der SLKK und kann zu einer Schwachstelle im System werden. Die SLKK übernimmt keine Verantwortung für Endgeräte, da sie keinen Einfluss darauf hat.

Folgende Risiken sind insbesondere zu beachten:

- Bei der Nutzung des Internets sind Benutzerinnen und Benutzer der Gefahren von Computer-Viren und sogenannter Spyware (Spionage-Software) ausgesetzt. Entsprechende Anti-Viren-Software unterstützen bei den Sicherheitsvorkehrungen.
- Es ist wichtig, dass Benutzerinnen und Benutzer nur mit Software aus vertrauenswürdigen Quellen arbeiten.
- Wenig komplexe und kurze Passwörter können von Computern in relativ kurzer Zeit erraten werden, daher wird eine Länge von mindestens 8 Zeichen empfohlen. Zudem können bekannte Wörter viel schneller erraten werden als zufällige Zeichenfolgen. Deshalb ist es ratsam, Buchstaben, Zahlen und Sonderzeichen aber keine ganzen Wörter zu verwenden. Die SLKK rät zudem davon ab, ein Kennwort zu verwenden, das auch bei E-Mail oder Social-Media-Plattformen verwendet wird.

Die SLKK übernimmt keine Gewähr für die Richtigkeit und Vollständigkeit der Daten auf der App *SLKKconnect* und haftet nicht für Schäden, die der Benutzerin und dem Benutzer infolge Übermittlungs-fehler, technischer Mängel, Überlastung Unterbrüche (auch systembedingte Wartungsarbeiten) oder Störungen der Telekommunikationseinrichtung entstehen.

Zum Schutz der Kunden behält sich die SLKK vor, bei Feststellung von Sicherheitsrisiken die Dienstleistungen der App *SLKKconnect* zu unterbrechen, solange bis die Sicherheitslücke geschlossen ist.

Zugangssperre

Die SLKK behält sich vor, den Zugang zur App *SLKKconnect* jederzeit ohne Angabe von Gründen zu sperren.