

Sicherheits-Eigenschaften von Siilo

Siilo erfüllt alle Datenschutzanforderungen, die im [Whitepaper](#) der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder im November 2019 definiert wurden.

Dazu zählen u.a.:

- **Gesicherter Zugang**
Zugang zur App nur via PIN-Code, Fingerabdruck Scan oder Face-ID
- **Verifizierte Profile**
Medizinisches Fachpersonal wird anhand eines Ausbildungsnachweises verifiziert
- **Sichere Datenübertragung**
Daten sind Ende-zu-Ende-verschlüsselt
ISO-27001 zertifiziert
- **Deutsche Server**
Siilo nutzt Server in Frankfurt. Diese werden nur zur Nachrichtenübermittlung genutzt, d.h. gesendete Nachrichten werden nach Abrufen durch das Empfänger-Endgerät vollständig vom Server gelöscht
- **Dezentrale Speicherung**
Nachrichten werden ausschließlich auf den Endgeräten in "Containern" gespeichert
- **Containerlösung**
Mit Siilo aufgenommene Daten (Nachrichten, Fotos, Videos) werden getrennt und daher nicht in der Medienbibliothek des Smartphones gespeichert, sondern in einem separaten Container. Die Vorteile dabei:
 - Keine Synchronisierung oder automatisches Backup mit Cloud-Diensten
 - Kein unautorisierter Zugang bei Verlust des Handys
 - Fernlöschfunktion



Pressekontakt:

The Medical Network

presse@siilo.com

Tel. +49 40 32 90 47 38 99