SpeechLive

Sicherheit & Zertifikate

Höchste Sicherheitsstandards

SpeechLive ist ein sehr sicherer Cloud-Speicher, der Benutzern dank höchster Sicherheitsstandards jederzeit maximalen Schutz gewährleistet. Durch Verwendung des HTTPS-Protokolls, garantiert die Lösung höchste Verbindungssicherheit.
Alle gespeicherten Daten werden automatisch verschlüsselt, während gespiegelte Server Ihre Daten sichern und jederzeit verfügbar machen. SpeechLive Sicherheitsstandards sind sogar höher als die Sicherheitsstandards von Banken.

Um unbefugten Zugriff zu verhindern, werden Diktatdateien in Echtzeit verschlüsselt. Dabei wird der fortschrittlichste Verschlüsselungsstandard eingesetzt, um Ihre Daten während des Up- und Downloads zu schützen. Darüber hinaus können Dateien mithilfe des DSS Pro-Formats ein drittes Mal verschlüsselt werden.

Es würde etwa drei Trillionen Jahre dauern, um unsere 256^{256} bit-Verschlüsselung zu knacken – und das mit einem Computer, der pro Sekunde eine Milliarde Schlüssel testet. Ein Ding der Unmöglichkeit.

SpeechLive-Datenschutzerklärung

Ihre persönlichen Daten werden gemäß unserer Datenschutzerklärung weder an Dritte verkauft noch bereitgestellt. Wir geben keine persönlichen finanziellen Informationen (wie Kreditkarteninformationen) an Dritte weiter, sofern dies nicht zur Bearbeitung Ihrer Bestellung oder Rechnung oder zur Vermeidung oder Bekämpfung von Betrug erforderlich ist.

Um Ihre Daten zu schützen, werden weder Kundendaten noch Dokumente an Dritte weitergegeben, und unsere Transkriptionisten sind an strenge Vertraulichkeitsvereinbarungen gebunden. Unser Service leitet keine Transkriptionsarbeiten an Selbstständige weiter.
Weitere Informationen finden Sie in unserer Datenschutzerklärung auf unserer Website.

Sicherheitszertifikate

Rechenzentren, die SpeechLive verwenden, verfügen über die wichtigsten Sicherheitszertifikate, die internationale, nationale und branchenspezifische Vorschriften erfüllen.

SpeechLive läuft über Microsoft Azure Rechenzentren, die für einen Rund-um-die-Uhr-Betrieb ausgelegt sind und verschiedene Maßnahmen zum Schutz vor Stromausfall, physischem Eindringen und Netzwerkausfall einsetzen. Sie erfüllen Branchenstandards hinsichtlich physikalischer Sicherheit und Zuverlässigkeit und werden von Microsoft-Mitarbeitern verwaltet, überwacht und angewendet. Weiterhin sind sie für einen überwachungsfreien Betrieb ausgelegt. Weitere Informationen zur physikalischen Sicherheit von Windows Azure finden Sie im Microsoft Vertrauenscenter.

SpeechLive erfüllt folgende Sicherheitszertifikate:

SO/IEC 27001:
2005 Audit und Zertifizierung

SOC 1 und SOC 2
SSAE 16/ISAE 3402 Attestations

Cloud Security Alliance
Cloud Controls Matrix

Federal Risk and Authorization Management Program (FedRAMP)

Payment Card Industry (PCI)
Data Security Standards (DSS) Level 1

United Kingdom G-Cloud
Impact Level 2 Accreditation

HIPAA Business Associate Agreement (BAA)

Family Educational Rights and Privacy Act (FERPA)

Einfachheit & höchste Sicherheit

Das Versenden von Diktatdateien über SpeechLive ist so einfach wie das Versenden per E-Mail, und so sicher, wie es nur irgend möglich ist. Im Vergleich zu anderen unsicheren Methoden zum Versand sensibler Diktatdateien wurde SpeechLive speziell zu diesem Zweck entwickelt. Während E-Mails aufgrund des Versands unverschlüsselter Daten über eine unverschlüsselte Verbindung von Hackern angegriffen werden können, verschlüsselt SpeechLive Daten vom Kunden bis hin zum Cloud-Speicher.

Andere Cloud-Speicher, die nicht für Diktate gedacht sind, verwenden möglicherweise beim Upload eine einfache Verschlüsselung und bieten darüber hinaus keine weiteren Sicherheitsmaßnahmen. SpeechLive bietet dagegen eine doppelte Verschlüsselung, durch die zusätzliche Verwendung des sicheren HTTPS-Protokolls. Darüber hinaus sind die höchsten Sicherheitsstandards durch unsere jederzeit aktuellen Sicherheitszertifikate garantiert.

E-MAIL WORKFLOW NIEDRIGE SICHERHEIT	GÄNGIGER CLOUD WORKFLOW DURCHSCHNITTLICHE SICHERHEIT	SPEECHLIVE WORKFLOW HÖCHSTE SICHERHEIT
KEINE VERSCHLÜSSELUNG	**EINFACHE VERSCHLÜSSELUNG**	**DOPPELTE VERSCHLÜSSELUNG**
		
• Unverschlüsselte Daten werden über eine unverschlüsselte Verbindung gesendet • Risiko von Hacker-Angriffen und Verlust von Daten • Risiko von Datenlecks • Standard-Firewall mit begrenzten oder keinen Sicherheitszertifikaten	• Nicht für Diktatworkflow gedacht • Einfach verschlüsselter Upload in einen unverschlüsselten Cloud-Speicher	• Höchste Sicherheitsstandards durch jederzeit aktuelle Sicherheitszertifikate • Https-Sicherheit • Eigener Diktatworkflow • Daten werden vom Kunden bis zum Cloud-Speicher verschlüsselt • Vorteile zusätzlicher Dienste • Voll skalierbarer Speicher