

PHILIPS



Philips SpeechLive

Umfassender Datenschutz
und maximale Sicherheit
für Ihre Diktate

Inhalt

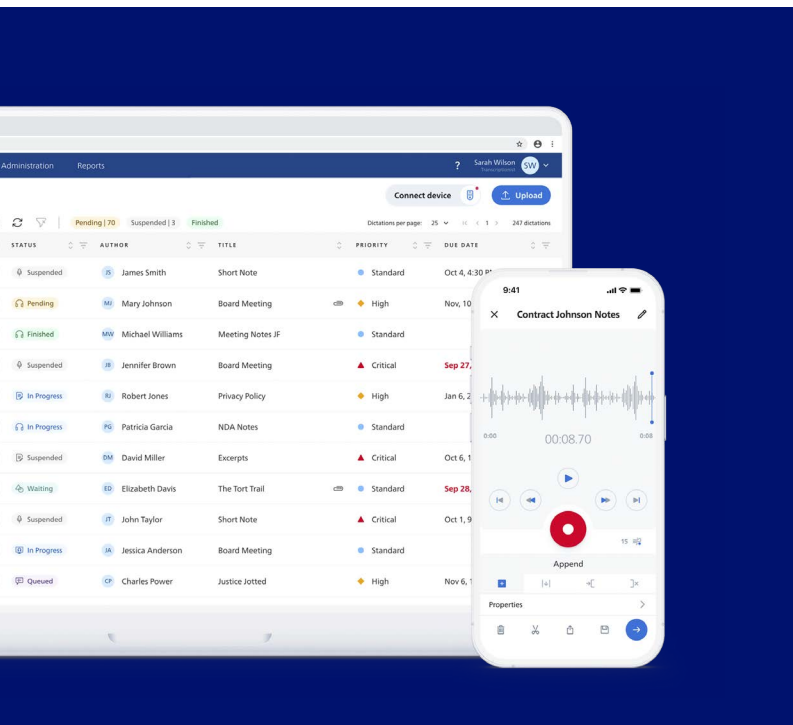
Höchste Zertifizierungsstufe	3
Datensicherheit und Verschlüsselung	4
Datenspeicherung	5
Spracherkennung und KI-Assistent	6
Sicherheit beim Personenzugriff	7
Transkriptionsservice und andere Dienstleister	8



Wir schützen
jedes Wort

Höchste Zertifizierungsstufe

Tausende Kunden aus der ganzen Welt und aus unterschiedlichsten Branchen vertrauen Philips SpeechLive ihre Daten an. Datensicherheit hatte für uns schon immer höchste Priorität, bereits in der Entwicklungsphase der Lösung.



Trust Center

Das SpeechLive Trust Center bietet transparenten Zugang zu unseren Informationen zu Sicherheit, Compliance und Datenschutz.

Erfahren Sie mehr unter
www.speechlive.com/trust



14001
Certified



GDPR
Compliant



9001
Certified



CCPA
Compliant



27001
Certified



EU AI Act
Compliant



HIPAA
Compliant

Datensicherheit und Verschlüsselung

Philips SpeechLive stellt sicher, dass Sie sicher und ohne Unterbrechungen arbeiten können. Dank zuverlässiger Backup- und Wiederherstellungsoptionen müssen Sie sich keine Sorgen machen, wichtige Diktate zu verlieren. Starke Verschlüsselung, Multi-Faktor-Authentifizierung und Single Sign-on schützen Ihre Daten und machen die Anmeldung einfach und sicher, sodass Sie darauf vertrauen können, dass Ihre Informationen privat bleiben und Ihre Arbeitsabläufe reibungslos funktionieren.



Backup und vollständige Datenwiederherstellung

Benutzer können Sicherungskopien aller Diktate erstellen, um sie bei Bedarf zu einem späteren Zeitpunkt wiederherzustellen. Versehentlich gelöschte Diktate können vom Kontoadministrator bis zu 30 Tage lang wiederhergestellt werden.



Geschützt durch HTTPS-Verschlüsselung

Diktate werden immer mit der branchenüblichen AES-256-Bit-Verschlüsselung erstellt, übertragen und gespeichert - in der Web-App in der sicheren Microsoft-Azure-Umgebung sowie in der iOS- oder Android-App auf dem Smartphone.



Zusätzliche Sicherheit mit Multifaktor-Authentifizierung

Die E-Mail-basierte Multi-Faktor-Authentifizierung (MFA) bietet eine zusätzliche Sicherheitsebene. SpeechLive verwendet einen sicheren Authentifizierungsdienst von Microsoft, der Sicherheitsrisiken wie Brute-Force-Angriffe verhindert. Die Einstellung kann vom Kontoadministrator verpflichtend aktiviert werden.



Einfache Anmeldung mit Single Sign-On (SSO)

Single Sign-on reduziert den Aufwand, sich weitere Passwörter merken zu müssen. Wenn SSO aktiviert ist, können sich Benutzer mit ihren Microsoft-Anmeldedaten einfach und sicher bei SpeechLive anmelden. Außerdem vereinfacht SSO die Arbeit von Administratoren, da weniger Benutzerkonten verwaltet werden müssen.



Sicherer Zahlungsprozess

Zahlungen werden über unsere Zahlungsdienstleister Unzer und authorize.net abgewickelt, die beide den Vorgaben des Payment Card Industry Data Security Standard (PCI DSS) entsprechen. So wird sichergestellt, dass Zahlungsinformationen stets in einer sicheren Umgebung verarbeitet, gespeichert und übertragen werden.



Datenspeicherung

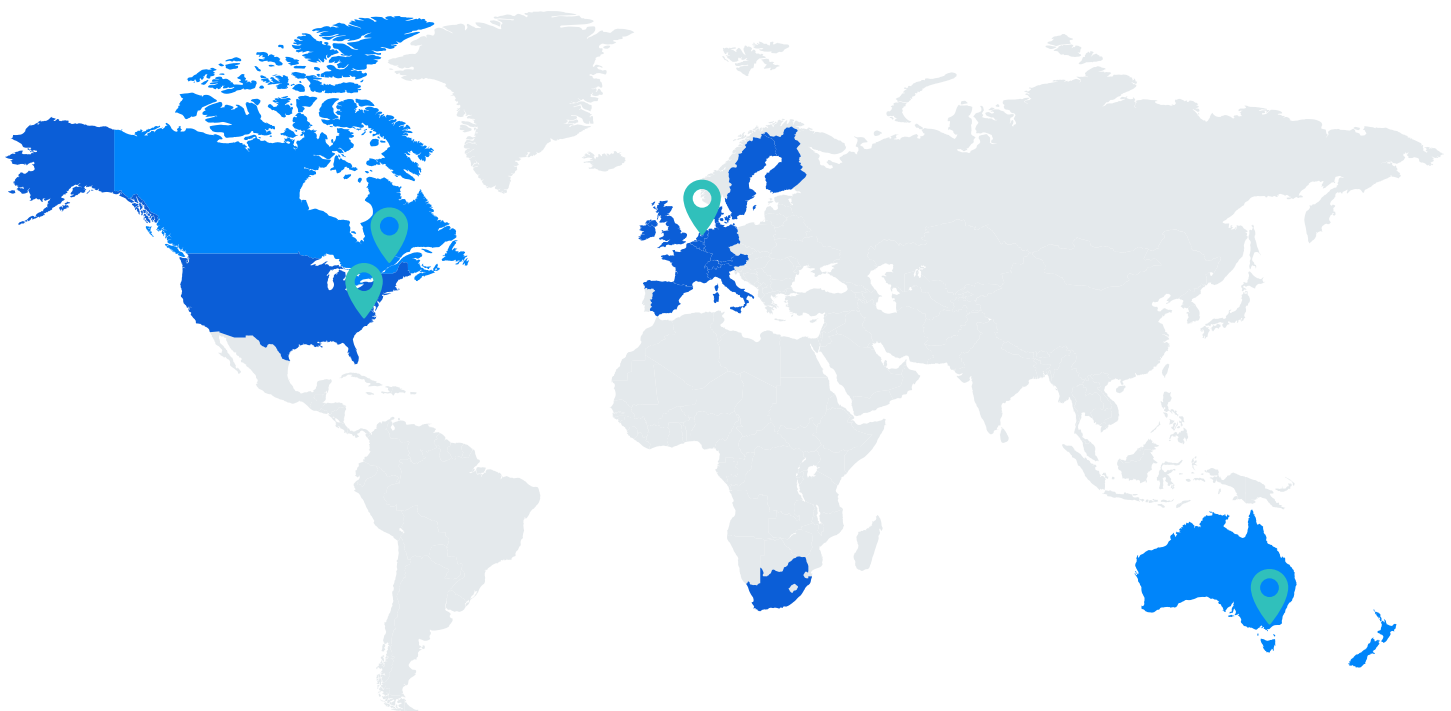
Philips SpeechLive nutzt Microsoft Azure zur Speicherung von Diktaten und Dateianhängen und setzt dabei auf eine der weltweit führenden Enterprise-Cloud-Plattformen. Azure bietet eine Verfügbarkeit von 99,9 % sowie einen robusten Schutz vor Stromausfällen, Angriffen und Netzausfällen.

Die Rechenzentren von Microsoft erfüllen höchste Branchenstandards und werden rund um die Uhr von spezialisierten Operationsteams überwacht. Mit Investitionen von über 4 Milliarden US-Dollar in Sicherheitsforschung und mehr als 10.000 Cybersicherheitsexperten gehört Azure zu den vertrauenswürdigsten Cloud-Anbietern weltweit. Die Plattform erfüllt über 100 internationale Vorschriften und wird regelmäßig auditiert.

Alle SpeechLive-Daten werden regional auf Azure-Servern gespeichert, um gesetzliche Anforderungen zu erfüllen und einen schnellen Zugriff zu gewährleisten.

Australien und Neuseeland	Victoria
Kanada	Quebec City
Europa und Südafrika	Niederlande
USA	Boydton, Virginia

[Azure-Compliance-Angebote ansehen](#)



Spracherkennung und KI-Assistent

Sowohl unsere Spracherkennung als auch unser KI-Assistent sind mit höchsten Sicherheitsstandards entwickelt, um Ihre Daten zu schützen. Ihre Daten werden nach der Verarbeitung automatisch gelöscht und in einer dedizierten, isolierten Umgebung verarbeitet.

Es findet keinerlei Zugriff durch OpenAI oder ein Training von KI-Modellen mit Ihren Daten statt. Wir halten strenge Compliance-Vorgaben ein und setzen durchgängige Datenverschlüsselung ein – betrieben in der besonders sicheren Microsoft-Azure-Cloudumgebung.



Sichere Datenübertragung

Alle Audiodateien, die an unsere Spracherkennung gesendet werden, werden sicher über einen verschlüsselten Kanal sicher übertragen. Wir verwenden HTTPS sowohl für die Kommunikation zwischen Client und Server als auch zwischen Servern. Transkriptionen werden über eine sichere SignalR-HTTPS-Verbindung übermittelt.



Datenspeicherung

Wenn Sie die Desktop- oder Mobil-App für unseren Spracherkennungsdienst verwenden, werden weder Audio- noch Textdateien auf unseren Servern gespeichert. ie Audio- und Textdateien werden lediglich über unsere Server durchgeleitet. Bei Nutzung der Webversion werden sowohl Ihr Audio als auch die Transkription während der Spracherkennung vorübergehend gespeichert und anschließend automatisch gelöscht. Die Dateien werden verschlüsselt in Ihrem SpeechLive-Konto abgelegt, ausschließlich für Ihren Zugriff.



Regionale Verarbeitung

Die Spracherkennungs-Engine nutzt Server mit den höchsten Sicherheitsstandards in den USA, Kanada, der EU und Australien.



Kein KI-Training

Ihre Daten bleiben vollständig privat und werden ausschließlich zur Unterstützung Ihrer eigenen Interaktionen genutzt. Sie werden niemals mit OpenAI, anderen Kunden oder Dritten geteilt und nicht zum Trainieren, Nachtrainieren oder Verbessern von KI-Modellen oder anderen Produkten verwendet, es sei denn, Sie erteilen ausdrücklich Ihre Zustimmung.

Sicherheit beim Personenzugriff

Die Kontrolle des Personenzugriffs ist entscheidend, um sensible Informationen zu schützen und unbefugten Zugriff zu verhindern. Unsere strengen Zugangskontrollen und regelmäßigen Audits stellen sicher, dass unsere Sicherheit auch in Zukunft höchsten Ansprüchen genügt.



Asset-Kontrolle

Alle Computer des Philips-Personals werden mit Antivirus-Software, Festplattenverschlüsselung, automatischer Gerätesperre und Sicherheits-Patches überwacht. Alle Philips-Mitarbeiter, die Zugriff auf Dateien von Nutzern haben, arbeiten mit diesen Daten ausschließlich auf Geräten mit geeigneten Zugriffskontrollen und Sicherheitsverfahren.



Geheimhaltungsvereinbarung

Alle Mitarbeitenden mit Zugriff auf Dateien von Nutzern müssen eine spezielle Sicherheitsschulung absolvieren und eine Geheimhaltungsvereinbarung (NDA) unterzeichnen. Diese Vereinbarung dient dem Schutz der vertraulichen und personenbezogenen Daten, die Speech Processing Solutions seinen Mitarbeitenden anvertraut.



Personalschulung

Nur geschultes Personal hat Zugriff auf das System für Wartung, Support und Weiterentwicklung.



Endpunktsicherheit

Wir verwenden eine VPN-Verbindung, um sicherzustellen, dass Mitarbeitende, die Zugriff auf sensible Daten haben, von unserem Unternehmensnetzwerk aus und über mehrere Endgeräte hinweg sicher darauf zugreifen können.



Transkriptionsservice und andere Dienstleister

Im Rahmen unserer strengen Richtlinien für das Lieferantenmanagement arbeiten wir ausschließlich mit branchenführenden Dienstleistern zusammen.

Diktate, die an den SpeechLive-Transkriptionsservice gesendet werden, werden von sorgfältig ausgewählten externen Partneragenturen verarbeitet und per verschlüsselter HTTPS-Verbindung an deren sichere Server übertragen. Die Diktate werden nach der Transkription gelöscht und nicht auf den Servern der Partner gespeichert.

Jeder neue Dienstleister durchläuft vor der Zusammenarbeit eine umfassende Sicherheitsprüfung. So stellen wir sicher, dass jederzeit höchste Sicherheits- und Compliance-Standards eingehalten werden.

