PHILIPS

SpeechLive

Sicherheit und Vertraulichkeit Ihrer Daten

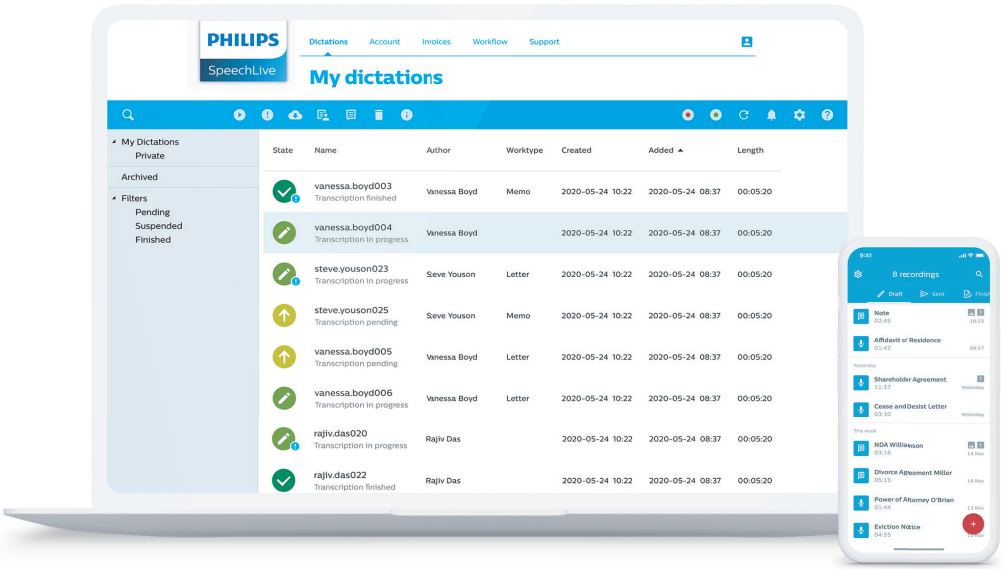
Webbasierte Diktier- und Transkriptionslösung Philips SpeechLive

Sicherheit Ihrer Daten

Die webbasierte Diktier- und Transkriptionslösung Philips SpeechLive ist ein browserbasierter Workflow-Dienst, mit dem professionelle Benutzer überall und jederzeit Gesprochenes in Text umwandeln können – schnell und effizient.

Mit der cloudbasierten Lösung kommen Benutzer im Büro, zu Hause und unterwegs in den Genuss eines konsistenten und zuverlässigen Spracherkennungs- und Dokumentations-Workflows. Als Eingabegerät kann sowohl ein PC als auch ein beliebiges Smartphone verwendet werden.

Die Zahl der Kunden aus den verschiedensten Branchen weltweit, die ihre Daten Philips SpeechLive anvertrauen, geht in die Tausende. Bei einem Angebot mit einer solch umfassenden Flexibilität war es für Philips von Anfang an klar, dass die Sicherheit der Daten allerhöchste Priorität genießen muss – und das bereits in der Entwicklungsphase.



ISO 9001:2015 CERTIFIED COMPANY

GDPR READY

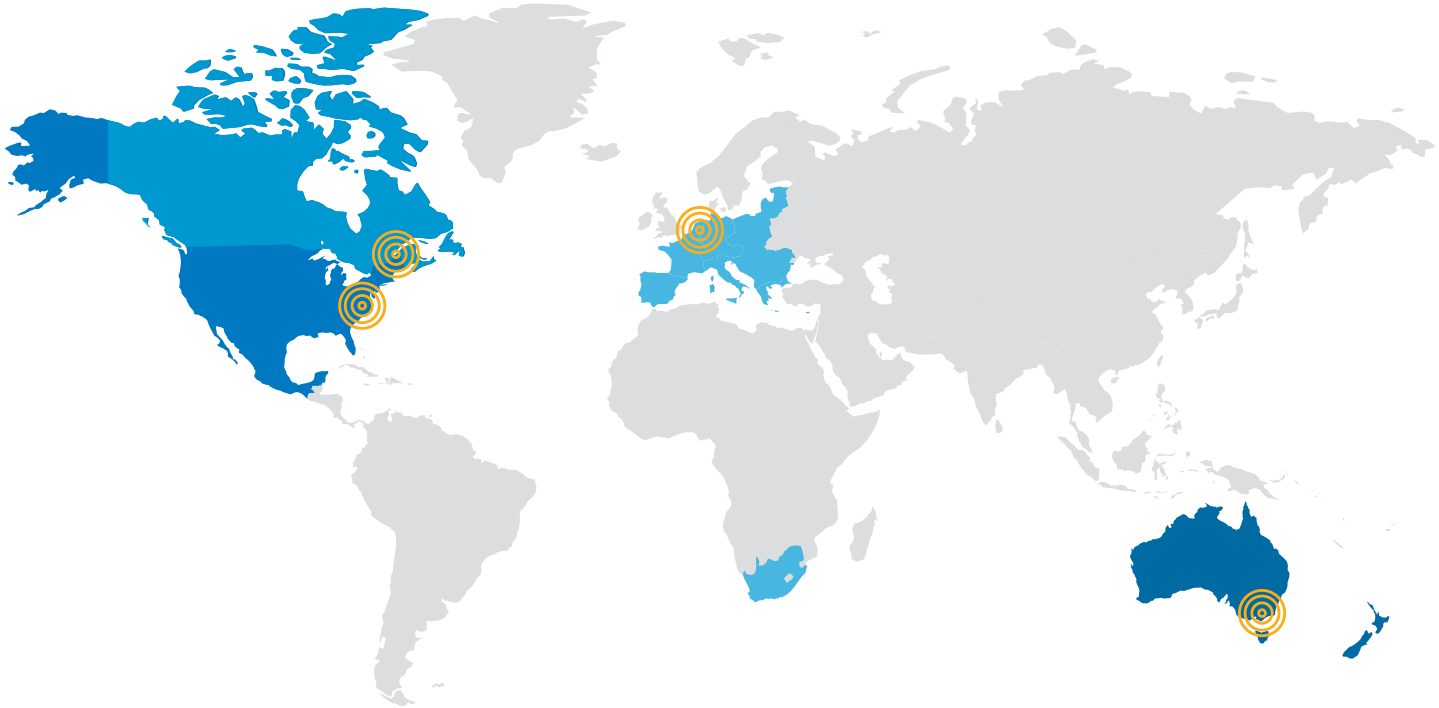
CCPA READY

Datenspeicher

Kontodaten (im Zusammenhang mit Ihrer Abrechnung) werden auf sicheren Datenservern in Österreich gespeichert.

Diktate (Audioaufnahmen und Dateianhänge wie z.B. Bilder und Dokumente) werden regional auf Microsoft Azure-Servern gespeichert, um die gesetzlichen Anforderungen zu erfüllen und den schnellsten Zugriff zu ermöglichen:

Vereinigte Staaten: Boydton, Virginia
Kanada: Quebec City
Europa und Süd Afrika: Niederlande
Australien und Neuseeland: Victoria



Microsoft Azure

Philips SpeechLive greift für das Hosting von Diktaten (Audioaufnahmen und Dateianhänge) auf Microsoft Azure zurück. Azure ist die weltweit führende Plattform für das Hosting von cloudbasierter Lösungen für Unternehmen.

Die Plattform zeichnet sich durch kompromisslose Sicherheitsstandards und prozesse aus, mit denen für ein Höchstmaß an Vertraulichkeit und Sicherheit der Daten gesorgt wird. Microsoft führt kontinuierlich Penetrationstests durch und arbeitet fortlaufend an der Erkennung und Vermeidung von Bedrohungen durch unbefugtes Eindringen, Denial-of-Service-Angriffe usw.

Verfügbarkeit
Microsoft Azure-Dienste sind in hohem Maße zuverlässig. Microsoft ist stolz darauf, eine Verfügbarkeitsgarantie von 99,9 % zu bieten – 24 Stunden am Tag, 7 Tage die Woche und 365 Tage im Jahr.

Bei Microsoft Azure gibt es eine „Lights-out"-Richtlinie, die verschiedene Maßnahmen zur Gewährleistung des unterbrechungsfreien Betriebs in den folgenden Fällen vorschreibt:

- Stromausfälle
- physisches Eindringen
- Netzwerkausfälle

Die Azure-Rechenzentren entsprechen den geltenden Industriestandards für physische Sicherheit und Zuverlässigkeit und sie werden von Microsoft-Mitarbeitern geleitet, überwacht und verwaltet. Laut Microsoft hat das Unternehmen außerdem über 1 Milliarde US-Dollar in seine Sicherheitsforschung und -entwicklung investiert und beschäftigt über 3.500 Experten für Cybersicherheit.

Daher ist Microsoft Azure eine der meistgenutzten Plattformen weltweit und wird auch von Großunternehmen geschätzt. Ausführlichere Informationen zu Microsoft Azure finden Sie hier.

Microsoft unterstützt mehr als 90 Compliancezertifizierungen für Regionen weltweit. Um sicherzustellen, dass stets auch die neuesten Sicherheits- und Compliance-Anforderungen erfüllt werden, wird Microsoft regelmäßig geprüft und überwacht – durch Audits und Selbsteinschätzungen, die an externe Prüfer gesendet werden.

Sicherheitszertifizierungen

ISO/ IEC 27000:2018 Informationstechnik
Sicherheitsverfahren – Informations-sicherheitsmanagementsysteme – Überblick und Terminologie

ISO/IEC 27001:2015 Informationstechnik
Sicherheitsverfahren – Informations-sicherheitsmanagementsysteme – Anforderungen

FedRAMP High
S Federal Risk and Authorization Management Program (NIST SP 800-53 800)

FIPS 140-2
Bundesstandard für Informationsverarbeitung

Security Organization Controls
(SOC 1, SOC 2, und SOC 3)

EU-Datenschutzgrundverordnung (DSGVO)

Health Information Trust Alliance (HITRUST)

National Health Service (NHS) Information Governance (IG) Toolkit (UK)

United Kingdom General Data Protection Regulation und Data Protection Act 2018

Hébergeurs de Données de Santé (HDS)

e Health Insurance Portability and Accountability Act (HIPAA)

FedRAMP

Azure

Datensicherheit und Verschlüsselung

HTTPS-Verschlüsselung
Diktate werden immer mit AES-256-Bit-Verschlüsselung nach Industriestandard erstellt, gesendet und gespeichert – in der Web-App mit sicherer Microsoft Azure-Umgebung, in der iOS- oder Android-App auf dem Smartphone.

Einloggen
Benutzer müssen ihr eigenes Passwort definieren, das jederzeit zurückgesetzt werden kann. Passwörter müssen mindestens 8 Zeichen lang sein (mit mindestens einem Großbuchstaben, einem Kleinbuchstaben und einer Ziffer).

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

Datensicherung & Wiederherstellung
Benutzer können Backups 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.

Dateizugriff
Diktate können nur von autorisierten Usern und mit Benutzername und Passwort abgerufen werden. Benutzerverwaltung und Backup sind nur für Administratoren (nicht alle SpeechLive-Benutzer) verfügbar.

Zahlung
Die Zahlungstransaktion erfolgt über eine unserer zertifizierten Zahlungsplattformen Unzer und authorized.net, die beide den Payment Card Industry Data Security Standard (PCI DSS) erfüllen, um sicherzustellen, dass Zahlungsinformationen in einer sicheren Umgebung verarbeitet, gespeichert oder übertragen werden.

Speech to Text Service

Datentransfer
Alle Audiodateien, die an unseren Speech to Text Service verschickt werden, werden sicher über einen verschlüsselten Kanal gesendet. Wir verwenden Https sowohl für die Client-zu-Server- als auch für die Server-zu-Server-Kommunikation. Abschriften werden über eine sichere SignalR-https-Verbindung gesendet.

Dateiverarbeitung
Die Spracherkennungs-Engine verwendet Datenserver in den USA und der EU, die den höchsten Sicherheitsstandards entsprechen.

Datenspeicher
Wenn Sie die Desktop- oder mobile App für unseren Speech to Text Service verwenden, werden keine Audio- oder Textdateien auf unseren Servern gespeichert. Die Audio- oder Textdateien werden lediglich durch unsere Server geschickt. Wenn Sie die Web Version verwenden, werden Ihre Audio- oder Textdateien kurzfristig zwischengespeichert und nach der Spracherkennung wieder automatisch gelöscht. Die Dateien werden in verschlüsselter Form in Ihrem SpeechLive Konto gespeichert und nur Sie können auf sie zugreifen.

Schreibservice

Die Verarbeitung der Diktate erfolgt durch sichere Anbieter von Spracherkennungslösungen. Die Diktate werden über verschlüsselte Https-Verbindungen an sichere Server übertragen. Diktate werden nach der Transkription gelöscht und nicht auf den Partnerservern gespeichert.

Mitarbeiter-Zugriffssicherheit

Zugang nur für geschulte Mitarbeiter
Nur geschulte Mitarbeiter haben Zugriff auf das System für Wartung, Support und Entwicklung.

Geheimhaltungsvereinbarung
Alle Mitarbeiter mit Zugriff auf Benutzerdateien müssen eine spezielle Sicherheitsschulung absolvieren und eine Geheimhaltungsvereinbarung (NDA) unterzeichnen. Diese Geheimhaltungsvereinbarung dient dem Schutz der vertraulichen und personenbezogenen Daten, die Speech Processing Solutions seinen Mitarbeitern anvertraut.

Geräte mit Zugriffskontrollverfahren
Alle geschulten Mitarbeiter von Philips, die Zugriff auf Benutzerdateien haben, interagieren sicher mit diesen Daten, indem sie ein Gerät mit entsprechenden Zugriffskontrollverfahren verwenden.

Endgerätesicherheit
Wir verwenden eine VPN-Verbindung, um sicherzustellen, dass Mitarbeiter, die Zugriff auf sensible Daten haben, dies sicher von mehreren Endpunkten aus über unser Unternehmensnetzwerk tun.

Mitarbeitercomputer-Kontrolle
Alle Computer der Mitarbeiter von Philips werden mit Virenschutz, Festplattenverschlüsselung, automatischer Geräteblockierung und Sicherheitspatches überwacht.

Lieferanten

Im Rahmen unserer strikten Lieferantenmanagementrichtlinie arbeiten wir nur mit branchenführenden Dienstleistern zusammen. Jeder neuer Anbieter wird einem umfassenden Sicherheitsaudit unterzogen, bevor wir mit ihm zusammenarbeiten. Auf diese Weise können wir sicherstellen, dass die höchsten Sicherheits- und Compliance-Standards erfüllt werden.

www.philips.com/dictation