PHILIPS

SpeechLive

Gegevensbeveiliging en - bescherming

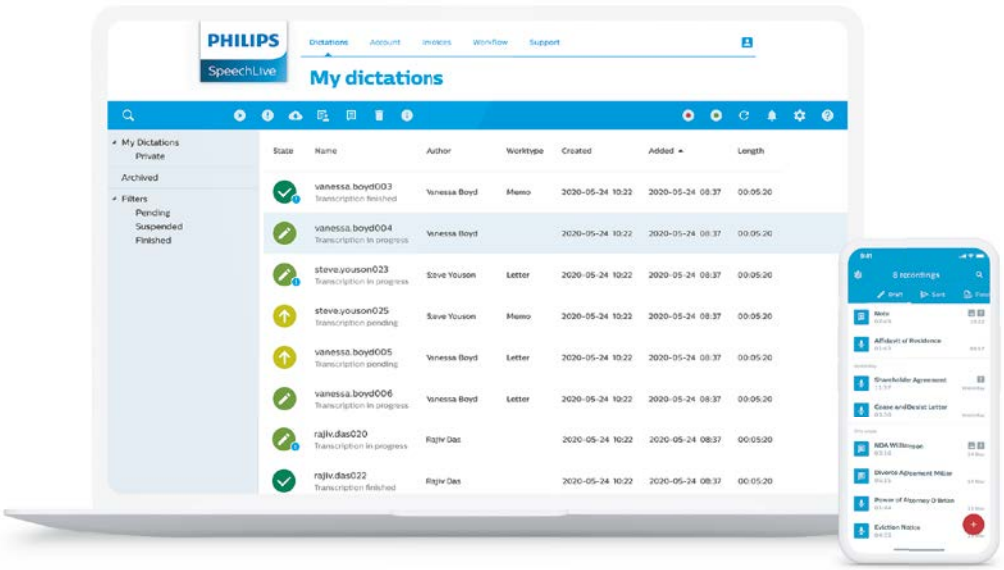
Philips SpeechLive dicteer- en transcriptieoplossing op het web

Gegevensbeveiliging en -bescherming

De Philips SpeechLive dicteer- en transcriptieoplossing op het web is een browsergebaseerde workflowservice waarmee drukbezette professionals hun stem snel en efficiënt in tekst kunnen omzetten, waar en wanneer ze maar willen.

De cloudgebaseerde oplossing biedt gebruikers een coherente en betrouwbare dienst voor spraak-naar-tekst en documentatiestroom, ongeacht of ze vanuit hun kantoor, thuis of onderweg werken. Ze kunnen ook eender welk invoerapparaat gebruiken om op te nemen, of het nu hun PC is, of hun mobiele telefoon.

Duizenden klanten over de hele wereld en uit diverse sectoren vertrouwen hun gegevens aan Philips SpeechLive toe. Bij het bieden van deze allesomvattende flexibiliteit heeft Philips steeds de grootste aandacht besteed aan de gegevensbeveiliging, zelfs in de ontwikkelingsfase van de oplossing.



ISO 9001:2015 CERTIFIED COMPANY

GDPR READY

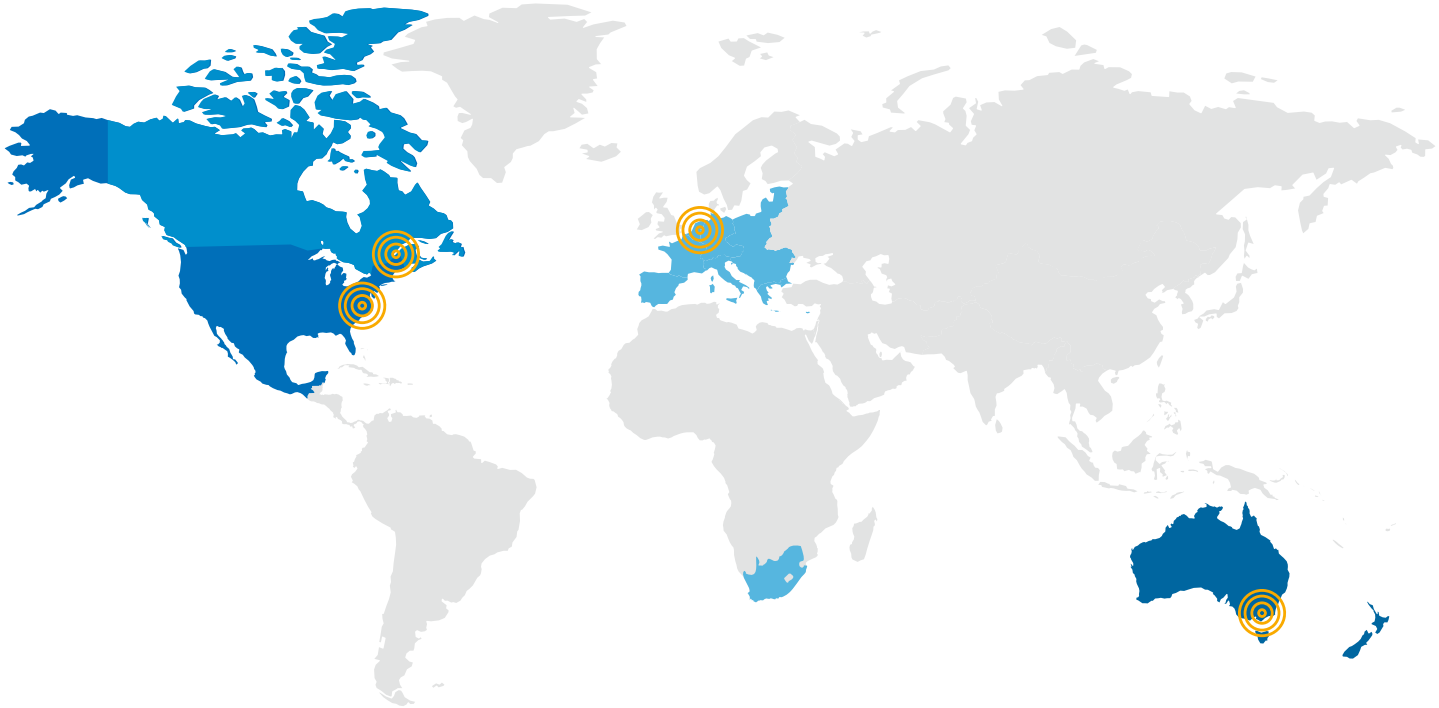
CCPA READY

Data opslag

Accountgegevens (met betrekking tot uw facturering) zijn opgeslagen op beveiligde dataservers in Oostenrijk.

Dictaten (geluidsopnamen en bestandsbijlagen zoals foto's en documenten) worden regionaal op Microsoft Azure servers opgeslagen om te voldoen aan de wettelijke vereisten, zodat ze snel toegankelijk zijn:

Verenigde Staten: Boydton, Virginia
Canada: Quebec City
Europa: Nederland
Australië en Nieuw-Zeeland: Victoria



Microsoft Azure

Philips SpeechLive heeft gekozen voor Microsoft Azure als hosting partner voor dictaten (geluidsopnamen en bestandsbijlagen), omdat zij ‘s werelds grootste leverancier op bedrijfsniveau zijn van een platform voor cloud-gehoste oplossingen.

Microsoft Azure hanteert de striktste veiligheidsnormen en -processen om het hoogste niveau van gegevensbeveiliging en -bescherming te garanderen. Het voert voortdurend penetratietests uit en werkt aan het opsporen en voorkomen van bedreigingen in domeinen als onbevoegde inbraak en denial-of-service.

Uptime betrouwbaarheid
Microsoft Azure services zijn zeer betrouwbaar. Microsoft gaat er prat op een uptime-garantie van 99.9% te beloven, 24 uur per dag, 7 dagen per week en 365 dagen per jaar.

Microsoft Azure voert een ‘lights out’-beleid, wat betekent dat verschillende maatregelen zijn genomen om verrichtingen te beschermen tegen:

- Stroomuitval
- Fysiek binnendringen
- Netwerkuitval

Hun datacenters voldoen aan de toepasselijke industrienormen voor fysieke beveiliging en betrouwbaarheid, en worden beheerd, gemonitord en bestuurd door operationele medewerkers van Microsoft. Microsoft heeft naar eigen zeggen ook meer dan 1 miljard dollar geïnvesteerd in zijn R&D voor beveiliging en beschikt over 3.500 cyberbeveiligingsexperts.

Microsoft Azure is dan ook een van de populairste providers wereldwijd, zelfs voor grote ondernemingen. Meer gedetailleerde informatie over Microsoft Azure is hier te vinden, klik hier.

Microsoft ondersteunt meer dan 90 wereldwijde voorschriften. Om ervoor te zorgen dat het aan alle ontwikkelingen en vereisten inzake beveiliging en compliance voldoet, wordt Microsoft geregeld geaudit en legt het zelfevaluaties voor aan externe auditors.

Azure

Beveiligingscertificaten

ISO/ IEC 27000:2018 Informatietechnologie
Beveiligingstechnieken –
Informatiebeveiligingsbeheersystemen –
Overzicht en vocabulaire

ISO/IEC 27001:2015 Informatietechnologie
Beveiligingstechnieken –
Informatiebeveiligingsbeheersystemen –
Vereisten

Verenigd Koninkrijk General Data Protection Regulation en Data Protection Act 2018

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

FIPS 140-2
Federal Information Processing Standard

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

EU Algemene Verordening Gegevensbescherming (AVG)

Health Information Trust Alliance (HITRUST)

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

Hébergeurs de Données de Santé (HDS)

e Health Insurance Portability and Accountability Act (HIPAA)

Gegevensbeveiliging en encryptie

HTTPS-encryptie
Dictaten worden altijd gecreëerd, verzonden en bewaard met de industriestandaard AES 256-bit encryptie – in de web app die gebruik maakt van de beveiligde Microsoft Azure omgeving, in de iOS of Android app op de telefoon.

Login
Gebruikers moeten hun eigen wachtwoord definiëren, dat op elk moment kan worden gereset. Wachtwoorden moeten minimaal 8 karakters bevatten (waarvan minstens één hoofdletter, één kleine letter en één cijfer).

Multifactorauthenticatie (MFA)
Multifactorauthenticatie op basis van e-mail voegt een extra beveiligingsniveau toe. SpeechLive maakt gebruik van een beveiligde authenticatiedienst van Microsoft, die veiligheidsrisico's zoals brute-force attacks voorkomt. Deze instelling kan worden opgelegd door de accountbeheerder.

Back-up en terughalen van gegevens
Gebruikers kunnen back-ups maken van alle dictaten om ze later, indien nodig, terug te halen. Per vergissing verwijderde bestanden kunnen tot 30 dagen door de accountbeheerder worden teruggehaald.

Toegang tot bestanden
Dictaten kunnen alleen worden bekeken door de eigenaar en met een gebruikersnaam en wachtwoord. Gebruikersbeheer en back-up zijn alleen beschikbaar voor beheerders (niet voor alle SpeechLive gebruikers).

Betalingen
Het betalingsproces verloopt via de betaalplatformen Unzer en authorize.net die beide voldoen aan de Payment Card Industry Data Security Standard (PCI DSS) om ervoor te zorgen dat betalingsinformatie wordt verwerkt, opgeslagen of verzonden in een veilige omgeving.

Speech-to-text service

Datatransfer
Alle geluidsbestanden die naar onze speech-to-text service worden gezonden, worden veilig verzonden via een versleuteld kanaal. Wij gebruiken zowel https voor client naar server, als server naar server communicatie. Transcripties worden verzonden via een beveiligde SignalR https verbinding.

Bestandsverwerking
De spraakherkenningsmotor maakt gebruik van servers met de hoogste veiligheidsnormen in de VS en de EU.

Gegevensopslag
Als u de desktop- of mobiele app voor onze speech-to-text service gebruikt, wordt er geen audio of tekst op onze servers opgeslagen. De geluids- en tekstbestanden passeren gewoon onze servers. Als u de webversie gebruikt, worden zowel de audio als de transcriptie tijdens de spraakherkenning tijdelijk opgeslagen en daarna automatisch gewist.
De bestanden worden versleuteld opgeslagen in uw SpeechLive account, alleen voor uw toegang.

Transcriptieservice

De dictaten worden verwerkt door zorgvuldig geselecteerde externe partnerbureaus en vervolgens via https naar hun beveiligde servers verzonden. De dictaten worden na transcriptie verwijderd en niet opgeslagen op de partnerservers. Deze service is enkel beschikbaar voor de talen Engels, Frans en Duits.

Toegangsbeveiliging voor personeel

Alleen voor opgeleid personeel
Alleen opgeleid personeel heeft toegang tot het systeem voor onderhoud, ondersteuning en verdere ontwikkeling.

Geheimhoudingsovereenkomst
Alle personeelsleden die toegang hebben tot de bestanden van de gebruikers moeten een speciale opleiding volgen en een geheimhoudingsverklaring (NDA) ondertekenen. Deze NDA dient ter berscherming van de vertrouwelijke en persoonlijke gegevens die Speech Processing Solutions aan haar medewerkers toevertrouwt.

Logische toegang
Alle getrainde Philips-medewerkers die toegang hebben tot de bestanden van gebruikers, gaan op een veilige manier met deze gegevens om, met behulp van een apparaat met procedures voor toegangscontrole.

Beveiliging van eindstations
Wij maken gebruik van een VPN-verbinding om ervoor te zorgen dat werknemers die toegang kunnen hebben tot gevoelige gegevens, dit veilig doen vanaf ons bedrijfsnetwerk vanaf meerdere eindpunten.

Personeelscomputercontrole
Alle computers van Philips-medewerkers worden gemonitord met antivirus, schijfversleuteling, automatische blokkering van apparaten en beveiligingspatches.

Leveranciers

Als onderdeel van ons strikte leveranciersbeleid werken wij alleen samen met dienstverleners die in de sector toonaangevend zijn. Elke nieuwe leverancier ondergaat een uitgebreide veiligheidsaudit voordat wij hem bij onze activiteiten betrekken. Op die manier kunnen wij garanderen dat aan de hoogste normen inzake veiligheid en naleving wordt voldaan.

www.philips.com/dictation