



PHILIPS

SpeechLive

Beveiliging



Gegevensbeveiliging en -bescherming

**Philips SpeechLive dicteer- en
transcriptieoplossing op het web**

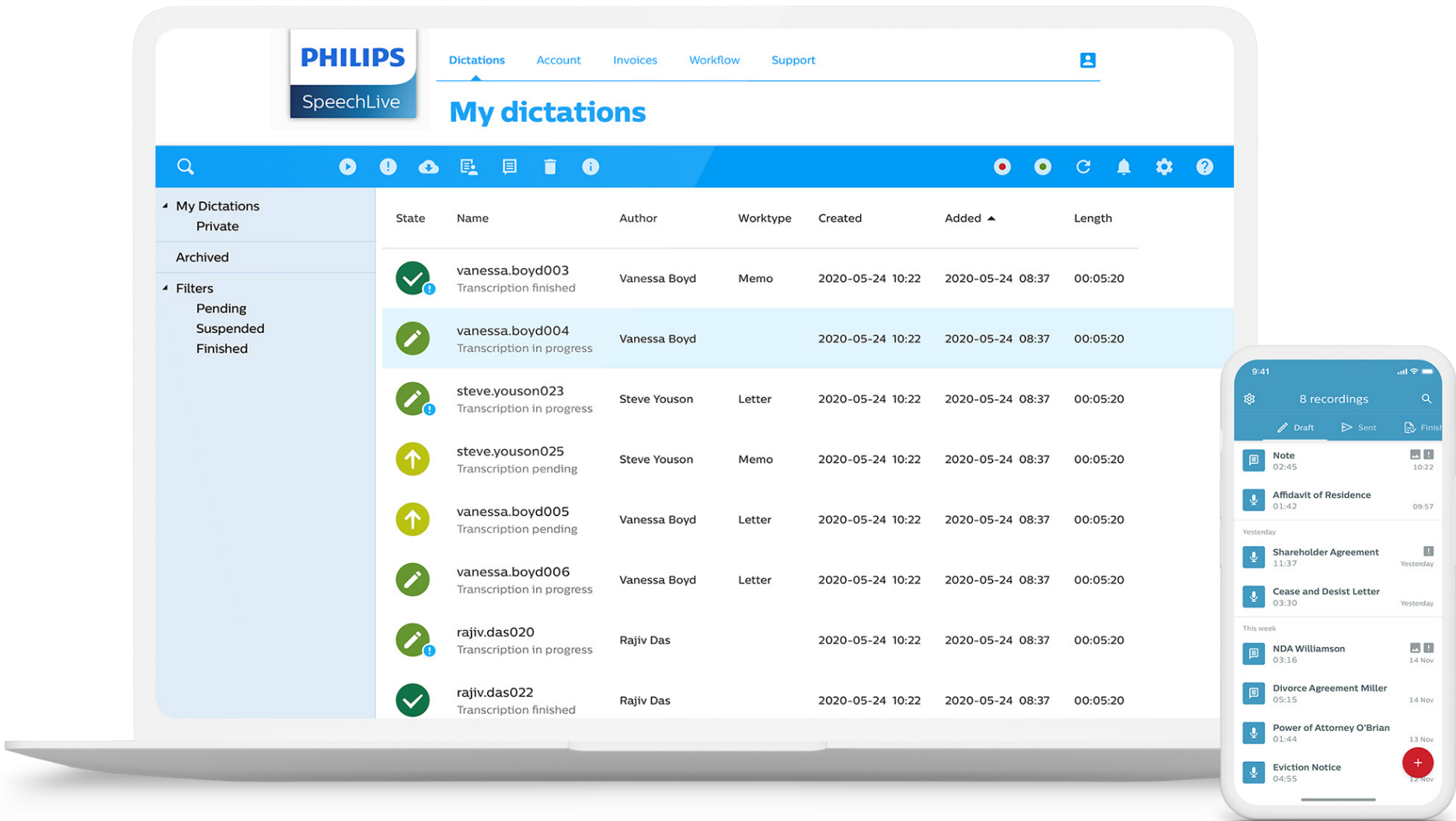
Gegevensbeveiliging en -bescherming

Philips SpeechLive

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. Onderweg kunnen ze ook eender welk invoerapparaat gebruiken om op te nemen (pc of mobiele telefoon).

Duizenden klanten van 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.



Ontworpen met het oog op veiligheid

Voor de hosting van Philips Speechlive werkt Philips Dictation met Microsoft Azure, dat als partner werd gekozen omdat het 's werelds grootste leverancier op bedrijfsniveau is van een platform voor cloud-gehoste oplossingen.

MS 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.

De Microsoft Azure diensten 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.

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

- stroomuitval
- fysiek binnendringen
- netwerkuitval

Microsoft Azure beveiligingscertificaten

AS/NZS ISO/IEC 27000 serie – Informatiebeveiligingsbeheer

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

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

ISO/IEC 27002:2015 – Informatietechnologie
- Beveiligingstechnieken - Praktijkcode voor
informatiebeveiligingscontroles

ISO/IEC 27003:2017 – Informatietechnologie
- Beveiligingstechnieken -
Informatiebeveiligingsbeheersysteem -
Begeleiding

AS ISO/IEC 27004:2018 –
Informatietechnologie - Beveiligingstechnieken
- informatiebeveiligingsbeheer - Monitoring,
meting, analyse en evaluatie

ISO/IEC 27005:2018 – Informatietechnologie
- Beveiligingstechnieken Beheer van
informatiebeveiligingsrisico's

Verenigd Koninkrijk General Data Protection
Regulation en Data Protection Act 2018

EU Algemene Verordening Gegevensbescherming
(AVG)

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

Security Organisation Controls (SOC 1, SOC 2
en SOC 3) General Data Protection Regulation
en Data Protection Act 2018 van het Verenigd
Koninkrijk

EU Algemene Verordening Gegevensbescherming
(AVG)

Security Organisation Controls (SOC 1, SOC 2, and
SOC 3)



De MS Azure datacenters voldoen aan de toepasselijke industriestandaarden 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 een team van meer dan 3.500 cyberbeveiligings-experts. Microsoft Azure is dan ook een van de populairste providers wereldwijd, zelfs voor grote ondernemingen. Meer gedetailleerde informatie over Microsoft Azure is te vinden op: <https://azure.microsoft.com/en-us/overview/trusted-cloud/>

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 zelfevaluatie voor aan externe auditors.

Data centers

Enkele van de voorschriften waaraan de datacenters voldoen:

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

Uw dictaten (geluidsopnamen + bijlagen zoals foto's en documenten) worden regionaal op servers opgeslagen om te voldoen aan de wettelijke vereisten, zodat ze snel toegankelijk zijn.

- Verenigde Staten: Oost-VS (Virginia)
- Canada: Oost-Canada (Quebec City)
- Europa: West-Europa (Nederland)
- Australië & Nieuw-Zeeland: Zuidoost-Australië (Victoria)



Gegevensbeveiliging & encryptie

HTTPS-encryptie

Dictaten worden altijd verzonden via versleutelde HTTPS-kanalen.

De dictaten worden versleuteld en opgeslagen in het MS Azure systeem.

De dictaten die door de mobiele apps worden gemaakt, worden versleuteld opgeslagen op de mobiele telefoon.

Welke encryptie wordt gebruikt

We gebruiken de industriestandaard AES 256-bit (bij direct gebruik van de software, bij gebruik van SpeechExec software of de smartphone app).

Is er DSGVO-conformiteit?

Als Europese organisatie zijn we wettelijk verplicht de DSGVO-wetgeving na te leven.

Dictaten back-up

Maak back-ups van al uw dictaten in SpeechLive, om ze later terug te halen.

Verwijderde dictaten terughalen

Per vergissing verwijderde bestanden kunnen tot 30 dagen door de accountbeheerder worden teruggehaald.

Login en toegangsbeveiliging

Elke workflowgebruiker moet zijn eigen wachtwoord definiëren, dat op elk moment kan worden gereset.

De 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).

Alleen getraind Philips Dictation-personeel heeft toegang tot het systeem voor onderhoud, ondersteuning en verdere ontwikkeling.

Multifactorauthenticatie (MFA)

Een extra beveiligingsniveau is mogelijk met behulp van de multifactor-authenticatie te gebruiken. De beheerder kan de extra login afdwingen.

SL maakt gebruik van een beveiligde authenticatiedienst van Microsoft, die veiligheidsrisico's zoals brute-force attacks voorkomt.

Veiligheid tijdens het betalingsproces

Gebruikers kunnen een Philips SpeechLive-abonnement aanschaffen met eender welke gangbare creditcard. De aankooptransactie verloopt via een gecertificeerd betaalplatform zoals Unser en authorized.net.

Extra functies van Philips SpeechLive

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.

Spraak-naar-tekst (STT)

De dictaten worden door een beveiligde STT-dienstverlener verwerkt. Ze worden via https verzonden en na transcriptie verwijderd.



