PHILIPS

SpeechLive

Seguridad y privacidad de datos

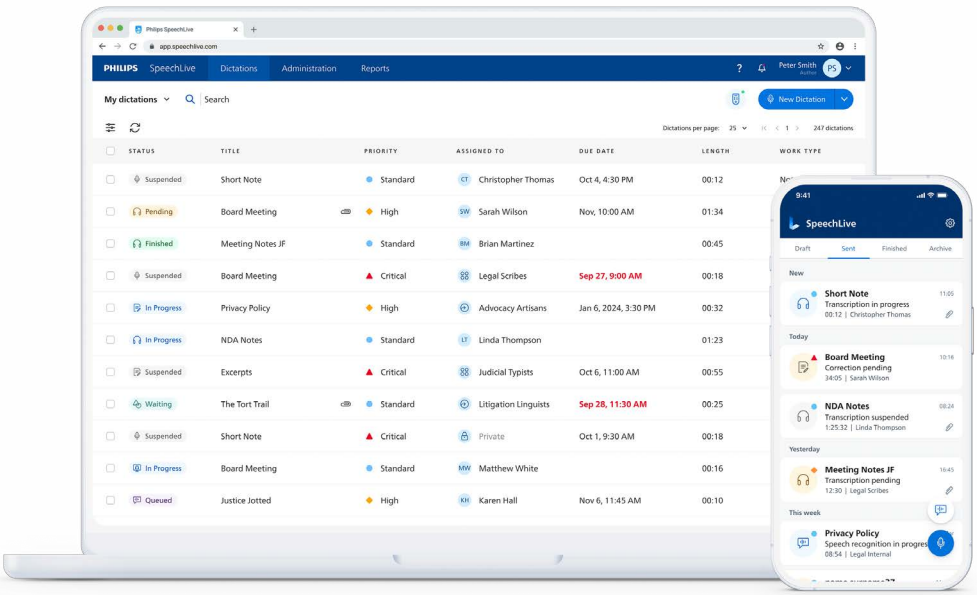
Solución de dictado y transcripción en la nube Philips SpeechLive

Seguridad y privacidad de datos

La solución de dictado y transcripción en la nube Philips SpeechLive es un servicio de flujo de trabajo basado en el navegador que ayuda a los profesionales atareados a convertir su voz rápida y eficientemente en texto, desde cualquier lugar y en cualquier momento.

La solución basada en la nube ofrece a sus usuarios un servicio de voz a texto y de flujo de trabajo de documentos coherente y fiable, trabajen los usuarios en su oficina, desde casa o sobre la marcha. También pueden utilizar cualquier dispositivo de entrada para grabar, ya sea su PC o su teléfono móvil cuando estén de camino.

Miles de clientes en el mundo entero y distintos sectores confían sus datos a Philips SpeechLive. Al ofrecer una flexibilidad tan amplia, la seguridad de los datos siempre ha sido una de las mayores preocupaciones para Philips, incluso en la fase de desarrollo de la solución.



ISO 9001:2015 CERTIFIED COMPANY

GDPR READY

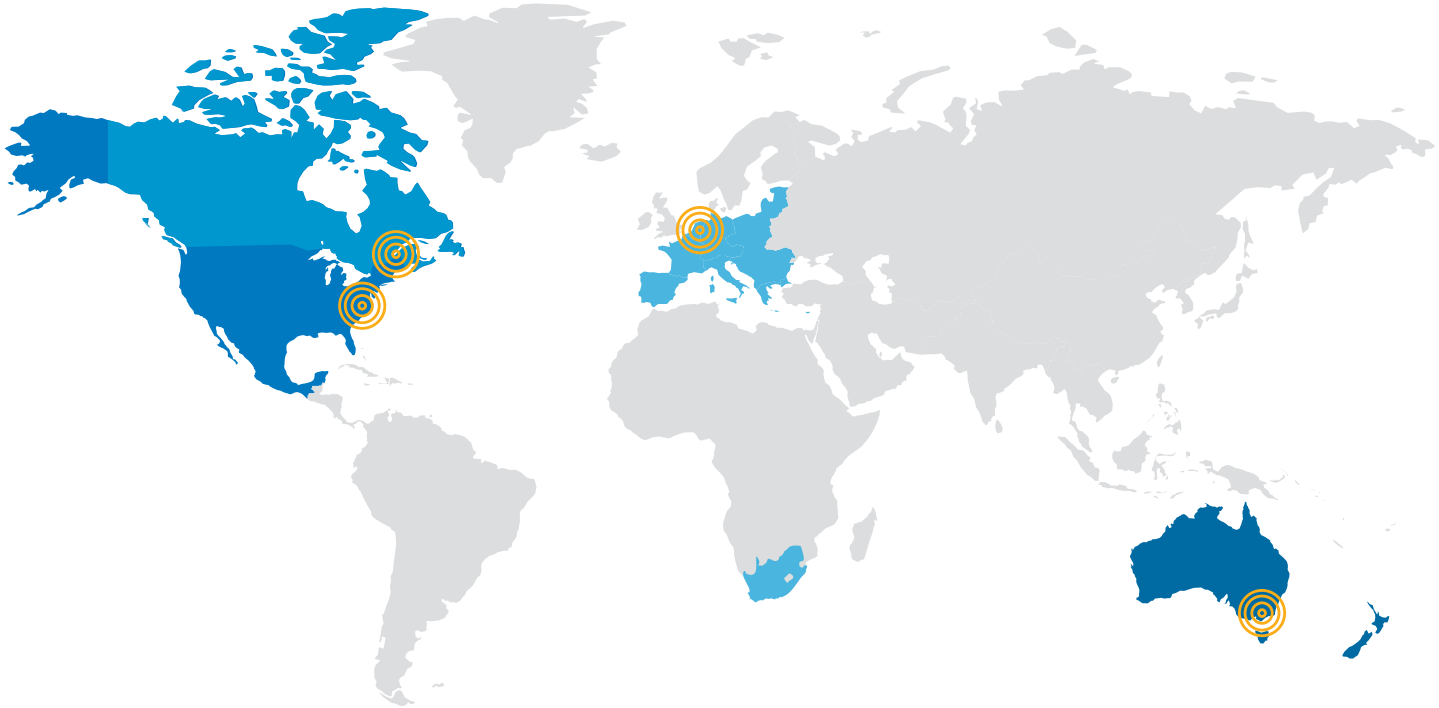
CCPA READY

Almacenamiento de datos

Los datos de la cuenta (relacionados con su facturación) se almacenan en servidores de datos seguros en Austria.

Sus dictados (grabaciones de audio + anexos como fotos y documentos) se guardan regionalmente en servidores de Microsoft Azure para cumplir los requisitos legales, lo cual permite un acceso más rápido:

Estados Unidos: Boydton, Virginia
Canadá: Ciudad de Quebec
Europa y Sudáfrica: Países Bajos
Australia y Nueva Zelanda: Victoria



Microsoft Azure

El dictado de Philips trabaja con Microsoft Azure para alojar Philips SpeechLive. Se optó por Microsoft Azure como socio por ser el principal proveedor mundial a nivel de empresas de una plataforma para soluciones alojadas en la nube.

Microsoft Azure mantiene estrictas normas y procesos de seguridad para garantizar el máximo nivel de privacidad y seguridad de los datos. Continuamente realizan pruebas de penetración y trabajan en la detección prevención de amenazas en áreas como la intrusión no autorizada y la denegación de servicio.

Fiabilidad en tiempo

Los servicios de Microsoft Azure son muy fiables. Microsoft se enorgullece de prometer una garantía de disponibilidad del 99,9%, 24 horas al día, 7 días a la semana y 365 días al año.

Microsoft Azure implementa una política “Lights out” lo cual significa que dispone de distintas medidas para proteger las operaciones de:

- Un fallo de alimentación
- Una intrusión física
- Interrupciones de la red.

Sus centros de datos cumplen las normas industriales aplicables en materia de seguridad física y fiabilidad; la gestión, el monitoreo y la administración corren a cargo de personal de operaciones de Microsoft. Microsoft afirma también que ha invertido mas de 1.000 millones de USD en su I+D de seguridad y cuenta con más de 3.500 expertos en ciberseguridad en su equipo.

Por consiguiente, Microsoft Azure es uno de los proveedores más populares a nivel mundial, incluso para empresas grandes. Para información más detallada sobre Microsoft Azure, visite esta página.

Microsoft apoya más de 90 reglamentos mundiales. Para garantizar que se cumplen todos los avances y requisitos en materia de seguridad y cumplimiento, Microsoft es auditada regularmente y somete autoevaluaciones a controles de auditores externos.

Azure

Certificados de seguridad

ISO/ IEC 27000:2018 Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Resumen y vocabularioI

SO/IEC 27001:2015 Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Requisitos

United Kingdom General Data Protection Regulation and 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

Controles de la organización de la seguridad (SOC 1, SOC 2, and SOC 3)

Reglamento General de Protección de Datos (RGPD) **de la UE**

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)

FedRAMP

Seguridad de datos y cifrado

Cifrado HTTPS
Los dictados se crean, envían y almacenan siempre con el cifrado AES de 256 bits estándar del sector en la aplicación web utilizando el entorno seguro de Microsoft Azure Microsoft Azure, en el aplicación para smartphones iOS o Android.

Acceso
Los usuarios deben establecer su propia contraseña, que se puede reiniciar en cualquier momento. Las contraseñas deben ser como mínimo de 8 caracteres (con al menos una mayúscula, minúscula y un número).

Autenticación multifactor (MFA)
La autenticación multifactor por correo añade una capa adicional de seguridad. SpeechLive utiliza un servicio de autenticación segura de que previene los riesgos de seguridad como los ciberataques. Esta opción se puede aplicar por el administrador de la cuenta.

Copia de seguridad y recuperación de datos
Los usuarios pueden hacer una copia de seguridad de los dictados y serán accesible en cualquier momento. Los archivos borrados por accidente se pueden recuperar por el administrador durante 30 días.

Acceso a los archivos
Los dictados sólo pueden consultarse por su propietario, utilizando un nombre de usuario y contraseña. La gestión de usuarios y las copias de seguridad solo están disponibles para los administradores (no todos los usuarios de SpeechLive).

Pago
La transacción se realiza a través de una plataforma de pago certificada, como Unzer, y de una red autorizada que cumple la norma de seguridad de datos de las tarjetas de pago (PCI DSS) para garantizar que la información de pago se procesa, almacena o transmite en un entorno seguro.

Reconocimiento de voz

Envío de datos
Todos los archivos de audio enviados al servicio de reconocimiento de voz se envían por un canal encriptado. Utilizamos tanto https para cliente-servidor y comunicación servidor-servidor. Las transcripciones son enviados a través de un sitio https seguro.

Procesamiento de datos
El motor de reconocimiento de voz utiliza los servidores con los más altos estándares de seguridad de Estados Unidos y la UE.

Almacenamiento de datos
Si utiliza la aplicación de PC o móvil para nuestro servicio de voz a texto, no se guarda ningún audio o texto en nuestros servidores. Los archivos de audio y texto simplemente pasan por nuestros servidores.
Si utiliza la versión web, tanto el audio como la transcripción se guardan temporalmente durante el reconocimiento del habla y luego se eliminan automáticamente.
Los archivos se guardan en un formato encriptado en su cuenta de SpeechLive, sólo para su acceso.

Acceso seguro para el personal

Acceso reservado a personal capacitado
Sólo el personal capacitado tiene acceso al sistema para el mantenimiento, la asistencia y el desarrollo posterior.

Acuerdo de no divulgación
Todo el personal con acceso a los archivos de los usuarios deben someterse a una formación especial en materia de seguridad y firmar un acuerdo de confidencialidad. Este acuerdo sirve para proteger los datos confidenciales y personales que Speech Processing Solutions confía a sus empleados.

Acceso lógico
Todo el personal formado de Philips que tiene acceso a los archivos de los usuarios interactúa con estos datos de forma segura, utilizando un dispositivo con control de acceso.

Seguridad del punto de acceso
Utilizamos una conexión VPN para garantizar que los empleados que puedan acceder a datos sensibles lo hagan de forma segura desde nuestra red interna desde múltiples puntos de acceso.

Control de herramientas
Todos los ordenadores del personal de Philips se controlan mediante encriptación, bloqueo automático de dispositivos y parches de seguridad.

Proveedores

Como parte de nuestra estricta política de gestión de proveedores, sólo cooperamos con los mejores proveedores de servicios de la industria. Cada nuevo proveedor se somete a una exhaustiva auditoría de seguridad antes de integrarlos en nuestras operaciones. De este modo, podemos garantizar el cumplimiento de las normas más estrictas de seguridad y conformidad.

www.philips.com/dictation