

PHILIPS



Philips SpeechLive

Privacidad y seguridad total
de los datos para sus dictados

Contenido

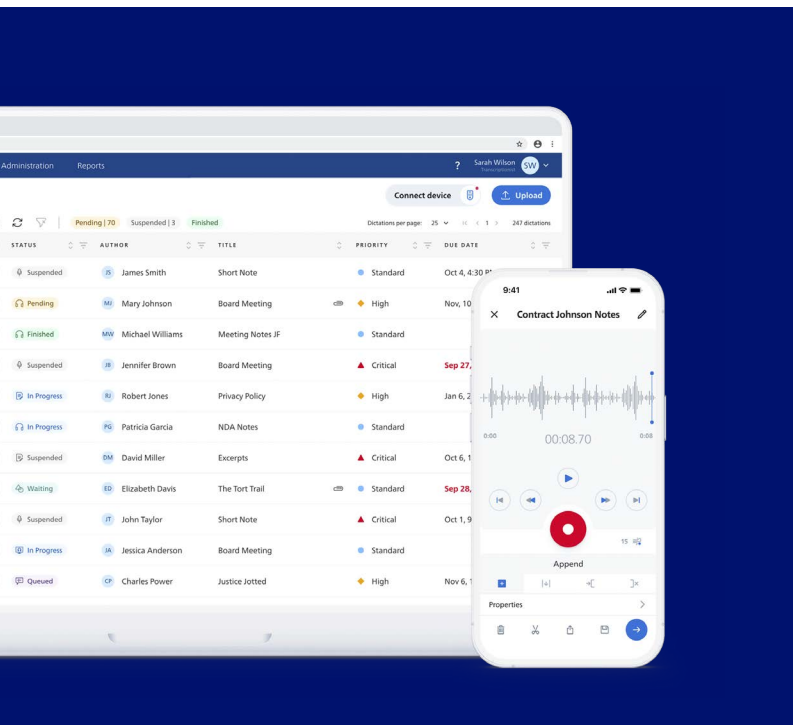
El más alto nivel de certificación	3
Seguridad y cifrado de datos	4
Almacenamiento de datos	5
Reconocimiento de voz y Asistente de IA	6
Seguridad de acceso del personal	7
Servicio de transcripción y otros proveedores	8



Protegiendo
cada palabra
que dice

El más alto nivel de certificación

Miles de clientes de todo el mundo y de diversas industrias confían sus datos a Philips SpeechLive. La seguridad de los datos siempre ha sido nuestra mayor prioridad, incluso en la fase de desarrollo de la solución.



Centro de confianza

El Centro de Confianza de SpeechLive ofrece acceso transparente a nuestra información de seguridad, cumplimiento y protección de datos.

Obtenga más información en
www.speechlive.com/trust



14001
Certified



GDPR
Compliant



9001
Certified



CCPA
Compliant



27001
Certified



EU AI Act
Compliant



HIPAA
Compliant

Seguridad y cifrado de datos

Philips SpeechLive garantiza que los usuarios puedan trabajar de forma segura y sin interrupciones. Con opciones confiables de respaldo y recuperación, no tiene que preocuparse por perder dictados importantes. El cifrado fuerte, la autenticación multifactor y el inicio de sesión único protegen sus datos y hacen que iniciar sesión sea simple y seguro, dándole la confianza de que su información permanece privada y su flujo de trabajo sigue siendo fluido.



Respaldo y recuperación total de datos

Los usuarios pueden crear copias de seguridad de todos los dictados para recuperarlos posteriormente si es necesario. Los dictados eliminados accidentalmente pueden ser restaurados por el administrador de la cuenta hasta 30 días después de haber sido eliminados.



Protegido por cifrado HTTPS

Los dictados siempre se crean, envían y almacenan con cifrado estándar de la industria AES de 256 bits, ya sea en la aplicación web utilizando el entorno seguro de Microsoft Azure, o en la aplicación iOS o Android en el teléfono.



Seguridad adicional con autenticación multifactor

La autenticación multifactor basada en correo electrónico (MFA) añade un nivel extra de seguridad. SpeechLive utiliza un servicio de autenticación seguro de Microsoft que previene riesgos de seguridad como ataques de fuerza bruta. La configuración puede ser aplicada por el administrador de la cuenta.



Inicio de sesión fácil con inicio de sesión único (SSO)

El inicio de sesión único reduce la molestia de tener que recordar más contraseñas. Cuando está activado, los usuarios pueden usar sus credenciales de Microsoft para iniciar sesión en SpeechLive de forma fácil y segura. El SSO también simplifica la vida de los administradores al reducir el número de cuentas de usuario gestionadas.



Proceso de pago seguro

Los pagos son procesados por nuestros proveedores de pago Unzer y Authorize.net, ambos cumplen con el Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS) para garantizar que la información de pago se procese, almacene o transmita en un entorno seguro.



Almacenamiento de datos

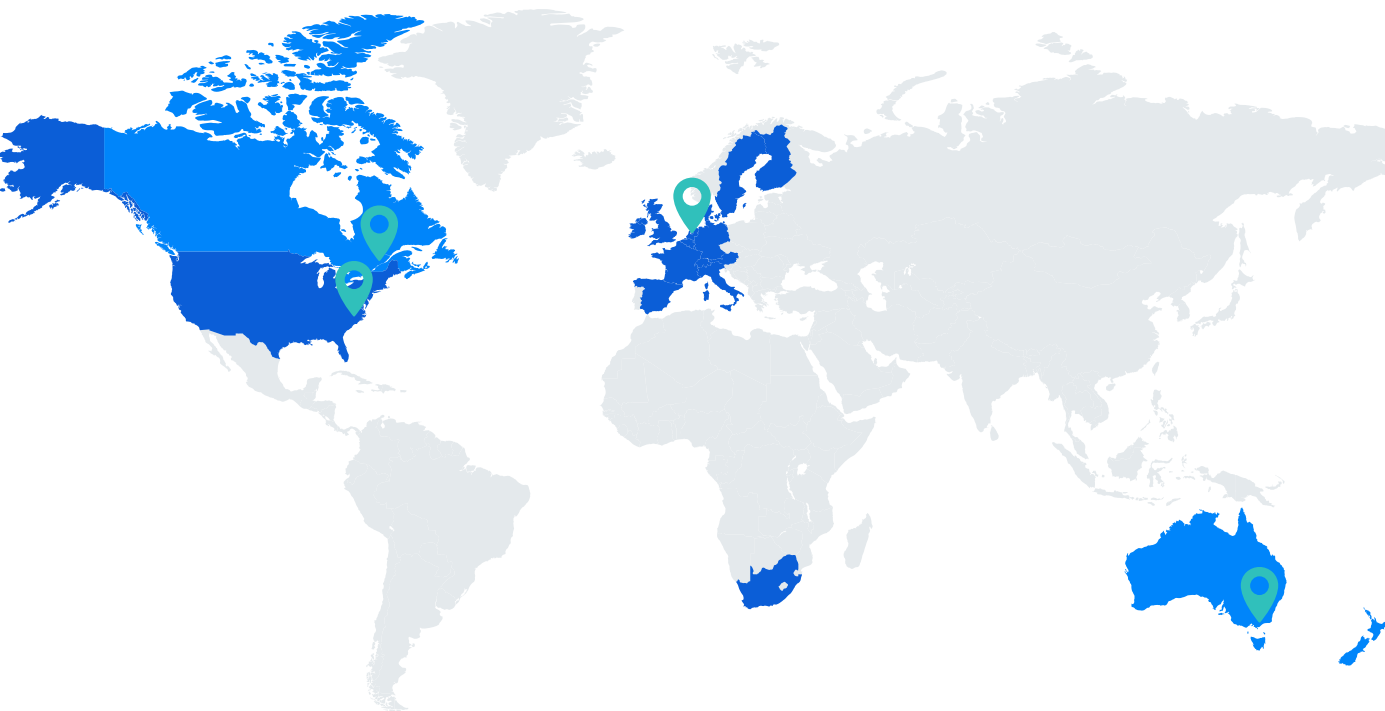
Philips SpeechLive utiliza Microsoft Azure para alojar dictados y archivos adjuntos, confiando en la principal plataforma de nube empresarial del mundo. Azure ofrece un 99,9% de tiempo de actividad y una protección robusta contra fallos de energía, intrusiones y caídas de red.

Los centros de datos de Microsoft cumplen con los más altos estándares de la industria y son monitoreados continuamente por equipos de operaciones dedicados. Con más de 4 mil millones de dólares invertidos en I+D de seguridad y más de 10.000 expertos en ciberseguridad, Azure es uno de los proveedores de nube más confiables a nivel mundial. Cumple con más de 100 regulaciones internacionales y se somete a auditorías regulares.

Todos los datos de SpeechLive se almacenan regionalmente en servidores de Azure para cumplir con los requisitos legales y garantizar un acceso rápido.

[Explore las ofertas de cumplimiento de Azure](#)

Australia y Nueva Zelanda	Victoria
Canadá	Ciudad de Quebec
Europa y Sudáfrica	Países Bajos
EE.UU.	Boydton, Virginia



Reconocimiento de voz y Asistente de IA

Tanto nuestro Reconocimiento de Voz como el Asistente de IA están diseñados con el más alto nivel de seguridad para mantener sus datos seguros. Su información se elimina automáticamente después del procesamiento y se almacena en un entorno dedicado y aislado.

Nos aseguramos de que no haya acceso a OpenAI ni entrenamiento de modelos de IA, y mantenemos estrictos estándares de cumplimiento con cifrado de datos de extremo a extremo, todo impulsado por el entorno de nube altamente seguro de Microsoft Azure.



Transferencia segura de datos

Todos los archivos de audio enviados a nuestro sistema de reconocimiento de voz se envían de forma segura a través de un canal cifrado. Utilizamos https tanto para la comunicación de cliente a servidor como de servidor a servidor. Las transcripciones se envían a través de una conexión https segura de SignalR.



Almacenamiento de datos

Si utiliza la aplicación de escritorio o móvil de nuestro servicio de reconocimiento de voz, no se guarda ningún audio ni texto en nuestros servidores. Los archivos de audio y texto simplemente pasan por nuestros servidores. Si utiliza la versión web, tanto su audio como la transcripción se guardan temporalmente durante el reconocimiento de voz y luego se eliminan automáticamente. Los archivos se guardan en formato cifrado en su cuenta de SpeechLive, solo para su acceso.



Procesamiento regional

El motor de reconocimiento de voz utiliza servidores con los más altos estándares de seguridad en EE. UU., Canadá, la UE y Australia.



Datos no utilizados para entrenamiento

Sus datos permanecen completamente privados y solo se utilizan para respaldar sus propias interacciones. Nunca se comparte con OpenAI, otros clientes o terceros, y no se utiliza para entrenar, reentrenar o mejorar ningún modelo de IA u otros productos sin su permiso explícito.

Seguridad de acceso del personal

Controlar el acceso del personal es clave para proteger la información sensible y prevenir el acceso no autorizado. Nuestros estrictos controles de acceso y auditorías regulares garantizan que nuestra seguridad se mantenga sólida y cumpla con los más altos estándares.



Control de activos

Todos los ordenadores del personal de Philips son monitoreados con antivirus, cifrado de disco, bloqueo automático de dispositivos y parches de seguridad. Todo el personal de Philips que tiene acceso a los archivos de los usuarios interactúa con estos datos de forma segura, utilizando un dispositivo con los procedimientos de control de acceso correspondientes.



Acuerdo de confidencialidad

Todo el personal con acceso a los archivos de los usuarios debe realizar una capacitación especial en seguridad y firmar un acuerdo de confidencialidad (NDA). Este NDA sirve para proteger los datos confidenciales y personales que Speech Processing Solutions confía a sus empleados.



Solo personal capacitado

Solo el personal capacitado tiene acceso al sistema para mantenimiento, soporte y desarrollo adicional.



Seguridad de los puntos finales

Utilizamos una conexión VPN para garantizar que los empleados que pueden tener acceso a datos sensibles puedan hacerlo de forma segura desde nuestra red corporativa y desde múltiples puntos finales.



Servicio de transcripción y otros proveedores

Como parte de nuestra estricta política de gestión de proveedores, solo cooperamos con proveedores de servicios líderes en la industria.

Las dictados enviados al servicio de transcripción SpeechLive son procesados por agencias externas asociadas, cuidadosamente seleccionadas, y luego enviados a través de https cifrado a sus servidores seguros. Las dictados se eliminan después de la transcripción y no se guardan en los servidores de los socios.

Cada nuevo proveedor se somete a una exhaustiva auditoría de seguridad antes de ser incorporado a nuestras actividades. De esta manera, podemos garantizar que se cumplan los más altos estándares de seguridad y cumplimiento.

