

PHILIPS



Philips SpeechLive

Full data privacy and
security for your dictations

Contents

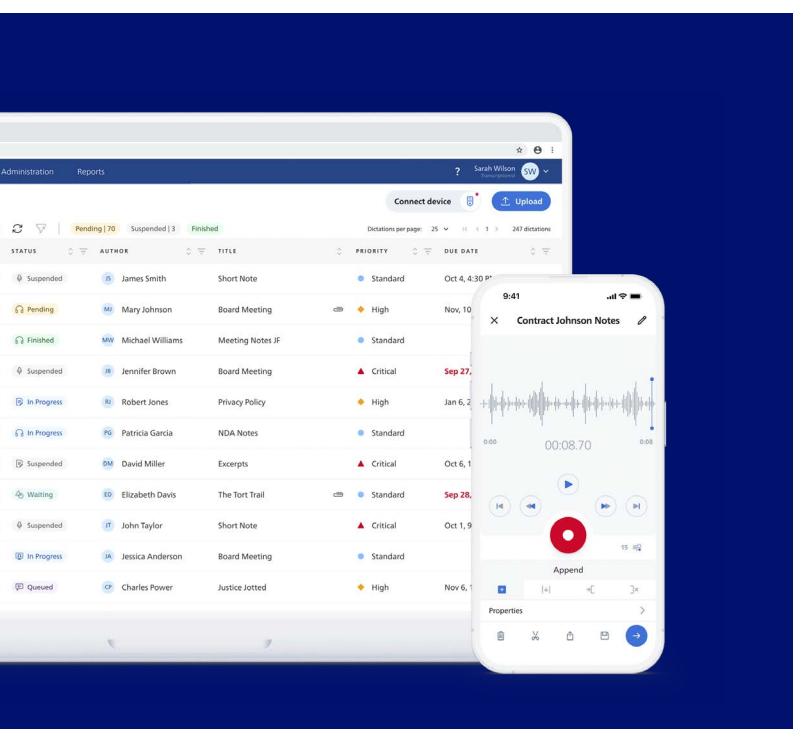
Highest level of certification	3
Data security and encryption	4
Data storage	5
Speech recognition and AI Assistant	6
Personnel access security	7
Transcription service and other vendors	8



Protecting
every word
you say

Highest level of certification

Thousands of customers from all over the world and various industries trust their data to Philips SpeechLive. Data security has always been our highest concern, even in the development phase of the solution.



Trust Center

The SpeechLive Trust Center offers transparent access to our security, compliance, and data protection information.

Learn more at www.speechlive.com/trust



14001
Certified



GDPR
Compliant



9001
Certified



CCPA
Compliant



27001
Certified



EU AI Act
Compliant



HIPAA
Compliant

Data security and encryption

Philips SpeechLive ensures that users can work securely and without interruption. With reliable backup and recovery options, you don't have to worry about losing important dictations. Strong encryption, multifactor authentication, and single sign-on protect your data and make logging in simple and safe – giving you confidence that your information stays private and your workflow remains smooth.



Backup and full data recovery

Users can create backups of all dictations, to recover them at a later point if necessary. Accidentally deleted dictations can be restored by the account administrator up to 30 days.



Protected by HTTPS encryption

Dictations are always created, sent, and stored with industry standard AES 256-bit encryption – in the web app using secure Microsoft Azure environment, in the iOS or Android app on the phone.



Extra security with Multifactor authentication

Email-based multi-factor authentication (MFA) adds an extra level of security. SpeechLive uses a secure authentication service by Microsoft that prevents security risks such as brute force attacks. The setting can be enforced by the account admin.



Easy login with Single sign-on (SSO)

Single sign-on reduces the hassle of having to remember more passwords. When activated, users can use their Microsoft credentials to easily and securely login to SpeechLive. SSO also simplifies administrators' lives by reducing the number of managed user accounts.



Secure payment process

Payments are processed by our payment providers Unzer and authorize.net that both meet Payment Card Industry Data Security Standard (PCI DSS) compliance to ensure that payment information is processed, stored, or transmitted in a secure environment.



Data storage

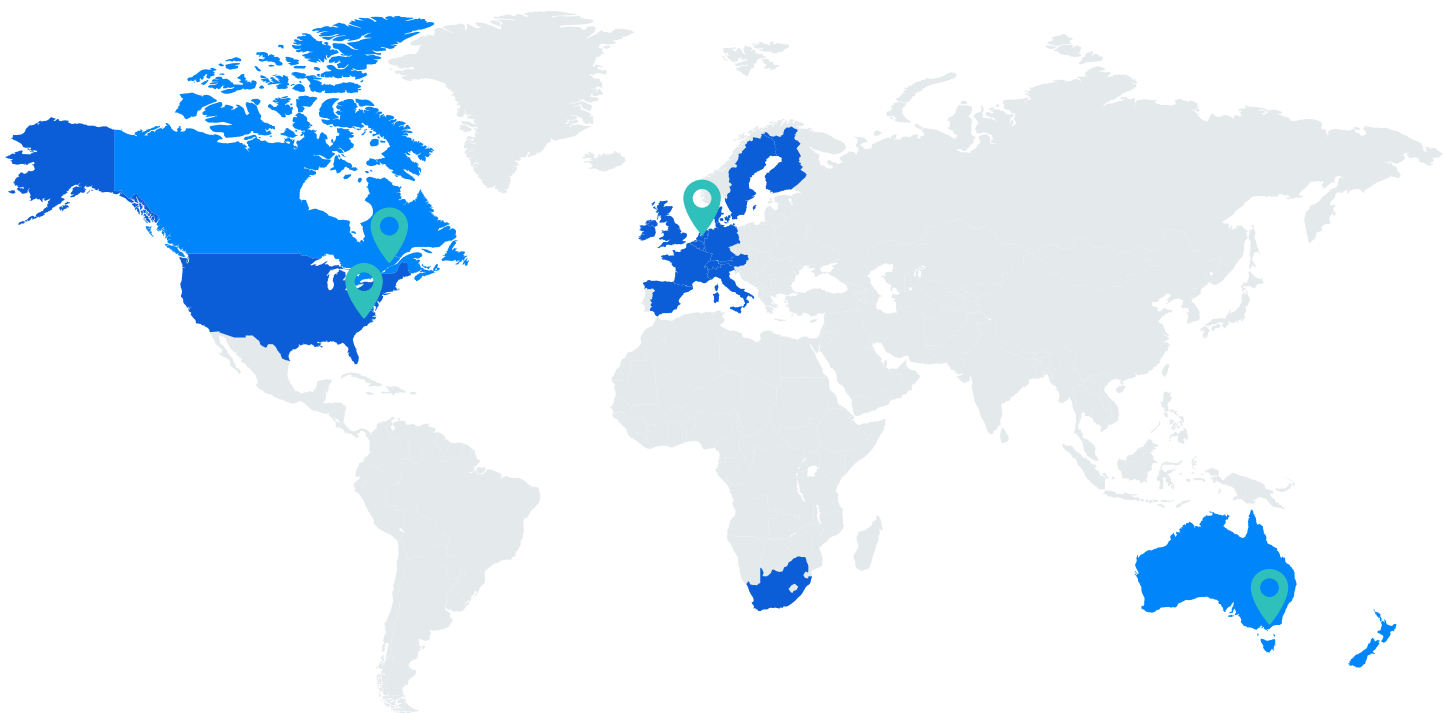
Philips SpeechLive uses Microsoft Azure to host dictations and file attachments, relying on the world’s leading enterprise cloud platform. Azure offers 99.9% uptime and robust protection against power failures, intrusions, and network outages.

Microsoft’s data centers meet top industry standards and are continuously monitored by dedicated operations teams. With over \$4 billion invested in security R&D and more than 10,000 cybersecurity experts, Azure is one of the most trusted cloud providers globally. It complies with 100+ international regulations and undergoes regular audits.

All SpeechLive data is stored regionally on Azure servers to meet legal requirements and ensure fast access.

[Explore Azure compliance offerings](#)

Australia and New Zealand	Victoria
Canada	Quebec City
Europe and South Africa	Netherlands
USA	Boydton, Virginia



Speech recognition and AI Assistant

Both our Speech Recognition and AI Assistant are built with the highest level of security to keep your data safe. Your information is automatically deleted after processing and stored in a dedicated, isolated environment.

We ensure there is no OpenAI access or AI model training, and we maintain strict compliance standards with end-to-end data encryption – all powered by Microsoft's highly secure Azure cloud environment.



Secure data transfer

All audio files sent to our speech recognition are sent securely through an encrypted channel. We use both https for client to server, and server to server communication. Transcriptions are sent via a secure SignalR https connection.



Data storage

If you are using the desktop or mobile app for our speech recognition service, no audio or text is saved on our servers. The audio and text files simply pass through our servers. If you are using the web version, both your audio and the transcription are saved temporarily during the speech recognition and then deleted automatically. The files are saved in an encrypted format in your SpeechLive account, for your access only.



Regional processing

The speech recognition engine uses the highest-security standards servers in the US, Canada, EU and Australia.



Data not used for training

Your data stays completely private and is only used to support your own interactions. It is never shared with OpenAI, other customers, or third parties, and is not used to train, retrain, or improve any AI models or other products without your explicit permission.

Personnel access security

Controlling personnel access is key to safeguarding sensitive information and preventing unauthorized entry. Our strict access controls and regular audits ensure our security remains strong and up to the highest standards.



Asset control

All computers of Philips personnel are monitored with antivirus, disk encryption, automatic device blocking and security patches. All Philips personnel who have access to users' files interact with this data securely, using a device with relevant access control procedures.



Non-disclosure agreement

All personnel with access to users' files must undergo a special security training and sign a non-disclosure agreement (NDA). This NDA serves to protect the confidential and personal data Speech Processing Solutions entrusts to its employees.



Trained personnel only

Only trained personnel have access to the system for maintenance, support, and further development.



Endpoint security

We use a VPN connection to ensure employees which can have access to sensitive data can do this safely from our corporate network from multiple endpoints.



Transcription service and other vendors

As part of our strict vendor management policy, we only cooperate with industry-leading service providers.

Dictations sent to the SpeechLive transcription service are processed by carefully selected external partner agencies and then sent through encrypted https to their secure servers. Dictations are deleted after transcription and not saved on the partner servers.

Each new vendor undergoes an extensive security audit before they we incorporate them in our activities. This way we can ensure the highest security and compliance standards are met.

