SpeechLive
Security & Certificates

Highest security standards

SpeechLive is an extremely secure cloud storage, utilizing the highest security standards available, to guarantee users maximum protection at all times. The solution works with highest connection security using the HTTPS protocol. All stored data is automatically encrypted and server mirroring keeps your data reliably secured and available anytime. Security standards are even higher than those used by banks.

To avoid unauthorized access, dictation files are encrypted in real time. The highest encryption standard available is used to protect your data, even during upload and download. Files can be encrypted for a third time if recorded in the DSS Pro format for maximum security.

It would take about three quintillion years, to crack our 256^{256} bit encryption – and that with a computer testing one billion keys per second. An impossible thing to do.

SpeechLive privacy policy

Per our privacy policy we will not sell or provide your personal data to other third parties allowing them to use your personal data for their own purposes. None of your personal financial information (such as credit card information) will be shared with other parties unless this is needed to handle your order, process our invoice, or prevent or combat fraud.

To protect your privacy, no client information or documentation is shared with anyone, in general and our transcriptionists are held to strict nondisclosure agreements. Our service does not forward transcription jobs to freelancers.
For more information, read the privacy policy on our website.

Security certificates

Data centers used by SpeechLive were awarded with the most important security certificates, by complying with international, country, and industry-specific regulatory requirements.

SpeechLive runs on Microsoft Azure data centers which are designed to run 24 × 7 and employ various measures to protect operations from power failure, physical intrusion, and network outages. They comply with industry standards for physical security and reliability and are managed, monitored, and administered by Microsoft operations personnel. They are designed for 'lights out' operation. Further details of Windows Azure's physical security can be found in the Microsoft trust center.

SpeechLive complies with the following security certificates:

SO/IEC 27001:
2005 Audit and Certification

SOC 1 and SOC 2
SSAE 16/ISAE 3402 Attestations

Cloud Security Alliance
Cloud Controls Matrix

HIPAA Business Associate Agreement (BAA)

Federal Risk and Authorization
Management Program (FedRAMP)

Payment Card Industry (PCI)
Data Security Standards (DSS) Level 1

United Kingdom G-Cloud
Impact Level 2 Accreditation

Family Educational Rights and Privacy Act (FERPA)

Simplicity & highest security

Sending dictation files via SpeechLive is as easy as sending them by e-mail, but as safe as it can possibly get. Compared to other, insecure methods for sending sensitive dictation files, SpeechLive was particularly designed for this purpose. While e-mail messages might be attacked by hackers, due to unencrypted data being sent via an unencrypted connection, SpeechLive encrypts data all the way from the client to the cloud storage. Other cloud storages, not dedicated to dictation, might use single encryption during upload, but then security measures end. SpeechLive offers double encryption, by additionally using the highly secure https protocol. On top of that, highest safety standards are guaranteed by always up-to-date security certificates.

E-MAIL WORKFLOW

LOW SECURITY

NO ENCRYPTION

- Unencrypted data get sent over an unencrypted connection
- Risk of hacker attacks and loss of data
- Risk of data leakage
- Standard firewall with limited or no security certificates

REGULAR CLOUD WORKFLOW

AVERAGE SECURITY

SINGLE ENCRYPTION

- Not dedicated to dictation workflow
- Single encrypted upload to an unencrypted cloud storage

SPEECHLIVE WORKFLOW

HIGHEST SECURITY

DOUBLE ENCRYPTION

- Highest security standards by always up-to-date security certificates
- Https security
- Dedicated dictation workflow
- Data is encrypted all the way from the client to the cloud storage
- Advantage of additional services
- Fully scaleable storage