PHILIPS

SpeechLive

Security

Data security and privacy

Philips SpeechLive Web Dictation and Transcription Solution

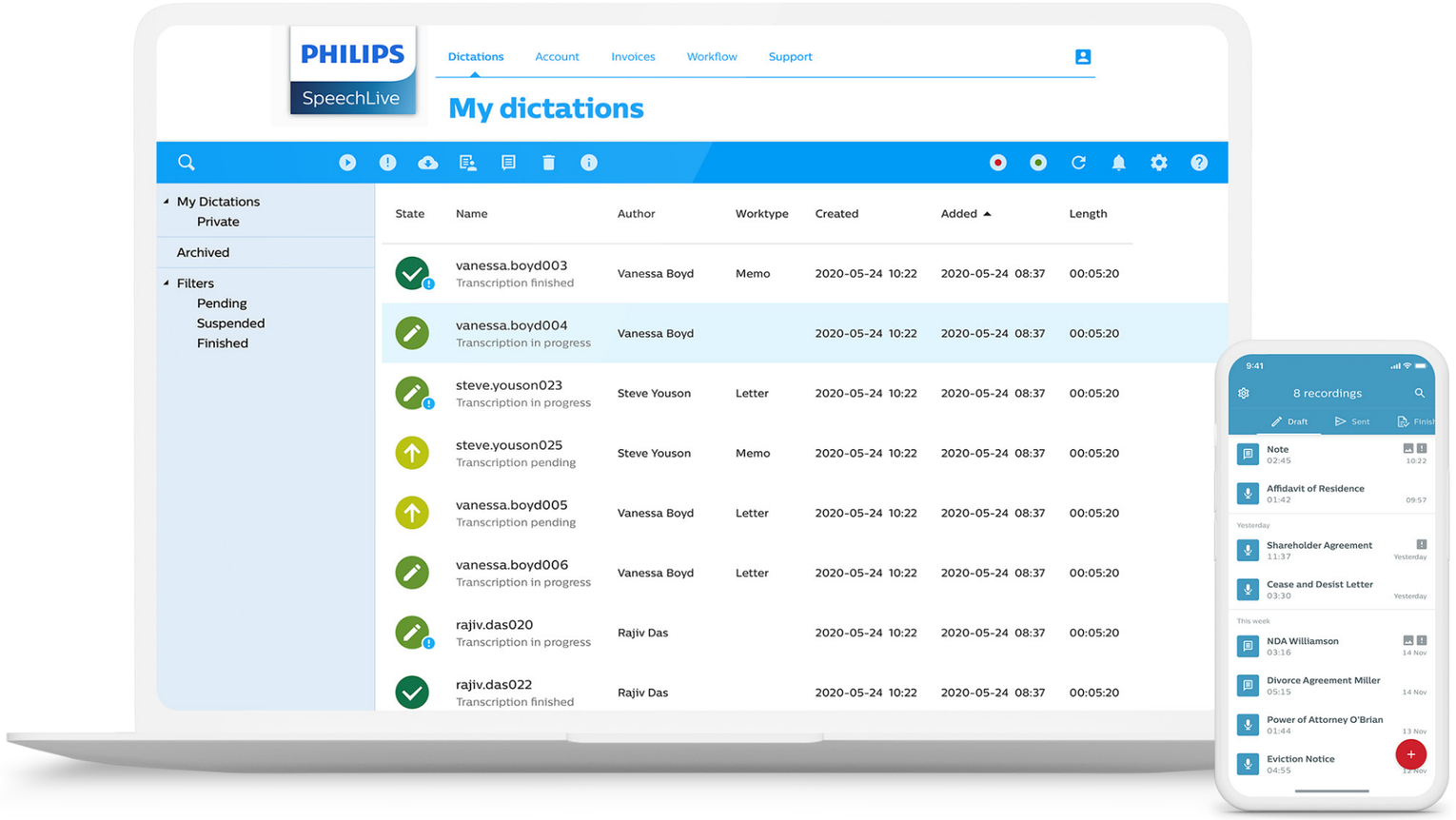
Data security and privacy

Philips SpeechLive

Philips SpeechLive Web Dictation and Transcription Solution is a browser-based workflow service which helps busy professionals turn their voice into text quickly and efficiently, from anywhere and anytime.

The cloud-based solution provides its users with consistent and reliable speech-to-text and documentation workflow service, whether the users are working from their office, their home, on the go. They can also use any input device to record, be it their PC or their mobile phone when on the go.

Thousands of customers from all over the world and various industries trust their data to Philips SpeechLive. When offering such all-encompassing flexibility, data security was always one of the highest concerns for Philips, even in the development phase of the solution.



Engineered for security

Philips Dictation works with Microsoft Azure to host Philips SpeechLive. Microsoft Azure was chosen as a partner, as they are the world's leading enterprise-level provider of a platform for cloud-hosted solutions.

MS Azure maintains uncompromising security standards and processes to ensure the highest level of data privacy and security. They continuously perform penetration testing and work on threat detection and prevention in areas such as unauthorized intrusion and denial of service.

Microsoft Azure services are highly reliable. Microsoft prides itself in promising a 99,9% uptime guarantee, 24 hours a day, 7 days a week and 365 days a year.

MS Azure have a "Lights out" policy meaning various measures are in place to protect operations from:

- **power failure**
- **physical intrusion**
- **network outages**

MS Azure's security certificates

o AS/NZS ISO/IEC 27000 series – Information Security Management

o ISO/ IEC 27000:2018 – Information technology – Security techniques – Information security management systems – Overview and vocabulary

o ISO/IEC 27001:2015 – Information technology – Security techniques – Information security management systems – Requirements

o ISO/IEC 27002:2015 – Information technology – Security techniques – Code of practice for information security controls

o ISO/IEC 27003:2017 – Information technology – Security techniques – Information security management system – Guidance

o AS ISO/IEC 27004:2018 – Information technology – Security techniques – information security management – Monitoring, measurement, analysis and evaluation

o ISO/IEC 27005:2018 – Information technology – Security techniques – Information security risk management

o United Kingdom General Data Protection Regulation and Data Protection Act 2018

o EU General Data Protection Regulation (GDPR)

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

o Security Organisation Controls (SOC 1, SOC 2, and SOC 3) United Kingdom General Data Protection Regulation and Data Protection Act 2018 o EU General Data Protection Regulation (GDPR)

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

Their datacenters are compliant with applicable industry standards for physical security and reliability; managed, monitored, and administered by Microsoft operations staff. Microsoft also states they invested over 1 billion US dollars into their security R&D and have over 3,500 cyber security experts on their team. Microsoft Azure is therefore among the most popular providers worldwide, even for large corporations. For more detailed information on Microsoft Azure, visit: https://azure.microsoft.com/ en-us/overview/trusted-cloud/

Microsoft supports over 90 global regulations. To ensure they are meeting all security and compliance advancements and requirements, Microsoft is regularly audited and submits self-assessments to third-party auditors.

Data centers

Some of the regulations the data centers comply with are as follow:

Account data (related to your billing) is stored on secure data servers in Austria.

Your dictations (audio recordings + attachments such as pictures and documents) are stored regionally on servers to comply with legal requirements, enable the quickest access.

- **United States: East US (Virginia)**
- **Canada: Canada East (Quebec City)**
- **Europe: West Europe (Netherlands)**
- **Australia & New Zealand: Australia Southeast (Victoria)**

Data Security & Encryption

HTTPS encryption

Dictations are always sent via encrypted HTTPS channels.

The dictations are encrypted and stored in the MS Azure system.

The dictations that are created by the mobile apps are encrypted stored on the mobile phone à Access of mobile phone.

Which encryption is being used?

We are using the industry standard AES 256-bit (when using the software directly, when using SpeechExec software or the smartphone app).

Is there a DSGVO-conformity?

As a European organization, we are legally obliged to comply with the DSGVO legislations.

Files are automatically backed up for 30 days

Every uploaded audio recording you create within SpeechLive will be backed up automatically for you to avoid accidental loss. Backups are only available for administrators (not all SpeechLive users)

Accidentally deleted files can be retrieved

Accidentally deleted files can be retrieved within 30 days. No need to contact SpeechLive Support.

Login & Access Safety

Every workflow user must define their own password, which can be reset anytime they want.

Dictations can only be viewed by the owner and with a user name and password.

User management and backup is only available for administrators (not all SpeechLive users).

Only trained Philips Dictation personnel has access to the system for maintenance, support and further development.

Multifactor Authentification (MFA)

Additional level of security can be enabled by using the multi-factor authentication. The admin can enforce the extra login.

SL uses a secure authentication service by Microsoft that prevents security risks such as brute force attacks.

Safety during the payment process

Users can purchase a Philips SpeechLive subscription with any major credit card. The purchase transaction happens through a certified payment platform such as Unzer and authorized.net.

Additional Philips SpeechLive features

Transcription service

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

Speech-to-text service (STT)

Dictations are processed by a secure STT service providers. Dictations are sent through https and deleted after transcription.

www.philips.com/dictation