PHILIPS

SpeechLive

Data security and privacy

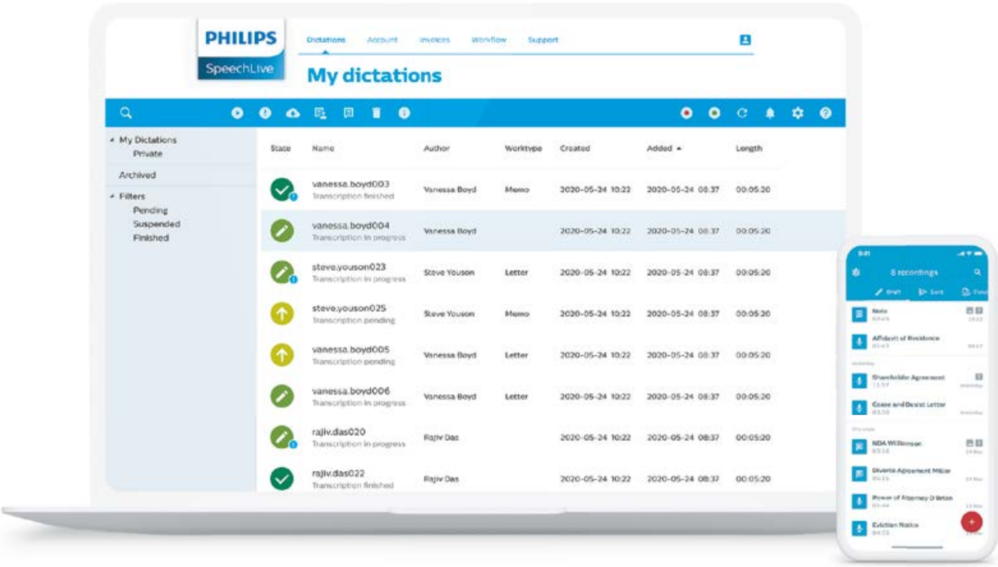
Philips SpeechLive Web Dictation and Transcription Solution

Data security and privacy

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, or 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.



State	Name	Author	Worktype	Created	Added ▲	Length
✓	vanessa.boyd003 Transcription finished	Vanessa Boyd	Memo	2020-05-24 10:22	2020-05-24 08:37	00:05:20
	vanessa.boyd004 Transcription in progress	Vanessa Boyd		2020-05-24 10:22	2020-05-24 08:37	00:05:20
	steve.youson023 Transcription in progress	Steve Youson	Letter	2020-05-24 10:22	2020-05-24 08:37	00:05:20
↑	steve.youson025 Transcription pending	Steve Youson	Memo	2020-05-24 10:22	2020-05-24 08:37	00:05:20
↑	vanessa.boyd005 Transcription pending	Vanessa Boyd	Letter	2020-05-24 10:22	2020-05-24 08:37	00:05:20
	vanessa.boyd006 Transcription in progress	Vanessa Boyd	Letter	2020-05-24 10:22	2020-05-24 08:37	00:05:20
	rajiv.das020 Transcription in progress	Rajiv Das		2020-05-24 10:22	2020-05-24 08:37	00:05:20
✓	rajiv.das022 Transcription finished	Rajiv Das		2020-05-24 10:22	2020-05-24 08:37	00:05:20

ISO 9001:2015
CERTIFIED COMPANY

GDPR READY

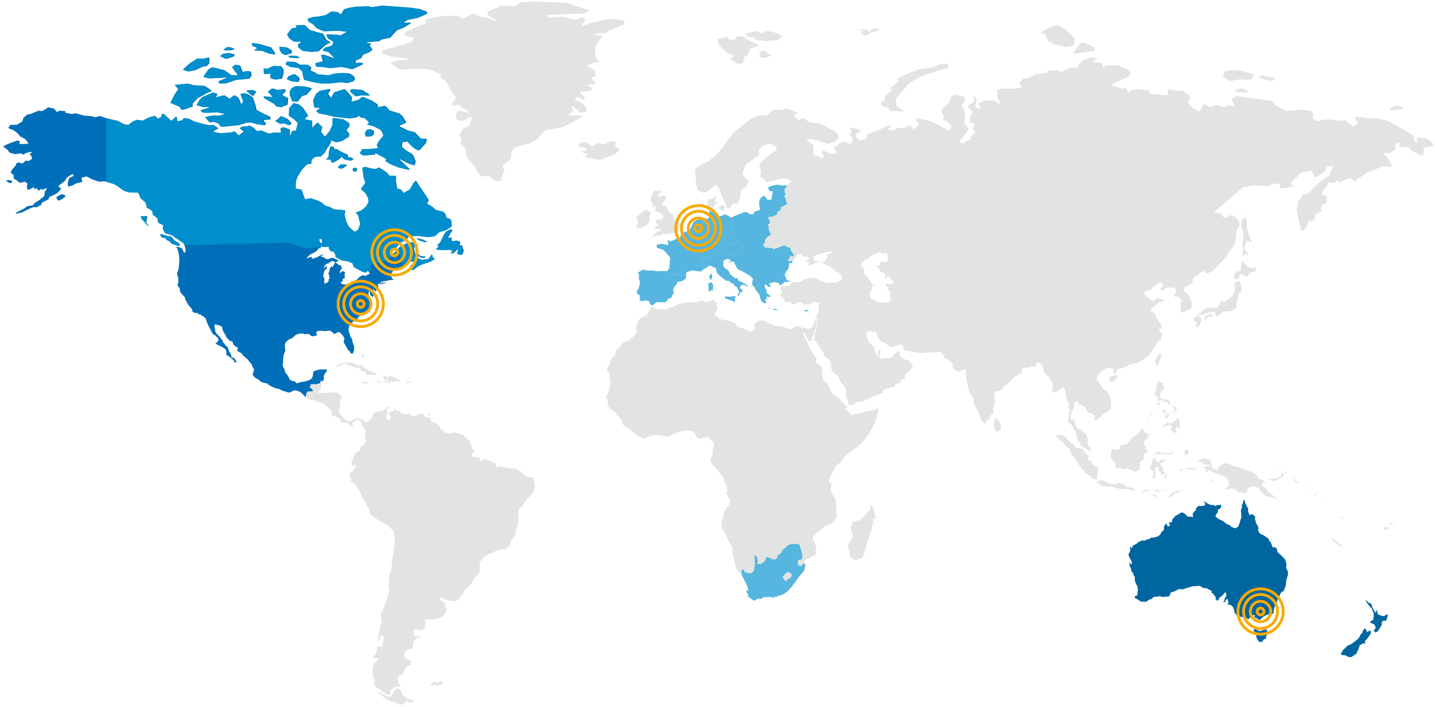
CCPA READY

Data storage

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

Dictations (audio recordings and file attachments such as pictures and documents) are stored regionally on Microsoft Azure servers to comply with legal requirements, enable the quickest access:

United States: Boydton, Virginia
Canada: Quebec City
Europe and South Africa: Netherlands
Australia and New Zealand: Victoria



Microsoft Azure

Philips SpeechLive has chosen Microsoft Azure as hosting partner for dictations (audio recordings and file attachments), as they are the world's leading enterprise-level provider of a platform for cloud-hosted solutions.

Microsoft 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 unauthorised intrusion and denial of service.

Uptime reliability

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.

Microsoft Azure have a 'lights out' policy meaning various measures are in place to protect operations from:

- Power failure
- Physical intrusion
- Network outages

Their data centers 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, click here.

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.

Azure

Security certificates

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

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

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

Security Organization Controls
(SOC 1, SOC 2, and SOC 3)

EU General Data Protection Regulation
(GDPR)

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)

FIPS 140-2 VALIDATED

ISO 27001 CERTIFIED

FR FedRAMP

Data security and encryption

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.

Login
Users must define their own password, which can be reset anytime they want. Passwords need to have a minimum of 8 characters (with at least one uppercase, one lowercase and one digit).

Multifactor authentication (MFA)
Email-based multi-factor authentication adds and 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.

Backup and 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.

File access
Dictations can only be viewed by authorised owners and with a user name and password. User management and backup is only available for administrators (not all SpeechLive users).

Payment
Payments are processed by our payment providers Unzer and authorise.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.

Speech-to-text service

Data transfer

All audio files sent to our speech-to-text service 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.

File processing

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

Data storage

If you are using the desktop or mobile app for our speech-to-text 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.

Transcription service

Dictations 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.

Personnel access security

Trained personnel access only

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

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.

Logical access

All trained Philips personnel who have access to users' files interact with this data securely, using a device with relevant access control procedures.

Endpoint security

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

Employee asset control

All computers of Philips personnel are monitored with antivirus, disk encryption, automatic device blocking and security patches.

Vendors

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

www.philips.com/dictation