PHILIPS

SpeechLive

Sécurité et confidentialité des données

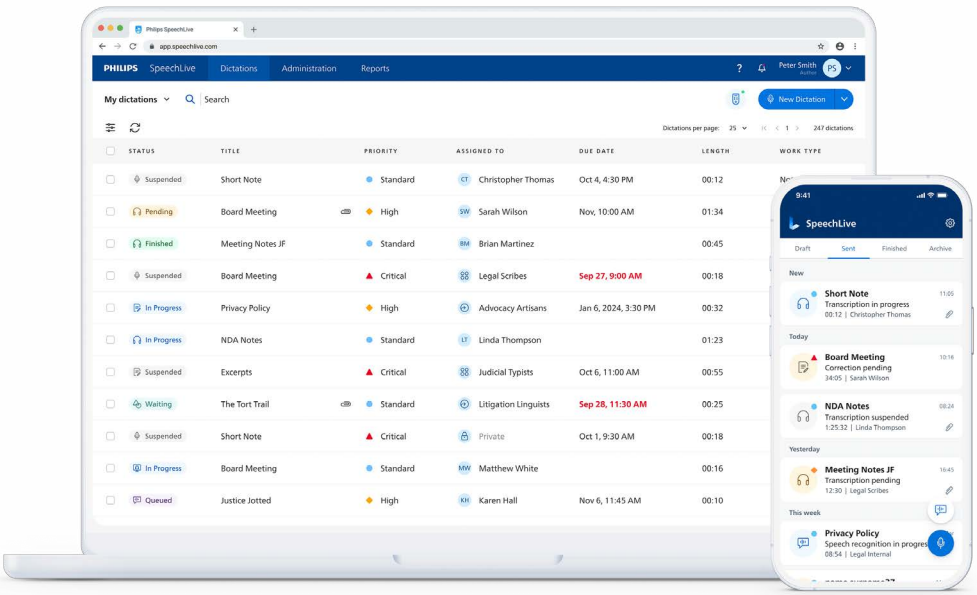
Solution de dictée et de transcription dans le cloud Philips SpeechLive

Sécurité et confidentialité des données

SpeechLive, la solution de dictée et de transcription dans le cloud de Philips est un service de flux de travail sur navigateur qui aide les professionnels très occupés à transcrire rapidement et efficacement leurs dictées, partout et à tout moment.

La solution dans le cloud offre à ses utilisateurs un service de reconnaissance vocale et de flux de travail de documentation fiable et constant, qu'ils se trouvent à leur bureau, chez eux ou en déplacement. L'enregistrement peut se faire depuis n'importe quel appareil, qu'il s'agisse d'un ordinateur ou d'un téléphone portable, en déplacement.

Des milliers de clients des quatre coins du monde et de différents secteurs font confiance à Philips SpeechLive. Pour proposer une telle flexibilité, la sécurité des données a toujours été l'une des principales préoccupations de Philips, même au cours de la phase de développement de la solution.



ISO 9001:2015 CERTIFIED COMPANY

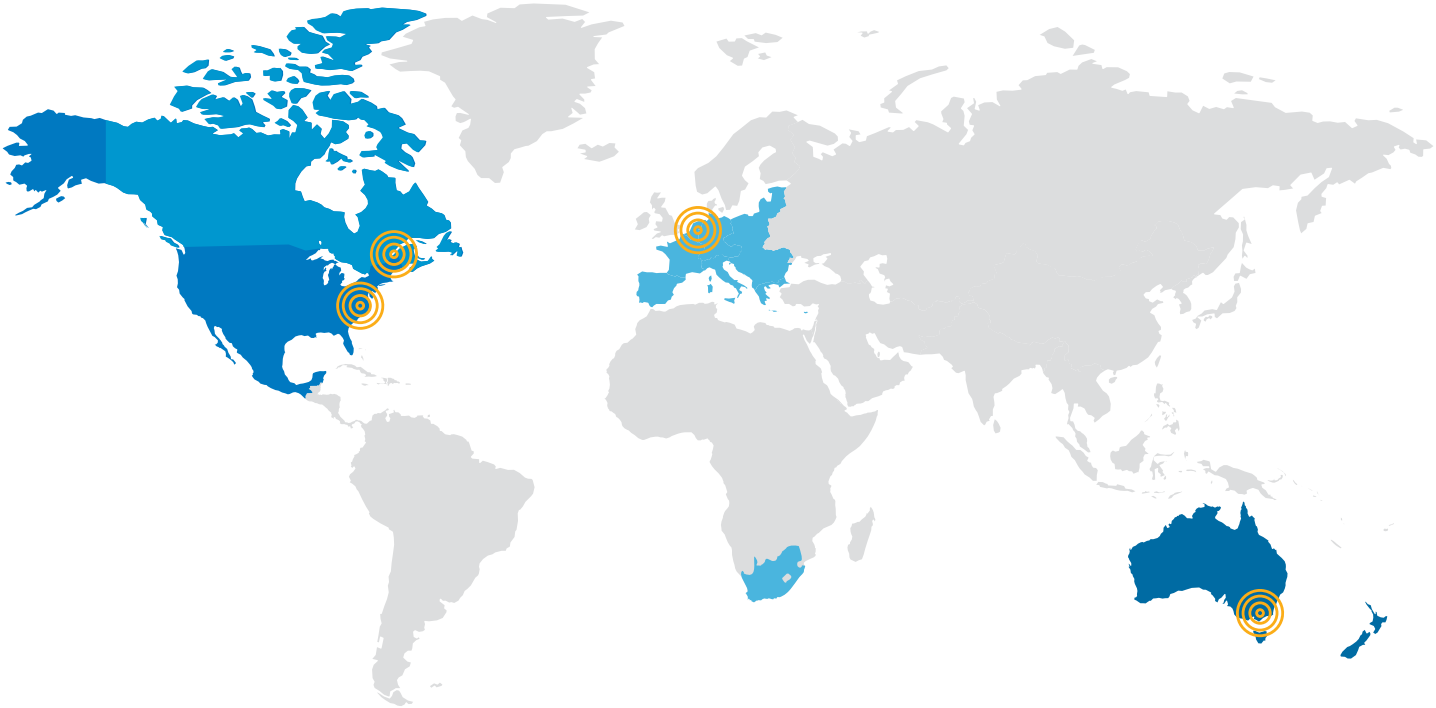
GDPR READY

CCPA READY

Stockage des données

Les données de votre compte et de vos dictées (enregistrements audio et pièces jointes, telles qu'images et documents) sont stockées au niveau régional sur des serveurs, conformément aux exigences légales, pour un accès plus rapide:

Etats-Unis: Boydton, Virginie
Canada: Ville de Quebec
Europe et Afrique du Sud: Pays-Bas
Australie et Nouvelle-Zélande: Victoria



Microsoft Azure

La dictée Philips fonctionne avec Microsoft Azure pour l'hébergement de Philips SpeechLive. Nous avons choisi Microsoft Azure comme partenaire car c'est le principal fournisseur professionnel de plate-forme pour les solutions dans le cloud.

Microsoft Azure applique des normes et des processus de sécurité sans compromis pour garantir le niveau le plus élevé de confidentialité et de sécurité des données. Des tests de pénétration sont réalisés préventant des menaces dans des domaines tels que les intrusions non autorisées et le refus de service.

Fiabilité en temps réel

Les services de Microsoft Azure sont très fiables. Microsoft s'engage à garantir une disponibilité de 99,9 %, 24 heures sur 24, 7 jours sur 7 et 365 jours par an.

Microsoft Azure a une politique « Lights-Out », mettant en place diverses mesures pour protéger des menaces suivantes :

- Pannes d'alimentation
- Intrusion physique
- Pannes du réseau

Les centres de données sont conformes aux normes applicables du secteur en matière de sécurité physique et de fiabilité ; ils sont gérés, surveillés et administrés par le personnel d'exploitation de Microsoft. Microsoft peut également se targuer d'avoir investi plus d'un milliard de dollars dans sa R&D dédiée à la sécurité et compte plus de 3 500 experts en cybersécurité dans son équipe.

Microsoft Azure compte donc parmi les fournisseurs les plus appréciés au monde, même chez les grandes entreprises. Pour plus d'informations sur Microsoft Azure, consultez.

Microsoft prend en charge plus de 90 réglementations internationales. Pour garantir le respect de l'ensemble des avancées et exigences en matière de sécurité et de conformité, Microsoft fait régulièrement l'objet d'audits et soumet des auto-évaluations à des auditeurs tiers.

Azure

Certificats de sécurité

ISO/ IEC 27000:2018 Technologies de l'information
Techniques de sécurité – Systèmes de management de la sécurité d'information – Vue d'ensemble et vocabulaire

ISO/IEC 27001:2015 Technologies de l'information
Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences

FedRAMP High
US Federal Risk and Authorization Management Program (NIST SP 800-53 800)

FIPS 140-2
Federal Information Processing Standard

Règlement général sur la protection des données de l'UE (RGPD)

Health Information Trust Alliance (HITRUST)

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

Contrôles de l'organisation de la sécurité (SOC 1, SOC 2, and SOC 3)

United Kingdom General Data Protection Regulation and Data Protection Act 2018

Hébergeurs de Données de Santé (HDS)

e Health Insurance Portability and Accountability Act (HIPAA)

Sécurité et cryptage des données

Cryptage HTTPS
Les dictées sont toujours créées, envoyées et stockées avec un cryptage AES 256 bits conforme aux normes industrielles– dans l'application web utilisant l'environnement sécurisé Microsoft Azure, dans l'application iOS ou Android sur smartphone.

Connexion
Les utilisateurs doivent définir leur propre mot de passe, qui peut être réinitialisé à tout moment. Les mots de passe doivent comporter un minimum de 8 caractères (avec au moins une majuscule, une minuscule et un chiffre).

Authentification multi-facteurs
L'authentification multifactorielle par e-mail ajoute un niveau de sécurité supplémentaire. SpeechLive utilise un service d'authentification sécurisé de Microsoft qui empêche les risques de sécurité tels que les cyberattaques. Ce paramètre peut être appliqué par l'administrateur du compte.

Sauvegarde et récupération des données
Les utilisateurs peuvent faire une sauvegarde des dictées, elles seront accessibles à tout moment. Les fichiers supprimés accidentellement peuvent être récupérés par l'administrateur pendant 30 jours.

Accès aux dictées
Les dictées ne sont consultables que par leur propriétaire, au moyen d'un nom d'utilisateur et d'un mot de passe. La gestion des utilisateurs et les copies de sécurité sont disponibles uniquement par les administrateurs (pas par tous les utilisateurs SpeechLive).

Paiement
La transaction se fait via une plateforme de paiement certifiée telle qu'Unzer et un réseau autorisé qui répondent à la norme de sécurité des données des cartes de paiement (PCI DSS) afin de garantir que les informations relatives aux paiements sont traitées, stockées ou transmises dans un environnement sécurisé.

Service de reconnaissance vocale

Transfert de données
Tous les fichiers audio envoyés au service de reconnaissance vocale sont envoyés par un canal crypté. Nous utilisons à la fois https pour la communication client-serveur et serveur-serveur. Les transcriptions sont envoyées via un site https sécurisé.

Traitement des données
Le moteur de reconnaissance vocale utilise les serveurs des normes de sécurité les plus élevées aux États-Unis et dans l'Union européenne.

Stockage des données
Si vous utilisez l'application de bureau ou l'application mobile de notre service de reconnaissance vocale, aucune dictée ou transcription texte ne sera enregistrée sur nos serveurs. Les fichiers audio et transcriptions transitent simplement par nos serveurs. Si vous utilisez la version Web, l'audio et la transcription sont enregistrés temporairement le temps de la reconnaissance vocale, puis supprimés automatiquement. Les fichiers sont enregistrés dans un format crypté dans votre compte SpeechLive, auquel vous seul avez accès.

Service de transcription

Les dictées sont traitées par des prestataires de services de reconnaissance vocale. Elles sont envoyées par site https sécurisé vers le serveur sécurisé. Les dictées sont supprimées après transcription, et ne sont pas sauvegardées sur le serveur du prestataire.

Accès sécurisé du personnel

Accès réservé au personnel formé
Seul le personnel formé a accès au système pour la maintenance, l'assistance et le développement ultérieur.

Accord de non-divulgation
Tout le personnel ayant accès aux fichiers des utilisateurs doit suivre une formation spéciale sur la sécurité et signer un accord de non-divulgation. Cet accord sert à protéger les données confidentielles et personnelles que Speech Processing Solutions confie à ses employés.

Accès logique
Tous les membres du personnel Philips formés qui ont accès aux fichiers des utilisateurs interagissent avec ces données de manière sécurisée, en utilisant un appareil doté de procédures de contrôle d'accès.

Sécurité des points d'accès
Nous utilisons une connexion VPN pour garantir que les employés qui peuvent accéder à des données sensibles le font en toute sécurité depuis notre réseau interne à partir de plusieurs points d'accès.

Contrôle des outils
Tous les ordinateurs du personnel de Philips sont surveillés au moyen d'un antivirus, du cryptage des disques, du blocage automatique des périphériques et des correctifs de sécurité.

Fournisseurs

Dans le cadre de notre politique stricte de gestion des fournisseurs, nous ne coopérons qu'avec les meilleurs prestataires de services du secteur. Chaque nouveau fournisseur est soumis à un audit de sécurité approfondi avant que nous ne l'intégrions dans nos activités. De cette façon, nous pouvons garantir le respect des normes de sécurité et de conformité les plus élevées.

www.philips.com/dictation