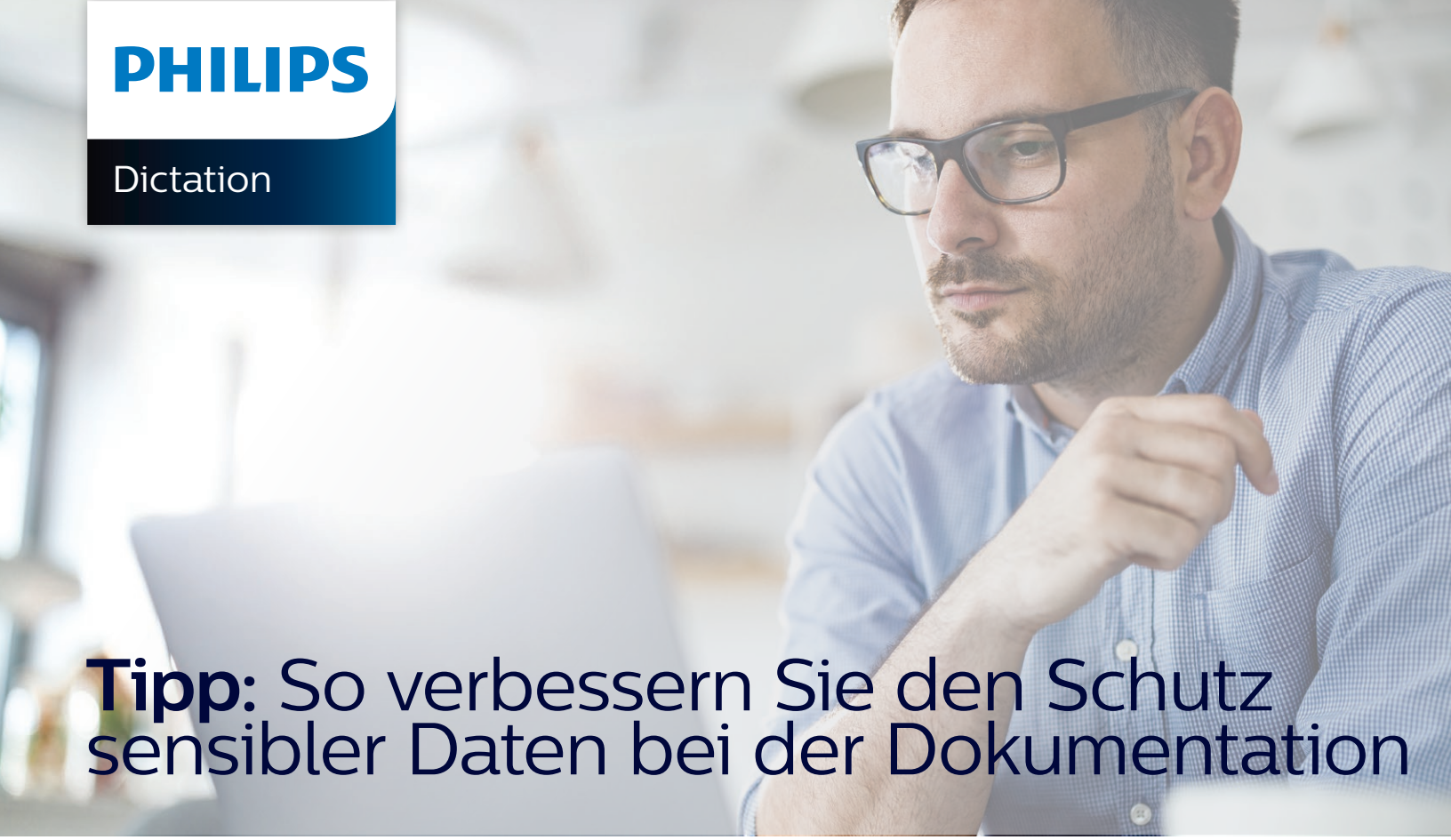
PHILIPS

Dictation



Tipp: So verbessern Sie den Schutz sensibler Daten bei der Dokumentation

Die Digitalisierung schreitet in vielen Unternehmen voran. Besserer Kundenservice, unternehmerische Agilität, flexiblere Arbeitsweisen – das sind nur einige der vielen Vorteile. Doch die neue Arbeitswelt birgt Risiken, speziell was die Datensicherheit betrifft. Je digitaler das Unternehmen, desto wahrscheinlicher werden Sicherheitsprobleme, sei es durch Nachlässigkeit von einzelnen Personen oder den gezielten Angriff durch Cyberkriminelle. Als Mitarbeiter kann ein solcher Vorfall dramatische Konsequenzen haben. **Kurzum: Datensicherheit ist im Interesse jedes einzelnen Mitarbeiters**. Speziell wenn Sie dokumentieren, das heißt sensible Daten erfassen, verarbeiten, transferieren und aufbewahren.

Dieser Quick-Guide hilft, Ihren Status in Sachen Datensicherheit unter die Lupe zu nehmen und gibt Tipps, wie Sie diesen verbesern:

1

Arbeiten Sie zeitweise mobil?

Schon vor COVID-19 gab es einen Trend zum mobilen Arbeiten. Dieser wird nun verstärkt. Mobile Geräte können zum Einfallstor für Cyberkriminelle werden. Arbeiten Sie zeitweise außerhalb Ihres stationären Arbeitsplatzes? Dann sollten Sie speziell bei der Dokumentation, bei der sensible Daten verarbeitet werden, gewisse Sicherheitsmerkmale beachten. Darunter zum Beispiel Echtzeit-Verschlüsselung und die Nutzung virtueller privater Netzwerke (VPN) für WiFi-Verbindungen. Mittels PIN oder biometrischen Daten geschützte Geräte, rollenbasierte Berechtigungen für verschiedene Anwendungen und Anforderungen an die Komplexität von Passwörtern sind schlagkräftige Möglichkeiten, die Datensicherheit beim mobilen Arbeiten zu erhöhen.

Cyberkriminalität steigt

PWC stellte in der Fraud Survey 2020 unter über 5.000 Teilnehmern fest, dass 34% der befragten Unternehmen in den letzten 24 Monaten Opfer von Cyberkriminalität wurden. Die Tendenz steigt. Besonders betroffen sind Technologie-Unternehmen, Finanzdienstleister, die öffentliche Verwaltung aber auch zunehmend das Gesundheitswesen.

Vorsicht vor Cybercrime in Zeiten von COVID-19

In Zeiten der globalen Pandemie COVID-19, in der viele Menschen weltweit um Ihre Gesundheit besorgt sind, ist auch ein Anstieg von Cybercrime zu beobachten. Einerseits, weil viele Mitarbeiter zu Hause arbeiten und andererseits, weil die Unsicherheit von Menschen ausgenutzt werden kann. Im Umlauf sind z.B. Fake-Websites zum Medikamentenkauf, Fake-E-Mails, dass man für Homeoffice Software downloaden sollte oder dergleichen. Vorsicht ist geboten!

2

Nutzen Sie Cloud-Technologie?

Überlegene Sicherheit ist einer der Hauptgründe, warum immer mehr Daten in der Cloud gespeichert werden. Da Cloud-Dienste in der Regel komplexere Sicherheitsmechanismen als lokale Server verwenden, bieten sie ein zusätzliches Maß an Schutz. Unabhängig davon, von wo Sie arbeiten, erhalten sensible Kundendaten in der Cloud immer denselben hohen Schutz. Und: Daten können auch nicht verloren gehen. Achten Sie beim Einsatz von Tools auf höchste Sicherheit, DSGVO-Konformität und Zertifizierungen (ISO, etc.).

3

Kennen Sie die Sicherheitsstandards?

Konsistenz in den Sicherheitsverfahren und -anforderungen verbessert die Sicherheitslage eines jeden Unternehmens. Es braucht formalisierte Standards und die konsequente Einhaltung dieser. Agiert man in Sicherheitsfragen ad-hoc, sind diese Praktiken oft nicht robust genug, um sich gegen Cyber-Angriffe zu schützen. Für jeden einzelnen gilt: Es müssen dieselben Regeln und Anweisungen gelten und Tag für Tag eingehalten werden.

4

Fühlen Sie sich eigen-verantwortlich?

Unabhängig davon, wie sicher Technologien sind, ist jeder Einzelne immer noch der Schlüssel zum Erfolg in Sachen Datenschutz, Sicherheit und Vertraulichkeit. Stellt Ihr Unternehmen Schulungs- und Ausbildungstools zur Verfügung, dann nehmen Sie diese Ernst. Sollte Ihr Unternehmen dies noch nicht bewerkstelligen, beweisen Sie Eigeninitiative und fordern Sie es ein. Denn es braucht selbstverständlich auch Eigenverantwortung für den Schutz sensibler Daten. Dies ist im Sinne Ihrer Kundinnen und Kunden.

Benötigen Sie weitere Informationen darüber, wie Sie bei der Dokumentation die Daten Ihrer Kunden schützen können?

Besuchen Sie die Website von Philips Speech oder senden Sie uns eine E-Mail an info.isr@speech.com, um mehr über sichere, hochmoderne Sprache-zu-Text-Lösungen zu erfahren.