RingCentral

Qu'est-ce que la conformité en matière de communications, et pourquoi c'est important ?

Comment s’y retrouver parmi les ISO, RGPD et autres HITRUST

Table des matières

Introduction

Les cyberattaques ont toujours représenté un risque majeur pour les entreprises, qui n’a fait que s’aggraver ces dernières années avec l'essor du télétravail.

Les employés qui travaillent de chez eux peuvent se connecter via des réseaux publics, ou utiliser leurs propres terminaux où sont installées des applications ne faisant pas l’objet du même degré de vigilance que sur les équipements de l'entreprise. Les société doivent être conscientes des risques accrus de cyberattaques liés aux nouveaux modèles de travail hybride.

À présent, alors même que les entreprises les plus prévoyantes ont du mal à anticiper et gérer les risques pour leur sécurité, il est plus important que jamais d’investir dans une sécurité plus efficace.

Ce guide vous explique de manière détaillée :

- l’impact que l’essor du télétravail a eu sur la sécurité informatique ;
- la signification et l’importance de la conformité ;
- les certificats et attestations à privilégier chez vos prestataires.

Qui dit télétravail, dit risques accrus pour la cybersécurité

Certes, les modèles de travail hybride ont beaucoup d'avantages. Mais ils s'accompagnent aussi de risques de taille pour votre sécurité informatique. D'après TechTarget, les principaux sont les suivants :

- « Shadow IT » (utilisation par les employés d'outils non autorisés par l'entreprise)
- Recours à des réseaux non sécurisés et vulnérables
- Surveillance moins étroite
- Plus de surfaces d'attaque
- Pratiques insuffisantes en matière de protection des données
- Utilisation de matériel non sécurisé et vulnérable
- Vulnérabilité face aux attaques d'hameçonnage (phishing)
- Exposition à des piratages par webcam
- Configurations inadéquates sur le cloud public

Gérer tous ces risques est très lourd pour les entreprises, quelles qu'elles soient. Heureusement, les solutions cloud vous permettent d'améliorer plus facilement votre sécurité, à condition toutefois de choisir le bon fournisseur et d'opter pour une plateforme sécurisée. Aujourd'hui, toute entreprise doit prendre le temps de s'assurer que les fournisseurs de technologie avec lesquels elle travaille garantissent un niveau de sécurité approprié et l'améliorent en continu.

L’importance de la conformité

Pour faire simple, la conformité se conçoit comme le respect d’un certain nombre de règles, spécifications, politiques, normes ou lois. Les principes que vous devez observer diffèrent selon votre secteur d’activité et les régions dans lesquelles vous opérez. Alors que l’environnement de travail devient toujours plus digital, et donc difficilement maîtrisable, la conformité ne cesse de gagner en importance. Si la tâche peut paraître colossale, sachez que la conformité peut vous aider à ne pas compromettre votre entreprise dans des activités illicites, à protéger votre activité, vos collaborateurs et vos clients, et à susciter la confiance chez ces derniers.

Des normes mondiales en matière de sécurité et de confidentialité

Trouver des fournisseurs cloud peut sembler facile. Bien plus, en tout cas, que de relever seul le défi titanesque de la conformité, quand tant de décisions cruciales doivent déjà être prises au quotidien. Or, quiconque choisit la facilité ou décide de suivre le mouvement au moment de choisir son fournisseur de communications cloud prend un gros risque - surtout en ce qui concerne la conformité. Au contraire, vous avez tout intérêt à choisir des partenaires et fournisseurs capables d’apporter la preuve de leur conformité dans tous les pays où vous opérez.

Les certificats suivants attestent de la maturité des processus et programmes d’un fournisseur vis-à-vis des normes mondiales les plus strictes. Selon le type de données que vous traitez et les régions du monde où vous intervenez, certaines de ces normes peuvent être particulièrement pertinentes pour vous.

Certification ISO 27001

Définition : ISO/IEC 27001 est la norme mondialement reconnue pour les systèmes de gestion de la sécurité de l'information (ISMS pour Information Security Management Systems) et les exigences liées à ces systèmes. Elle permet aux entreprises de toutes tailles et de tous secteurs de superviser la sécurité de leurs données sensibles en toute sécurité, qu'il s'agisse d'informations relatives à leurs finances, à leurs collaborateurs, ou à la propriété intellectuelle.

Signification : cette certification est délivrée aux fournisseurs ayant développé et mis en place un ensemble de contrôles et de mesures pour gérer efficacement les risques et être conforme en continu, afin de protéger les données et informations relatives aux clients. Il prouve aussi que les fournisseurs correspondants ont adopté un programme de sécurité robuste assorti d'une gestion et de contrôles techniques rigoureux, aptes à satisfaire aux principes de confidentialité, d'intégrité et de disponibilité propres à la sécurité de l'information.

Certification ISO 27017

Définition : la certification ISO/IEC 27017 a trait à tout un ensemble de directives en matière de contrôles de sécurité informatique qui s'appliquent spécifiquement à l'utilisation de solutions et de services cloud, et contient des conseils pour la mise en œuvre des contrôles appropriés spécifiés dans la norme ISO/IEC 27002. Cette norme de sécurité mondiale exige de la part des fournisseurs de services cloud et de leurs clients le respect de pratiques éprouvées en matière de contrôles et de mise en œuvre.

Signification : cette certificat prouve que l'entreprise qui le détient étend la rigueur de son système de gestion de la sécurité de l'information (ISMS) à l'exploitation de ses services cloud. Il est décerné aux fournisseurs appliquant des principes de contrôle stricts pour sécuriser l'accès à leurs services.

Certification ISO 27018

Définition : cette certification est axée sur l'établissement de contrôles et de directives communément admis, ainsi que sur la mise en place de mesures aptes à protéger au mieux les données d'identification, pour les environnements de cloud public.

Signification : la certification ISO/IEC 27018 est décernée aux fournisseurs utilisant un cloud public qui s'engagent à respect la confidentialité des données de leurs clients. Il atteste aussi que les fournisseurs qui le détiennent ont, en tant que responsables du traitement des données d'identification de leurs clients, mis en place des contrôles suffisants pour protéger ces informations.

Attestation SOC 2

Définition : SOC est l'acronyme de « Service Organization Controls ». L'attestation SOC 2 est la norme de reporting de l'American Institute of CPAs (AICPA) fixant les critères de gestion et de traitement des données clients. De nombreuses entreprises, en particulier dans le secteur des SaaS (Software as a Service), respectent des procédures strictes en matière de sécurité de l'information. L'attestation SOC 2 est l'audit tiers qui évalue et certifie leur conformité.

Signification : les fournisseurs qui reçoivent une attestation SOC 2 ont été soumis à un audit strict axé sur les contrôles de la disponibilité, de la sécurité et de la confidentialité des données clients.

Attestation SOC 3

Définition : contrairement au SOC 2, l'attestation SOC 3 est un rapport public. Ainsi, alors que le SOC 2 ne peut être partagé qu'avec des clients ou des entités liées par un accord de confidentialité, le rapport SOC 3 peut être partagé librement ou publié en ligne. Il est source de transparence au sujet des contrôles internes de l'entreprise en matière de sécurité, disponibilité, intégrité du traitement et confidentialité.

Signification : le SOC 3 atteste que l'entreprise qui le détient applique des contrôles appropriés en matière de sécurité, de disponibilité et de confidentialité. Il n'est pas nécessaire, pour comprendre le SOC 3, de posséder les connaissances approfondies requises pour exploiter le SOC 2.

STIR/SHAKEN

Définition : STIR/SHAKEN est l'acronyme de « Secure Telephone Identity Revisited (STIR) » et « Signature-based Handling of Asserted information using tokens (SHAKEN) ». Il s'agit d'un cadre de normes interconnectées permettant aux destinataires d'un appel de vérifier l'identifiant de la personne qui cherche à les joindre.

Signification : STIR/SHAKEN permet aux appels passant par des réseaux de téléphonie interconnectés d'être « signés » par l'opérateur d'origine et validés par d'autres fournisseurs avant de parvenir au destinataire. Les fournisseurs de téléphonie ayant recours à ce cadre normatif protègent leurs utilisateurs du risque qu'une personne non autorisée ne les contacte ou n'intercepte un appel.

Attestation de conformité HIPAA

Définition : le secteur de la santé ne peut plus se passer de technologies. Pour autant, les établissements de santé doivent aujourd'hui satisfaire à tout un ensemble de règles. Le « Health Insurance Portability and Accountability Act (HIPPA) » est une attestation répandue aux États-Unis dédiée à ce secteur.

Signification : les entreprises qui opèrent sur le sol américain doivent respecter les principes édictés dans le HIPAA. Les fournisseurs qui reçoivent l'attestation de conformité HIPAA s'engagent à préserver les données et informations de leurs patients ou membres ainsi que les professionnels de santé, et justifient de protocoles de sécurité suffisants pour garantir leur protection.

Certification HITRUST

Définition : HITRUST est l'acronyme de « Health Information Trust Alliance ». Le certificat HITRUST permet aux entreprises de tous les secteurs, en particulier celui de la santé, de superviser leurs données, leurs risques en matière d'information et leur conformité.

Signification : les fournisseurs titulaires d'un certificat HITRUST, délivré par la HITRUST Alliance, ont prouvé qu'ils avaient adopté un cadre standardisé justifiant de leur conformité vis-à-vis des exigences du HIPAA.

RGPD

Définition : le Règlement général sur la protection des données (RGPD) de l'Union Européenne s'applique à toutes les entreprises opérant au sein de l'UE. Il s'agit du texte réglementaire relatif à la confidentialité et à la sécurité le plus strict au monde. Le RGPD contient des directives relatives à la collecte et au traitement de données et vise à protéger les données personnelles de tous les citoyens de l'UE. Les entreprises qui enfreignent ces normes de sécurité et de confidentialité s'exposent à de lourdes sanctions.

Signification : les fournisseurs qui prouvent leur respect du RGPD affichent leur engagement vis-à-vis de la protection de toutes les données personnelles qu'ils enregistrent, transfèrent ou traitent. Comme les entreprises sont responsables de la protection des données de leurs clients, y compris lorsque le traitement est réalisé par un sous-traitant, la conformité vis-à-vis du RGPD est une nécessité absolue pour tous les fournisseurs dont les clients opèrent au sein de l'UE.

Commerçant certifié PCI

Définition : les normes PCI DSS (« Payment Card Industry Data Security Standard ») visent à garantir que les entreprises qui traitent, enregistrent et transmettent des informations relatives à des cartes de paiement offrent un environnement sécurisé.

Signification : les entreprises certifiées s'engagent à respecter une procédure spécifique quant au traitement et à l'enregistrement de données relatives aux cartes de paiement, et s'engagent à appliquer certaines mesures en cas d'incident de sécurité. Les fournisseurs conformes aux normes PCI DSS, comme RingCentral, respectent un ensemble de principes et de directives définis par le conseil des normes PCI dans le cadre du traitement de données relatives aux cartes de crédit des clients.

LPRPDE

Définition : la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE ou PIPEDA en anglais) est une loi relative à la protection de la confidentialité des données pour les entreprises du secteur privé au Canada. Comparable au RGPD de l'Union européenne, la LPRPDE régit la collecte, l'utilisation et la publication d'informations personnelles. Entrée en vigueur en 2000, cette loi a été établie afin de renforcer la confiance vis-à-vis de l'économie numérique.

Signification : la LPRPDE s'applique à toutes les entreprises privées au Canada. Portant sur les informations personnelles, c'est-à-dire les données obtenues dans le cadre d'activités commerciales, cette loi protège les consommateurs du risque d'utilisation abusive d'informations personnelles. Les fournisseurs conformes à la LPRPDE montrent leur engagement vis-à-vis de la confidentialité des données personnelles.

C5

Définition : la certification C5 est un cadre normatif soutenu par le gouvernement allemand et mis en œuvre par l'Office Fédéral Allemand pour la Sécurité de l'Information (BSI). Elle doit son nom à la première lettre des mots clés « Cloud », « Computing », « Compliance » (conformité), « Contrôles » et « Catalogue ».

Signification : le cadre C5 s'applique aux fournisseur de services cloud. À travers le certificat C5, ces derniers peuvent ainsi prouver à leurs utilisateurs, clients, prospects et parties prenantes qu'ils appliquent des mesures de sécurité efficaces pour limiter les risques de cyberattaques dans le cadre de l'utilisation de leurs services cloud.

Communiquez en toute confiance

Les entreprises doivent pouvoir avoir une confiance totale envers leurs systèmes de communication. Face aux nombreux défis liés aux modèles de travail hybrides, elles doivent impérativement nouer un partenariat de confiance avec un fournisseur déterminé à faire de leur sécurité et de la protection de leurs données une priorité.

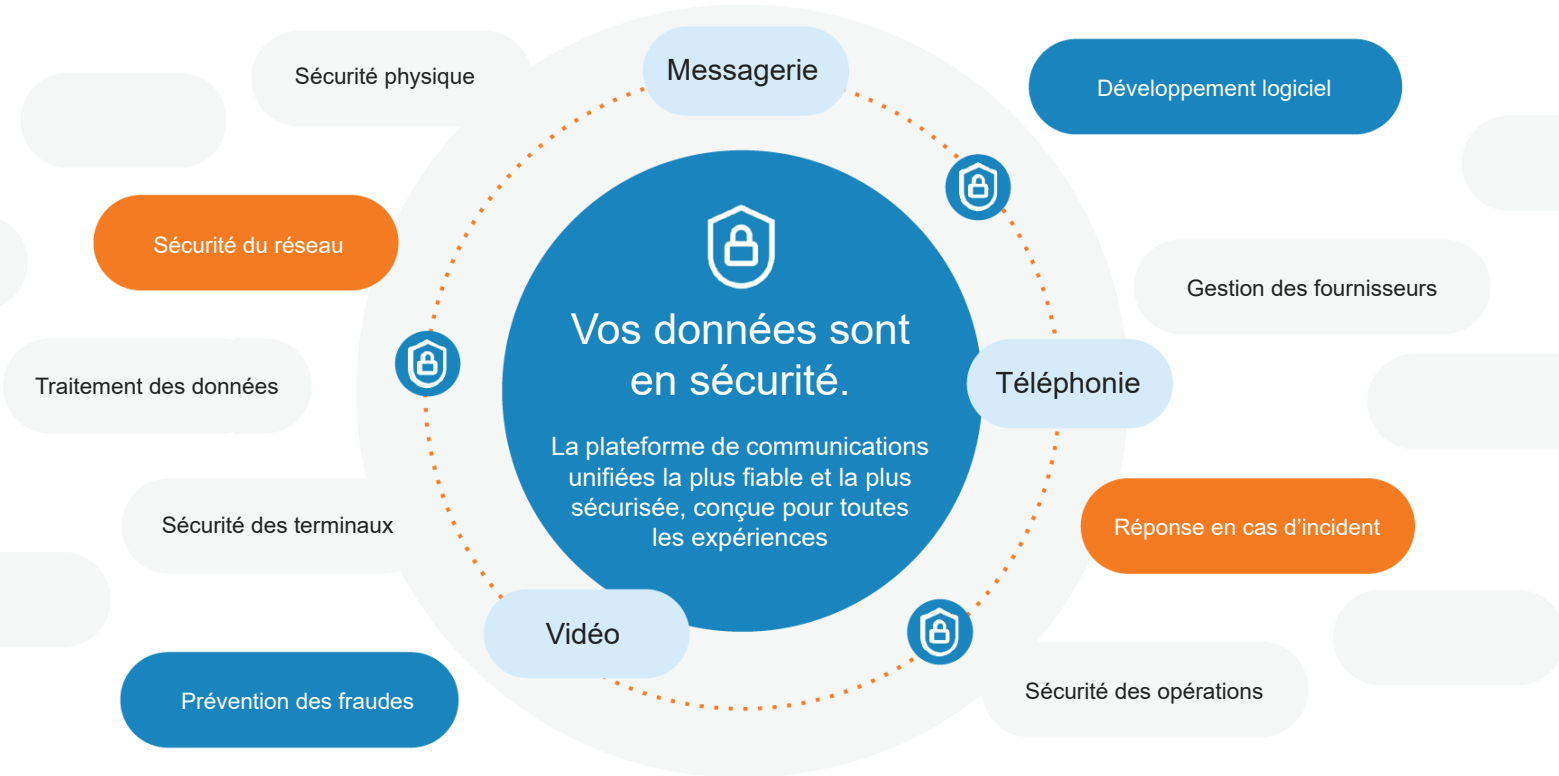
RingCentral est la solution qu'il vous faut. Possédant divers certifications et attestations de tiers, respectant des lois internationales et nous conformant à de nombreuses réglementations, nous vous prouvons notre engagement vis-à-vis de la sécurité, de la transparence et de la confidentialité de vos données. Développée sur une plateforme cloud sécurisée, la solution RingCentral satisfait à un ensemble d'exigences plus strictes les unes que les autres. Ainsi, nos clients ont l'assurance de bénéficier d'une sécurité de pointe sur le cloud et savent que leurs données et informations personnelles sont préservées.

Les données des utilisateurs de RingCentral, mais aussi celles qui sont traitées via nos services, sont donc sécurisées et protégées en cas de partage via la messagerie, la vidéo, la téléphonie ou le fax. Et ce n'est pas tout : avec une disponibilité de 99,999% garantie par SLA, nos clients profitent de la plateforme cloud unifiée la plus fiable et la plus sécurisée du marché.

Au-delà de la conformité

N’oubliez pas que la conformité n’est qu’un aspect parmi d’autres de votre écosystème de sécurité informatique. Vous avez tout intérêt à évaluer les mesures prises par les potentiels partenaires supportant vos communications en matière de sécurité des informations et des produits, de protection des données et de fiabilité de leurs solutions.

Outre son haut niveau de conformité, RingCentral vous offre aussi une sécurité, une confidentialité et une fiabilité inégalées pour assurer la sécurité de vos données à tous les niveaux.



Sécurité

La solution de communications unifiées de RingCentral vous garantit une sécurité optimale. Incluant un ensemble de contrôles de sécurité, comme l'authentification unique (SSO), le chiffrement de bout en bout (E2EE) et l'authentification des participants, elle offre à ses utilisateurs l'accès à des contrôles administratifs complets pour la messagerie, la vidéo et la téléphonie. À la clé : des discussions pleinement sécurisées. Grâce aux meilleures pratiques DevSecOps, nous vous promettons une plateforme de sécurité robuste intégrant des principes de sécurité essentiels à tous les niveaux.

Protection des données

En devenant client RingCentral, vous bénéficiez de notre engagement en matière de confidentialité et de transparence. Conserver la confiance de nos clients dans nos pratiques de gestion de données et respecter la confidentialité de leurs données est l'une de nos priorités. Notre promesse de confidentialité s'articule autour des principes clés suivants :

- Responsabilité
- Transparence
- Minimisation des données
- « Privacy by design » (confidentialité native) et par défaut
- Protection des droits des personnes concernées
- Sécurité des données
- Sauvegardes des transferts de données

Fiabilité

Nous savons combien il est décisif de garantir la continuité de l'activité et de rester connecté quoi qu'il arrive. Aussi avons-nous pour ambition de veiller à ce que vous soyez opérationnel, partout et à tout moment. Nouveaux bureaux, modèles de travail différents, ou encore catastrophe naturelle : dans certains cas, les entreprises doivent être prêtes à changer de lieu de travail. Où qu'ils soient, les clients RingCentral restent opérationnels grâce à un temps de fonctionnement de 99,999 % garanti par SLA et à des connexions Internet redondantes pour rester en ligne même en cas de panne, de catastrophe ou d'attaque informatique.

À retenir

Peut-être avez-vous eu l’impression de trouver la solution de communication idéale quand le télétravail est devenu la nouvelle norme du jour au lendemain. Mais il est temps aujourd’hui de passer au crible l’intégrité de votre fournisseur de communications cloud.

Que vos collaborateurs travaillent sur site et/ou à distance, la protection de vos communications et de la sécurité de vos données doit compter parmi vos priorités, surtout que le nombre d'attaques informatiques ne cesse de progresser. Examinez soigneusement les garanties que vous offrent vos fournisseurs en termes de sécurité, de fiabilité, de confidentialité et de conformité. Il est plus important que jamais de vous assurer que le partenaire pour vos communication vous assure une conformité optimale et possède les attestations et certificats dont vous avez besoin, afin de préserver vos données et la confidentialité de vos communications.

À propos de RingCentral

RingCentral, Inc. (NYSE: RNG) est un fournisseur leader de solutions de communications et de centre de contact dans le cloud pour les entreprises, basées sur la plateforme mondiale Message Video Phone (MVP[MD]). Plus flexible et rentable que les PBX sur site et les systèmes de visioconférences qu'elles remplacent, les solutions RingCentral permettent aux collaborateurs de communiquer en tout lieu et sur tout terminal. RingCentral propose trois produits phares dans son portefeuille. RingCentral MVP[MD] combine la messagerie d'équipe, les visioconférence, la téléphonie cloud et d'autres fonctionnalités, en une seule interface. RingCentral Video[MD], dotée aussi d'une messagerie d'équipe, permet des réunions de type Smart Video Meetings. RingCentral Centre de Contact[MD] apporte aux entreprises les outils dont ils ont besoin pour se connecter avec leurs clients sur tous les canaux. Ces produits sont disponibles sur la plateforme ouverte de RingCentral, qui intègre des centaines d'applications tierces et facilite la personnalisation de la gestion des flux. Le siège de RingCentral est situé à Belmont en Californie, et l'entreprise possède des bureaux dans le monde entier.

Pour plus d'informations, n'hésitez pas à prendre contact avec un représentant commercial. Rendez-vous sur ringcentral.com/fr/fr/ ou composez le 0800 90 39 18.

RingCentral

RingCentral France SAS, 3-5 rue Saint-Georges, 75009 Paris, France. ringcentral.com/fr/fr/

03/2023