ADDENDUM SUR LA SECURITE DE RINGCENTRAL

1. Portée

Le présent document décrit les mesures de sécurité de l'information (**« Mesures »**) que RingCentral a mises en place lors du traitement des Données Protégées par le biais des Services RingCentral.

2. Définitions

Aux fins du présent addendum de sécurité seulement, les termes en majuscules, qui ne sont pas autrement définis dans les présentes, ont le sens qui leur est donné dans le Contrat.

A. Les **« Services RingCentral »**, ou **« Services »**, désignent les services offerts par RingCentral et acquis par le Client.

B. **« Client »** désigne l'entité qui a conclu le Contrat avec RingCentral.

C. **« Données Protégées »** désigne les données du Client et des partenaires traitées par les Services RingCentral, telles que définies dans le DPA ou le Contrat RingCentral applicable, y compris les "données personnelles "et les "informations personnelles "telles que définies par les lois applicables en matière de protection de la vie privée, les données confidentielles telles que définies dans le Contrat, les données de compte, les données de configuration, le contenu des communications, y compris les messages, la messagerie vocale et l'enregistrement vidéo.

D. **« Contrat »** désigne le contrat en place entre RingCentral et le Client pour la fourniture des Services.

E. **« Personnel »** désigne les employés de RingCentral, les contractants ou le personnel des Services Professionnels sous-traités.

3. Gestion de la Sécurité de l'information

A. Programme de Sécurité

RingCentral maintient un programme écrit de sécurité de l'information qui :

i. Comprend des politiques ou des normes documentées appropriées pour régir le traitement des Données Protégées conformément à l'accord et au droit applicable.

ii. Est géré par un employé principal chargé de superviser et de mettre en œuvre le programme.

iii. Comprend des mesures de protection administratives, techniques et physiques raisonnablement conçues pour protéger la confidentialité, l'intégrité et la disponibilité des Données Protégées.

iv. Est approprié à la nature, la taille et la complexité des opérations commerciales de RingCentral.

B. Gestion des Politiques de Sécurité

Les politiques, normes et procédures de sécurité de RingCentral :

i. S'aligner sur les normes industrielles établies en matière de sécurité de l'information.

ii. font l'objet d'une révision permanente.

iii. Peut être révisé pour refléter les changements dans les meilleures pratiques de l'industrie.

C. Gestion des Risques

RingCentral :

i. Effectuer, au moins une fois par an, des évaluations des risques en matière de cybersécurité afin d'identifier les menaces pesant sur leurs activités ou leurs opérations.

ii. Mettre à jour les politiques, procédures et normes de RingCentral, si nécessaire, pour faire face aux menaces qui pèsent sur les activités ou les opérations de RingCentral.

4. Évaluations Indépendantes de la Sécurité

A. Audit Externe

RingCentral :

i. Fait appel à des auditeurs tiers indépendants qualifiés pour effectuer des audits de sécurité couvrant les systèmes, les environnements et les réseaux dans lesquels les Données Protégées sont traitées, y compris :

a. SOC2 Type II.

b. IES/ISO 27001.

ii. Maintient des audits supplémentaires et des certifications de conformité selon les besoins de l'activité de RingCentral et selon ce qui est identifié sur www.ringcentral.com/trust-center.html.

B. Distribution des Rapports

Copies des rapports d'audit et des certifications pertinentes :

i. Seront fournis au Client sur demande.

ii. Sont sujet à un accord de non-divulgation/confidentialité.

C. Questionnaire Annuel d'évaluation des Risques

Le Client peut, une (1) fois au cours d'une période de douze (12) mois, demander à RingCentral de remplir un questionnaire d'évaluation des risques d'un tiers dans un délai raisonnable.

En cas de conflit entre cette section et la section équivalente dans le DPA de RingCentral, le DPA a la priorité.

5. Sécurité des Ressources Humaines

A. Vérification des Antécédents

RingCentral exige des vérifications préalables à l'embauche de tous les employés. RingCentral assure la vérification des antécédents criminels de ses employés dans la mesure permise par la loi. Chaque vérification des antécédents aux États-Unis comprend :

i. Une vérification d'identité (trace du SSN).

ii. Vérification des antécédents criminels jusqu'à sept (7) ans pour les crimes et délits au niveau local, étatique et fédéral, le cas échéant.

iii. Terroriste (OFAC), comme l'autorise la loi.

Au niveau international, les vérifications des antécédents criminels sont effectuées conformément à la législation locale.

Les vérifications des antécédents sont effectuées par un membre de la National Association of Professional Background Screeners ou par une entreprise compétente reconnue par le secteur dans la juridiction locale.

B. Formation

RingCentral veillera à ce que tous les employés, y compris les contractants :

i. Complétent la formation annuelle pour démontrer la familiarité avec les politiques de sécurité de RingCentral.

ii. Suivent une formation annuelle sur les exigences en matière de sécurité et de confidentialité, notamment la sensibilisation à la cybersécurité, le GDPR et le CCPA.

iii. Disposent des compétences et de l'expérience raisonnables et adaptées à un emploi et à un poste de confiance au sein de RingCentral.

C. Sécurité des Postes de Travail

RingCentral veillera à ce que :

i. Les employés de RingCentral utilisent soit des appareils appartenant à RingCentral et gérés par RingCentral dans l'exercice de leurs fonctions, soit un appareil Bring Your Own Device (BYOD).

ii. Tous les appareils, qu'il s'agisse d'appareils appartenant à RingCentral et gérés par RingCentral ou d'appareils Bring Your Own Device (BYOD), soient inscrits dans le programme complet d'appareils gérés par RingCentral.

D. Prévention des Pertes de Données

RingCentral utilise un système complet pour empêcher de compromettre involontairement ou intentionnellement des données RingCentral et des Données Protégées.

E. Diligence Raisonnable à l'égard des Sous-Traitants

RingCentral veillera a :

i. Maintenir un processus de sécurité pour effectuer une diligence raisonnable appropriée avant d'engager des sous-traitants.

ii. Évaluer périodiquement les capacités de sécurité de ces sous-traitants afin de s'assurer de leur capacité à se conformer aux mesures décrites dans le présent document.

iii. Appliquer des exigences écrites en matière de sécurité des informations qui obligent les sous-traitants à adhérer aux principales politiques et normes de RingCentral en matière de sécurité des informations, cohérentes avec les présentes Mesures et non moins protectrices.

F. Non-Divulgation

RingCentral veille à ce que les employés et les contractants/sous-contractants qui traitent des Données Protégées soient liés par écrit par des obligations de confidentialité.

6. Sécurité Physique

A. Général

RingCentral :

i. Restreint l'accès à, contrôle, et surveille toutes les zones physiques où les services RingCentral traitent des Données Protégées (**« zones sécurisées »**).

ii. Maintient des contrôles de sécurité physique appropriés, 24 heures sur 24 et 7 jours sur 7 (**« 24/7 »**).

iii. Révoque tout accès physique aux zones sécurisées rapidement après la cessation de la nécessité d'accéder aux bâtiments et au(x) système(s).

iv. Effectue une révision des droits d'accès au moins une fois par an.

B. Processus d'accès et d'autorisation

RingCentral maintient un processus documenté d'entrée et d'autorisation d'accès. Le processus d'autorisation et d'entrée comprendra au minimum les éléments suivants :

i. Rapports détaillant tous les accès aux zones sécurisées, y compris les identités et les dates et heures d'accès.

ii. Les rapports doivent être conservés pendant au moins un an, dans la mesure où les lois et réglementations applicables le permettent.

iii. Un équipement de vidéosurveillance pour surveiller et enregistrer l'activité à tous les points d'entrée et de sortie des zones sécurisées, 24 heures sur 24 et 7 jours sur 7, dans la mesure où les lois et réglementations applicables le permettent.

iv. L'enregistrement vidéo doit être conservé pendant au moins 30 jours ou selon les politiques du fournisseur de lieux physiques.

C. Centres de Données

Dans la mesure où RingCentral exploite ou utilise un centre de données, RingCentral s'assure que les contrôles de sécurité physique sont conformes aux normes de l'industrie telles que ISO 27001 et SSAE 16 ou ISAE 3402 ou une norme similaire, notamment :

i. Sécurité du périmètre, y compris clôtures/barrières et vidéosurveillance.

ii. Accès sécurisé comprenant un garde de sécurité/réception.

iii. Accès intérieur contrôlé par des cartes RFID, 2FA, contrôles anti-taillement.

iv. Alimentation redondante des services publics et prise en charge de la livraison continue par des systèmes de sauvegarde.

v. Connexion réseau redondante provenant de plusieurs fournisseurs.

7. Sécurité Logique

A. Identification et Authentification de l'utilisateur

RingCentral :

i. Maintient un processus documenté de gestion du cycle de vie de la gestion des utilisateurs qui comprend des processus manuels et/ou automatisés pour la création, la suppression et la modification des comptes approuvés pour toutes les ressources d'information et dans tous les environnements.

ii. Assure que les utilisateurs de RingCentral ont un compte individuel pour une traçabilité unique.

iii. S'assure que les utilisateurs de RingCentral n'utilisent pas de comptes partagés ; lorsque les comptes partagés sont techniquement nécessaires, des contrôles sont en place pour garantir la traçabilité.

iv. Les mots de passe des utilisateurs de RingCentral sont configurés conformément aux directives actuelles du NIST.

Pour les applications destinées aux Clients, les Clients peuvent choisir d'intégrer le SSO (Single Sign on) afin que le Client conserve le contrôle de ses paramètres de mot de passe requis, y compris les solutions MFA/2FA existantes du Client.

B. Autorisation des Utilisateurs et Contrôle d'accès

RingCentral :

i. Configure l'accès à distance à tous les réseaux stockant ou transmettant des Données Protégées pour exiger une authentification multifactorielle pour cet accès.

ii. Révoque l'accès aux systèmes et applications qui contiennent ou traitent des Données Protégées rapidement après la cessation de la nécessité d'accéder au(x) système(s) ou application(s).

iii. A la capacité de détecter, d'enregistrer et de signaler les accès au système et au réseau ou les tentatives de violation de la sécurité du système ou du réseau.

RingCentral emploie des mécanismes de contrôle d'accès qui sont destinés à :

i. Limiter l'accès aux Données Protégées aux seuls membres du Personnel qui ont un besoin raisonnable d'accéder aux dites données pour permettre à RingCentral d'exécuter ses obligations en vertu du Contrat.

ii. Empêcher l'accès non autorisé aux Données Protégées.

iii. Limitez l'accès aux utilisateurs qui ont un besoin professionnel de savoir.

iv. Suivre le principe du moindre privilège, en permettant l'accès aux seules informations et ressources nécessaires.

v. Effectuer un examen des contrôles d'accès sur une base annuelle minimum pour tous les systèmes de RingCentral qui transmettent, traitent ou stockent des Données Protégées.

8. Télécommunications et Sécurité des Réseaux

A. Gestion du Réseau

RingCentral :

i. Maintient le programme de sécurité du réseau qui comprend une protection par pare-feu conforme aux normes industrielles et une authentification à deux facteurs pour l'accès aux réseaux de RingCentral.

ii. Déploie un système de détection des intrusions (IDS) et/ou un système de prévention des intrusions (IPS) pour générer, surveiller et répondre aux alertes qui pourraient indiquer un compromit potentielle du réseau et/ou de l'hôte.

iii. Surveille le trafic web provenant d'Internet et de sources internes afin de détecter les cyber-attaques, notamment les attaques par déni de service distribué (DDoS) contre les sites/services web, et de bloquer le trafic malveillant.

B. Segmentation du Réseau

RingCentral :

i. Met en œuvre la segmentation du réseau entre le réseau d'entreprise de l'entreprise et les installations d'hébergement des Services.

ii. Assure la séparation entre les environnements dédiés au développement, au staging et à la production.

iii. Restreint l'accès entre les environnements aux dispositifs autorisés.

iv. Contrôle la configuration et la gestion de la séparation des réseaux et des règles de pare-feu par le biais d'un processus formel de demande et d'approbation.

C. Analyse de la Vulnérabilité du Réseau

RingCentral :

i. Effectue au moins une fois par trimestre des analyses de la vulnérabilité des réseaux internes et externes des systèmes de traitement de l'information.

ii. Évalue les résultats en fonction (le cas échéant) du score CVSS et de l'évaluation de l'impact, de la probabilité et de la gravité.

iii. Corriger les résultats en suivant les délais standard du secteur.

9. Sécurité des Opérations

A. Gestion des Actifs

RingCentral :

i. Tient un registre des actifs précis et à jour couvrant les actifs matériels et logiciels utilisés pour la prestation de Services.

ii. Maintient la responsabilité des actifs tout au long de leur cycle de vie.

iii. Maintient des processus pour effacer ou détruire physiquement les actifs physiques avant leur élimination.

B. Gestion de la Configuration

RingCentral :

i. Maintient les configurations de base des systèmes d'information et des applications sur la base des meilleures pratiques du secteur, notamment :

a. Suppression de tous les mots de passe fournis par les fournisseurs.

b. Suppression/désactivation des services et paramètres inutilisés

c. Protection contre les logiciels malveillants et les points finaux, dans la mesure où cela est techniquement possible.

ii. Applique les paramètres de configuration de sécurité pour les systèmes utilisés dans la fourniture des services.

iii. Assure que les horloges de tous les systèmes de traitement de l'information sont synchronisées avec une ou plusieurs sources de temps de référence.

C. Protection Contre les Codes Malveillants

i. Dans la mesure du possible, RingCentral a mis en place une protection des points d'extrémité, sous la forme d'un logiciel de détection et de réponse aux points d'extrémité (EDR) et/ou d'un logiciel antivirus, installé et fonctionnant sur les serveurs et les postes de travail.

ii. Les alertes EDR sont surveillées et des mesures immédiates sont prises pour examiner et corriger tout comportement anormal.

iii. Lorsqu'il est utilisé, le logiciel antivirus est à jour et fonctionne pour rechercher et supprimer rapidement ou mettre en quarantaine les virus et autres logiciels malveillants sur les serveurs et les postes de travail Windows.

D. Vulnérabilité, Correctifs de Sécurité

RingCentral :

i. Surveille les vulnérabilités et les expositions divulguées publiquement afin de déterminer leur impact sur les systèmes d'information et les produits du fournisseur.

ii. Assure les tests d'assurance qualité des correctifs avant le déploiement.

iii. S'assure que tous les résultats de l'analyse des vulnérabilités du réseau et des vulnérabilités et expositions pertinentes divulguées publiquement sont corrigés conformément aux meilleures pratiques

du secteur, y compris le score CVSS et l'évaluation de l'impact, de la probabilité et de la gravité, et qu'ils sont corrigés en respectant les délais standard du secteur.

E. Journalisation et Surveillance

RingCentral doit s'assurer que :

i. Tous les systèmes, dispositifs ou applications associés à l'accès, au traitement, au stockage, à la communication et/ou à la transmission de Données Protégées, génèrent des journaux d'audit.

ii. L'accès aux Données Protégées est enregistré.

iii. Les journaux comportent suffisamment de détails pour pouvoir être utilisés afin de détecter une activité non autorisée importante.

iv. Les journaux sont protégés contre les accès, les modifications et les suppressions non autorisés.

v. Les journaux sont envoyés à un emplacement centralisé pour l'agrégation et la surveillance.

10. Développement et Maintenance de Logiciels

A. Cycle de Vie du Développement Sécurisé

RingCentral :

i. Applique les pratiques du cycle de développement sécurisé, notamment pendant les cycles de conception, de développement et de test.

ii. S'assure que les produits font l'objet d'un examen de la conception de la sécurité, y compris les considérations relatives aux menaces et les pratiques de traitement des données.

iii. Veille à ce que les Services fassent l'objet d'une révision de la version sécurisée avant leur mise en production.

B. Test de Sécurité

Dans le cadre du cycle de vie du développement sécurisé, RingCentral :

i. Effectue des tests de sécurité rigoureux, y compris, dans la mesure où cela est techniquement possible :

a. l'analyse statique du code.

b. des examens par les pairs du code source.

c. des tests de sécurité dynamiques et interactifs.

d. la logique de sécurité, ou les tests « QA » de sécurité.

ii. Veille à ce que les applications orientées vers l'Internet soient soumises à des examens et à des tests d'évaluation de la sécurité des applications afin d'identifier les vulnérabilités de sécurité communes identifiées par des organisations reconnues par l'industrie (par exemple, les 10 principales vulnérabilités de l'OWASP, les 25 principales vulnérabilités du CWE/SANS).

iii. Pour toutes les applications mobiles (c'est-à-dire fonctionnant sur Android, Blackberry, iOS, Windows Phone) qui collectent, transmettent ou affichent des Données Protégées, effectuer un examen de l'évaluation de la sécurité des applications afin d'identifier et de remédier aux vulnérabilités spécifiques aux applications mobiles reconnues par l'industrie.

iv. N'utilise PAS de Données Protégées pour les tests.

v. Fait tous les efforts raisonnables pour identifier et corriger les vulnérabilités des logiciels avant leur diffusion.

C. Test de Pénétration Annuel

RingCentral :

i. Engage des testeurs de pénétration tiers qualifiés et indépendants pour effectuer un test de pénétration annuel contre ses produits et les environnements où les Données Protégées sont hébergées.

ii. Exige que les sous-traitants effectuent des tests de pénétration similaires sur leurs systèmes, environnements et réseaux.

iii. Veille à ce que tous les résultats soient corrigés dans un délai commercialement raisonnable.

D. Gestion de la Vulnérabilité des Produits

RingCentral :

i. Fait des efforts commercialement raisonnables pour identifier régulièrement les vulnérabilités de sécurité logicielle dans les services RingCentral.

ii. Fournit des mises à jour, des mises à niveau et des corrections de bug pertinents pour les vulnérabilités de sécurité logicielle connues, pour tout logiciel fourni ou dans lequel des Données Protégées sont traitées.

iii. S'assure que tous les résultats des tests internes et externes sont évalués selon les meilleures pratiques du secteur, y compris le score CVSS et l'évaluation de l'impact, de la probabilité et de la gravité, et qu'il y est remédié selon les délais standard du secteur.

E. Logiciels Libres et Tiers

RingCentral :

i. Tient un registre des actifs de tous les logiciels tiers (TPS) et des logiciels libres (OSS) incorporés dans les Services.

ii. Utilise des efforts commercialement raisonnables pour assurer le développement et la sécurité des logiciels open source et des logiciels tiers utilisés par RingCentral.

iii. Déploie des efforts commercialement raisonnables pour évaluer, suivre et corriger les vulnérabilités des logiciels libres (OSS) et autres bibliothèques de tiers qui sont incorporés dans les Services.

11. Traitement des Données

A. Classification des Données

RingCentral maintient des normes de classification des données, notamment :

i. Données publiques, données qui sont généralement disponibles ou censées être connues du public.

ii. Données confidentielles, données qui ne sont pas accessibles au grand public.

Les Données Protégées sont classées comme des données confidentielles RingCentral.

B. Ségrégation des Données

RingCentral :

i. Assure la ségrégation physique ou logique des Données Protégées par rapport aux données des autres clients.

ii. Assurer la séparation physique et le contrôle d'accès pour séparer les Données Protégées des données RingCentral.

C. Cryptage des Données

RingCentral :

i. Doit assurer le cryptage des Données Protégées sous forme électronique en transit sur tous les réseaux publics câblés (par exemple, Internet) et tous les réseaux sans fil (à l'exclusion des communications sur les réseaux téléphoniques publics commutés).

ii. À l'exception de la fonction Engage Communities d'Engage Digital, doit assurer le cryptage des Données Protégées sous forme électronique lorsqu'elles sont stockées au repos.

iii. Utilise des algorithmes de cryptage et des forces de clés conformes aux normes industrielles pour crypter les Données Protégées en transit sur tous les réseaux publics câblés (par exemple, Internet) et tous les réseaux sans fil.

D. Destruction des Données

RingCentral doit :

i. Assurer la suppression sécurisée des données lorsqu'elles ne sont plus nécessaires.

ii. S'assurer que les supports électroniques qui ont été utilisés dans le cadre de la fourniture de services au Client seront nettoyés avant d'être éliminés ou réutilisés, en utilisant un processus qui garantit la suppression des données et empêche leur reconstruction ou leur lecture.

iii. Détruire tout équipement contenant des Données Protégées qui est endommagé ou non fonctionnel.

12. Réponse aux Incidents

La capacité de réponse aux incidents de RingCentral est conçue pour se conformer aux obligations légales et réglementaires régissant la réponse aux incidents. En tant que tel, RingCentral :

A. Maintient une capacité de réponse aux incidents pour répondre aux événements susceptibles d'avoir un impact sur la confidentialité, l'intégrité et/ou la disponibilité des services et/ou des données, y compris les Données Protégées.

B. Dispose d'un plan de réponse aux incidents documenté, basé sur les meilleures pratiques du secteur.

C. Dispose d'un processus de traitement des preuves qui protège l'intégrité des preuves recueillies, notamment en permettant la détection d'accès non autorisés à ces preuves.

D. Prendra les dispositions et les mesures appropriées pour se conformer aux obligations légales et réglementaires régissant la réponse aux incidents.

Lorsque RingCentral apprend ou découvre un événement de sécurité qui a un impact sur les Données Protégées, RingCentral en informera le Client sans délai excessif et prendra des mesures commercialement raisonnables pour isoler, atténuer et/ou remédier à cet événement.

13. Continuité des Activités et Reprise Après Sinistre

A. La Continuité des Activités

RingCentral :

i. S'assure que les responsabilités en matière de continuité des services sont clairement définies et documentées et qu'elles ont été attribuées à une personne disposant d'une autorité suffisante.

ii. A mis en place un plan de continuité des activités (PCA) conçu pour assurer la fourniture continue des Services au Client.

iii. Développe, met en œuvre et maintient un programme de gestion de la continuité des activités pour répondre aux besoins de l'entreprise et des Services fournis au Client. À cette fin, RingCentral réalise un niveau minimum d'analyse de l'impact sur l'entreprise, de gestion de crise, de continuité de l'activité et de planification de la reprise après sinistre.

iv. S'assurer que le champ d'application du PCA englobe tous les sites, le personnel et les systèmes d'information pertinents utilisés pour fournir les Services.

v. Veille à ce que son PCA comprenne, sans s'y limiter, des éléments tels que des solutions de rechange pour les lieux, les applications, les fournisseurs et le personnel, et qu'il soit exercé au moins une fois par an.

vi. Examiner, mettre à jour et tester le PCA au moins une fois par an.

B. La Reprise Après Sinistre

RingCentral :

i. Maintient un plan de reprise après sinistre, qui comprend, sans s'y limiter, des détails sur l'infrastructure, la technologie et le(s) système(s), les activités de reprise, et identifie les personnes/équipes nécessaires à cette reprise, exercé au moins une fois par an.

ii. S'assurer que le plan de reprise après sinistre prévoit les mesures que RingCentral prendra en cas d'interruption prolongée du service.

iii. Veille à ce que ses plans prévoient les mesures et les ressources nécessaires pour assurer (i) le fonctionnement continu de RingCentral et (ii) en cas d'interruption, le rétablissement des fonctions nécessaires pour permettre à RingCentral de fournir les services, y compris les systèmes, le matériel, les logiciels, les ressources, le personnel et les données nécessaires pour soutenir ces fonctions.