ADDENDUM SULLA SICUREZZA DI RINGCENTRAL

1. Portata

Questo documento descrive le Misure di Sicurezza delle Informazioni (**"Misure"**) che RingCentral ha messo in atto nel trattamento dei Dati Protetti attraverso i Servizi RingCentral.

2. Definizioni

Solo ai fini del presente Addendum di sicurezza, i termini in maiuscolo, non altrimenti definiti nel presente documento, hanno il significato stabilito nel Contratto.

A. **"Servizi Ring Central"**, o **"Servizi"**, indica i servizi offerti da RingCentral e acquistati dal Cliente.

B. **"Cliente"** indica l'entità che ha stipulato l'Accordo con RingCentral.

C. **"Dati protetti"** indica i dati del Cliente e dei partner trattati nell'ambito dei Servizi RingCentral, come definiti nel DPA o nell'Accordo RingCentral applicabile, inclusi i "dati personali" e le "informazioni personali" come definiti dalle leggi sulla privacy applicabili, i dati riservati come definiti nell'Accordo, i dati dell'account, i dati di configurazione, il contenuto delle comunicazioni inclusi i messaggi, la segreteria telefonica e la registrazione video.

D. **"Accordo"** indica l'accordo in essere tra RingCentral e il Cliente per la fornitura dei Servizi.

E. **"Personale"** indica i dipendenti di RingCentral, gli appaltatori o il personale dei Servizi in subappalto.

3. Gestione della Sicurezza delle Informazioni

A. Programma di Sicurezza

RingCentral mantiene un programma scritto di sicurezza delle informazioni che:

i. Include politiche documentate o standard appropriati per governare il trattamento dei Dati Protetti in conformità con l'Accordo e con la legge applicabile.

ii. È gestito da un dipendente senior responsabile della supervisione e dell'attuazione del programma.

iii. Include garanzie amministrative, tecniche e fisiche ragionevolmente progettate per proteggere la riservatezza, l'integrità e la disponibilità dei dati protetti.

iv. È appropriato alla natura, alle dimensioni e alla complessità delle operazioni commerciali di RingCentral.

B. Gestione dei Criteri di Sicurezza

Politiche, standard e procedure di sicurezza di RingCentral:

i. Sono allineati agli standard industriali stabiliti per la sicurezza delle informazioni.

ii. Sono soggetti a revisione continua.

iii. Possono essere rivisti per riflettere i cambiamenti nelle migliori pratiche del settore.

C. Gestione del Rischio

RingCentral:

i. Esegue valutazioni del rischio di cybersecurity per identificare le minacce alle attività o alle operazioni almeno annualmente.

ii. Aggiorna le proprie politiche, procedure e standard, se necessario, per affrontare le minacce all'attività o alle operazioni di RingCentral.

4. Valutazioni di Sicurezza Indipendenti

A. Audit Esterno

RingCentral:

i. Utilizza revisori indipendenti qualificati di terze parti per eseguire controlli di sicurezza su sistemi, ambienti e reti in cui vengono elaborati i Dati Protetti, tra cui:

a. SOC2 Tipo II.

b. IES/ISO 27001.

ii. Mantiene ulteriori controlli e certificazioni di conformità come appropriato per l'attività di RingCentral e come identificato in www.ringcentral.com/trust-center.html.

B. Distribuzione dei Rapporti

Copie dei rapporti di audit e delle certificazioni pertinenti:

i. Saranno fornite al cliente su richiesta.

ii. Sono soggetti all'accordo di non divulgazione.

C. Questionario Annuale di Valutazione del Rischio

Il cliente può, in una (1) occasione all'interno di ogni periodo di dodici (12) mesi, richiedere che RingCentral completi un questionario di valutazione dei rischi di terzi entro un periodo di tempo ragionevole.

In caso di conflitto tra questa sezione e la sezione equivalente nel DPA di RingCentral, il DPA prevale.

5. Sicurezza delle Risorse Umane

A. Controlli sul Passato

RingCentral effettua controlli pre-assunzione per tutti i dipendenti. RingCentral garantisce ricerche sui precedenti penali dei suoi dipendenti nella misura consentita dalla legge. Ogni controllo dei precedenti penali negli Stati Uniti include:

i. Una verifica dell'identità (traccia SSN).

ii. Controlli dei precedenti penali fino a sette (7) anni per reati a livello locale, statale e federale, se del caso.

iii. Ricerca sulla lista dei terroristi (OFAC), come consentito dalla legge.

A livello internazionale, i controlli dei precedenti penali sono condotti come consentito dalla legge locale.

I controlli dei precedenti penali sono condotti da un membro della National Association of Professional Background Screeners o da un'azienda competente riconosciuta nella giurisdizione locale.

B. Formazione

RingCentral si assicurerà che tutti i dipendenti, compresi gli appaltatori, abbiano:

i. Completato la formazione annuale per dimostrare la conoscenza delle politiche di sicurezza di RingCentral.

ii. Completato la formazione annuale per i requisiti di sicurezza e privacy, compresa la conoscenza di CyberSecurity, GDPR e CCPA.

iii. La abilità ed esperienza ragionevolmente adatta per ricoprire una posizione di fiducia all'interno di RingCentral.

C. Sicurezza della Stazione di Lavoro

RingCentral assicura che:

i. I dipendenti RingCentral utilizzano dispositivi posseduti e gestiti da RingCentral nello svolgimento delle loro mansioni o dispositivi BYOD (Bring Your Own Device).

ii. Tutti i dispositivi, sia quelli posseduti e gestiti da RingCentral che quelli BYOD (Bring Your Own Device), sono iscritti al programma completo di gestione dei dispositivi RingCentral.

D. Prevenzione della Perdita di Dati

RingCentral impiega un sistema completo per prevenire la compromissione involontaria o intenzionale dei dati RingCentral e dei Dati Protetti.

E. Due Diligence sui Subappaltatori

RingCentral:

i. Mantiene un processo di sicurezza per condurre un'adeguata due diligence prima di nominare subappaltatori.

ii. Valuta periodicamente le capacità di sicurezza di tali subappaltatori per garantire la capacità di questi di rispettare le misure descritte in questo documento.

iii. Applica requisiti di sicurezza delle informazioni che obblighino i subappaltatori ad aderire alle politiche e agli standard di sicurezza delle informazioni chiave di RingCentral, coerenti e non meno protettivi rispetto a queste Misure.

F. Non Divulgazione

RingCentral assicura che i dipendenti e gli appaltatori/subappaltatori che trattano i Dati Protetti sono vincolati per iscritto da obblighi di riservatezza.

6. Sicurezza Fisica

A. Generale

RingCentral:

i. Limita l'accesso, controlla e monitora tutte le aree fisiche in cui i Servizi RingCentral elaborano i Dati Protetti (**"Aree Protette"**).

ii. Mantiene adeguati controlli di sicurezza fisica 24 ore al giorno, 7 giorni alla settimana (**"24/7"**).

iii. Revoca qualsiasi accesso fisico alle Aree Protette prontamente dopo la cessazione della necessità di accedere agli edifici e ai sistemi.

iv. Esegue la revisione dei diritti di accesso su base almeno annuale.

B. Processi di Accesso e Autorizzazione

RingCentral mantiene un processo di autorizzazione e registrazione degli accessi documentato. Il processo di autorizzazione e registrazione includerà come minimo:

i. Rapporti che dettagliano tutti gli accessi alle aree sicure, comprese le identità e le date e gli orari di accesso.

ii. I rapporti devono essere mantenuti per almeno un anno come previsto dalla legge.

iii. Apparecchiature di videosorveglianza per monitorare e registrare l'attività in tutti i punti di entrata e uscita delle aree sicure 24 ore su 24, 7 giorni su 7, nella misura consentita dalle leggi e dai regolamenti applicabili.

iv. Le registrazioni video devono essere mantenute per almeno 30 giorni o secondo le politiche del fornitore del luogo fisico.

C. Centri Dati

Nella misura in cui RingCentral gestisce o utilizza un data center, RingCentral garantisce che i controlli di sicurezza fisica siano in linea con gli standard di settore come ISO 27001 e SSAE 16 o ISAE 3402 o standard simili che includono:

i. Sicurezza perimetrale con recinzioni/barriere e videosorveglianza.

ii. Accesso sicuro con guardia di sicurezza/reception.

iii. Accesso interno controllato tramite carte RFID, 2FA, controlli anti-tailgating.

iv. Alimentazione ridondante e supporto per la consegna continua attraverso sistemi di backup.

v. Connessione di rete ridondante da più fornitori.

7. Sicurezza Logica

A. Identificazione ed Autenticazione dell'utente

RingCentral:

i. Mantiene un processo documentato di gestione del ciclo di vita della gestione degli utenti che include processi manuali e/o automatizzati per la creazione di account approvati, la rimozione di account e la modifica di account per tutte le risorse informative e in tutti gli ambienti.

ii. Assicura che gli utenti di RingCentral abbiano un account individuale per una tracciabilità unica.

iii. Assicura che gli utenti di RingCentral non usino account condivisi; dove gli account condivisi sono tecnicamente richiesti, i controlli sono in atto per assicurare la tracciabilità.

iv. Le password degli utenti RingCentral sono configurate in linea con l'attuale guida NIST.

Per le applicazioni rivolte al cliente, i clienti possono scegliere di integrarsi con SSO (Single Sign on) in modo che il cliente mantenga il controllo sulle impostazioni delle password richieste, comprese le soluzioni MFA/2FA esistenti del cliente.

B. Autorizzazione dell'utente e Controllo dell'accesso

RingCentral:

i. Configura l'accesso remoto a tutte le reti che memorizzano o trasmettono Dati Protetti per richiedere l'autenticazione a più fattori per tale accesso.

ii. Revoca l'accesso ai sistemi e alle applicazioni che contengono o elaborano Dati Protetti prontamente dopo la cessazione della necessità di accedere ai sistemi o alle applicazioni.

iii. Ha la capacità di rilevare, registrare e segnalare l'accesso al sistema e alla rete o i tentativi di violare la sicurezza del sistema o della rete.

RingCentral impiega meccanismi di controllo dell'accesso che hanno lo scopo di:

i. Limitare l'accesso ai Dati Protetti solo a quel Personale che ha una ragionevole necessità di accedere a tali dati per consentire a RingCentral di adempiere ai propri obblighi previsti dall'Accordo.

ii. Prevenire l'accesso non autorizzato ai Dati Protetti.

iii. Limitare l'accesso agli utenti che hanno un bisogno aziendale di sapere.

iv. Seguire il principio del minimo privilegio, permettendo l'accesso solo alle informazioni e alle risorse che sono necessarie.

v. Eseguire i controlli di accesso su base almeno annuale per tutti i sistemi RingCentral che trasmettono, elaborano o memorizzano Dati Protetti.

8. Sicurezza delle Telecomunicazioni e delle Reti

A. Gestione della Rete

RingCentral:

i. Mantiene il programma di sicurezza della rete che include la protezione firewall standard del settore e l'autenticazione a due fattori per l'accesso alle reti RingCentral.

ii. Distribuisce un sistema di rilevamento delle intrusioni (IDS) e/o un sistema di prevenzione delle intrusioni (IPS) per generare, monitorare e rispondere agli avvisi che potrebbero indicare una potenziale compromissione della rete e/o dell'host.

iii. Monitora il traffico web da Internet e da fonti interne per rilevare i cyber-attacchi compresi gli attacchi Distributed Denial of Service (DDoS) contro i siti web / servizi e per bloccare il traffico dannoso.

B. Segmentazione della Rete

RingCentral:

i. Implementa la segmentazione della rete tra la rete aziendale e le strutture di hosting per i servizi.

ii. Assicura la separazione tra gli ambienti dedicati allo sviluppo, alla messa in scena e alla produzione.

iii. Limita l'accesso tra gli ambienti ai dispositivi autorizzati.

iv. Controlla la configurazione e la gestione della segregazione della rete e delle regole del firewall attraverso un processo formale di richiesta e approvazione.

C. Scansione delle Vulnerabilità di Rete

RingCentral:

i. Esegue scansioni di vulnerabilità di rete interne ed esterne contro i sistemi di elaborazione delle informazioni almeno trimestralmente.

ii. Valuta i risultati in base al punteggio CVSS (se applicabile) e alla valutazione di impatto, probabilità e gravità.

iii. Rimedia ai risultati seguendo le tempistiche standard del settore.

9. Sicurezza delle Operazioni

A. Gestione delle Risorse

RingCentral:

i. Mantiene un registro dei beni accurato e aggiornato che copre i beni hardware e software utilizzati per la fornitura di servizi.

ii. Mantiene la responsabilità dei beni per tutto il loro ciclo di vita.

iii. Mantiene i processi per cancellare o distruggere fisicamente le risorse fisiche prima del loro smaltimento.

B. Gestione della Configurazione

RingCentral:

i. Mantiene le configurazioni di base dei sistemi informativi e delle applicazioni basate sulle migliori pratiche del settore, tra cui:

a. Rimozione di tutte le password fornite dal fornitore.

b. Rimuovere/disattivare i servizi e le impostazioni non utilizzati.

c. Protezione anti-malware/endpoint come tecnicamente possibile.

ii. Applica le impostazioni di configurazione di sicurezza per i sistemi utilizzati nella fornitura dei Servizi.

iii. Assicura che gli orologi di tutti i sistemi di elaborazione delle informazioni siano sincronizzati con una o più fonti di tempo di riferimento.

C. Protezione dal Codice Maligno

i. Per quanto possibile, RingCentral dispone di una protezione degli endpoint, sotto forma di Endpoint Detection and Response (EDR) e/o software antivirus, installati e funzionanti su server e workstation.

ii. Gli avvisi EDR sono monitorati e vengono intraprese azioni immediate per indagare e porre rimedio a qualsiasi comportamento anomalo.

iii. Dove usato, il software antivirus sarà aggiornato e funzionante per scansionare e rimuovere prontamente o mettere in quarantena virus e altri malware su server e workstation Windows.

D. Vulnerabilità, Patch di Sicurezza

RingCentral:

i. Monitora le vulnerabilità e le esposizioni divulgate pubblicamente per l'impatto sui sistemi informativi e sui prodotti del fornitore.

ii. Assicura il test di garanzia della qualità delle patch prima della distribuzione.

iii. Assicura che tutti i risultati derivanti dalla scansione delle vulnerabilità di rete e le vulnerabilità rilevanti divulgate pubblicamente e le esposizioni siano corrette secondo le migliori pratiche del settore, compreso il punteggio CVSS e la valutazione dell'impatto, della probabilità e della gravità e siano corrette seguendo le tempistiche standard del settore.

E. Registrazione e Monitoraggio

RingCentral deve garantire che:

i. Tutti i sistemi, i dispositivi o le applicazioni associati all'accesso, all'elaborazione, all'archiviazione, alla comunicazione e/o alla trasmissione di Dati Protetti, generano registri di controllo.

ii. L'accesso ai Dati Protetti è registrato.

iii. I registri includono dettagli sufficienti che possono essere utilizzati per rilevare attività significative non autorizzate.

iv. I registri sono protetti da accessi, modifiche e cancellazioni non autorizzate.

v. I registri vengono inviati a una posizione centralizzata per l'aggregazione e il monitoraggio.

10. Sviluppo e manutenzione del software

A. Ciclo di Vita di Sviluppo Sicuro

RingCentral:

i. Applica pratiche sicure del ciclo di vita dello sviluppo, incluso, durante i cicli di progettazione, sviluppo e test.

ii. Assicura che i prodotti siano soggetti alla revisione del design di sicurezza, comprese le considerazioni sulle minacce e le pratiche di gestione dei dati.

iii. Assicura che i servizi siano soggetti a una revisione sicura del rilascio prima della promozione alla produzione.

B. Test di Sicurezza

Come parte del ciclo di vita dello sviluppo sicuro, RingCentral:

i. Esegue rigorosi test di sicurezza, tra cui, come tecnicamente fattibile:

a. Analisi statica del codice.

b. Revisioni tra pari del codice sorgente.

c. Test di sicurezza dinamici e interattivi.

d. Logica di sicurezza, o test “QA” di sicurezza.

ii. Assicura che le applicazioni rivolte a Internet siano soggette a revisioni e test di valutazione della sicurezza delle applicazioni per identificare le vulnerabilità di sicurezza comuni come identificate da organizzazioni riconosciute dal settore (ad esempio, OWASP Top 10 Vulnerabilities, CWE/SANS Top 25 vulnerabilità).

iii. Per tutte le applicazioni mobili (cioè in esecuzione su Android, Blackberry, iOS, Windows Phone) che raccolgono, trasmettono o visualizzano dati protetti, conduce una revisione della valutazione della sicurezza delle applicazioni per identificare e rimediare alle vulnerabilità riconosciute dal settore specifiche delle applicazioni mobili.

iv. NON utilizza Dati Protetti per i test.

v. Fa ogni ragionevole sforzo per identificare e correggere le vulnerabilità del software prima del rilascio.

C. Test di Penetrazione Annuale

RingCentral:

i. Ingaggia dei penetration tester qualificati e indipendenti di terze parti per eseguire dei penetration test annuali contro i suoi prodotti e gli ambienti in cui sono ospitati i Dati Protetti.

ii. Richiede ai sub-responsabili di eseguire simili test di penetrazione contro i loro sistemi, ambienti e reti.

iii. Assicura il rimedio di tutti i risultati in un periodo di tempo commercialmente ragionevole.

D. Gestione della Vulnerabilità dei Prodotti

RingCentral:

i. Utilizza sforzi commercialmente ragionevoli per identificare regolarmente le vulnerabilità di sicurezza del software nei Servizi RingCentral.

ii. Fornisce aggiornamenti, upgrade e bug fix per le vulnerabilità di sicurezza note del software, per qualsiasi software fornito o in cui vengono elaborati i Dati Protetti.

iii. Assicura che tutti i risultati derivanti dai test interni ed esterni siano valutati secondo le migliori prassi del settore, compreso il punteggio CVSS e la valutazione dell’impatto, della probabilità e della gravità, e siano risolti seguendo le tempistiche standard del settore.

E. Software Open Source e di Terze Parti

RingCentral:

i. Mantiene un registro delle risorse di tutto il software di terze parti (TPS) e del software open source (OSS) incorporato nei servizi.

ii. Utilizza sforzi commercialmente ragionevoli per garantire lo sviluppo sicuro e la sicurezza del software open source e del software di terze parti utilizzato da RingCentral.

iii. Utilizza sforzi commercialmente ragionevoli per valutare, tracciare e porre rimedio alle vulnerabilità del software open source (OSS) e di altre librerie di terze parti che sono incorporate nei Servizi.

11. Trattamento dei Dati

A. Classificazione dei Dati

RingCentral mantiene degli standard di classificazione dei dati che includono:

i. Dati pubblici, dati che sono generalmente disponibili o che ci si aspetta siano conosciuti dal pubblico.

ii. Dati confidenziali, dati che non sono disponibili al pubblico.

I Dati Protetti sono classificati come dati riservati RingCentral.

B. Segregazione dei Dati

RingCentral:

i. Assicura la segregazione fisica o logica dei Dati Protetti dai dati di altri clienti.

ii. Assicura la separazione fisica e il controllo degli accessi per separare i Dati Protetti dai dati RingCentral.

C. Crittografia dei Dati

RingCentral:

i. Deve garantire la crittografia dei Dati Protetti in forma elettronica in transito su tutte le reti pubbliche cablate (ad esempio, Internet) e tutte le reti wireless (escluse le comunicazioni su reti telefoniche pubbliche).

ii. Ad eccezione della funzione Engage Communities di Engage Digital, deve garantire la crittografia dei Dati Protetti in forma elettronica quando sono conservati a riposo.

iii. Utilizza algoritmi di crittografia standard del settore e la forza delle chiavi per crittografare i Dati Protetti in transito su tutte le reti pubbliche cablate (ad esempio, Internet) e tutte le reti wireless.

D. Distruzione dei Dati

RingCentral deve:

i. Assicurare la cancellazione sicura dei dati quando non sono più necessari.

ii. Garantire che i supporti elettronici che sono stati utilizzati nella fornitura dei Servizi al Cliente saranno disinfettati prima dello smaltimento o del riuso, utilizzando un processo che assicura la cancellazione dei dati e impedisce la ricostruzione o la lettura dei dati.

iii. Distruggere qualsiasi apparecchiatura *contenente* dati protetti *che sia danneggiata o non funzionante.*

12. Risposta Agli Incidenti

La capacità di risposta agli incidenti di RingCentral è progettata per rispettare gli obblighi legali e normativi che regolano la risposta agli incidenti. Come tale, RingCentral:

A. Mantiene una capacità di risposta agli incidenti per rispondere agli eventi che potenzialmente hanno un impatto sulla riservatezza, l'integrità e/o la disponibilità dei servizi e/o dei dati, compresi i Dati Protetti.

B. Ha un piano documentato di risposta agli incidenti basato sulle migliori prassi del settore.

C. Ha un processo per la gestione delle prove che salvaguarda l'integrità delle prove raccolte, incluso il rilevamento di accessi non autorizzati.

D. Prenderà provvedimenti e misure appropriate per rispettare gli obblighi legali e normativi che regolano la risposta agli incidenti.

Quando RingCentral viene a conoscenza o scopre un evento di sicurezza che ha un impatto sui Dati Protetti, RingCentral informerà il Cliente senza indebito ritardo e prenderà misure commercialmente ragionevoli per isolare, mitigare e/o rimediare a tale evento.

13. Buiness Continuity e Disaster Recovery

A. Continuità del Business

RingCentral:

i. Assicura che le responsabilità per la continuità del servizio siano chiaramente definite e documentate e che siano state assegnate a un individuo con sufficiente autorità.

ii. Ha un piano di continuità aziendale (BCP) in atto progettato per fornire la fornitura continua dei Servizi al Cliente.

iii. Sviluppa, implementa e mantiene un programma di gestione della continuità aziendale per rispondere alle esigenze dell'azienda e dei Servizi forniti al Cliente. A tal fine, RingCentral completa un livello minimo di analisi dell'impatto aziendale, gestione delle crisi, continuità aziendale e pianificazione del disaster recovery.

iv. Assicura che l'ambito del BCP comprenda tutte le sedi, il personale e i sistemi informativi pertinenti utilizzati per fornire i servizi.

v. Assicurarsi che il suo BCP includa, ma non solo, elementi quali soluzioni alternative per l'ubicazione, soluzioni alternative per le applicazioni, soluzioni alternative per i fornitori e soluzioni alternative per il personale, esercitate almeno annualmente.

vi. Rivede, aggiorna e testa il BCP almeno annualmente.

B. Recupero da Disastri

RingCentral:

i. Mantiene un piano di disaster recovery, che include, ma non si limita a, i dettagli dell'infrastruttura, della tecnologia e dei sistemi, le attività di recupero e identifica le persone/squadre necessarie per tale recupero, esercitato almeno annualmente.

ii. Assicura che il piano di disaster recovery affronti le azioni che RingCentral intraprenderà in caso di un'interruzione prolungata del servizio.

iii. Assicura che i suoi piani affrontino le azioni e le risorse necessarie per fornire (i) il funzionamento continuo di RingCentral, e (ii) in caso di interruzione, il recupero delle funzioni necessarie per consentire a RingCentral di fornire i Servizi, compresi i sistemi necessari, l'hardware, il software, le risorse, il personale e i dati che supportano tali funzioni.