Misure tecniche e organizzative
Rescue e Rescue Lens

Sommario esecutivo

Il presente documento sulle Misure tecniche e organizzative ("TOM") definisce gli impegni di GoTo in materia di privacy, sicurezza e responsabilità per Rescue e Rescue Lens. In particolare, GoTo mantiene solidi programmi globali di privacy e sicurezza e salvaguardie organizzative, amministrative e tecniche progettate per: (i) garantire la riservatezza, l'integrità e la disponibilità dei Contenuti del Cliente; (ii) proteggere dalle minacce e dai pericoli per la sicurezza dei Contenuti del Cliente; (iii) proteggere da qualsiasi perdita, abuso, accesso non autorizzato, divulgazione, alterazione e distruzione dei Contenuti del Cliente; e (iv) mantenere la conformità alle leggi e ai regolamenti applicabili, incluse le leggi sulla protezione dei dati e sulla privacy. Tali misure includono:

- **Crittografia:**
  - *In transito* Transport Layer Security (TLS) versione 1.2.
  - *A riposo* Transparent Data Encryption (TDE) con Advanced Encryption Standard (AES) a 256 bit per i Contenuti del Cliente.
- **Centri dati:**[1] I centri dati in Stati Uniti, Germania e Irlanda supportano la ridondanza e la stabilità.
- **Sicurezza fisica:** Sono in atto controlli ambientali e di sicurezza fisica adeguati, intesi per proteggere, controllare e limitare l'accesso fisico ai sistemi e ai server che gestiscono i Contenuti del Cliente per supportare la disponibilità, le prestazioni e la scalabilità.
- **Audit di conformità:** Rescue detiene le certificazioni ISO/IEC 27001:2013, SOC 2 Tipo II, PCI DSS, PCAOB, TRUSTe Enterprise Privacy e CBPR e PRP dell'APEC.
- **Conformità legale/normativa:** GoTo mantiene in essere un programma completo per la protezione dei dati, con processi e criteri progettati per garantire che i Contenuti del Cliente siano gestiti in conformità con le leggi sulla privacy applicabili, tra cui GDPR, CCPA/CPRA e LGPD.
- **Valutazioni della sicurezza**: Oltre ai test interni, GoTo si avvale della collaborazione di aziende esterne per la conduzione di regolari valutazioni della sicurezza e/o test di penetrazione.
- **Controlli di accesso logico:** I controlli di accesso logico sono implementati e progettati per prevenire o limitare la minaccia di accesso non autorizzato alle applicazioni e la perdita di dati negli ambienti aziendali e di produzione.
- **Segregazione dei dati**: GoTo utilizza un'architettura multi-tenant e separa logicamente gli account dei clienti a livello di database.
- **Sicurezza perimetrale e rilevamento delle intrusioni**: Gli strumenti, le tecniche e i servizi di protezione perimetrale sono progettati per impedire al traffico di rete non autorizzato l'ingresso nell'infrastruttura di prodotti. La rete GoTo dispone di firewall rivolti all'esterno e di una segmentazione interna della rete.
- **Conservazione dei dati:**
  - I Clienti di Rescue possono richiedere in qualsiasi momento la restituzione o la cancellazione dei Contenuti del Cliente, e questa avverrà entro trenta (30) giorni dalla richiesta del Cliente.
  - I Contenuti del Cliente saranno automaticamente cancellati entro 140 giorni dalla scadenza dell'ultimo periodo di abbonamento del Cliente.

[1] Le sedi di hosting possono variare (ad esempio, a seconda della residenza dei dati scelta). Consultare l'Informativa sui sub-incaricati di Rescue applicabile, che si trova nella sezione Risorse sui prodotti del Trust & Privacy Center di GoTo (https://www.goto.com/company/trust/resource-center).

Sommario

Fare clic sui numeri di pagina sottostanti per accedere alla sezione corrispondente delle TOM

1 Presentazione del prodotto

Rescue è un servizio di supporto remoto online utilizzato dai tecnici per fornire assistenza remota via Internet, senza la necessità di un software preinstallato. Con l'autorizzazione dell'Utente o di un'altra persona che utilizza Rescue/riceve supporto da un tecnico (Utente finale), Rescue consente al tecnico di accedere e visualizzare e/o assumere il controllo del computer di un Utente finale. Comunicando tramite una finestra di chat, il tecnico può esaminare, diagnosticare e riparare i problemi del computer e assistere in altro modo l'Utente finale con i problemi del sistema operativo e delle applicazioni software.

Rescue Lens consente agli Utenti finali di trasmettere le fotocamere dei loro dispositivi mobili (attraverso l'applicazione mobile Lens) a un tecnico remoto, permettendo a quest'ultimo di visualizzare l'hardware problematico, come un router mal configurato o un componente automobilistico danneggiato. Rescue Lens è una funzione opzionale di Rescue e può essere attivata nel Centro amministrativo di Rescue. Per maggiori dettagli su Rescue Lens, consultare la Guida per l'utente di Rescue Lens.

I termini in maiuscolo presenti in questo documento che non sono definiti all'interno del testo, sono definiti nei Termini di servizio.

2 Misure tecniche

I prodotti GoTo sono progettati per fornire soluzioni sicure, affidabili e private. Le misure tecniche definite di seguito descrivono il modo in cui GoTo implementa tale progetto e lo applica nella pratica per Rescue e Rescue Lens.

2.1 Misure di sicurezza

L'implementazione di misure di sicurezza, funzioni e pratiche da parte di GoTo implica quanto segue:

I. Realizzare prodotti che tengano conto della sicurezza e della privacy per progettazione e per impostazione predefinita, e includere ulteriori livelli di sicurezza per proteggere i Contenuti del Cliente;

II. Mantenere i controlli organizzativi che rendono operativi i criteri e le procedure interni relativi alla conformità agli standard, alla gestione degli incidenti, alla sicurezza delle applicazioni, alla sicurezza del personale e ai regolari programmi di formazione; e

III. Garantire l'adozione di pratiche di privacy per disciplinare il trattamento e la gestione dei dati in conformità con la legge applicabile, tra cui il GDPR, il CCPA/CPRA, la LGPD, nonché il nostro Addendum sul trattamento dei dati (DPA) e le politiche e gli impegni GoTo applicabili.

Integrando le misure di sicurezza nel prodotto, ci impegniamo a proteggere i Contenuti del Cliente GoTo dalle minacce e a garantire che i controlli di sicurezza siano adeguati alla natura e all'ambito dei Servizi. Le funzioni di sicurezza configurabili di GoTo possono aiutare gli amministratori a minimizzare le minacce e i rischi per i sistemi e per le reti posti dalle persone che utilizzano i servizi GoTo.

3 Architettura del prodotto

Rescue è una soluzione di supporto remoto basata sul Software-as-a-Service (SaaS) costituita da tre componenti principali: la console dei tecnici, un'app mobile o un'applet desktop per l'Utente finale e un centro amministrativo.

La console dei tecnici è l'interfaccia utilizzata dai tecnici del per condurre le sessioni di supporto remoto. I tecnici possono avviare nuove sessioni o rispondere alle richieste dei online degli Utenti finali che sono in attesa in una coda condivisa. I tecnici comunicano con gli utenti finali e forniscono loro assistenza attraverso l'app mobile di Rescue (Android o iOS) o l'applet desktop (Windows, macOS o Linux). L'applet viene scaricata sul PC remoto dell'Utente finale ed è progettata per venire rimossa automaticamente al termine della sessione.

La console dei tecnici di Rescue interagisce con l'app o l'applet Rescue utilizzando una connessione di rete peer-to-peer (P2P) (vedere la Figura 1 nella sezione 3.1). All'avvio dell'applet, ha inizio il processo P2P che si connette a un gateway Rescue dove viene negoziata la sessione con la console dei tecnici.

Il protocollo di inoltro proprietario di GoTo per lo scambio di chiavi è progettato per garantire la sicurezza contro le intercettazioni o lo spionaggio sull'infrastruttura di GoTo. In particolare, la connessione tra l'Utente finale e l'host è facilitata dal gateway, per garantire che l'Utente finale possa connettersi all'host indipendentemente dalla configurazione della rete.

L'host stabilisce una connessione TLS al gateway, che inoltra lo scambio di chiavi TLS dell'Utente finale all'host tramite una richiesta proprietaria di rinegoziazione delle chiavi. In questo modo, l'Utente finale e l'host si scambiano chiavi TLS senza che il gateway apprenda la chiave.

3.1 Chiave concordata

Quando ha inizio una sessione di supporto e viene stabilita la connessione tra l'Utente finale e il tecnico, i rispettivi computer devono concordare un algoritmo di crittografia tra le opzioni disponibili supportate e la chiave corrispondente da utilizzare per la durata della sessione.

I computer utilizzano i certificati per convalidare la loro identità. Poiché né il tecnico né l'Utente finale dispongono di un software in grado di intermediare la connessione e di convalidare i certificati di sicurezza installati e un certificato SSL installato sui loro computer, entrambi si rivolgono a uno dei server Rescue ed eseguono la fase iniziale dell'accordo sulla chiave. La verifica del certificato da parte della console dei tecnici e dell'app o dell'applet dell'Utente finale assicura che solo un server Rescue possa mediare il processo.

3.2 Panoramica del processo di handoff del gateway di Rescue

Quando l'app o l'applet Rescue firmata digitalmente viene avviata su una macchina, contiene un GUID (Globally Unique Identifier) di autenticazione della sessione. Il GUID è incorporato in un'app o applet eseguibile (ad esempio un file .exe) come risorsa dal sito quando viene scaricato. L'app o l'applet scarica quindi l'elenco dei gateway disponibili da secure.logmeinrescue.com o secure.logmeinrescue.eu, sceglie un gateway dall'elenco e vi si connette utilizzando TLS. Il gateway viene autenticato dall'applet con il suo certificato SSL. Il gateway autentica l'applet nel database con il GUID e registra il fatto che l'Utente finale sia in attesa di un tecnico.

Quando un tecnico preleva una sessione nella console dei tecnici di Rescue, al gateway viene inviata la richiesta con il GUID di autenticazione della sessione di inoltrare le connessioni tra la console dei tecnici e l'app o l'applet dell'Utente finale. Il gateway è l'intermediario che autentica la connessione e inizia a inoltrare i dati a livello di trasporto (non decrittografa i dati inoltrati)

All'inizio dell'inoltro di una connessione, le parti tentano di stabilire una connessione peer-to-peer (P2P). Il processo è il seguente:

- L'applet attende una connessione TCP (Transmission Control Protocol) su una porta assegnata da Windows, macOS o Linux.
- Se non è possibile stabilire una connessione TCP entro 10 secondi, viene tentata una connessione UDP (User Datagram Protocol) con l'ausilio del gateway.
- Se viene stabilita una connessione TCP o UDP, le parti autenticano il canale P2P (utilizzando il GUID di autenticazione della sessione), e questo prende in carico il traffico della connessione inoltrata.
- Se è stata stabilita una connessione UDP, sui datagrammi UDP viene emulato il protocollo TCP utilizzando XTCP, un protocollo proprietario di GoTo basato sullo stack TCP di BSD (Berkeley Software Distribution).
- Tutte le connessioni sono protette con il protocollo TLS (utilizzando la crittografia AES256 con MAC (Media Access Controls) SHA256). Il GUID di autenticazione delle sessioni è un valore intero, crittograficamente casuale, a 128 bit.

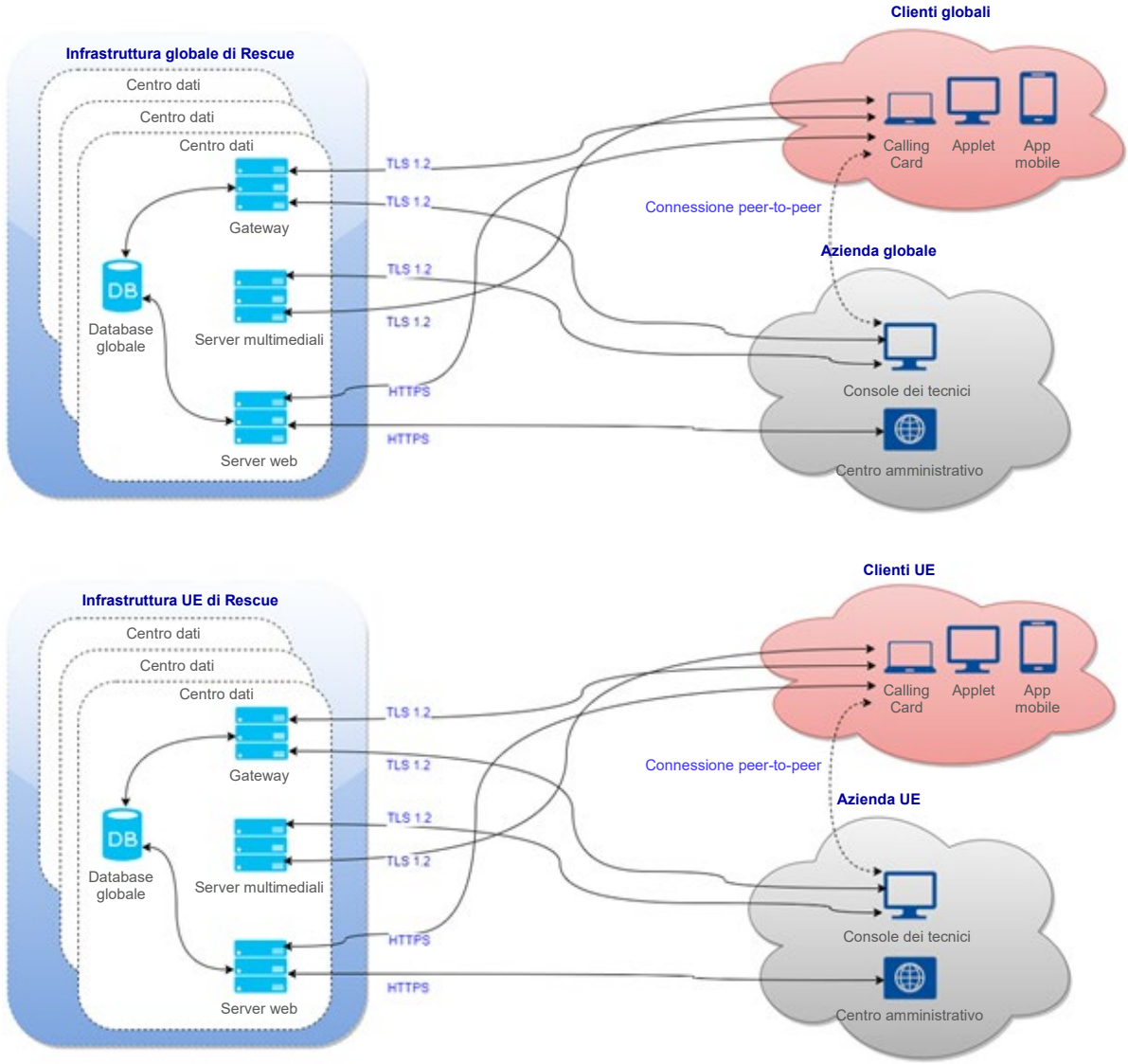

Figura 1: Architettura di Rescue

3.3 Architettura multimediale di Rescue

Il servizio multimediale di Rescue è un servizio autonomo basato su WebRTC (Web Real-Time Communication) che consente lo streaming video di Rescue Lens. Gestisce le conferenze per le sessioni di Rescue che utilizzano la funzione Lens. I partecipanti alle conferenze (peer) si uniscono e lasciano le conferenze e gli Utenti finali inviano streaming video e audio che vengono ricevuti dagli altri partecipanti. Lens invia contenuti video in uno streaming unidirezionale dall'app Lens alla console dei tecnici.

Il servizio multimediale è costituito da tre componenti principali: Media SDK (Media Software Development Kit), il gestore di sessione e il server di streaming. Questi componenti gestiscono il processo di creazione/distruzione e di partecipazione/uscita dalle conferenze. Questi componenti comunicano attraverso le connessioni sicure esistenti tra la console dei tecnici e il sito web e tra l'app Lens e il sito web.

3.3.1 Media SDK

Il servizio multimediale è costruito su WebRTC con un leggero wrapper sulla base del codice WebRTC. La console dei tecnici e l'app mobile Lens utilizzano Media SDK.

3.3.2 Gestore di sessione

Il gestore di sessioni è un sito web a carico bilanciato che fornisce un'API REST (Representational State Transfer) per gestire (creare/distruggere/partecipare) le conferenze. Il gestore di sessione accetta solo richieste dal sito web.

3.3.3 Server di streaming

Il servizio multimediale utilizza una soluzione server di streaming personalizzata per gestire i flussi tra i peer (la console dei tecnici e l'app Lens). Sia la console dei tecnici che l'app Lens sono collegate al server di streaming. Una sessione Lens ha due streaming (uno è inviato, l'altro è ricevuto): l'app Lens trasmette il suo contenuto video al server di streaming, mentre la console dei tecnici riceve il contenuto video dal server. Il server di streaming si comporta come un server di inoltro tra peer.

4 Controlli tecnici di sicurezza

GoTo impiega controlli tecnici di sicurezza che sono progettati per salvaguardare l'infrastruttura dei Servizi e i dati che vi risiedono.

4.1 Riservatezza dei dati

Il sistema online sicuro di Rescue è supportato da Secure Sockets Layer e Transport Layer Security (SSL/TLS) e soddisfa i seguenti obiettivi:

- Autenticazione delle parti comunicanti
- Negoziazione delle chiavi di crittografia senza intercettazioni
- Scambio riservato di messaggi
- Capacità di rilevamento di eventuali modifiche dei messaggi in transito

Rescue utilizza OpenSSL e, al momento della pubblicazione, la versione utilizzata da Rescue è la 1.1.1n.

4.2 Crittografia

GoTo rivede regolarmente i propri standard di crittografia e può aggiornare i cifrari e/o le tecnologie utilizzati in base al rischio valutato e all'accettazione dei nuovi standard da parte del mercato.

4.2.1 Crittografia in transito

Tutto il traffico di rete in entrata e in uscita dai centri dati di Rescue, compresi tutti i Contenuti del Cliente, viene crittografato in transito con TLS 1.2 e HTTPS. Inoltre, le sessioni di supporto di Rescue sono protette da crittografia AES a 256 bit e hash MD5 per una maggiore tracciabilità dei trasferimenti di file.

Poiché tutti e tre i componenti del sistema di comunicazione di Rescue sono sotto il controllo di GoTo, la soluzione di crittografia utilizzata da tali componenti è sempre lo stesso: AES256-SHA in modalità Cipher-Block Chaining con chiave concordata RSA. Ciò significa quanto segue:

- L'algoritmo di crittografia/decrittografia è AES
- La lunghezza della chiave di crittografia è di 256 bit
- Le chiavi di crittografia vengono scambiate utilizzando coppie di chiavi RSA private/pubbliche, come descritto nella sezione precedente
- La base del MAC è SHA-2. MAC è una breve informazione utilizzata per autenticare un messaggio. Il valore MAC protegge sia l'integrità del messaggio che la sua autenticità, consentendo alle parti comunicanti di rilevare eventuali modifiche al messaggio.
- La modalità CBC (Cipher-Block Chaining) assicura che ciascun blocco di testo crittografato dipenda dai blocchi di testo normale fino a quel punto, e che messaggi simili non possano essere distinti in rete.

I dati trasmessi tra l'Utente finale supportato e il tecnico sono crittografati end-to-end e solo le rispettive parti hanno accesso alle informazioni contenute nel flusso di messaggi.

4.2.2 Crittografia a riposo

I Contenuti del Cliente di Rescue sono crittografati a riposo sia a livello di server che di database con AES256 e TDE. Ad esempio, i Contenuti del Cliente includono i registri delle chat e i campi personalizzati, che sono campi creati dal titolare dell'account principale o dall'amministratore principale.

4.3 Controlli di accesso di Rescue

Gli amministratori di Rescue possono personalizzare i controlli di accesso. Ad esempio, gli amministratori di Rescue possono configurare un criterio per le password che preveda una forza minima e una durata massima delle password, imporre la reimpostazione della password, imporre l'autenticazione a due fattori per l'accesso a Rescue, limitare ai tecnici l'accesso a Rescue da indirizzi IP pre-approvati per compiti specifici, o concedere ai tecnici l'accesso solo ad applicazioni predefinite, utilizzando un unico ID SSO per accedere a tali applicazioni. Se necessario, gli amministratori possono disabilitare l'ID SSO di un tecnico.

I controlli di accesso aggiuntivi includono:

- Accesso basato su autorizzazioni a livello capillare (consentendo ad esempio ad alcuni tecnici di usare la sola visualizzazione remota ma non il controllo remoto)
- Non archiviare i dati dei dispositivi remoti sui server GoTo. Vengono archiviati solo i registri delle sessioni, gli indirizzi IP degli Utenti finali e i registri di chat, ed è possibile rimuovere i registri dei testi di chat dai dettagli delle sessioni.

- Impedire ai tecnici di trasferire file
- Richiedere che l'Utente finale sia presente presso il dispositivo remoto per consentire l'accesso remoto
- Richiedere che l'Utente finale mantenga il controllo e possa terminare la sessione in qualsiasi momento
- Impedire ai tecnici di utilizzare determinate funzioni fino a quando l'Utente finale non abbia concesso loro esplicitamente l'autorizzazione (ad esempio controllo remoto, visualizzazione del desktop, trasferimento di file, informazioni sul sistema, riavvio e riconnessione)
- Revoca automatica dei diritti di accesso al termine della sessione
- La possibilità di imporre la disconnessione automatica in base a un tempo di inattività predeterminato
- Bloccare un account dopo cinque tentativi di accesso non riusciti

4.3.1 Controllo dell'accesso basato su autorizzazioni

Gli amministratori di Rescue possono concedere o negare autorizzazioni specifiche nel centro amministrativo. Tali autorizzazioni di gruppo includono:

- Consentire la sincronizzazione degli Appunti
- Consentire la condivisione dello schermo con gli Utenti e gli Utenti finali
- Distribuzione di script
- Avvio della visualizzazione del desktop
- Avvio di gestione file
- Avvio del controllo remoto
- Riavvio
- Registrazione delle sessioni
- Richiesta di credenziali
- Invio e ricezione di file
- Invio di URL
- Avvio di sessioni private
- Trasferimento delle sessioni
- Utilizzo di una richiesta singola per tutte le autorizzazioni
- Visualizzazione delle informazioni di sistema

Per maggiori dettagli sulle autorizzazioni di gruppo, consultare la Guida per gli amministratori di Rescue. I tecnici di Rescue Lens sono identificati dal loro indirizzo e-mail e autenticati con una password.

4.3.2 Autenticazione

I sistemi di autenticazione di Rescue sono progettati per proteggere il prodotto impiegando misure che consentono solo ai tecnici o agli amministratori di accedere al sistema. Gli amministratori assegnano ai tecnici degli ID di accesso (generalmente corrispondenti ai loro indirizzi e-mail) e le password corrispondenti. All'inizio del loro turno, i tecnici inseriscono come minimo queste credenziali nel modulo di accesso sul sito web di Rescue. Gli amministratori possono configurare i controlli per richiedere l'autenticazione con maggiore frequenza (ad esempio, dopo cinque minuti di inattività).

Il sistema Rescue viene prima autenticato al browser del tecnico mediante il suo avanzato certificato SSL con chiave RSA a 2048 bit, assicurando che il tecnico inserisca il suo nome utente e la sua password nel sito web corretto. Il tecnico accede quindi al sistema con le sue credenziali. Rescue non memorizza alcuna password, utilizza invece scrypt per creare hash dalle password che vengono poi

memorizzate nel database di Rescue. Gli hash vengono combinati con un salt con una stringa di 24 caratteri generata da CSPRNG per ciascuna password univoca.

Il sistema Rescue viene autenticato anche all'Utente finale al quale viene fornito supporto. L'app o l'applet, scaricata ed eseguita dall'Utente finale, è firmata con il certificato per la firma del codice di GoTo (basato su una chiave RSA a 2048 bit), e questa informazione viene generalmente visualizzata all'Utente finale nel browser quando questi sta per eseguire il software. Rescue non autentica l'Utente finale al tecnico.

Rescue consente inoltre agli amministratori di implementare un criterio Single-Sign-On (SSO). Viene utilizzato il Security Assertion Markup Language (SAML), che è uno standard XML (Extensible Markup Language) per lo scambio di dati di autenticazione e autorizzazione tra domini di protezione, ovvero tra un provider di identità e un provider di servizi.

Gli amministratori possono anche richiedere la verifica in due passaggi per accedere a Rescue. La funzione di verifica in due passaggi può ricorrere all'autenticazione mediante e-mail, SMS o password monouso a tempo (TOTP) per aggiungere un secondo livello di protezione agli account Rescue, richiedendo a membri selezionati dell'azienda di impostare un metodo aggiuntivo per verificare la propria identità. L'impostazione dell'app di autenticazione viene attivata in uno dei seguenti casi:

- Il membro selezionato tenta di accedere al proprio account Rescue sul sito web sicuro
- Il membro selezionato tenta di accedere alla Console del tecnici desktop
- Il membro selezionato tenta di cambiare la propria password di Rescue

4.3.3 Autorizzazione

L'autorizzazione avviene almeno una volta nel corso di ciascuna sessione di supporto remoto. L'Utente finale che riceve supporto, dopo aver scaricato ed eseguito l'applet, verrà contattato da un tecnico. Il tecnico può chattare con l'Utente finale tramite l'applet, ma qualsiasi altra sua azione, come l'invio di un file o la visualizzazione del desktop dell'Utente finale, richiede l'autorizzazione da parte dell'Utente finale stesso. È possibile anche implementare una "richiesta singola" per gli interventi di supporto prolungati nel tempo, nei quali l'Utente finale potrebbe non essere presente per l'intera durata della sessione. Abilitando questa impostazione per un gruppo di tecnici, i tecnici di tale gruppo possono richiedere all'Utente finale un'autorizzazione "globale" che, se concessa, consentirà loro di eseguire azioni quali la visualizzazione delle informazioni di sistema o l'accesso a una sessione di controllo remoto senza ulteriori autorizzazioni da parte dell'Utente finale. Gli amministratori possono anche imporre limitazioni sugli indirizzi IP, in modo che i tecnici assegnati a un compito particolare possano accedere a Rescue ed eseguire quel compito solo da indirizzi IP pre-approvati. L'amministratore di un gruppo di tecnici può anche disattivare determinate funzioni nel Centro amministrativo.

Le autorizzazioni che un amministratore può concedere o negare includono:

- Avvio del controllo remoto
- Riavvio
- Avvio della visualizzazione del desktop
- Registrazione delle sessioni
- Invio e ricezione di file
- Avvio di sessioni private
- Avvio di gestione file

- Richiesta di credenziali
- Invio di URL
- Consentire la sincronizzazione degli Appunti
- Visualizzazione delle informazioni di sistema
- Distribuzione di script
- Utilizzo di una richiesta singola per tutte le autorizzazioni
- Trasferimento delle sessioni
- Consentire la condivisione dello schermo con gli Utenti e gli Utenti finali

4.4 Controlli di audit

I seguenti controlli di audit sono disponibili per gli Utenti e gli Utenti finali di Rescue:

- Possibilità di rendere obbligatoria la registrazione delle sessioni e memorizzare i file di audit su una rete condivisa protetta.
- Registrazione sul computer host delle sessioni dei tecnici e delle attività durante le sessioni remote per garantire la sicurezza e mantenere il controllo qualitativo (accessi riusciti/non riusciti, inizio/fine del controllo remoto, riavvio, disconnessione).
- Autenticazione delle persone o delle organizzazioni
- Autenticazione dei tecnici tramite il loro indirizzo e-mail univoco o tramite un ID SSO
- Possibilità di consentire l'accesso ai tecnici solo da indirizzi IP approvati.
- Il report di audit disponibile nel Centro amministrativo include le modifiche alle impostazioni dell'account e i dati relativi a ogni azione eseguita dagli amministratori sull'elemento selezionato della struttura dell'organizzazione durante un determinato periodo di tempo

5 Aggiornamenti del programma di sicurezza

GoTo rivede e aggiorna il proprio programma di sicurezza e si avvale di terze parti indipendenti per valutare i controlli di sicurezza pertinenti almeno annualmente per garantire che si evolva adeguatamente per il panorama attuale delle minacce e per assicurare la conformità con i quadri di riferimento, gli standard di settore, gli impegni del Cliente e, se del caso, i cambiamenti delle leggi e dei regolamenti relativi alla sicurezza dei dati di GoTo.

6 Backup dei dati, Disaster Recovery e disponibilità

L'architettura di GoTo è progettata per eseguire la replica quasi in tempo reale in sedi geograficamente diverse. Il backup dei database viene eseguito con una strategia di backup incrementale continuo. In caso di disastro o di guasto totale del sito in una qualsiasi delle varie sedi attive, le sedi rimanenti sono progettate per bilanciare il carico delle applicazioni. Il Disaster Recovery relativo a questi sistemi viene testato periodicamente.

Il database di Rescue viene sincronizzato ogni cinque minuti con un altro centro dati. Ogni notte viene inoltre completato un backup differenziale e ogni fine settimana vengono eseguiti dei backup completi. Il database di backup è memorizzato con la stessa crittografia dell'originale. I backup vengono conservati in sede per un mese e poi trasferiti su un servizio cloud, non più elaborati attivamente e conservati in base ai nostri criteri interni di conservazione dei dati. In caso di avaria totale del centro dati che ospita il database primario, l'architettura Rescue è progettata per venire ripristinata rapidamente.

7 Centri dati

L'infrastruttura GoTo è progettata per aumentare l'affidabilità del servizio e ridurre il rischio di interruzioni dovute a un singolo punto di guasto mediante:

a) centri dati ridondanti, attivi-passivi; oppure
b) centri dati di provider di cloud hosting.

Al momento della creazione dell'account, i Clienti Rescue possono scegliere di utilizzare l'infrastruttura di dati dell'Unione Europea o globale di GoTo per archiviare i Contenuti del Cliente. Le sedi di hosting/archiviazione sono specificate di seguito:[2]

- **Unione Europea:** Germania e Irlanda
- **Globale:** Stati Uniti, Germania, Australia e Regno Unito

Tutti i centri dati includono il monitoraggio delle condizioni ambientali e dispongono di misure di sicurezza fisica 24 ore su 24, come indicato di seguito.

7.1 Sicurezza fisica del centro dati

GoTo stipula contratti con centri dati per fornire sicurezza fisica e controlli ambientali per i sistemi e i server che contengono i Contenuti del Cliente. Questi controlli includono i seguenti:

- Sorveglianza e registrazione video
- Controllo della temperatura di riscaldamento, ventilazione e climatizzazione
- Soppressione incendi e rilevatori di fumo
- Gruppi di continuità
- Pavimenti rialzati o gestione completa dei cavi
- Monitoraggio e avvisi continui
- Protezioni contro i comuni disastri naturali e antropici, come richiesto dalla geografia e dall'ubicazione del centro dati in questione
- Manutenzione programmata e convalida di tutti i controlli di sicurezza e ambientali critici

GoTo limita l'accesso fisico ai centri dati di produzione solo alle persone autorizzate. L'accesso a una sala server locale o a una struttura di hosting di terzi richiede la presentazione di una richiesta attraverso il relativo sistema di ticketing e l'approvazione da parte del responsabile appropriato, nonché la revisione e l'approvazione da parte del team tecnico operativo di GoTo. Tutti gli accessi fisici ai centri dati e alle sale server sono registrati e la direzione di GoTo esamina i registri con cadenza almeno trimestrale. Inoltre, l'autorizzazione all'accesso fisico al centro dati viene rimossa tempestivamente in caso di cambio di ruolo (laddove tale accesso non sia più necessario) o in caso di licenziamento del personale precedentemente autorizzato. Per le aree altamente sensibili, che includono i centri dati, è richiesto l'accesso a più fattori (come ad esempio mediante biometria, badge e tastiera).

8 Conformità agli standard

GoTo valuta regolarmente la propria conformità ai requisiti legali, di sicurezza, finanziari, di privacy e normativi applicabili. I programmi di privacy e sicurezza di GoTo hanno soddisfatto standard rigorosi e riconosciuti a livello internazionale, sono stati valutati in base a standard di audit esterni completi e hanno ottenuto importanti certificazioni, quali:

[2]Le sedi di hosting possono variare (ad esempio, a seconda della residenza dei dati scelta). Consultare l'Informativa sui sub-incaricati di Rescue applicabile, che si trova nella sezione Risorse sui prodotti del Trust & Privacy Center di GoTo (https://www.goto.com/company/trust/resource-center).

- **Certificazione TRUSTe Enterprise Privacy & Data Governance Practices** per affrontare i controlli operativi sulla privacy e sulla protezione dei dati che sono allineati con le principali leggi sulla privacy e con i quadri di riferimento sulla privacy riconosciuti. Per ulteriori informazioni, consultare il nostro post sul blog.
- **Certificazioni TRUSTe CBPR e PRP dell'APEC** per il trasferimento dei Contenuti del Cliente tra i paesi membri dell'APEC, ottenute e convalidate in modo indipendente tramite TrustArc, società leader nella conformità alla protezione dei dati approvata dall'APEC. Per ulteriori informazioni sulle nostre certificazioni APEC, fare clic qui.
- Organizzazione internazionale per la standardizzazione – Certificazione **ISO/IEC 27001:2013** del sistema di gestione della sicurezza delle informazioni (ISMS).
- Report di attestazione **SOC (Service Organization Control) 2 di tipo II** dell'AICPA (American Institute of Certified Public Accountants)
- Conformità al **PCI DSS (Payment Card Industry Data Security Standard)** per gli ambienti di eCommerce e di pagamento di GoTo.
- Valutazione dei controlli interni come richiesto nell'ambito di una revisione dei bilanci annuali del **PCAOB (Public Company Accounting Oversight Board)**.

9 Sicurezza delle applicazioni

Il programma di sicurezza delle applicazioni di GoTo segue il Security Development Lifecycle (SDL) di Microsoft per proteggere il codice del prodotto. Il programma SDL di Microsoft include la revisione manuale del codice, la modellazione delle minacce, l'analisi statica del codice, l'analisi dinamica e l'hardening del sistema. I team GoTo eseguono anche periodicamente attività di test di vulnerabilità statica e dinamica delle applicazioni e di test di penetrazione per ambienti mirati.

10 Registrazione, monitoraggio e avvisi

GoTo mantiene politiche e procedure relative alla registrazione, al monitoraggio e agli avvisi, che definiscono i principi e i controlli che vengono implementati per rafforzare la nostra capacità di rilevare le attività sospette e di rispondervi tempestivamente. GoTo raccoglie il traffico identificato come anomalo o sospetto nei registri di sicurezza pertinenti nei sistemi di produzione applicabili.

Il registri di chat di Rescue vengono salvati nel database di Rescue. Il registro di chat viene trasmesso dalla console dei tecnici ai server Rescue in tempo reale, e contiene sia gli eventi che i messaggi di chat di una data sessione di supporto. I file di registro includono le seguenti azioni dei tecnici: ora di inizio e di fine di una sessione di controllo remoto, casi di condivisione di file da parte dei tecnici con gli Utenti Finali e metadati relativi alla condivisione di file (ad esempio, il nome e l'impronta Hash MD5 di un file trasmesso). Il database di tali registri di chat può essere sottoposto a query dal centro amministrativo.

Per gli account attivi, il contenuto dei registri sarà reso disponibile online per due anni dopo la fine di una sessione di supporto remoto e archiviato per altri due anni.

Per agevolare l'integrazione con i sistemi CRM, Rescue può inviare i dettagli delle sessioni a un URL e gli amministratori possono scegliere di escludere il testo delle chat da questi dettagli. Il testo delle chat è incluso per impostazione predefinita, ma i Clienti possono modificare questa impostazione nel centro amministrativo. I testi delle chat tra i tecnici e gli Utenti finali possono inoltre essere omessi automaticamente dai dettagli delle sessioni memorizzati nel centro dati di Rescue. Rescue consente ai tecnici di registrare in un file video gli eventi che avvengono durante una sessione di visualizzazione del desktop o di controllo remoto. I file delle registrazioni vengono memorizzati in una directory specificata dal tecnico.

11 Endpoint Detection and Response

Il software EDR (Endpoint Detection and Response) con creazione di registri di audit è distribuito su tutti i server GoTo per ridurre al minimo le interruzioni o l'impatto sulle prestazioni del Servizio. Al rilevamento di attività sospette, vengono avviate le indagini di sicurezza adeguate e necessarie, in conformità con le nostre procedure di risposta agli incidenti. Vedere la sezione 17 per maggiori informazioni sul Security Operations Center di GoTo e sulle procedure di risposta agli incidenti.

12 Gestione delle minacce

Il Cyber Security Incident Response Team ("CSIRT") di GoTo è composto da più team ed è responsabile della protezione dalle minacce informatiche. In particolare, il team Cyber Threat Intelligence all'interno del CSIRT raccoglie, analizza e diffonde le informazioni relative alle minacce correnti ed emergenti. GoTo rimane al passo con l'intelligence sulle minacce informatiche e la loro limitazione attraverso l'esame di fonti aperte e chiuse e la partecipazione a gruppi di condivisione e ad associazioni di settore (IT-ISAC, FIRST.org ecc.).

13 Scansione di sicurezza e vulnerabilità e gestione delle patch

GoTo mantiene un programma formale di gestione delle patch e, con cadenza almeno trimestrale, esegue attività di gestione delle patch su tutti i sistemi, i dispositivi, i firmware, i sistemi operativi, le applicazioni e altri software pertinenti che elaborano i Contenuti del Cliente. GoTo valuta e scansiona le vulnerabilità a livello di sistema, di host/rete interni ed esterni ("Sistemi"), con cadenza almeno mensile, nonché dopo qualsiasi modifica sostanziale di tali Sistemi, e pone rimedio alle vulnerabilità rilevate in conformità con i criteri documentati che danno priorità al rimedio in base al rischio.

14 Controllo di accesso logico di GoTo

Le procedure di controllo di accesso logico sono in atto per ridurre il rischio di accesso non autorizzato alle applicazioni e di perdita di dati negli ambienti aziendali e di produzione. Ai dipendenti di GoTo viene concesso l'accesso ai sistemi, alle applicazioni, alle reti e ai dispositivi GoTo specificati, in base al principio del minor privilegio. I privilegi degli utenti sono segregati in base al ruolo funzionale (controllo degli accessi basato sui ruoli) e all'ambiente, utilizzando controlli, processi e/o procedure di segregazione dei ruoli.

15 Segregazione dei dati

GoTo sfrutta un'architettura multi-tenant, logicamente separata a livello di database, in base all'account GoTo di un Utente o di un'organizzazione. Le parti devono essere autenticate per accedere a un account. GoTo ha anche implementato dei controlli per impedire agli Utenti o agli Utenti finali di vedere i dati di altri Utenti o Utenti finali.

16 Sicurezza perimetrale e rilevamento delle intrusioni

GoTo utilizza strumenti, tecniche e servizi di protezione perimetrale per proteggere dal traffico di rete non autorizzato in ingresso nell'infrastruttura dei prodotti di GoTo. Tra questi si trovano ad esempio i seguenti:

- Sistemi di rilevamento delle intrusioni che monitorano i sistemi, i servizi, le reti e le applicazioni alla ricerca di accessi non autorizzati
- Monitoraggio critico del sistema e dei file di configurazione per prevenire o ridurre la probabilità di modifiche non autorizzate
- Servizio di firewall per applicazioni web (WAF) e di prevenzione DDoS a livello di applicazione, attraverso il quale il traffico di GoTo viene proxato per bloccare il traffico dannoso sul server
- Un firewall per applicazioni locali che fornisce un ulteriore livello di protezione contro le Top 10 di OWASP e altre vulnerabilità e il traffico dannoso delle applicazioni web
- Firewall basati su host sui server web di GoTo che filtrano le connessioni in entrata e in uscita, comprese le connessioni interne tra i sistemi GoTo.

17 Operazioni di sicurezza e gestione degli incidenti

Il Security Operations Center (SOC) di GoTo è responsabile del rilevamento e della risposta agli eventi di sicurezza. Il SOC utilizza sensori di sicurezza e sistemi di analisi per identificare potenziali problemi e ha sviluppato procedure di risposta agli incidenti, compreso un Piano di risposta agli incidenti documentato.

Il Piano di risposta agli incidenti di GoTo è allineato con i processi di comunicazione critici, i criteri e le procedure operative standard di GoTo. È progettato per gestire, identificare e risolvere gli eventi di sicurezza rilevanti sospetti o identificati nei suoi sistemi e servizi, compreso Rescue. Il Piano di risposta agli incidenti stabilisce i meccanismi per i dipendenti che devono segnalare gli eventi di sicurezza sospetti e i percorsi di escalation da seguire quando necessario. Gli eventi sospetti vengono documentati ed escalati in modo appropriato tramite ticket standardizzati e gestiti in base alla criticità.

18 Cancellazione e restituzione dei Contenuti

Cancellazione e/o restituzione: I Clienti possono richiedere la restituzione e/o la cancellazione dei loro Contenuti presentando una richiesta usando il Portale di gestione dei diritti individuali ("IRM") di GoTo, tramite support.logmeinrescue.com o inviando un'e-mail a privacy@goto.com. Le richieste saranno elaborate entro trenta (30) giorni dal ricevimento da parte di GoTo, tuttavia, nell'improbabile caso in cui avessimo bisogno di più tempo, forniremo una notifica il prima possibile per qualsiasi ritardo e modifica del termine di completamento previsti.

Programma di conservazione dei Contenuti del Cliente: Se non diversamente richiesto dalla legge applicabile, i Contenuti del Cliente saranno automaticamente cancellati entro 140 giorni dalla cessazione, la cancellazione o la scadenza e, in ogni caso, il deprovisioning dell'abbonamento finale del Cliente.

Su richiesta scritta, GoTo può fornire una conferma/certificazione scritta della cancellazione del Contenuto.

19 Controlli organizzativi

19.1 Criteri e procedure di sicurezza

GoTo mantiene una serie completa di criteri e procedure di sicurezza che vengono periodicamente rivisti e aggiornati, se necessario, per supportare gli obiettivi di sicurezza di GoTo, i cambiamenti delle leggi applicabili, gli standard del settore e il mantenimento della conformità.

19.2 Gestione delle modifiche

GoTo mantiene un adeguato processo di gestione delle modifiche e le modifiche ai sistemi GoTo vengono valutate, testate e approvate prima dell'implementazione per ridurre il rischio di interruzione dei servizi GoTo.

19.3 Programmi di sensibilizzazione e formazione in materia di sicurezza

Il programma di sensibilizzazione alla privacy e alla sicurezza di GoTo prevede la formazione dei dipendenti sull'importanza di gestire i Dati Personali e le informazioni riservate in modo etico, responsabile, in conformità alla legge applicabile e con la dovuta attenzione. I dipendenti, gli appaltatori e gli stagisti appena assunti vengono informati sui criteri di sicurezza e sul Codice di condotta e di etica aziendale di GoTo durante il processo di onboarding. I dipendenti di GoTo completano la formazione di sensibilizzazione alla privacy e alla sicurezza almeno una volta all'anno. Le attività di sensibilizzazione vengono svolte nel corso dell'intero anno e possono includere campagne per la Giornata della protezione dei dati, il Mese della consapevolezza della sicurezza informatica, webinar con il Chief Information Security Officer e un Security Champions Program.

Laddove appropriato, ai dipendenti può essere richiesto di completare una formazione specifica per il loro ruolo. Inoltre, tutti i dipendenti, gli appaltatori e le filiali di GoTo devono esaminare e rispettare i criteri di GoTo relativi alla sicurezza e alla protezione dei dati.

20 Pratiche relative alla privacy

GoTo prende molto sul serio la privacy dei suoi Clienti, Utenti e Utenti finali e si impegna a divulgare le sue pratiche di trattamento e gestione dei dati in modo aperto e trasparente.

20.1 Programma relativo alla privacy

GoTo mantiene un programma completo sulla privacy che prevede il coordinamento di più funzioni all'interno dell'azienda, tra cui Privacy, Sicurezza, Governance, Rischio e Conformità (GRC), Legale, Prodotto, Ingegneria e Marketing. Questo programma sulla privacy è incentrato sull'impegno per il mantenimento della conformità e prevede l'implementazione e il mantenimento di criteri, standard e addendum interni ed esterni per disciplinare le pratiche dell'azienda.

20.2 Conformità normativa

20.2.1 GDPR

Il Regolamento generale sulla protezione dei dati (GDPR) è una legge dell'Unione Europea (UE) che riguarda la protezione dei dati e la privacy delle persone all'interno dell'UE. GoTo mantiene un programma completo di conformità al GDPR e nella misura in cui GoTo si impegna nell'elaborazione di Dati personali soggetti al GDPR per conto del Cliente, lo fa in conformità con i requisiti applicabili del GDPR. Per ulteriori informazioni, visitare https://www.goto.com/company/trust/privacy.

20.2.2 CCPA

Il California Consumer Privacy Act, emendato dal California Privacy Rights Act (collettivamente denominato "CCPA") garantisce ai californiani ulteriori diritti e tutele in merito a come le aziende possono utilizzare le loro informazioni personali. GoTo mantiene un programma completo di conformità e nella misura in cui GoTo si impegna nell'elaborazione di Dati personali soggetti al CCPA per conto del Cliente, lo fa in conformità con i requisiti applicabili del CCPA. Per ulteriori informazioni sulla nostra conformità al CCPA, consultare l'Informativa sulla privacy di GoTo e l'Informativa supplementare sul California Consumer Privacy Act.

20.2.3 LGPD

La Legge brasiliana sulla protezione dei dati (LGPD) regola il trattamento dei Dati personali in Brasile e/o di persone che si trovano in Brasile al momento della raccolta. GoTo mantiene un programma completo di conformità e nella misura in cui GoTo si impegna nell'elaborazione di Dati personali soggetti alla LGDP per conto del Cliente, lo fa in conformità con i requisiti applicabili della LGDP. Per ulteriori informazioni, visitare https://www.goto.com/company/trust/privacy.

20.3 Addendum sul trattamento dei dati

GoTo offre un Addendum globale sul trattamento dei dati (DPA), disponibile in inglese e tedesco. Il presente DPA soddisfa i requisiti del GDPR, del CCPA, della LGPD e di altre normative applicabili e regola il trattamento dei Contenuti del Cliente da parte di GoTo.

In particolare, il nostro DPA include svariate misure di protezione della privacy dei dati incentrate sul GDPR, tra cui:

(a) i dettagli del trattamento dei dati e le comunicazioni dei dati ai sub-incaricati come richiesto dall'Articolo 28;
(b) le clausole contrattuali tipo riviste (2021) (ovvero le Clausole modello dell'UE); e
(c) le misure tecniche e organizzative specifiche per i prodotti GoTo.

Inoltre, per tenere conto dei requisiti del CCPA, il nostro DPA globale include:

a) le definizioni riviste specificamente per il CCPA;
b) i diritti di accesso e cancellazione; e
c) le garanzie che GoTo non venderà le informazioni personali dei Clienti, Utenti e Utenti finali.

Il nostro DPA globale include anche disposizioni per:

(a) tenere conto della conformità di GoTo alla LGPD;
(b) supportare i trasferimenti leciti di Dati personali da/verso il Brasile; e
(c) assicurare che i nostri Utenti possano godere degli stessi vantaggi in termini di privacy dei nostri altri Utenti globali

20.4 Quadri normativi sul trasferimento

GoTo supporta i trasferimenti di dati internazionali leciti ai sensi dei seguenti quadri normativi:

20.4.1 Clausole contrattuali tipo

Le Clausole contrattuali tipo (SCC), dette anche Clausole modello dell'UE, sono termini contrattuali standard, riconosciuti e adottati dalla Commissione europea, che assicurano che i Dati personali in uscita dallo Spazio economico europeo (SEE) vengano trasferiti nel rispetto della normativa europea sulla protezione dei dati. Le SCC, riviste ed emesse nel 2021, sono incluse nel DPA globale di GoTo

per consentire ai Clienti GoTo di trasferire i dati fuori dal SEE in conformità con il GDPR.

20.4.2 Certificazioni CBPR e PRP dell'APEC

GoTo ha conseguito le certificazioni del Sistema delle norme transfrontaliere in materia di privacy (CBPR) e del Riconoscimento della privacy per i Responsabili del trattamento (PRP) della Cooperazione economica Asia-Pacifico (APEC). Il CBPR e il PRP dell'APEC sono i primi quadri normativi approvati per il trasferimento dei Dati personali tra i paesi membri dell'APEC e sono stati ottenuti e convalidati in modo indipendente tramite TrustArc, società leader nella conformità alla protezione dei dati approvata dall'APEC.

20.5 Misure supplementari

Oltre alle misure specificate in queste TOM, GoTo ha creato una FAQ progettata per delineare le misure supplementari implementate per supportare i trasferimenti leciti ai sensi del Capitolo 5 del GDPR e per affrontare e guidare qualsiasi analisi caso per caso secondo i dettami dalla Corte di Giustizia Europea in relazione all'uso delle SCC.

20.6 Richieste dei dati

GoTo mantiene processi completi per facilitare la ricezione di richieste relative alla protezione dei dati e alla sicurezza, tra cui il portale IRM, l'indirizzo e-mail per la privacy (privacy@goto.com) e il Supporto clienti all'indirizzo https://support.goto.com.

20.7 Informative sui sub-incaricati e sui Centri dati

GoTo pubblica le Informative sui sub-incaricati sul suo Trust & Privacy Center (https://www.goto.com/company/trust/resource-center). Tali informative riportano i nomi, le sedi e le finalità di elaborazione dei fornitori di hosting dei dati e di altre terze parti che elaborano i Contenuti del Cliente nell'ambito della fornitura del Servizio ai clienti GoTo.

20.8 Dati sensibili Limitazioni all'elaborazione

A meno che non sia espressamente richiesto da GoTo o il Cliente abbia altrimenti ricevuto un'autorizzazione scritta da GoTo, i seguenti tipi di dati sensibili non devono essere caricati su Rescue o altrimenti forniti a GoTo:

- Numeri di identificazione rilasciati dal governo e immagini di documenti di identificazione.
- Informazioni relative alla salute di un individuo, incluse, ma non solo, le Informazioni sanitarie protette (PHI) come identificate nel Health Insurance Portability and Accountability Act (HIPAA, Atto sulla Portabilità e Rendicontabilità dell'Assicurazione Sanitaria statunitense), nonché in altre leggi e regolamenti applicabili.
- Informazioni relative a conti finanziari e strumenti di pagamento, compresi, ma non solo, i dati delle carte di credito. L'unica eccezione generale a questa disposizione è rappresentata dai moduli e dalle pagine di pagamento esplicitamente identificati che sono utilizzati da GoTo per raccogliere i pagamenti per il Servizio.
- Qualsiasi informazione particolarmente protetta dalle leggi e dai regolamenti applicabili, in particolare le informazioni sulla razza, l'etnia, le convinzioni religiose o politiche, l'appartenenza a organizzazioni ecc.

20.9 Conformità in ambienti regolamentati

I Clienti sono responsabili dell'implementazione di criteri, procedure e altre misure di sicurezza adeguate relative all'uso di Rescue per fornire supporto ai dispositivi in ambienti regolamentati.

21 Controlli sulla sicurezza e privacy di terze parti

Prima di affidare a fornitori terzi l'elaborazione dei Contenuti del Cliente o dati riservati, sensibili o dei dipendenti, GoTo esamina e analizza le pratiche di sicurezza e privacy del fornitore utilizzando i canali di approvvigionamento adeguati. A seconda dei casi, GoTo può ottenere e valutare periodicamente la documentazione o i rapporti di conformità dei fornitori per garantire che il loro ambiente di controllo e i loro standard continuino ad essere sufficienti.

GoTo stipula accordi scritti con tutti i fornitori terzi e utilizza modelli di approvvigionamento approvati da GoTo o negozia i termini e le condizioni standard di tali terzi per soddisfare gli standard di privacy e sicurezza accettati da GoTo, ove ritenuto necessario. I team Finanza, Legale, Privacy e Sicurezza sono coinvolti nel processo di revisione dei fornitori e verificano che i fornitori soddisfino i requisiti contrattuali e di trattamento dei dati obbligatori, come necessario e/o appropriato. I criteri di rischio relativi a terze parti di GoTo regolano i requisiti di privacy e sicurezza dei fornitori in base al tipo e alla durata del trattamento dei dati e al livello di accesso. Laddove appropriato (ad esempio, nel caso in cui i Contenuti del Cliente vengano elaborati o archiviati), gli accordi con i fornitori includono i requisiti di "conformità alla legge applicabile", un DPA o un documento simile che affronta argomenti quali GDPR, CCPA, LGPD e le restrizioni all'uso e alla vendita, a seconda dei casi. Allo stesso modo, con i fornitori rilevanti sono stati creati degli addendum di sicurezza con controlli e requisiti di sistema adeguati. La DPA per i fornitori di GoTo prevede restrizioni sulla "vendita" dei dati, come definita dalla CCPA.

22 Contattare GoTo

Per richieste generali, i Clienti possono contattare GoTo all'indirizzo https://support.goto.com. Per domande o richieste relative ai Dati personali o alla privacy, visitare il nostro portale IRM o inviare un'e-mail a privacy@goto.com.