Misure tecniche e organizzative
GoTo Meeting, GoTo Webinar, GoTo Training e GoTo Stage

Sommario esecutivo

Il presente documento sulle Misure tecniche e organizzative ("TOM") definisce gli impegni di GoTo in materia di privacy, sicurezza e responsabilità per GoTo Meeting, GoTo Webinar, GoTo Training e GoTo Stage. 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) o Datagram Transport Layer Security (DTLS)
  - *A riposo* Transparent Data Encryption (TDE) e Advanced Encryption Standard (AES) a 256 bit per i Contenuti del Cliente che sono crittografati a riposo.
- **Centri dati:** GoTo si avvale di provider di hosting su cloud che adottano misure per garantire un'elevata sicurezza logica e fisica, disponibilità e scalabilità.
- **Audit di conformità:** GoTo Meeting, GoTo Webinar e GoTo Training detengono le certificazioni SOC 2 Tipo II, C5, 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 condurre 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 archiviazione.
- **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 GoTo Meeting, GoTo Webinar, GoTo Training e GoTo Stage 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.
  - Per GoTo Meeting, GoTo Webinar e GoTo Training, i Contenuti del Cliente saranno eliminati automaticamente tra novanta e cento (90-100) giorni dopo la scadenza dell'ultimo periodo di abbonamento del Cliente.

Sommario

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

1 Presentazione del prodotto

GoTo Meeting, GoTo Webinar, GoTo Training e GoTo Stage (collettivamente il "Servizio") sono soluzioni di comunicazione online che consentono a persone e organizzazioni di interagire utilizzando varie funzionalità, a seconda dell'offerta di servizi, che includono la condivisione dello schermo del desktop, le videoconferenze la chat e l'audio integrato. GoTo Meeting, GoTo Webinar, GoTo Training e GoTo Stage condividono l'infrastruttura e vengono forniti tramite una CDN ai browser web o alle applicazioni installabili.

- GoTo Meeting, GoTo Webinar e GoTo Training consentono agli organizzatori di programmare, convocare e moderare sessioni online con audio, webcam, condivisione dello schermo e altro ancora, utilizzando le applicazioni web, desktop e mobili di GoTo.
- GoTo Training offre funzioni specifiche per la formazione basata sul web, come l'accesso online a test e materiali nonché cataloghi dei corsi disponibili.
- GoTo Webinar offre un supporto speciale per consentire di condurre eventi di presentazione di informazioni uno-a-molti, raggiungendo partecipanti locali e globali tramite Internet.
- GoTo Stage è un estensione di GoTo Webinar in cui gli organizzatori di GoTo Webinar possono creare canali personalizzabili e pubblicare le registrazioni dei propri webinar. Nella pagina iniziale di GoTo Stage si trovano le registrazioni pubblicate, organizzate per categorie aziendali. Gli organizzatori hanno la facoltà di annullare in qualsiasi momento la pubblicazione delle loro registrazioni su GoTo Webinar, il che ne rimuove i video dal rispettivo canale nonché dall'ecosistema di GoTo Stage.

1.1 Gestione e registrazione delle conferenze

Gli organizzatori possono programmare le sessioni direttamente all'interno del Servizio. Possono regolare varie impostazioni delle sessioni future e preparare i contenuti e i partecipanti.

1.2 Audio

La funzionalità di conferenza audio integrata nelle sessioni di GoTo Meeting, GoTo Webinar e GoTo Training è disponibile tramite VoIP (Voice over Internet Protocol) e tramite la rete telefonica pubblica (PSTN).

1.3 Video

Tutti i prodotti offrono video da webcam di alta qualità che si adattano alla larghezza di banda e alla latenza dell'utente.

1.4 Caricamento dei contenuti (solo webinar e formazione)

Gli organizzatori possono caricare file e contenuti multimediali da utilizzare durante le sessioni, sia prima della sessione che a sessione iniziata.

1.5 Creazione di report sulle sessioni

Gli organizzatori possono vedere le statistiche di partecipazione e altre statistiche delle sessioni nella loro cronologia delle sessioni.

1.6 Registrazioni e trascrizioni

Le sessioni possono essere registrate localmente e su cloud. Gli amministratori degli account e gli organizzatori delle sessioni possono scegliere di attivare le registrazioni su cloud in aggiunta o al posto delle registrazioni locali. Le registrazioni locali vengono memorizzate sul sistema dell'organizzatore e non sono soggette ai limiti di conservazione di GoTo, indicati nella sezione 18 (Cancellazione e restituzione dei Contenuti) di seguito.

Le registrazioni su cloud sono automaticamente disponibili direttamente nella cronologia delle sessioni dell'organizzatore e le trascrizioni vengono create automaticamente quando questa funzione è abilitata dall'amministratore. Le trascrizioni delle registrazioni delle sessioni vengono create utilizzando la tecnologia GoTo Voice AI o Google Cloud Speech-to-Text.

Per **GoTo Meeting**, un amministratore dell'account può scegliere di abilitare le registrazioni e decidere se archiviarle localmente o su cloud. Se le registrazioni su cloud sono abilitate, l'organizzatore della riunione può scegliere di registrare una determinata riunione e di archiviarla su cloud. Le trascrizioni vengono create automaticamente per le registrazioni su cloud.

Per **GoTo Webinar**, gli organizzatori possono scegliere di trascrivere automaticamente tutte le registrazioni su cloud. Solo un organizzatore può avviare una registrazione e se l'impostazione di trascrizione automatica è abilitata, verrà creata una trascrizione.

Per **GoTo Training**, gli amministratori dell'account possono controllare se gli organizzatori abbiano la facoltà di salvare le registrazioni su cloud. Gli amministratori dell'account non possono impedire agli organizzatori di registrare le sessioni localmente. Le formazioni non possono essere trascritte.

1.7 Messaggistica aziendale (solo Meeting)

Messaggistica aziendale, un'estensione di GoTo Meeting, consente agli utenti di GoTo Meeting di vedere lo stato di presenza di altri utenti all'interno del loro account, di scambiare messaggi istantanei e di condividere file. L'amministratore dell'account definisce l'ambito di visibilità e reperibilità dei vari utenti.

Gli utenti di messaggistica aziendale possono vedere lo stato di presenza di qualsiasi altro utente all'interno del loro account, una volta che è stato incluso nel loro elenco di contatti. I messaggi possono essere scambiati con tutti i membri di un team e con gli utenti esterni se sono stati esplicitamente inclusi tramite un invito tramite e-mail. Gli utenti esterni sono utenti di messaggistica aziendale che non fanno parte del team interno di un Cliente (sono ad esempio clienti, potenziali clienti o partner). I messaggi possono essere diretti (tra due partecipanti), in un gruppo privato o in un gruppo pubblico.

Gli utenti possono anche condividere altri contenuti all'interno della messaggistica aziendale, caricando e scaricando file. I file condivisi sono disponibili per il download da parte di tutti gli utenti che hanno accesso ai messaggi in una determinata conversazione o in un determinato gruppo.

1.8 Webcast (solo Webinar)

I webcast di GoTo Webinar utilizzano gateway di trasmissione, motori di streaming di terze parti e reti di distribuzione dei contenuti progettati per fornire in modo affidabile le funzioni di condivisione dello schermo, audio e video ai partecipanti che si collegano da un browser. I gateway ricevono i dati multimediali dai server multimediali e li transcodificano in codec standard. Il motore di streaming produce HLS (HTTP Live Streaming) a più bitrate per consentire di fornire contenuti adatti agli utenti con connessioni di rete non ottimali.

1.9 GoTo Stage (solo Webinar)

I video pubblicati su GoTo Stage si possono trovare sulla homepage di GoTo Stage e nei risultati dei motori di ricerca, a meno che l'organizzatore non ne limiti la scopribilità utilizzando le impostazioni amministrative sulla sua pagina del canale. Le registrazioni non scopribili possono essere consultate da chiunque sia registrato a GoTo Stage utilizzando un URL diretto al canale o alla pagina "Guarda ora" esclusiva del video. I visitatori si registrano a GoTo Stage utilizzando il loro nome e il loro indirizzo e-mail, oppure possono collegarsi tramite il loro account su alcuni social media, quali LinkedIn, Facebook e Gmail. Gli URL che consentono ai visitatori di accedere ai video sono attivi per un periodo di tempo limitato, per limitare le condivisioni indesiderate.

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 GoTo Meeting, GoTo Webinar e GoTo Training.

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'esistenza di pratiche di privacy per governare il trattamento e la gestione dei dati in conformità con il GDPR, il CCPA/CPRA, la LGPD e il nostro Addendum sul trattamento dei dati (DPA), nonché le politiche e le informative al pubblico di 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 che possono essere configurate nel servizio aiutano gli amministratori a ridurre al minimo le minacce e i rischi per i Contenuti del Cliente.

3 Architettura del prodotto

GoTo Meeting, GoTo Webinar, GoTo Training e GoTo Stage sono soluzioni SaaS (Software as a Service) progettate per garantire elevate prestazioni, affidabilità, scalabilità e sicurezza. Questi Servizi sono supportati da server e apparecchiature di rete ad alta capacità, con controlli di sicurezza adeguati e un'infrastruttura ridondante progettata per evitare che si verifichi anche un solo singolo punto di errore. Vengono utilizzati cluster di server e sistemi di backup ad alta capacità per supportare la continuità operativa dei processi applicativi anche nell'eventualità di un carico eccessivo o un errore di sistema.

Il carico delle sessioni di applicazioni/server è bilanciato su cluster geograficamente distribuiti, progettati per garantire prestazioni e latenza adeguate.

L'infrastruttura e i dati del Servizio sono ospitati da provider di hosting su cloud.

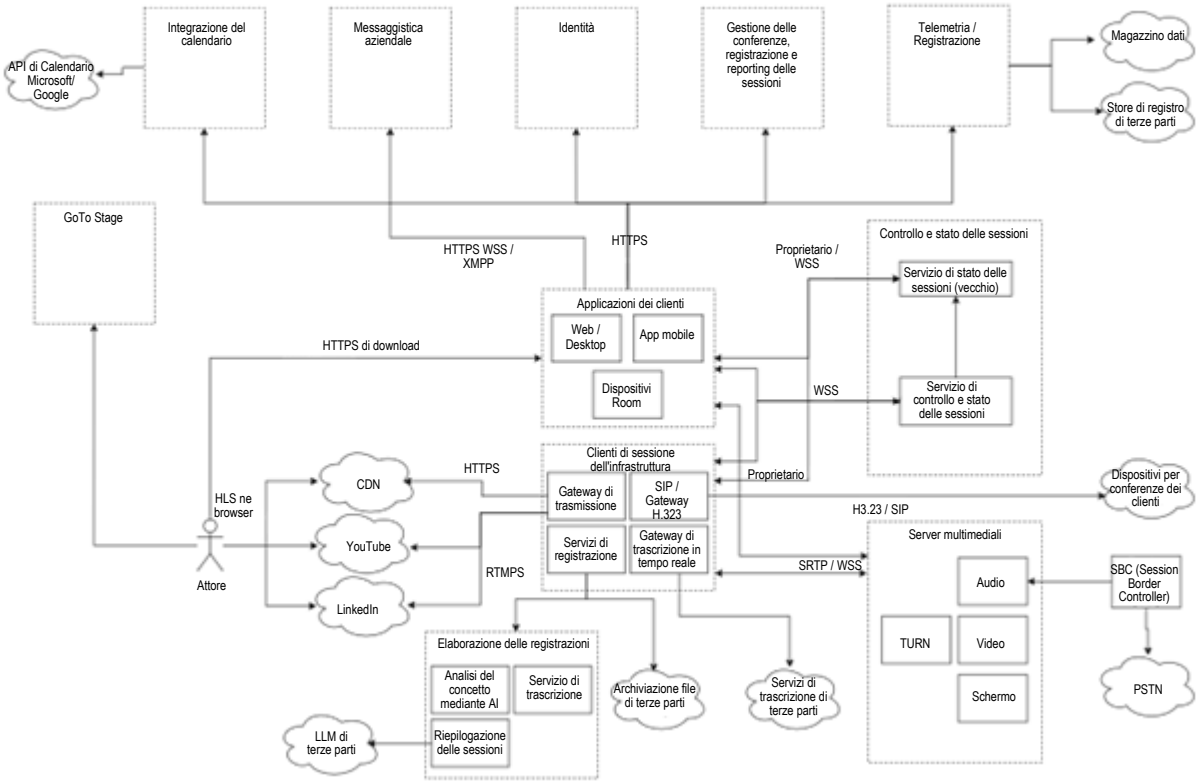

Figura 1: Architettura di Central

Applicazioni del Cliente (applicazioni web, desktop e mobili di GoTo o "client"; un dispositivo chiamato GoTo Room (solo per Meeting)): Le Applicazioni del Cliente forniscono la funzionalità del Servizio come descritto sopra nella Sezione 1 (Presentazione del prodotto).

Servizi di identità: Gestiscono gli account degli utenti e consentono le autorizzazioni e gli accessi sicuri e standardizzati.

Servizi di gestione delle conferenze, di registrazione e di reporting delle sessioni: La gestione delle conferenze fornisce informazioni sulle sessioni pianificate e consente di pianificare nuove sessioni e di modificare quelle esistenti. I servizi di registrazione consentono la registrazione delle sessioni in cui è richiesta. Il reporting delle sessioni fornisce informazioni sulle sessioni passate, comprese le registrazioni, le trascrizioni, le presenze e altro ancora.

Messaggistica aziendale: Gestione dei canali, nonché invio, ricezione e archiviazione di messaggi e allegati; utilizzata solo per la messaggistica fuori sessione.

Integrazione del calendario: Consente agli utenti di sincronizzare i loro calendari Microsoft Outlook o Google per ricevere notifiche sulle sessioni GoTo.

Telemetria/Registrazione: Invio di sonde di telemetria o dichiarazioni di log per aiutare a raccogliere le statistiche di utilizzo e diagnosticare i problemi.

Servizi di controllo e di stato delle sessioni: Forniscono la funzionalità utilizzata dalle applicazioni client per avviare e ricevere modifiche non legate ai contenuti multimediali allo stato delle sessioni.

Server multimediali: Sono responsabili della ricezione, della modifica e della distribuzione di contenuti audio e video e della condivisione dello schermo.

PSTN: La rete telefonica pubblica commutata consente agli utenti di accedere alle sessioni tramite telefoni fisici o IP.

SBC (Session Border Controller): Collega la funzionalità VoIP di GoTo con i fornitori di telefonia commerciale.

Servizi di registrazione: Consentono di registrare l'audio delle sessioni, i video, le condivisioni dello schermo e i contenuti della messaggistica aziendale.

Gateway di trasmissione: Utilizzato per i webcast di GoTo Webinar, supporta il layout, la transcodifica e la pacchettizzazione dei flussi multimediali in flussi HLS, che vengono distribuiti tramite CDN ai client basati su browser o inviati alle piattaforme di streaming abilitate RTMP come YouTube o LinkedIn.

Gateway H.323-/SIP: Consente la connessione alle sessioni audio tramite i dispositivi di conferenza SIP o H.323.

Gateway di trascrizione in tempo reale (RTT): Fornisce la trascrizione in diretta del parlato dei partecipanti alla sessione.

Servizi GoTo Stage: Gestione dei contenuti video di GoTo Webinar da parte degli organizzatori; offre un'esperienza di visualizzazione ai visitatori.

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 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.

4.1.1 Crittografia in transito

GoTo implementa misure di sicurezza per i dati in transito progettate per fronteggiare attacchi sia attivi sia passivi contro la riservatezza, l'integrità e la disponibilità. I controlli di sicurezza delle comunicazioni sono implementati per la condivisione di schermi e video, il VoIP, i video delle webcam, il controllo di tastiera/mouse, le informazioni delle chat testuali e altri dati delle sessioni.

GoTo utilizza i protocolli TLS standard di Internet Engineering Task Force (IETF) per proteggere la comunicazione TCP tra gli endpoint.

HTTPS e WSS sono utilizzati per proteggere i dati non multimediali, mentre i dati multimediali in sessione sono protetti da SRTP, WSS o DTLS.

Internamente, GoTo utilizza anche l'autenticazione reciproca basata sui certificati (mTLS) sui server che gestiscono i dati multimediali.

4.1.1.1 Sicurezza di audio e video

Per proteggere la riservatezza e l'integrità delle connessioni VoIP tra gli endpoint e i server, viene utilizzato un protocollo basato su SRTP che utilizza meccanismi di crittografia standard che impiegano come minimo AES128.

4.1.1.2 Sicurezza dei siti web, delle API e del servizio web interno

Tutte le connessioni ai siti web del Servizio, alle API e ai servizi web interni sono protette da TLS. Questo include il caricamento dei contenuti, il reporting delle sessioni, le registrazioni, le trascrizioni e altro ancora.

4.1.1.3 Messaggistica aziendale

Gli aggiornamenti sulla presenza, i messaggi e i file vengono trasferiti tramite un canale protetto da TLS ai servizi di chat e poi agli utenti. I contenuti dei file vengono messi a disposizione mediante URL di collegamento firmati crittograficamente.

4.1.1.4 Sicurezza dei webcast (solo Webinar)

I gateway di streaming dei webcast inoltrano il traffico al motore di streaming tramite SRTP, il tutto all'interno della rete interna protetta di GoTo. I CDN prelevano i dati dal motore di streaming in modo sicuro tramite HTTPS. Anche i client prelevano i dati in modo sicuro dalle CDN tramite HTTPS.

4.1.2 Crittografia a riposo

4.1.2.1 Dati del profilo

I contenuti sono archiviati in un database relazionale con crittografia AES a 256 bit.

4.1.2.2 Gestione delle conferenze, registrazione e reporting delle sessioni

I contenuti sono archiviati in un database relazionale con crittografia AES a 256 bit.

4.1.2.3 Caricamento dei contenuti

I contenuti caricati e i relativi meta dati sono archiviati in AWS S3, Amazon Aurora e Amazon Dynamo DB, tutti con crittografia AES a 256 bit. I metadati vengono inoltre archiviati in Apache Cassandra senza crittografia a riposo.

4.1.2.4 Registrazioni e trascrizioni

Le registrazioni su cloud sono archiviate in AWS S3. I file vengono crittografati a riposo utilizzando la crittografia lato server con AES256.

I file audio per la trascrizione vengono crittografati con AES256 ed eliminati subito dopo il completamento dell'elaborazione speech-to-text.

4.1.2.5 Sicurezza della messaggistica aziendale

I messaggi vengono archiviati in un database AWS Aurora e i file condivisi vengono archiviati in AWS S3, entrambi con crittografia AES a 256 bit a riposo.

4.1.2.6 GoTo Stage

I contenuti caricati e i relativi metadati vengono archiviati in AWS S3 con crittografia AES a 256 bit. I metadati vengono archiviati in Apache Cassandra e l'indice di ricerca in Elasticsearch, entrambi non crittografati a riposo.

4.2 Compatibilità con firewall e proxy

Nel Servizio è integrata la logica di rilevamento proxy e di gestione della connessione, per agevolare l'automatizzazione dell'installazione del software, evitare la necessità di una complessa (ri)configurazione della rete e massimizzare la produttività degli utenti. I firewall e i proxy già presenti nella rete di un utente generalmente non necessitano di alcuna configurazione speciale per consentire l'utilizzo del Servizio.

Per maggiori dettagli e per informazioni precise sui domini, sugli IP e sulle porte utilizzati, visitare le relative pagine del supporto di Meeting, Webinar e Training.

4.3 Caratteristiche di sicurezza dei client installabili

I client installabili sono progettati con caratteristiche di sicurezza adeguate e impiegano misure crittografiche forti, tra cui il software endpoint firmato e le connessioni “solo client”.

4.3.1 Software per endpoint con firma digitale

Gli eseguibili del Servizio sono firmati digitalmente per proteggerne l'integrità e l'autenticità. Il software dell'applicazione client di GoTo segue adeguate procedure di controllo della qualità, procedure di gestione della configurazione e un modello di SDL (Security Development Lifecycle) durante lo sviluppo e la distribuzione.

4.3.2 Connessioni “solo client”

Per ridurre il rischio che sistemi remoti possano bersagliarli con malware e virus, i client installabili non sono configurati per ricevere connessioni in entrata. Questo aiuta a proteggere gli utenti che partecipano a una sessione dall'essere infettati da un host compromesso utilizzato da un altro partecipante.

4.3.3 Implementazione del sottosistema crittografico

Le funzioni crittografiche e i protocolli di sicurezza implementati nei client installabili utilizzano le librerie crittografiche open source BoringSSL o OpenSSL. Non vengono esposte API esterne che consentirebbero ad altri software di accedere alle librerie crittografiche incluse nel client.

L'applicazione web utilizza le librerie crittografiche del browser. Non vi sono impostazioni crittografiche configurabili dall'utente finale che possano consentire un'errata configurazione accidentale o intenzionale.

4.4 Autenticazione degli utenti

L'autorizzazione basata sui ruoli e i controlli di accesso appropriati dipendono dalla capacità di identificare e autenticare gli utenti. Per garantire che gli organizzatori e i partecipanti abbiano i giusti privilegi, nel Servizio sono integrate le funzioni di autenticazione degli account e delle sessioni.

4.4.1 Accesso all'account

I siti web del Servizio offrono i seguenti metodi di accesso:

- Accesso diretto con nome utente e password;
- Accesso tramite un provider di account social o altro provider utilizzando LastPass, Google, Facebook, LinkedIn, Microsoft oppure Apple. (https://support.goto.com/meeting/help/connect-your-social-or-other-account-for-sign-in); e

- SSO (Single Sign-on) basato su SAML.

Per l'accesso diretto, tutte le password hanno requisiti minimi di caratteri e complessità. Sono presenti meccanismi di protezione contro gli attacchi di forza bruta e le attività di accesso insolite.

GoTo non memorizza le password degli account come testo non crittografato. Piuttosto, le password vengono memorizzate utilizzando una funzione crittografica di hash con salt, progettata per essere resistente agli attacchi di dizionario e di forza bruta. Le password vengono trasmesse tramite connessioni protette (TLS).

4.4.2 Autenticazione dei partecipanti alle sessioni

Per consentire sessioni con partecipazione limitata, ogni sessione ha un ID univoco e casuale. Gli organizzatori possono anche scegliere di richiedere ai partecipanti una password per partecipare a una sessione.

Per partecipare a una sessione, i partecipanti devono fornire l'ID univoco facendo clic su un URL che contiene l'ID o inserendo manualmente il valore in un modulo presentato dal Servizio. Se i partecipanti si connettono mediante telefono, devono digitare l'ID sulla tastiera. Se l'ID è valido, ciascun partecipante riceve un token di ruolo che viene presentato ai server di comunicazione durante il processo di accesso alla sessione.

4.4.3 Controllo dell'accesso basato sui ruoli

I ruoli definiti dall'applicazione possono essere assegnati agli utenti del Servizio e supportano i Clienti nell'applicazione dei criteri di accesso aziendali relativi all'uso del Servizio e delle sue funzioni. Gli utenti possono accedere ai controlli e ai privilegi in base al ruolo loro assegnato:

Gli **organizzatori** (o i formatori per GoTo Training) sono autorizzati a pianificare riunioni, webinar e/o sessioni di formazione. L'organizzatore imposta ciascuna sessione, invita i partecipanti, avvia e conclude le sessioni e designa il relatore corrente.

I **partecipanti** sono persone invitate a partecipare alle sessioni. I partecipanti possono visualizzare lo schermo condiviso del relatore, chattare con altri partecipanti e visualizzare l'elenco dei partecipanti.

I **relatori** sono partecipanti che possono condividere il loro schermo con altri partecipanti. I relatori possono anche concedere agli altri partecipanti il controllo condiviso della loro tastiera e del loro mouse.

Gli **amministratori** sono persone autorizzate a gestire un account multiutente. Gli amministratori possono configurare le caratteristiche degli account, autorizzare gli organizzatori e accedere a una gamma di strumenti di reporting.

Gli **amministratori interni di GoTo** sono membri del personale GoTo autorizzati a gestire i servizi e gli account GoTo Meeting, GoTo Webinar e GoTo Training per conto dei nostri Clienti.

4.5 Controllo dell'accesso alle registrazioni

Al termine delle sessioni, gli organizzatori possono facilmente condividerne le registrazioni con i partecipanti tramite collegamenti diretti e univoci che consentono loro di riprodurle sui propri browser.

Per GoTo Webinar, gli URL di condivisione non scadono finché la registrazione è disponibile. Per disabilitare l'accesso a una registrazione, gli organizzatori possono cancellare la registrazione in qualsiasi momento.

Per GoTo Meeting, le registrazioni possono essere condivise tramite URL che utilizzano un token casuale con validità limitata. La condivisione può essere limitata a parti definite del contenuto, ed essere disponibile per tutti coloro che dispongono dell'URL o solo per gli utenti con indirizzi e-mail configurabili. Queste restrizioni possono essere modificate anche dopo la condivisione dell'URL.

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.

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 utilizzando i centri dati dei provider di hosting su cloud.

Per i dettagli sui provider dei centri dati e sulla loro ubicazione, consultare l'Informativa sui sub-incaricati del Servizio (Sub-Processor Disclosure) nel Trust & Privacy Center di GoTo.

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

7.1 Sicurezza fisica del centro dati

I provider di hosting su cloud forniscono controlli di sicurezza fisica e ambientale 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

I provider di hosting su cloud limitano l'accesso fisico ai centri dati di produzione solo alle persone autorizzate. L'accesso alle sale server 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. Tutti gli accessi fisici ai centri dati e alle sale server sono ridotti al minimo, registrati ed esaminati dai provider 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, 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:

- **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.
- Report di attestazione **SOC (Service Organization Control) 2 di tipo II** dell'AICPA (American Institute of Certified Public Accountants), compreso il **C5 (BSI Cloud Computing Catalog)**.
- 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.

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 e i sistemi operativi che elaborano i Contenuti del Cliente. GoTo valuta e scansiona le vulnerabilità a livello di sistema, di host/rete ("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

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 viene concesso l'accesso a determinati sistemi, applicazioni, reti e dispositivi GoTo in base al “principio del minimo 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.

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;
- Firewall della rete cloud che filtrano le connessioni in entrata e in uscita, comprese le connessioni interne tra i sistemi GoTo; e
- Segmentazione della rete interna.

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 sospetti o identificati nei suoi sistemi e servizi, compresi Central e Pro. 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.goto.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 vengono automaticamente contrassegnati per l'eliminazione entro novanta (90) giorni ed eliminati entro cento (100) 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.

Le tempistiche di cui sopra sono applicabili a tutti i Servizi, e le tempistiche di cancellazione aggiuntive specifiche di ciascuno Servizio sono indicate di seguito:

GoTo Meeting

Durante il periodo di abbonamento: La cronologia delle sessioni di GoTo Meeting e le registrazioni su cloud saranno eliminate automaticamente a rotazione su base di un (1) anno durante il periodo di abbonamento attivo del Cliente, sia per gli account a pagamento che per quelli gratuiti.

Dopo la scadenza dell'abbonamento: Al termine di un abbonamento a pagamento a GoTo Meeting, gli account del Cliente che contengono una licenza gratuita torneranno ad essere account gratuiti e i Contenuti saranno conservati. Per gli account che non contengono una licenza gratuita o che sono stati esplicitamente annullati o cessati, il Contenuto sarà automaticamente contrassegnato per l'eliminazione entro novanta (90) giorni e cancellato entro cento (100) giorni dalla cessazione, la cancellazione o la scadenza e, in ogni caso, dal deprovisioning dell'abbonamento finale del Cliente. Inoltre, gli account GoTo Meeting gratuiti saranno automaticamente eliminati dopo due (2) anni di inattività dell'utente (se ad esempio non viene effettuato nessun accesso).

Rimozione di un utente da un account a pagamento: Se un utente viene eliminato o rimosso in altro modo da un account attivo a pagamento, le sessioni pianificate vengono automaticamente contrassegnate per la cancellazione dopo novanta (90) giorni e cancellate entro cento (100) giorni dalla rimozione dell'utente.

GoTo Stage: Gli utenti di GoTo Stage con un abbonamento attivo a GoTo Webinar possono annullare la pubblicazione/rimuovere qualsiasi webinar pubblicato in qualsiasi momento tramite self-service attraverso l'ambiente dei servizi GoTo Webinar e/o inviando una richiesta di supporto a GoTo.

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 con le leggi applicabili 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 propri Clienti, Utenti e altre persone che utilizzano i servizi GoTo (“Utenti finali”) e si impegna a divulgare le pratiche di trattamento e gestione dei dati rilevanti 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 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 Quadro normativo sulla privacy dei dati

I quadri normativi sulla privacy dei dati (DPF) UE-USA e Svizzera-USA e l'estensione UK-USA del DPF UE-USA sono accordi volontari che forniscono rispettivamente alle aziende dei meccanismi per il trasferimento dei dati personali dall'Unione Europea, dalla Svizzera e dal regno Unito agli Stati Uniti in conformità con le normative sulla protezione dei dati in

queste giurisdizioni. GoTo è conforme a ciascuno di tali quadri normativi per quanto riguarda la raccolta, l'utilizzo e la conservazione dei dati personali provenienti rispettivamente dall'Unione Europea, dalla Svizzera e dal Regno Unito. Per maggiori informazioni sui DPF e per visualizzare la certificazione di GoTo, visitare il sito web dei DPF.

20.4.3 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.

20.4.4 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.

20.5 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.

20.6 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.

20.7 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 GoTo né forniti a GoTo in altro modo:

- 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.

20.8 Conformità in ambienti regolamentati

I Clienti sono responsabili dell'implementazione di criteri, procedure e altre misure di sicurezza adeguate relative all'uso di GoTo Resolve 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. Ad esempio, il DPA per i fornitori di GoTo prevede restrizioni sulla “vendita” dei dati, come definito dal CCPA. Allo stesso modo, con i fornitori rilevanti sono stati creati degli addendum di sicurezza con controlli e requisiti di sistema adeguati.

22 Contattare GoTo

I Clienti possono contattare GoTo all'indirizzo support.goto.com per richieste di carattere generale. Per domande o richieste relative alla protezione dei dati o alla sicurezza, visitare il nostro portale IRM o inviare un'e-mail a privacy@goto.com.