Medidas Técnicas e Organizacionais
Rescue e Rescue Lens

Resumo Executivo

Este documento denominado Medidas Técnicas e Organizacionais ("TOMs") define os compromissos de privacidade, segurança e responsabilidade da GoTo em relação ao Rescue e ao Rescue Lens. Em especial, a GoTo mantém programas globais robustos de privacidade e segurança e proteções organizacionais, administrativas e técnicas projetadas para: (i) garantir a confidencialidade, a integridade e a disponibilidade do Conteúdo do Cliente; (ii) proteger contra ameaças e riscos à segurança do Conteúdo do Cliente; (iii) proteger contra qualquer perda, uso indevido, acesso não autorizado, divulgação, alteração e destruição do Conteúdo do Cliente; e (iv) manter a conformidade com as leis e regulamentos aplicáveis, incluindo leis de proteção de dados e privacidade. Essas medidas incluem:

- **Criptografia:**
  - Transport Layer Security (TLS) v1.2 *em trânsito*.
  - Transparent Data Encryption (TDE) com Advanced Encryption Standard (AES) de 256 bits para o Conteúdo do Cliente *em repouso*.
- **Data centers:**[1] localizados nos Estados Unidos, Alemanha e Irlanda para oferecer redundância e estabilidade.
- **Segurança física:** controles ambientais e de segurança física adequados estão em vigor e foram projetados para proteger, controlar e restringir o acesso físico aos sistemas e servidores que mantêm o Conteúdo do Cliente para dar suporte a compromissos de tempo de atividade, desempenho e escalabilidade.
- **Auditorias de Conformidade:** o Rescue detém as certificações ISO/IEC 27001:2013, SOC 2 Tipo II, PCI DSS, PCAOB, Privacidade Empresarial TRUSTe e APEC CBPR e PRP.
- **Conformidade legal/regulatória:** a GoTo mantém um programa abrangente de proteção de dados com processos e políticas projetados para garantir que o Conteúdo do Cliente seja tratado de acordo com as leis de privacidade aplicáveis, incluindo GDPR, CCPA/CPRA e LGPD.
- **Avaliações de segurança**: além dos testes internos, a GoTo contrata empresas externas para realizar avaliações regulares de segurança e/ou testes de penetração.
- **Controles de acesso lógico:** os controles de acesso lógico são implementados e projetados para evitar ou atenuar a ameaça de acesso não autorizado a aplicativos e a perda de dados em ambientes corporativos e de produção.
- **Segregação de dados**: a GoTo emprega uma arquitetura multilocatário e separa logicamente as contas dos clientes no nível do banco de dados.
- **Defesa de perímetro e detecção de intrusão**: as ferramentas, as técnicas e os serviços de proteção de perímetro são projetados para impedir que o tráfego de rede não autorizado entre na infraestrutura dos produtos. A rede da GoTo tem firewalls externos e segmentação de rede interna.
- **Retenção de dados:**
  - Os Clientes do Rescue podem solicitar a devolução ou a exclusão do Conteúdo do Cliente a qualquer momento, o que será atendido em até 30 (trinta) dias após a solicitação do Cliente.
  - O Conteúdo do Cliente será automaticamente excluído no prazo de 140 dias após o término do período de assinatura final do Cliente.

[1] Os locais de hospedagem podem variar (por exemplo, de acordo com a escolha da residência dos dados). Consulte a Divulgação do Subprocessador do Rescue, encontrada na seção "Recursos do produto" do GoTo Trust and Privacy Center (https://www.goto.com/company/trust/resource-center), para mais detalhes.

Conteúdo

Clique nos números das páginas abaixo para acessar a seção relevante das TOMs

1 Introdução ao produto

O **Rescue** é um serviço de suporte remoto online usado por técnicos para fornecer assistência remota pela Internet, sem a necessidade de software pré-instalado. Com a permissão do usuário ou de outro indivíduo que esteja usando o Rescue ou recebendo suporte de um técnico (Usuário Final), o Rescue permite que um técnico acesse e visualize e/ou assuma o controle do computador de um Usuário Final. Comunicando-se por meio de uma janela de bate-papo, o técnico pode examinar, diagnosticar e consertar problemas do computador, além de ajudar o Usuário Final com problemas do sistema operacional e dos aplicativos de software.

O **Rescue Lens** permite que os Usuários Finais transmitam as câmeras de seus dispositivos móveis (por meio do aplicativo móvel Lens) para um técnico remoto, permitindo que este visualize o hardware problemático, como um roteador mal configurado ou um componente automotivo danificado. O Rescue Lens é um recurso opcional do Rescue e pode ser ativado no Centro de Administração do Rescue. Para obter mais detalhes sobre o Rescue Lens, consulte o Guia do usuário do Rescue Lens.

Os termos em letras maiúsculas neste documento que não estão definidos no texto são definidos nos Termos de Serviço.

2 Medidas técnicas

Os produtos da GoTo são projetados para fornecer soluções seguras, confiáveis e privadas. As medidas técnicas definidas abaixo descrevem como a GoTo implementa esse design e o aplica na prática para o Rescue e o Rescue Lens.

2.1 Salvaguardas

A implementação de salvaguardas, recursos e práticas da GoTo envolve:

I. Criar produtos que levem em conta a segurança e a privacidade por design e padrão, e incluir camadas adicionais de segurança para proteger o Conteúdo do Cliente;

II. Manutenção de controles organizacionais que operacionalizam políticas e procedimentos internos relacionados à conformidade com padrões, gerenciamento de incidentes, segurança de aplicativos, segurança de pessoal e programas de treinamento regulares; e

III. Garantir que as práticas de privacidade estejam em vigor para governar o manuseio e o gerenciamento de dados de acordo com a legislação aplicável, incluindo GDPR, CCPA/CPRA e LGPD, bem como nosso próprio Adendo de Processamento de Dados (DPA) e as políticas e compromissos aplicáveis da GoTo.

Ao incorporar salvaguardas de segurança ao produto, nós nos esforçamos para proteger o Conteúdo do Cliente da GoTo contra ameaças e garantir que os controles de segurança sejam adequados à natureza e ao escopo dos Serviços. Os recursos de segurança configuráveis da GoTo podem ajudar os administradores a minimizar as ameaças e os riscos aos sistemas e às redes representados por indivíduos que usam os serviços da GoTo.

3 Arquitetura do produto

O Rescue é uma solução SaaS de suporte composta por três componentes principais: um console técnico, um aplicativo móvel ou miniaplicativo desktop para o Usuário Final e um centro de administração.

O console técnico é a interface usada pelos técnicos para conduzir sessões de suporte remoto. Os técnicos podem iniciar novas sessões ou responder a solicitações online de Usuários Finais que aguardam em uma fila compartilhada. Os técnicos se comunicam e prestam suporte aos Usuários Finais pelo aplicativo móvel (Android ou iOS) ou do miniaplicativo desktop (Windows, macOS ou Linux) do Rescue. O miniaplicativo é baixado no PC remoto do Usuário Final e foi projetado para ser removido quando a sessão for concluída.

O console técnico do Rescue interage com o aplicativo ou miniaplicativo do Rescue usando uma conexão de rede ponto a ponto (P2P) (consulte a Figura 1 na seção 3.1). Quando o miniaplicativo é iniciado, o processo P2P é iniciado e se conecta a um gateway do Rescue, onde a sessão com o console técnico é negociada.

O protocolo proprietário de encaminhamento de troca de chaves da GoTo foi projetado para oferecer segurança contra interceptação ou espionagem na infraestrutura da GoTo. Especificamente, a conexão entre o Usuário Final e o host é facilitada pelo gateway para garantir que o Usuário Final possa se conectar ao host independentemente da configuração da rede.

O host estabelece uma conexão TLS com o gateway, que encaminha a troca de chaves TLS do Usuário Final para o host por meio de uma solicitação de renegociação de chave proprietária. Assim, o Usuário Final e o host trocam chaves TLS sem que o gateway saiba a chave.

3.1 Acordo de chaves

Quando uma sessão de suporte é iniciada e uma conexão é estabelecida entre o Usuário Final que será atendido e o técnico, seus computadores precisam entrar em acordo quanto ao algoritmo de criptografia dentre as opções disponíveis e à chave correspondente a ser usada durante a sessão.

Os computadores usam certificados para validar suas identidades. Como nem o técnico nem o Usuário Final têm software capaz de intermediar a conexão e validar os certificados de segurança instalados e um certificado SSL instalado em seus computadores, ambos recorrem a um dos servidores do Rescue e realizam a fase inicial do acordo de chaves. A verificação do certificado pelo console técnico e pelo aplicativo ou miniaplicativo do Usuário Final garante que somente um servidor do Rescue possa mediar o processo.

3.2 Visão geral do processo de entrega do gateway do Rescue

Quando o aplicativo ou miniaplicativo do Rescue assinado digitalmente é iniciado em um computador, ele contém um GUID (Globally Unique Identifier) de autenticação de sessão. O GUID é incorporado em um aplicativo ou miniaplicativo executável (por exemplo, um arquivo .exe) como um recurso do site no ato do download. O aplicativo ou miniaplicativo baixa uma lista de gateways disponíveis em secure.logmeinrescue.com ou secure.logmeinrescue.eu, escolhe uma das opções e se conecta a ela usando TLS. Em seguida, o gateway é autenticado pelo miniaplicativo usando seu certificado SSL. O gateway autentica o miniaplicativo no banco de dados com o GUID e registra que o Usuário Final está aguardando um técnico.

Quando um técnico inicia uma sessão no console técnico do Rescue, uma solicitação é enviada ao gateway com o GUID de autenticação de sessão para passar conexões entre o console técnico e o aplicativo ou miniaplicativo do Usuário Final. O gateway é o intermediário que autentica a conexão e começa a retransmitir os dados no nível de transporte (ele não descriptografa os dados retransmitidos).

Quando uma retransmissão de conexão é iniciada, as partes tentam estabelecer uma conexão P2P. O processo é o seguinte:

- O miniaplicativo começa a escutar uma conexão TCP (Transmission Control Protocol) em uma porta atribuída pelo Windows, macOS ou Linux.
- Se a conexão TCP não puder ser estabelecida em 10 segundos, será feita uma tentativa de estabelecer uma conexão UDP (User Datagram Protocol) com a ajuda do gateway.
- Se uma conexão TCP ou UDP for estabelecida, as partes autenticarão o canal P2P (usando o GUID de autenticação de sessão), que assume o tráfego da conexão retransmitida.
- Se uma conexão UDP tiver sido estabelecida, o TCP será emulado sobre os datagramas UDP usando XTCP, um protocolo proprietário da GoTo baseado na pilha TCP da Berkeley Software Distribution ("BSD").
- Toda conexão é protegida com o protocolo TLS (usando criptografia AES256 com SHA256 Media Access Controls [MAC]). O GUID de autenticação de sessão é um valor inteiro criptograficamente aleatório de 128 bits.

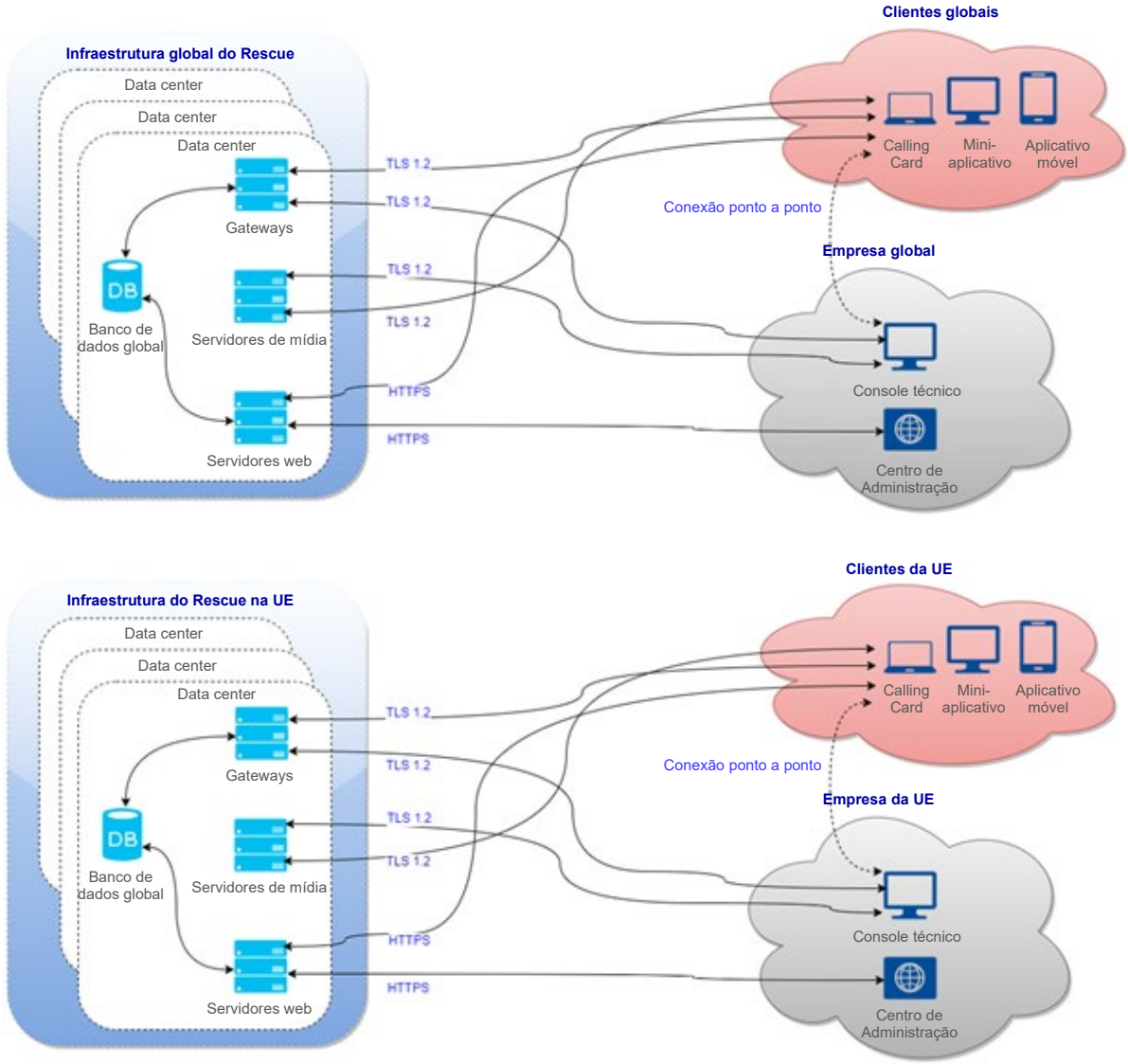

Figura 1: arquitetura do Rescue

3.3 Arquitetura de mídia do Rescue

O serviço de mídia do Rescue é um serviço autônomo baseado em comunicação em tempo real na web (WebRTC) que permite o streaming de vídeo do Rescue Lens. Ele gerencia conferências para sessões do Rescue que usam o recurso Lens. Os participantes da conferência (pares) entram e saem das conferências, e os Usuários Finais enviam streams de vídeo e áudio para que outros participantes os recebam. O Lens envia conteúdo de vídeo em um fluxo unidirecional do aplicativo Lens para o console técnico.

Há três componentes principais do serviço de mídia: o Media Software Development Kit (Media SDK), o gerenciador de sessão e o servidor de streaming. Esses componentes gerenciam o processo de criação/destruição e entrada/saída de conferências. Esses componentes se comunicam por meio das conexões seguras existentes entre o console técnico e o site, e entre o aplicativo Lens e o site.

3.3.1 Media SDK

O serviço de mídia foi criado usando WebRTC com um wrapper fino na base de código do WebRTC. O console técnico e o aplicativo móvel Lens usam o Media SDK.

3.3.2 Gerenciador de sessão

O gerenciador de sessões é um site com balanceamento de carga que fornece uma API REST (Representational State Transfer) para gerenciar (criar, destruir ou ingressar) as conferências. O gerenciador de sessões só aceita solicitações do site.

3.3.3 Servidor de streaming

O serviço de mídia usa uma solução de servidor de streaming personalizada para gerenciar os streams entre pares (o console técnico e o aplicativo Lens). Tanto o console técnico quanto o aplicativo Lens se conectam ao servidor de streaming. Uma sessão do Lens tem dois streams (um é enviado, e o outro é recebido): o aplicativo Lens transmite seu conteúdo de vídeo para o servidor de streaming, enquanto o console técnico recebe o conteúdo de vídeo do servidor. O servidor de streaming se comporta como um servidor de retransmissão entre pares.

4 Controles técnicos de segurança

A GoTo emprega controles técnicos de segurança desenvolvidos para proteger a infraestrutura do Serviço e os dados que residem nela.

4.1 Confidencialidade dos dados

O sistema online seguro do Rescue tem proteção Secure Sockets Layer e Transport Layer Security (SSL/TLS) e atende aos seguintes objetivos:

- Autenticação das partes em comunicação;
- Negociação de chaves de criptografia sem interceptação;
- Troca confidencial de mensagens;
- Capacidade de detectar se uma mensagem foi modificada em trânsito.

O Rescue usa o OpenSSL e, no momento da publicação, a versão usada pelo Rescue é a 1.1.1n.

4.2 Criptografia

A GoTo revisa regularmente seus padrões de criptografia e pode atualizar as cifras e/ou tecnologias usadas de acordo com o risco avaliado e a aceitação de novos padrões pelo mercado.

4.2.1 Criptografia em trânsito

Todo o tráfego de rede que entra e sai dos data centers do Rescue, incluindo todo o Conteúdo do Cliente, é criptografado em trânsito com TLS 1.2 e HTTPS. Além disso, as sessões de suporte do Rescue são protegidas com criptografia AES de 256 bits e MD5 Hash para rastreabilidade aprimorada das transferências de arquivos.

Como todos os três componentes do sistema de comunicações do Rescue estão sob o controle da GoTo, o conjunto de criptografia usado por eles é sempre o mesmo: AES256-SHA no modo de encadeamento de blocos de criptografia com acordo de chave RSA. Isso significa o seguinte:

- O algoritmo de criptografia/descriptografia é o AES;
- A chave de criptografia tem 256 bits de comprimento;
- As chaves de criptografia são trocadas usando pares de chaves públicas/privadas RSA, conforme descrito na seção anterior;
- A base do MAC é o SHA-2. MAC é um pequeno trecho de informação usado para autenticar uma mensagem. O valor MAC protege tanto a integridade quanto a autenticidade de uma mensagem, permitindo que as partes em comunicação detectem quaisquer alterações na mensagem;
- O modo de encadeamento de blocos de cifras (CBC) garante que cada bloco de texto cifrado dependa dos blocos de texto simples até aquele ponto e que mensagens semelhantes não possam ser distinguidas na rede.

Os dados que trafegam entre o Usuário Final atendido e o técnico são criptografados de ponta a ponta, e somente as respectivas partes têm acesso às informações contidas no fluxo de mensagens.

4.2.2 Criptografia em repouso

O Conteúdo do Cliente do Rescue é criptografado em repouso nos níveis do servidor e do banco de dados com AES256 e TDE. Por exemplo, o Conteúdo do Cliente inclui registros de bate-papo e campos personalizados, criados pelo titular da conta principal ou pelo administrador principal.

4.3 Controles de acesso ao Rescue

Os administradores do Rescue podem personalizar os controles de acesso. Por exemplo, os administradores do Rescue podem configurar uma política de senha com força mínima exigida, idade máxima, redefinição obrigatória, autenticação de dois fatores para os logins do Rescue, permissão de acesso de técnicos ao Rescue apenas a partir de endereços IP pré-aprovados para tarefas específicas, ou conceder aos técnicos acesso apenas a aplicativos predefinidos usando um único ID de SSO para fazer login nesses aplicativos. Se necessário, os administradores podem desativar o ID de SSO de um técnico.

Os controles de acesso adicionais incluem:

- Conceder acesso baseado em permissão em um nível granular (como permitir que alguns técnicos usem a visualização remota, mas não o controle remoto);
- Não armazenar dados de dispositivos remotos nos servidores da GoTo. Apenas os registros de sessão, os endereços IP do Usuário Final e os registros de bate-papo são armazenados. Os registros de texto do bate-papo podem ser removidos dos detalhes da sessão;
- Impedir que os técnicos transfiram arquivos;
- Exigir que o Usuário Final esteja presente no dispositivo remoto para permitir o acesso remoto;
- Exigir que o Usuário Final mantenha o controle e possa encerrar a sessão a qualquer momento;
- Impedir que os técnicos usem determinados recursos até que o Usuário Final tenha concedido permissão explícita (por exemplo, controle remoto, visualização da área de trabalho, transferência de arquivos, informações do sistema, reinicialização e reconexão);
- Revogar automaticamente os direitos de acesso quando a sessão é encerrada;
- Forçar o logoff automático com base em um tempo predeterminado de inatividade;
- Bloquear uma conta após cinco tentativas de login sem sucesso.

4.3.1 Controle de acesso baseado em permissão

Os administradores do Rescue também podem conceder ou negar permissões específicas no centro de administração. Essas permissões de grupo incluem:

- Permissão de sincronização da área de transferência;
- Permissão de compartilhamento de tela com Usuários e Usuários Finais;
- Implementação de scripts;
- Inicialização da visualização da área de trabalho;
- Inicialização do gerenciador de arquivos;
- Inicialização do controle remoto;
- Reinicialização;
- Sessões de gravação;
- Solicitação de credenciais;
- Envio e recebimento de arquivos;
- Envio de URLs;
- Início de sessões privadas;
- Transferência de sessões;
- Uso de um único prompt para todas as permissões;
- Visualização de informações do sistema.

Para obter mais detalhes sobre permissões de grupo, consulte o Guia do administrador do Rescue. Os técnicos do Rescue Lens são identificados por seu endereço de e-mail e autenticados com uma senha.

4.3.2 Autenticação

As medidas de autenticação do Rescue são projetadas para proteger o produto, de modo que apenas técnicos ou administradores podem fazer login no sistema. Os administradores atribuem aos técnicos IDs de login (por exemplo, iguais aos endereços de e-mail) e senhas correspondentes. Os técnicos inserem essas credenciais no formulário de login do site do Rescue pelo menos no início de seu turno. Os administradores podem configurar os controles para exigir autenticação com mais frequência (por exemplo, após cinco minutos de inatividade).

O sistema do Rescue é autenticado no navegador do técnico com seu certificado RSA SSL premium de 2048 bits para confirmar se o técnico digitou o nome de usuário e a senha no site correto. Em seguida, o técnico faz login no sistema com suas credenciais. O Rescue não armazena senhas, mas usa scrypt para criar hashes a partir das senhas armazenadas no banco de dados do Rescue. Os hashes recebem sal com uma string de 24 caracteres gerada pelo CSPRNG para cada senha exclusiva.

O sistema do Rescue também é autenticado para o Usuário Final atendido. O aplicativo ou miniaplicativo baixado e executado pelo Usuário Final é assinado com o certificado de assinatura de código da GoTo (baseado em uma chave RSA de 2048 bits), e essa informação é normalmente exibida ao Usuário Final pelo navegador quando ele está prestes a executar o software. O Rescue não autentica o Usuário Final para o técnico.

O Rescue também permite que os administradores implementem uma política de SSO (logon único). É utilizada a SAML (Security Assertion Markup Language), que é um padrão XML (Extensible Markup Language) para troca de dados de autenticação e autorização entre domínios de segurança (entre um provedor de identidade e um provedor de serviços).

Os administradores também podem exigir a verificação em duas etapas para fazer login no Rescue. O recurso de verificação em duas etapas pode usar e-mail, SMS ou qualquer autenticador de TOTP (senha única baseada em tempo) para fornecer uma segunda camada de proteção a uma conta do Rescue, exigindo que membros selecionados da organização configurem uma maneira adicional de verificar sua identidade. A configuração do aplicativo autenticador é acionada em qualquer um dos seguintes casos:

- O membro selecionado tenta fazer login em sua conta do Rescue no site seguro;
- O membro selecionado tenta fazer login no console do técnico de desktop;
- O membro selecionado tenta alterar sua senha do Rescue.

4.3.3 Autorização

A autorização ocorre pelo menos uma vez durante cada sessão de suporte remoto. Depois de fazer o download e executar o miniaplicativo, o Usuário Final com suporte será contatado por um técnico. O técnico pode conversar com o Usuário Final por meio do miniaplicativo, mas qualquer outra ação, como enviar um arquivo ou visualizar a área de trabalho do Usuário Final, requer a permissão expressa do Usuário Final. Um "prompt único" também pode ser implementado para trabalhos longos de suporte remoto em que o Usuário Final pode não estar presente durante toda a sessão. Se essa configuração estiver ativada para um grupo de técnicos, os técnicos desse grupo poderão solicitar uma permissão "global" do Usuário Final e, se concedida, poderão executar ações como visualizar informações do sistema ou entrar em uma sessão de controle remoto sem precisar de mais autorizações do Usuário Final. Os administradores também podem impor restrições de endereço IP para que os técnicos designados para uma tarefa específica só possam acessar o Rescue e executar essa tarefa a partir de endereços IP pré-aprovados. O administrador de um grupo de técnicos também pode desativar determinados recursos no centro de administração.

As permissões que um administrador pode conceder ou negar incluem:

- Iniciar o controle remoto;
- Reiniciar;
- Iniciar a exibição da área de trabalho;
- Gravar sessões;
- Enviar e receber arquivos;
- Iniciar sessões privadas;
- Abrir o gerenciador de arquivos;
- Solicitar credenciais;
- Enviar URLs;
- Permitir a sincronização da área de transferência;
- Visualizar informações do sistema;
- Implementar scripts;
- Usar prompts únicos para todas as permissões;
- Transferir sessões;
- Permitir o compartilhamento de tela com Usuários e Usuários Finais.

4.4 Controles de auditoria

Os seguintes controles de auditoria estão disponíveis para os Usuários e Usuários Finais do Rescue:

- A opção de forçar a gravação da sessão, com a capacidade de armazenar arquivos de auditoria em uma rede compartilhada segura;
- As atividades das sessões dos técnicos e das sessões remotas ficam registradas no computador host para garantir a segurança e manter o controle de qualidade (logins bem-sucedidos, falhas de logins, controle remoto iniciado, controle remoto encerrado, reinicialização efetuada, logout);
- Autenticação de pessoa ou entidade;
- Autenticação do técnico usando seu endereço de e-mail exclusivo ou ID de SSO;
- Exigência de os técnicos façam login somente a partir de endereços IP aprovados.
- O relatório de auditoria disponível no Centro de Administração inclui alterações nas configurações da conta e dados de cada ação dos administradores no item da Árvore da Organização selecionado durante um período específico.

5 Atualizações do programa de segurança

A GoTo revisa e atualiza seu programa de segurança e contrata terceiros independentes para avaliar seus controles de segurança relevantes pelo menos uma vez por ano. Isso é feito para garantir que ela está se desenvolvendo em relação ao cenário atual de ameaças, bem como para assegurar a conformidade com estruturas relevantes, padrões do setor, comprometimentos com o Cliente e, conforme aplicável, alterações nas leis e nos regulamentos relativos à segurança dos dados da GoTo.

6 Backup de dados, recuperação de desastres e disponibilidade

A arquitetura da GoTo foi projetada para realizar a replicação quase em tempo real em locais geograficamente diferentes. O backup dos bancos de dados é feito usando uma estratégia de backup incremental contínuo. No caso de um desastre ou falha total da instalação de qualquer um dos vários locais ativos, os locais restantes são projetados para equilibrar a carga do aplicativo. A recuperação de desastres relacionada a esses sistemas é testada periodicamente.

O banco de dados do Rescue sincroniza com outro data center a cada cinco minutos. Além disso, um backup diferencial é feito todas as noites, e backups completos são realizados todos os finais de semana. O banco de dados de backup é armazenado com a mesma criptografia que o original. Os backups são retidos no local por um mês e depois transferidos para um serviço de nuvem, não são mais processados ativamente e são retidos de acordo com nossas políticas internas de retenção de registros. No caso de uma falha completa do data center que hospeda o banco de dados primário, a arquitetura do Rescue foi projetada para ser restaurada rapidamente.

7 Data centers

A infraestrutura da GoTo foi projetada para aumentar a confiabilidade do serviço e reduzir o risco de tempo de inatividade provocado por um único ponto de falha. Para isso, foram adotados:

a) data centers ativos-passivos redundantes; ou
b) data centers de provedores de hospedagem em nuvem.

Após a criação da conta, os Clientes do Rescue podem optar por utilizar a infraestrutura de dados da União Europeia ou Global da GoTo para armazenar o Conteúdo do Cliente. Os locais de hospedagem e armazenamento estão especificados abaixo:[2]

- **União Europeia:** Alemanha e Irlanda
- **Global:** Estados Unidos, Alemanha, Austrália e Reino Unido

Todos os data centers incluem o monitoramento das condições ambientais e adotam as medidas de segurança física ininterruptas abordadas abaixo.

7.1 Segurança física do data center

A GoTo contrata data centers para fornecer segurança física e controles ambientais para sistemas e servidores que contêm o Conteúdo do Cliente. Esses controles incluem:

- Vigilância e gravação de vídeo
- Controle de temperatura por aquecimento, ventilação e ar-condicionado
- Supressão de incêndio e detectores de fumaça
- Fonte de alimentação ininterrupta
- Pisos elevados ou gerenciamento abrangente de cabos
- Monitoramento e alertas contínuos
- Proteções contra desastres naturais e causados pelo homem, conforme exigido pela geografia e localização do data center relevante
- Manutenção programada e validação de todos os controles críticos de segurança e ambientais

A GoTo limita o acesso físico aos data centers de produção apenas a indivíduos autorizados. O acesso a uma sala de servidor local ou a uma instalação de hospedagem de terceiros requer o envio de uma solicitação pelo sistema de criação de tickets relevante e a aprovação do gerente apropriado, bem como a análise e a aprovação da equipe de operações técnicas da GoTo. Todos os acessos físicos aos data centers e salas de servidores são registrados, e a gerência da GoTo analisa os registros pelo menos trimestralmente. Além disso, a autorização de acesso físico ao data center é removida imediatamente após a mudança de função (quando esse acesso não é mais necessário) ou após o desligamento de qualquer pessoa previamente autorizada. O acesso com vários fatores (por exemplo, biometria, crachá e teclado) é necessário para áreas altamente sensíveis, que incluem data centers.

8 Conformidade com os padrões

A GoTo avalia regularmente sua conformidade com os requisitos legais, de segurança, financeiros, de privacidade de dados e regulatórios aplicáveis. Os programas de privacidade e segurança da GoTo atendem a padrões rigorosos e reconhecidos internacionalmente, foram avaliados de acordo com padrões abrangentes de auditoria externa e obtiveram certificações importantes, incluindo:

- **Certificação de Privacidade Empresarial e Práticas de Governança de Dados da TRUSTe** para abordar a privacidade operacional e os controles de proteção de dados que estão alinhados com as principais leis de privacidade e estruturas de privacidade reconhecidas. Para saber mais, visite nossa publicação no blog.
- **Certificações TRUSTe APEC CBPR e PRP** para a transferência do Conteúdo do Cliente entre países-membros da APEC, obtidas e validadas de forma independente pela TrustArc, uma líder terceirizada aprovada pela APEC em conformidade com a proteção de dados. Para saber mais sobre nossas certificações APEC, clique aqui.

[2]Os locais de hospedagem podem variar (por exemplo, de acordo com a escolha da residência dos dados). Consulte a Divulgação do Subprocessador do Rescue aplicável, encontrada na seção "Recursos do produto" do GoTo Trust and Privacy Center (https://www.goto.com/company/trust/resource-center).

- Organização Internacional de Padronização – Certificação do Sistema de Gerenciamento de Segurança da Informação (ISMS) **ISO/IEC 27001:2013**.
- Relatório de atestado do **Service Organization Control (SOC) 2 Tipo 2** do American Institute of Certified Public Accountants (AICPA).
- Conformidade com o **Payment Card Industry Data Security Standard (PCI DSS)** para os ambientes de comércio eletrônico e pagamento da GoTo.
- Avaliação dos controles internos, conforme exigido pela auditoria anual das demonstrações financeiras feitas pelo **Public Company Accounting Oversight Board (PCAOB)**.

9 Segurança do aplicativo

O programa de segurança de aplicativos da GoTo segue o Microsoft Security Development Lifecycle (SDL) para proteger o código do produto. O programa Microsoft SDL inclui revisões manuais de código, modelagem de ameaças, análise estática de código, análise dinâmica e fortalecimento do sistema. As equipes da GoTo também realizam periodicamente testes de vulnerabilidade de aplicativos dinâmicos e estáticos e atividades de teste de penetração para ambientes específicos.

10 Registro em log, monitoramento e alertas

A GoTo mantém políticas e procedimentos de registro em log, monitoramento e alerta, que definem os princípios e controles implementados para reforçar nossa capacidade de detectar atividades suspeitas e responder a elas em tempo hábil. A GoTo coleta o tráfego anômalo ou suspeito identificado nos registros de segurança relevantes nos sistemas de produção aplicáveis.

Os registros de bate-papo do Rescue ficam salvos no banco de dados do Rescue. O registro de bate-papo é transmitido aos servidores do Rescue pelo console técnico em tempo real e contém eventos e mensagens de bate-papo relacionados a uma determinada sessão de suporte. Os arquivos de registro contêm as seguintes ações dos técnicos: hora de início e término de uma sessão de controle remoto; instâncias de técnicos compartilhando arquivos com Usuários Finais; e metadados relacionados ao compartilhamento de arquivos (por exemplo, o nome e a impressão digital MD5 Hash de um arquivo transmitido). O banco de dados de registros de bate-papos está disponível para consulta na central de administração.

Para contas ativas, o conteúdo dos registros será disponibilizado online por dois anos após o término de uma sessão de suporte remoto e arquivado por mais dois anos depois disso.

Para facilitar a integração com os sistemas de CRM, o Rescue pode publicar detalhes da sessão em um URL, e os administradores podem optar por excluir o texto do bate-papo desses detalhes. O texto do bate-papo é incluído por padrão, mas os Clientes podem alterar essa configuração no centro de administração. Além disso, todos os registros de textos de bate-papo entre técnicos e Usuários Finais podem ser automaticamente omitidos dos detalhes da sessão armazenados em um data center do Rescue. O Rescue permite que os técnicos gravem em um arquivo de vídeo os eventos que ocorrem durante uma sessão de visualização da área de trabalho ou de controle remoto. Os arquivos de gravação são armazenados em um diretório especificado pelo técnico.

11 Detecção e resposta de endpoints

O software de detecção e resposta de endpoints com registro em log de auditoria é implantado em todos os servidores da GoTo para minimizar a interrupção ou o impacto no desempenho do Serviço. As investigações de segurança serão iniciadas de acordo com nossos procedimentos de resposta a incidentes se for detectada atividade suspeita, conforme apropriado e necessário. Consulte a seção 17 para obter mais informações sobre o Centro de Operações de Segurança da GoTo e os procedimentos de resposta a incidentes.

12 Gerenciamento de ameaças

A Equipe de Resposta a Incidentes de Segurança Cibernética ("CSIRT") da GoTo é composta por várias equipes e é responsável pela proteção contra ameaças cibernéticas. Especificamente, a Equipe de Inteligência de Ameaças Cibernéticas da CSIRT coleta, examina e divulga informações relativas a ameaças atuais e emergentes. A GoTo se mantém atualizada com a inteligência e a mitigação de ameaças por meio da análise de fontes abertas e fechadas e da participação em grupos de compartilhamento e associações do setor (IT-ISAC, FIRST.org, etc.).

13 Varredura de segurança e vulnerabilidade e gerenciamento de patches

A GoTo mantém um programa formal de gerenciamento de patches e, pelo menos trimestralmente, realiza atividades de gerenciamento de patches em todos os sistemas, dispositivos, firmware, sistemas operacionais, aplicativos e outros softwares relevantes que processam o Conteúdo do Cliente. A GoTo avalia e examina as vulnerabilidades de host/rede interna e externa em nível de sistema ("Sistemas"), no mínimo mensalmente, bem como após qualquer alteração material nesses Sistemas, e corrige as vulnerabilidades relevantes descobertas de acordo com políticas documentadas que priorizam a correção com base no risco.

14 Controle de acesso lógico da GoTo

Os procedimentos de controle de acesso lógico estão em vigor para reduzir o risco de acesso não autorizado a aplicativos e de perda de dados em ambientes corporativos e de produção. Os funcionários da GoTo recebem acesso a sistemas, aplicativos, redes e dispositivos da GoTo específicos com base no princípio do menor privilégio. Os privilégios do Usuário são segregados com base na função funcional (controle de acesso baseado na função) e no ambiente, usando controles, processos e/ou procedimentos de segregação de funções.

15 Segregação de dados

A GoTo utiliza uma arquitetura multilocatário, logicamente separada no nível do banco de dados, com base na conta GoTo de um Usuário ou organização. As partes devem ser autenticadas para obter acesso a uma conta. A GoTo também implementou controles para impedir que os Usuários ou Usuários Finais vejam os dados de outros Usuários ou Usuários Finais.

16 Defesa de perímetro e detecção de intrusão

A GoTo utiliza ferramentas, técnicas e serviços de proteção de perímetro para impedir que tráfego de rede não autorizado entre na infraestrutura de produtos da GoTo. Isso inclui, sem limitações:

- Sistemas de detecção de intrusão que monitoram sistemas, serviços, redes e aplicativos em busca de acesso não autorizado;
- Monitoramento de arquivos críticos de sistema e configuração para evitar ou reduzir a probabilidade de modificações não autorizadas;
- Firewall de aplicativos da Web (WAF) e serviço de prevenção de DDoS na camada de aplicativos, por meio dos quais o tráfego da GoTo é enviado por proxy para bloquear o tráfego de servidores mal-intencionados;
- Um firewall de aplicativo local que fornece uma camada adicional de proteção contra as dez principais vulnerabilidades do OWASP e outras vulnerabilidades e tráfego mal-intencionado de aplicativos web;
- Firewalls baseados em host nos servidores web da GoTo que filtram conexões de entrada e saída, incluindo conexões internas entre sistemas da GoTo.

17 Operações de segurança e gerenciamento de incidentes

O Centro de Operações de Segurança (SOC) da GoTo é responsável por detectar e responder a eventos de segurança. O SOC usa sensores de segurança e sistemas de análise para identificar possíveis problemas e desenvolveu procedimentos de resposta a incidentes, incluindo um Plano de Resposta a Incidentes documentado.

O Plano de Resposta a Incidentes da GoTo está alinhado com nossas medidas críticas de processos de comunicação, políticas e procedimentos operacionais padrão. Ele foi projetado para gerenciar, identificar e resolver eventos de segurança relevantes, suspeitos ou identificados, em seus sistemas e serviços, incluindo o Rescue. O Plano de Resposta a Incidentes estabelece mecanismos para que os funcionários relatem suspeitas de eventos de segurança e rotas de encaminhamento a serem seguidas quando apropriado. Os eventos suspeitos são documentados e encaminhados conforme apropriado por tickets de eventos padronizados e são organizados conforme o nível de gravidade.

18 Exclusão e devolução de conteúdo

Exclusão e/ou Devolução: os Clientes podem solicitar a devolução e/ou exclusão de seu Conteúdo do Cliente ao enviar uma solicitação pelo Portal de Gerenciamento de Direitos Individuais ("IRM") da GoTo, pelo site support.logmeinrescue.com ou pelo e-mail privacy@goto.com. As solicitações serão processadas no prazo de 30 (trinta) dias após o recebimento pela GoTo. No entanto, na eventualidade improvável de precisarmos de mais tempo, avisaremos o mais rápido possível sobre qualquer atraso previsto e informaremos o novo prazo de conclusão.

Cronograma de Retenção de Conteúdo do Cliente: a menos que exigido de outra forma pela legislação aplicável, o Conteúdo do Cliente será automaticamente excluído no prazo de 140 dias após a rescisão, o cancelamento ou o término do período e, em cada caso, o desprovisionamento da assinatura final do Cliente.

Mediante solicitação por escrito, a GoTo poderá fornecer confirmação/certificação por escrito da exclusão do Conteúdo.

19 Controles organizacionais

19.1 Políticas e procedimentos de segurança

A GoTo mantém um conjunto abrangente de políticas e procedimentos de segurança que são periodicamente revisados e atualizados conforme necessário para apoiar os objetivos de segurança da GoTo, as mudanças na legislação aplicável, os padrões do setor e os esforços de conformidade.

19.2 Gerenciamento de mudanças

A GoTo mantém um processo adequado de gerenciamento de mudanças, e as mudanças nos sistemas da GoTo são avaliadas, testadas e aprovadas antes da implementação para reduzir o risco de interrupção dos serviços da GoTo.

19.3 Programas de conscientização e treinamento em segurança

O programa de conscientização sobre privacidade e segurança da GoTo envolve o treinamento de funcionários sobre a importância de manusear Dados Pessoais e informações confidenciais com ética, responsabilidade, conformidade com a lei aplicável e o devido cuidado. Os funcionários, prestadores de serviços e estagiários recém-contratados são informados sobre as políticas de segurança e o Código de Conduta e Ética Comercial da GoTo durante a integração. Os Funcionários da GoTo recebem treinamento em conscientização sobre privacidade e segurança pelo menos uma vez por ano. As atividades de conscientização ocorrem durante todo o ano e podem incluir campanhas para o Dia da Privacidade de Dados, Mês de Conscientização sobre Segurança Cibernética, webinars com o Chief Information Security Officer e um programa de campeões de segurança.

Quando apropriado, os funcionários também podem ser solicitados a realizar treinamentos específicos para suas funções. Além disso, todos os funcionários, contratantes e subsidiárias da GoTo devem analisar e aderir às políticas da GoTo relacionadas à segurança e à proteção de dados.

20 Práticas de privacidade

A GoTo leva muito a sério a privacidade de nossos Clientes, Usuários e Usuários Finais e tem o compromisso de divulgar práticas relevantes de manuseio e gerenciamento de dados de forma aberta e transparente.

20.1 Programa de privacidade

A GoTo mantém um programa de privacidade abrangente que envolve a coordenação de várias funções dentro da empresa, como Privacidade, Segurança, Governança, Risco e Conformidade (GRC), Jurídico, Produto, Engenharia e Marketing. Esse programa de privacidade está centrado nos esforços de conformidade e envolve a implementação e a manutenção de políticas internas e externas, padrões e adendos para reger as práticas da empresa.

20.2 Conformidade regulatória

20.2.1 RGPD

O Regulamento Geral de Proteção de Dados (RGPD) é uma lei da União Europeia (UE) referente à proteção de dados e à privacidade de indivíduos na UE. A GoTo mantém um programa abrangente de conformidade com o RGPD e, na medida em que a GoTo se envolver no processamento de Dados Pessoais sujeitos ao

RGPD em nome do Cliente, nós o faremos de acordo com os requisitos aplicáveis do RGPD. Para mais informações, acesse https://www.goto.com/company/trust/privacy.

20.2.2 CCPA

A Lei de Privacidade do Consumidor da Califórnia, conforme alterada pela Lei de Direitos de Privacidade da Califórnia (coletivamente denominadas "CCPA"), concede aos californianos direitos e proteções adicionais em relação à forma como as empresas podem usar suas informações pessoais. A GoTo mantém um programa de conformidade abrangente e, na medida em que a GoTo se envolver no processamento de Dados Pessoais sujeitos à CCPA em nome do Cliente, nós o faremos de acordo com os requisitos aplicáveis da CCPA. Para obter mais informações sobre nossa conformidade com a CCPA, consulte a Política de Privacidade da GoTo e as Divulgações Suplementares da Lei de Privacidade do Consumidor da Califórnia.

20.2.3 LGPD

A Lei Geral de Proteção de Dados (LGPD) regulamenta o processamento de Dados Pessoais no Brasil e/ou de indivíduos localizados no Brasil no momento da coleta. A GoTo mantém um programa de conformidade abrangente e, na medida em que a GoTo se envolver no processamento de Dados Pessoais sujeitos à LGPD em nome do Cliente, nós o faremos de acordo com os requisitos aplicáveis da LGPD. Para mais informações, acesse https://www.goto.com/company/trust/privacy.

20.3 Adendo de Processamento de Dados

A GoTo oferece um Adendo de Processamento de Dados (DPA) global, disponível em inglês e alemão. Este DPA atende aos requisitos do RGPD, CCPA, LGPD e outros regulamentos aplicáveis e rege o processamento do Conteúdo do Cliente pela GoTo.

Especificamente, nosso DPA incorpora várias proteções de privacidade de dados com foco no RGPD, incluindo:

(a) detalhes de processamento de dados e divulgações de subprocessadores, conforme exigido pelo Artigo 28;
(b) Cláusulas Contratuais Padrão revisadas (2021) (também conhecidas como as Cláusulas Modelo da UE); e
(c) medidas técnicas e organizacionais específicas dos produtos da GoTo.

Além disso, para atender aos requisitos da CCPA, nosso DPA global inclui:

a) definições revisadas mapeadas conforme a CCPA;
b) direitos de acesso e exclusão; e
c) garantias de que a GoTo não venderá as informações pessoais de nossos Clientes, Usuários e Usuários Finais.

Nosso DPA global também inclui disposições para:

(a) abordar a conformidade da GoTo com a LGPD;
(b) respaldar transferências legais de Dados Pessoais de/para o Brasil; e
(c) garantir que nossos Usuários desfrutem dos mesmos benefícios de privacidade que nossos outros Usuários globais.

20.4 Estruturas de transferência

A GoTo executa transferências de dados internacionais legais de acordo com as seguintes estruturas:

20.4.1 Cláusulas Contratuais Padrão

As Cláusulas Contratuais Padrão (SCCs), às vezes chamadas de Cláusulas Modelo da UE, são termos contratuais padronizados, reconhecidos e adotados pela Comissão Europeia, para garantir que quaisquer Dados Pessoais que saiam do Espaço Econômico Europeu (EEE) sejam transferidos em conformidade com a lei de proteção de dados da UE. As SCCs, revisadas e emitidas em 2021, são incorporadas ao DPA global da GoTo para permitir que os clientes da GoTo transfiram dados para fora do EEE em conformidade com o RGPD.

20.4.2 Certificações APEC CBPR e PRP

A GoTo obteve as certificações CBPR (Cross-Border Privacy Rules) e PRP (Privacy Recognition for Processors) da Cooperação Econômica Ásia-Pacífico (APEC). As estruturas CBPR e PRP da APEC são as primeiras estruturas de regulamentação de dados aprovadas para a transferência de dados pessoais entre os países membros da APEC e foram obtidas e validadas de forma independente pela TrustArc, um fornecedor terceirizado de conformidade de proteção de dados aprovado pela APEC.

20.5 Medidas Suplementares

Além das medidas especificadas nestas TOMs, a GoTo criou um documento de perguntas frequentes destinado a delinear as medidas suplementares implementadas para executar as transferências legais nos termos do Capítulo 5 do RGPD e abordar e orientar quaisquer análises caso a caso recomendadas pelo Tribunal de Justiça Europeu em conjunto com o uso das SCCs.

20.6 Solicitações de dados

A GoTo mantém processos abrangentes para facilitar o recebimento de solicitações relacionadas à proteção de dados e à segurança, incluindo o portal IRM, o endereço de e-mail de privacidade (privacy@goto.com) e o suporte ao Cliente em https://support.goto.com.

20.7 Divulgações de subprocessadores e data centers

A GoTo publica as divulgações de subprocessadores em seu Trust & Privacy Center (https://www.goto.com/company/trust/resource-center). Essas divulgações mostram os nomes, os locais e as finalidades de processamento dos provedores de hospedagem de dados e outros terceiros que processam o Conteúdo do Cliente como parte do fornecimento do Serviço aos Clientes da GoTo.

20.8 Restrições de processamento de dados sensíveis

A menos que expressamente solicitado pela GoTo ou que o Cliente tenha recebido permissão por escrito da GoTo, os seguintes tipos de dados confidenciais não devem ser carregados no Rescue nem fornecidos de outra forma à GoTo:

- Números de identificação emitidos pelo governo e imagens de documentos de identificação.

- Informações relacionadas à saúde de um indivíduo, incluindo, entre outras, Informações Protegidas de Saúde (PHI), conforme identificadas na Lei de Portabilidade e Responsabilidade de Seguro de Saúde (HIPAA) dos EUA , bem como em outras leis e regulamentações relevantes aplicáveis.
- Informações relacionadas a contas financeiras e instrumentos de pagamento, incluindo, entre outras, dados de cartão de crédito. A única exceção geral a essa disposição se estende aos formulários e páginas de pagamento explicitamente identificados usados pela GoTo para coletar o pagamento pelo Serviço.
- Quaisquer informações especialmente protegidas pelas leis e regulamentos aplicáveis, especificamente informações sobre raça, etnia, crenças religiosas ou políticas, filiação a organizações etc.

20.9 Conformidade em ambientes regulamentados

Os clientes são responsáveis pela implementação de políticas, procedimentos e outras proteções apropriadas relacionadas ao uso do Rescue para oferecer suporte a dispositivos em ambientes regulamentados.

21 Controles de segurança e privacidade de terceiros

Antes de contratar fornecedores terceirizados que processam o Conteúdo do Cliente ou dados confidenciais, sensíveis ou de funcionários, a GoTo revisa e analisa as práticas de segurança e privacidade do fornecedor usando os canais de Aquisição apropriados. Conforme apropriado, o GoTo pode obter e avaliar periodicamente a documentação ou os relatórios de conformidade dos fornecedores para garantir que seu ambiente de controle e seus padrões continuem sendo suficientes.

A GoTo celebra contratos por escrito com todos os fornecedores terceirizados e utiliza modelos de aquisição aprovados pela GoTo ou negocia os termos e condições padrão desses terceiros para atender aos padrões de privacidade e segurança aceitos pela GoTo quando necessário. As equipes de Finanças, Jurídico, Privacidade e Segurança estão envolvidas no processo de análise de fornecedores e verificam se eles atendem aos requisitos contratuais e de tratamento de dados obrigatórios específicos, conforme necessário e/ou apropriado. As políticas de risco de terceiros da GoTo regem os requisitos de privacidade e segurança dos fornecedores com base no tipo e na duração do processamento de dados e no nível de acesso. Quando apropriado (por exemplo, quando o Conteúdo do Cliente é processado ou armazenado), os contratos com fornecedores incluem requisitos de "conformidade com a lei aplicável", um DPA ou documento semelhante que aborda tópicos como RGPD, CCPA, LGPD e restrições de uso e venda, conforme apropriado. Da mesma forma, adendos de segurança com controles adequados e requisitos de sistemas são implementados com fornecedores relevantes. O DPA do fornecedor da GoTo tem restrições quanto à "venda" de dados, conforme definido na CCPA.

22 Como entrar em contato com a GoTo

Os clientes podem entrar em contato com a GoTo pelo site https://support.goto.com para tratar de consultas gerais. Para perguntas ou solicitações relacionadas a Dados Pessoais ou privacidade, acesse nosso portal IRM ou envie um e-mail para privacy@goto.com.