# Mesures techniques et d'organisation
## Rescue et Rescue Lens

## Synthèse

Ce document sur les mesures techniques et organisationnelles (« TOMs ») définit les engagements de GoTo en matière de confidentialité, de sécurité et de responsabilité pour Rescue et Rescue Lens. Plus précisément, GoTo maintient de solides programmes de confidentialité et de sécurité au niveau mondial, ainsi que des mesures de protection organisationnelles, administratives et techniques conçues pour : (i) assurer la confidentialité, l'intégrité et la disponibilité du Contenu Client ; (ii) protéger contre les menaces et les risques pour la sécurité du Contenu Client ; (iii) protéger contre toute perte, mauvaise utilisation, accès non autorisé, divulgation, altération et destruction du Contenu Client ; et (iv) maintenir la conformité avec les lois et règlements applicables, y compris les lois sur la protection des données et de la vie privée. Ces mesures comprennent notamment :

- **Chiffrement :**
  - *En transit* Sécurité de la couche transport TLS (Transport Layer Security) v1.2.
  - *Statique* Transparent Data Encryption (TDE) par la norme Advanced Encryption Standard (AES) 256 bits pour le Contenu Client.
- **Centres de données :**[1] centres de données situés aux États-Unis, en Allemagne et en Irlande pour assurer la redondance et la stabilité.
- **Sécurité physique :** Une sécurité physique et des contrôles environnementaux appropriés sont en place et conçus pour protéger, contrôler et restreindre l'accès physique aux systèmes et aux serveurs qui conservent le Contenu Client afin de respecter les engagements en matière disponibilité, de performance et d'évolutivité.
- **Audits de conformité :** Rescue a obtenu les certifications ISO/IEC 27001:2013, SOC 2 Type II, PCI DSS, PCAOB, TRUSTe Enterprise Privacy et APEC CBPR/PRP.
- **Conformité légale/réglementaire :** GoTo maintient un programme complet de protection des données avec des processus et des politiques conçus pour s'assurer que le Contenu Client est traité conformément aux lois de protection de la vie privée applicables, y compris le RGPD, CCPA/CPRA et LGPD.
- **Évaluations de sécurité** : En plus des tests internes, GoTo passe des contrats avec des sociétés externes pour effectuer des évaluations régulières de la sécurité et/ou des tests d'introduction.
- **Contrôles d'accès logiques :** Les contrôles d'accès logiques sont mis en œuvre et conçus pour prévenir ou atténuer la menace d'accès non autorisé aux applications et de perte de données dans les environnements d'entreprise et de production.
- **Séparation des données** : GoTo utilise une architecture multi-entité et sépare logiquement les comptes clients au niveau de la base de données.
- **Défense du périmètre et détection des intrusions** : Les outils, techniques et services de protection du périmètre sont conçus pour empêcher le trafic réseau non autorisé de pénétrer dans l'infrastructure du produit. Le réseau GoTo est doté de pare-feu externes et d'une segmentation interne du réseau.
- **Conservation :**
  - Les clients de Rescue peuvent demander la restitution ou la suppression du Contenu Client à tout moment, ce qui sera fait dans les trente (30) jours suivant la demande du Client.
  - Le Contenu Client sera automatiquement supprimé dans les cent quarante (140) jours après l'expiration de la dernière période d'abonnement du Client.

[1] Les lieux d'hébergement peuvent varier (par exemple en fonction du choix de la résidence des données). Consultez la déclaration de sous-traitance de Rescue dans la section Ressources produits du GoTo Trust and Privacy Center (https://www.goto.com/company/trust/resource-center) pour plus de détails.

# Table des matières

Cliquez sur les numéros de page ci-dessous pour accéder à la section correspondante des mesures TOM.

# 1 Présentation du produit

**Rescue** est un service de téléassistance en ligne utilisé par les techniciens pour fournir une assistance à distance par l'Internet, sans nécessiter de logiciel préinstallé. Avec l'autorisation de l'utilisateur ou de toute autre personne utilisant Rescue ou recevant l'assistance d'un technicien (utilisateur final), Rescue permet à un technicien d'accéder à l'ordinateur de l'utilisateur final, d'en afficher le contenu et/ou d'en prendre le contrôle. En communiquant par une fenêtre de chat, le technicien peut examiner, diagnostiquer et réparer les problèmes informatiques et aider l'utilisateur final à résoudre les problèmes de système d'exploitation et d'applications logicielles.

**Rescue Lens** permet aux utilisateurs finaux de diffuser l'image de la caméra de leur appareil mobile (par l'application mobile Lens) à un technicien à distance, ce qui permet à ce dernier de voir le matériel problématique, comme un routeur mal configuré ou un composant automobile endommagé. Rescue Lens est une fonction en option de Rescue qui peut être activée dans le centre d'administration de Rescue. Pour plus de détails sur Rescue Lens, veuillez consulter le Manuel d'utilisation de Rescue Lens.

*Les termes en majuscule dans ce document qui ne sont pas définis dans le texte sont définis dans les Conditions d'utilisation des Services*.

# 2 Mesures techniques

Les produits GoTo sont conçus pour fournir des solutions sécurisées, fiables et privées. Les mesures techniques définies ci-dessous décrivent comment GoTo met en œuvre ce principe et l'applique dans la pratique pour Rescue et Rescue Lens.

## 2.1 Mesures de protection

La mise en œuvre par GoTo de mesures de protection, de fonctionnalités et de pratiques implique notamment :

I. Construire des produits qui prennent en compte la sécurité et le respect de la vie privée dès la conception et par défaut, et inclure des couches de sécurité supplémentaires afin de protéger le Contenu Client ;

II. Maintenir des contrôles organisationnels qui assurent de l'application des politiques et procédures internes de respect des normes, de gestion des incidents, de sécurité des applications, de sécurité du personnel et de programmes de formation réguliers ; et

III. Veiller à ce que des pratiques de confidentialité soient en place pour régir le traitement et la gestion des données conformément à la législation applicable, y compris le RGPD, les lois CCPA/CPRA, LGPD, ainsi que notre propre Addendum de traitement des données (ATD) et les politiques et engagements applicables de GoTo.

En intégrant des mesures de protection et de sécurité dans le produit, nous nous efforçons de protéger le Contenu Client GoTo contre les menaces et de veiller à ce que les contrôles de sécurité soient adaptés à la nature et à la portée des Services. Les fonctions de sécurité configurables de GoTo peuvent aider les administrateurs à minimiser les menaces et les risques pour les systèmes et les réseaux posés par les personnes qui utilisent les services GoTo.

# 3 Architecture du produit

Rescue est une solution d'assistance à distance de logiciel en tant que service (SaaS) composée de trois éléments principaux : une console d'assistance, une application mobile ou un applet de bureau pour l'utilisateur final, et un centre d'administration.

La console d'assistance est l'interface utilisée par les techniciens pour mener des sessions d'assistance à distance. Les techniciens peuvent lancer de nouvelles sessions ou répondre à des demandes d'utilisateurs finaux en ligne qui attendent dans une file d'attente partagée. Les techniciens communiquent avec les utilisateurs finaux et leur fournissent une assistance par le biais de l'application mobile (Android ou iOS) ou l'applet de bureau (Windows, macOS ou Linux) de Rescue. L'applet est téléchargé sur le PC distant de l'utilisateur final et conçu pour s'effacer à la fin de la session.

La console d'assistance Rescue interagit avec l'application ou l'applet Rescue par une connexion réseau de pair à pair (P2P) (voir la figure 1 à la section 3.1). Lorsque l'applet est lancé, le processus P2P est initié et se connecte à une passerelle Rescue où est négociée la session avec la console d'assistance.

Le protocole d'échange de clés propriétaire de GoTo est conçu pour assurer la sécurité contre l'interception ou l'écoute de l'infrastructure de GoTo. Plus précisément, la connexion entre l'utilisateur final et l'hôte est facilitée par la passerelle pour que l'utilisateur final puisse se connecter à l'hôte indépendamment de la configuration du réseau.

L'hôte établit une connexion TLS avec la passerelle, qui transmet l'échange de clés TLS de l'utilisateur final à l'hôte par une demande de renégociation de clé propriétaire. Ainsi, l'utilisateur final et l'hôte échangent des clés TLS sans que la passerelle n'en prenne connaissance.

## 3.1 Négociation des clés

Lorsqu'une session d'assistance démarre et qu'une connexion est établie entre l'utilisateur final assisté et le technicien, leurs ordinateurs négocier un algorithme de chiffrement parmi les options disponibles et une clé correspondante à utiliser pendant la durée de la session.

Les ordinateurs valident leur identité par des certificats. Étant donné que ni le technicien ni l'utilisateur final n'ont de logiciel capable d'établir la connexion et de valider les certificats de sécurité installés et un certificat SSL installé sur leurs ordinateurs, ils se tournent tous deux vers l'un des serveurs Rescue pour la phase initiale de négociation de clé. La vérification du certificat par la console d'assistance et par l'application ou l'applet de l'utilisateur final garantit que seul un serveur Rescue peut servir de médiateur.

## 3.2 Présentation du processus de transmission de la passerelle LogMeIn Rescue

Au lancement de l'application ou l'applet Rescue signé numériquement sur une machine, elle contient un identificateur global unique (GUID) d'authentification de session. Le GUID est intégré dans une application ou applet exécutable (par exemple, un fichier .exe) en tant que ressource du site au téléchargement. L'application ou l'applet télécharge ensuite une liste des passerelles disponibles sur secure.logmeinrescue.com ou secure.logmeinrescue.eu, choisit une passerelle dans la liste et s'y connecte en utilisant TLS. La passerelle est ensuite authentifiée par l'applet par son certificat SSL. La passerelle authentifie l'applet dans la base de données avec le GUID et enregistre que l'utilisateur final attend un technicien.

Lorsqu'un technicien ouvre une session dans la console d'assistance Rescue, une demande est envoyée à la passerelle avec le GUID d'authentification de la session pour transmettre les connexions entre la console d'assistance et l'application ou l'applet de l'utilisateur final. La passerelle est l'intermédiaire qui authentifie la connexion et commence à relayer les données sur la couche transport (elle ne déchiffre pas les données relayées).

Lorsqu'un relais de connexion est mis en place, les parties tentent d'établir une connexion P2P. La procédure est la suivante :

- L'applet se met à l'écoute d'une connexion TCP (Transmission Control Protocol) sur un port attribué par Windows, macOS ou Linux.
- Si la connexion TCP ne peut pas être établie dans les 10 secondes, une tentative est faite pour établir une connexion UDP (User Datagram Protocol) avec l'aide de la passerelle.
- Lorsqu'une connexion TCP ou UDP est établie, les parties authentifient le canal P2P (avec le GUID d'authentification des sessions) qui prend alors le contrôle du trafic
- Si une connexion UDP a été établie, le protocole TCP est émulé au-dessus des datagrammes UDP par XTCP, un protocole propriétaire de GoTo basé sur la pile TCP de Berkeley Software Distribution (« BSD »).
- Chaque connexion est sécurisée par le protocole TLS (utilisant le chiffrement AES256 avec SHA256 Media Access Controls [MAC]). Le GUID d'authentification de session est une valeur entière aléatoire cryptographique à 128 bits.

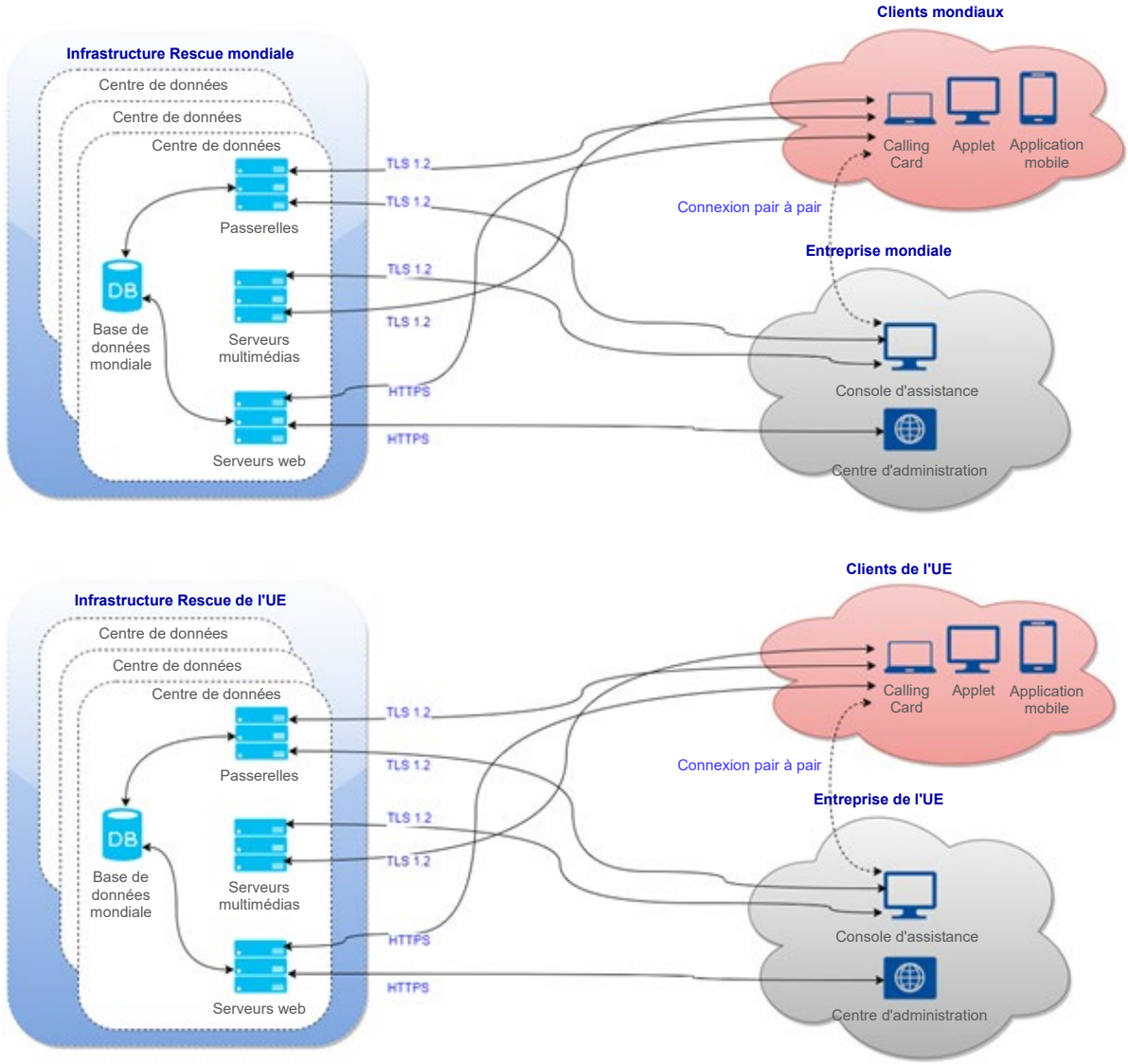


Figure 1 : Architecture de Rescue

## 3.3 Architecture multimédia de Rescue

Le service multimédia Rescue est un service autonome de communication web en temps réel (WebRTC) permettant la diffusion vidéo de Rescue Lens. Il gère les conférences pour les sessions Rescue qui utilisent la fonction Lens. Les participants à la conférence (pairs) rejoignent et quittent les conférences et les utilisateurs finaux envoient des flux vidéo et audio que les autres participants peuvent recevoir. Lens envoie le contenu vidéo dans un flux unidirectionnel de l'application Lens à la console d'assistance.

Le service multimédia se compose de trois éléments principaux : le kit de développement logiciel pour les médias (Media SDK), le gestionnaire de session et le serveur de diffusion en continu. Ces composants gèrent les processus de création/destruction et de connexion/déconnexion des conférences. Ces composants communiquent par les canaux de communication sécurisés existants entre la console d'assistance et le site web, et entre l'application Lens et le site web.

### 3.3.1 Media SDK

Le service multimédia s'appuie sur WebRTC, avec une fine enveloppe autour du code WebRTC. La console d'assistance et l'application mobile Lens utilisent Media SDK.

### 3.3.2 Gestionnaire de session

Le gestionnaire de session est un site web à charge équilibrée qui fournit une API REST (Representational State Transfer) pour gérer (créer/détruire/rejoindre) les conférences. Le gestionnaire de session n'accepte des requêtes que de la part du site web.

### 3.3.3 Serveur de diffusion en continu

Le service multimédia utilise une solution de serveur de streaming personnalisée pour gérer les flux entre les pairs (la console d'assistance et l'application Lens). La Console d'assistance et l'application Lens sont tous deux connectés au serveur de diffusion en continu. Une session Lens comporte deux flux (l'un est envoyé, l'autre est reçu) : l'application Lens diffuse son contenu vidéo vers le serveur, tandis que la console d'assistance diffuse le contenu vidéo provenant du serveur. Le serveur de streaming se comporte comme un serveur relais entre pairs.

# 4 Contrôles techniques de sécurité

GoTo utilise des contrôles techniques de sécurité conçus pour protéger l'infrastructure du Service et les données qui y résident.

## 4.1 Confidentialité des données

Le système en ligne sécurisé de Rescue s'appuie sur la technologie Secure Sockets Layer et Transport Layer Security (SSL/TLS) et répond aux objectifs suivants :

- Authentification des parties en communication
- Négociation de clés de chiffrement sans interception
- Échange confidentiel des messages
- Possibilité de détecter la modification éventuelle d'un message en transit

Rescue utilise OpenSSL (version 1.1.1n au moment de la publication de ce document).

## 4.2 Chiffrement

GoTo revoit régulièrement ses normes de chiffrement et peut mettre à jour les modes de chiffrement et/ou les technologies utilisés en fonction du risque évalué et de l'acceptation par le marché des nouvelles normes.

### 4.2.1 Chiffrement en transit

Tout le trafic réseau entrant et sortant des centres de données de Rescue, y compris tout le Contenu Client, est chiffré en transit avec TLS 1.2 et HTTPS. En outre, les sessions d'assistance Rescue sont protégées par un chiffrement AES 256 bits et un hachage MD5 pour une meilleure traçabilité des transferts de fichiers.

Puisque les trois composantes du système de communication Rescue sont contrôlés par GoTo, la suite de chiffrement utilisée par ces composants est invariable : AES256-SHA en mode de chaînage de blocs avec négociation de clé RSA. Ceci implique que :

- L'algorithme de chiffrement/déchiffrement est AES

- La clé de chiffrement a une longueur de 256 bits
- Les clés de chiffrement sont échangées sous forme de paires de clés RSA privée/publique, comme décrit à la section précédente
- La base du MAC est SHA-2. Un MAC est un court segment de données servant à l'authentification d'un message. La valeur MAC garantit l'intégrité du message ainsi que son authenticité en permettant aux parties en communication de détecter toute modification éventuelle du message.
- Le mode CBC (cipher-block chaining) permet d'assurer que chaque bloc de texte chiffré est dépendant des blocs de texte en clair jusqu'à ce point, et que des messages similaires ne peuvent pas être identifiés sur le réseau.

Les données circulant entre l'utilisateur final assisté et le technicien sont chiffrées de bout en bout et seules les parties concernées ont accès aux informations contenues dans le flux de messages.

### 4.2.2 Chiffrement des données statiques

Le Contenu Client de Rescue est chiffré en stockage à la fois au niveau du serveur et de la base de données par AES256 et TDE. Par exemple, le Contenu Client comprend les journaux de chat et les champs personnalisés, champs créés par le titulaire du compte principal ou l'administrateur principal.

## 4.3 Contrôles d'accès Rescue

Les administrateurs de Rescue peuvent personnaliser les contrôles d'accès. Par exemple, les administrateurs de Rescue peuvent configurer une politique exigeant une force de mot de passe minimale et un âge de mot de passe maximal, forcer les réinitialisations de mot de passe, appliquer une authentification à deux facteurs pour les connexions à Rescue, restreindre l'accès des techniciens à Rescue à des adresses IP préapprouvées pour des tâches spécifiques, ou accorder aux techniciens l'accès à des applications prédéfinies uniquement seulement avec un identifiant SSO unique pour se connecter à ces applications. Si nécessaire, les administrateurs peuvent désactiver l'identifiant SSO d'un technicien.

Les contrôles d'accès supplémentaires comprennent :

- Accès par autorisations granulaires (comme limiter certains techniciens à l'utilisation de l'affichage à distance sans contrôle à distance)
- Ne pas stocker les données des appareils distants sur les serveurs GoTo. Seuls les journaux de session, les adresses IP des utilisateurs finaux et les journaux de chat sont stockés – les journaux de texte de chat peuvent être supprimés des détails de la session
- Empêcher les techniciens de transférer des fichiers
- Exiger que l'utilisateur final soit présent sur l'appareil distant pour autoriser l'accès à distance
- Exiger que l'utilisateur final garde le contrôle et puisse mettre fin à la session à tout moment
- Empêcher les techniciens d'utiliser certaines fonctions tant que l'utilisateur final ne leur en a pas explicitement donné l'autorisation (par exemple, contrôle à distance, affichage du bureau, transfert de fichiers, informations sur le système, redémarrage et reconnexion)
- Révocation automatique des droits d'accès à la fin de la session
- La possibilité de forcer la déconnexion automatique après un temps d'inactivité prédéterminé
- Verrouillage d'un compte après cinq tentatives de connexion infructueuses

### 4.3.1 Contrôle d'accès basé par autorisations

Les administrateurs Rescue peuvent également accorder ou refuser des autorisations spécifiques dans le centre d'administration. Ces autorisations de groupe sont les notamment :

- Autorisation de synchronisation du Presse-papiers
- Autorisation de partage d'écran avec des Utilisateurs et des Utilisateurs finaux
- Déploiement de scripts
- Lancement de l'affichage du bureau
- Lancement du gestionnaire de fichiers
- Lancement du contrôle à distance
- Redémarrage
- Enregistrement des sessions
- Demande d'identifiants
- Envoi et réception de fichiers
- Envoi d'URL
- Démarrage de sessions privées
- Transfert de sessions
- Invite unique pour toutes les autorisations
- Consultation des informations système

Pour plus de détails sur les autorisations de groupe, veuillez consulter le Guide de l'administrateur Rescue. Les techniciens de Rescue Lens sont identifiés par leur adresse e-mail et authentifiés par un mot de passe.

### 4.3.2 Authentification

Les mesures d'authentification de Rescue sont conçues pour sécuriser le produit par des mesures qui n'autorisant que les techniciens ou les administrateurs à se connecter au système. Les administrateurs attribuent aux techniciens des identifiants de connexion (correspondant par exemple à leur adresse e-mail) et des mots de passe correspondants. Les techniciens saisissent ces identifiants dans le formulaire de connexion du site web de Rescue au moins au début de leur service. Les administrateurs peuvent configurer les contrôles pour une authentification plus fréquente (par exemple, après cinq minutes d'inactivité).

Le système Rescue est d'abord authentifié auprès du navigateur web du technicien par son certificat RSA SSL 2048 bits, ce qui garantit que le technicien saisira son nom d'utilisateur et son mot de passe sur le bon site web. Le technicien se connecte ensuite au système avec ses identifiants. Rescue ne stocke aucun mot de passe, mais utilise scrypt pour créer des hachages à partir des mots de passe, qui sont ensuite stockés dans la base de données de Rescue. Les hachages reçoivent ensuite graine aléatoire, chaîne de 24 caractères générée par CSPRNG pour chaque mot de passe unique.

Le système Rescue s'authentifie également auprès de l'utilisateur final. L'application ou l'applet, téléchargée et exécutée par l'utilisateur final, est signée avec le certificat de signature de code de GoTo (basé sur une clé RSA de 2048 bits) et cette information est généralement présentée à l'utilisateur final dans son navigateur web avant de lancer le logiciel. Rescue n'authentifie pas l'utilisateur final auprès du technicien.

Rescue permet également aux administrateurs de mettre en œuvre un système de connexion unique (SSO). Le langage SAML (Security Assertion Markup Language) utilisé est une norme XML (Extensible Markup Language) pour

l'échange de données d'authentification et d'autorisation entre domaines de sécurité (entre un fournisseur d'identité et un fournisseur de services).

Les administrateurs peuvent également exiger une vérification en deux étapes pour la connexion à Rescue. La fonction de vérification en deux étapes peut se faire par courrier électronique, SMS ou n'importe quel authentificateur TOTP (Time-based One-time Password) à usage unique comme deuxième couche de protection à un compte Rescue en demandant à certains membres de l'organisation de mettre en place un moyen supplémentaire de vérification de leur identité. La configuration de l'app Authenticator est déclenchée dans les cas suivants :

- Le membre sélectionné essaie de se connecter à son compte Rescue sur le site web sécurisé.
- Le membre sélectionné essaie de se connecter à la console d'assistance de bureau.
- Le membre sélectionné essaie de changer son mot de passe Rescue.

### 4.3.3 Autorisation

L'autorisation intervient au moins une fois au cours de chaque session d'assistance à distance. Après avoir téléchargé et exécuté l'applet, l'utilisateur final bénéficiant de l'assistance sera contacté par un technicien. Le technicien peut discuter avec l'utilisateur final par l'applet, mais toute autre action, telle que l'envoi d'un fichier ou l'affichage du bureau de l'utilisateur final, nécessite l'autorisation expresse de ce dernier. Une « invite unique » peut également être mise en œuvre pour les travaux d'assistance à distance de longue durée où l'utilisateur final peut ne pas être présent pendant toute la durée de la session. Si ce paramètre est activé pour un groupe de techniciens, les techniciens de ce groupe peuvent demander une autorisation « globale » à l'utilisateur final et, si cette autorisation est accordée, ils peuvent effectuer des actions telles que consulter des informations sur le système ou entrer dans une session de contrôle à distance sans autre autorisation de l'utilisateur final. Les administrateurs peuvent également imposer des restrictions d'adresses IP pour que les techniciens affectés à une tâche particulière ne puissent accéder à Rescue et effectuer cette tâche qu'à partir d'adresses IP préapprouvées. L'administrateur d'un groupe de techniciens peut également désactiver certaines fonctionnalités dans le Centre d'administration.

Les autorisations qu'un administrateur peut accorder ou refuser sont notamment :

- Lancer le contrôle à distance
- Redémarrer
- Lancer l'affichage du bureau
- Enregistrer les sessions
- Envoyer et recevoir des fichiers
- Démarrer des sessions privées
- Lancer le gestionnaire de fichiers
- Demander des identifiants
- Envoyer les URL
- Autoriser la synchronisation du Presse-papiers
- Afficher des informations système
- Déployer des scripts
- Utiliser des invites uniques pour toutes les autorisations
- Transférer des sessions
- Autoriser le partage d'écran avec des Utilisateurs et des Utilisateurs finaux

## 4.4 Contrôles d'audit

Les contrôles d'audit suivants sont à la disposition des Utilisateurs de Rescue et des Utilisateurs finaux :

- La possibilité de forcer l'enregistrement des sessions, avec la possibilité de stocker les fichiers d'audit sur un réseau partagé sécurisé
- Enregistrement des sessions de techniciens et de l'activité des sessions à distance sur l'ordinateur hôte pour garantir la sécurité et maintenir le contrôle de la qualité (connexions réussies, connexions infructueuses, contrôle à distance commencé, contrôle à distance terminé, redémarrage initié, déconnexion)
- Authentification de personnes ou d'entités
- Authentification du technicien par son adresse e-mail unique ou un identifiant SSO
- N'autoriser les techniciens à se connecter qu'à partir d'adresses IP approuvées
- Le rapport d'audit disponible dans le centre d'administration comprend les modifications apportées aux paramètres du compte et les données relatives à chaque action effectuée par les administrateurs sur l'élément sélectionné de l'arborescence de l'organisation au cours d'une période donnée

# 5 Mises à jour du programme de sécurité

GoTo examine et met à jour son programme de sécurité et engage des tiers indépendants pour évaluer ses contrôles de sécurité pertinents au moins une fois par an afin de s'assurer qu'il suit l'évolution du paysage actuel des menaces et de garantir la conformité avec les cadres pertinents, les normes de l'industrie, les engagements du Client et, le cas échéant, les évolutions dans les lois et les règlements de sécurité des données de GoTo.

# 6 Sauvegarde des données, reprise après sinistre et disponibilité

L'architecture de GoTo est conçue pour effectuer une réplication en temps quasi réel vers des sites géographiquement diversifiés. Les bases de données sont sauvegardées par une stratégie incrémentielle. En cas de catastrophe ou de défaillance totale d'un des sites actifs, les autres sites sont conçus pour équilibrer la charge des applications. La reprise après sinistre de ces systèmes est testée périodiquement.

La base de données Rescue est synchronisée toutes les cinq minutes avec un autre centre de données. En outre, une sauvegarde différentielle est effectuée chaque nuit et des sauvegardes complètes sont réalisées chaque week-end. La base de données de sauvegarde est stockée avec le même chiffrement que l'original. Les sauvegardes sont conservées sur place pendant un mois, puis transférées vers un service dans le cloud, ne sont plus traitées activement et sont conservées conformément à nos politiques internes de conservation des documents. En cas de défaillance complète du centre de données hébergeant la base de données primaire, l'architecture Rescue est conçue pour être rapidement restaurée.

# 7 Centres de données

L'infrastructure GoTo est conçue pour accroître la fiabilité du service et réduire le risque d'indisponibilité due à un seul point de défaillance :

a) centres de données redondants, actifs-passifs ; ou
b) centres de données des fournisseurs d'hébergement en cloud.

À la création de leur compte, les Clients de Rescue peuvent choisir d'utiliser l'infrastructure de données de GoTo de l'Union européenne ou Mondiale pour stocker leur Contenu Client. Les lieux d'hébergement/stockage sont précisés ci-dessous :[2]

- **Union européenne :** Allemagne et Irlande
- **Au niveau mondial :** États-Unis, Allemagne, Australie et Royaume-Uni

Tous les centres de données font l'objet d'une surveillance des conditions environnementales et sont dotés de mesures de sécurité physique permanentes (voir ci-dessous).

## 7.1 Sécurité physique des centres de données

GoTo passe des contrats avec des centres de données pour assurer la sécurité physique et des contrôles environnementaux pour les systèmes et les serveurs qui hébergent le Contenu Client. Ces contrôles sont notamment les suivants :

- Vidéosurveillance et enregistrement
- Contrôle de la température du chauffage, de la ventilation et de la climatisation
- Moyens d'extinction et détecteurs de fumée
- Alimentation sans coupure
- Faux planchers ou gestion complète des câbles
- Surveillance continue et alertes
- Protections contre les catastrophes naturelles et anthropiques courantes, en fonction de la géographie et de l'emplacement du centre de données concerné
- Maintenance programmée et validation de tous les contrôles critiques en matière de sécurité et d'environnement

GoTo limite l'accès physique aux centres de données de production aux seules personnes autorisées. L'accès à une salle de serveur sur site ou à une installation d'hébergement tierce nécessite une demande par le système de gestion de tickets approprié et l'approbation du responsable concerné, ainsi que l'examen et l'approbation de l'équipe d'exploitation technique de GoTo. Tous les accès physiques aux centres de données et aux salles de serveurs sont consignés et la direction de GoTo examine les registres au moins une fois par trimestre. En outre, l'autorisation d'accès physique au centre de données est retirée rapidement en cas de changement de rôle (lorsque cet accès n'est plus nécessaire) ou en cas de licenciement du personnel précédemment autorisé. Le contrôle d'accès à plusieurs facteurs (par exemple, biométrie, badge et clavier) est exigé pour les zones très sensibles, dont les centres de données.

# 8 Respect des normes

GoTo évalue régulièrement sa conformité avec les exigences légales, sécuritaires, financières, de confidentialité des données et réglementaires applicables. Les programmes de protection de la vie privée et de sécurité de GoTo répondent à des normes rigoureuses et internationalement reconnues, ont été évalués conformément à des normes d'audit externe exhaustives et ont obtenu des certifications clés, notamment :

- **Certification TRUSTe Enterprise Privacy & Data Governance Practices** pour des contrôles opérationnels de confidentialité et de protection des données conformes aux principales lois et cadres reconnus sur la protection de la vie privée. Pour en savoir plus, consultez notre article de blog.
- Les **certifications TRUSTe APEC CBPR/PRP** pour le transfert de Contenu Client entre les pays membres de l'APEC ont été obtenues et validées de manière indépendante par l'intermédiaire de TrustArc, une tierce partie approuvée par l'APEC leader en matière de

[2] Les lieux d'hébergement peuvent varier (par exemple en fonction du choix de la résidence des données), consultez la déclaration de sous-traitance de Rescue applicable dans la section Ressources produits du GoTo Trust and Privacy Center (https://www.goto.com/company/trust/resource-center).

conformité à la protection des données. Pour en savoir plus sur nos certifications APEC, cliquez ici.

- Organisation internationale de normalisation – Certification **ISO/CEI 27001:2013** Systèmes de gestion de sécurité de l'information
- Rapport d'attestation de l'American Institute of Certified Public Accountants (AICPA) **Service Organization Control (SOC) 2 Type II**
- Conformité à la **norme de sécurité de l'industrie des cartes de paiement (PCI DSS)** pour les environnements de commerce électronique et de paiement de GoTo
- Évaluation des contrôles internes telle qu'exigée dans le cadre d'un audit des rapports financiers annuels du **Public Company Accounting Oversight Board (PCAOB)**

# 9 Sécurité des applications

Le programme de sécurité des applications de GoTo suit le cycle de développement de la sécurité (SDL) de Microsoft pour sécuriser le code du produit. Le programme SDL de Microsoft comprend des révisions manuelles du code, la modélisation des menaces, l'analyse statique du code, l'analyse dynamique et le durcissement du système. Les équipes de GoTo effectuent aussi périodiquement des tests de vulnérabilité des applications dynamiques et statiques et des activités de test d'intrusion pour les environnements ciblés.

# 10 Journalisation, surveillance et alerte

GoTo maintient des politiques et des procédures en matière de journalisation, de surveillance et d'alerte, qui définissent les principes et les contrôles mis en œuvre pour renforcer notre capacité à détecter les activités suspectes et à y répondre en temps opportun. GoTo enregistre le trafic anormal ou suspect identifié dans les journaux de sécurité pertinents des systèmes de production concernés.

Les journaux de chat de Rescue sont enregistrés dans la base de données de Rescue. Le journal de chat est transmis aux serveurs de Rescue en temps réel par la console d'assistance. Il contient les événements et les messages associés à une session d'assistance donnée. Les fichiers journaux affichent les actions suivantes des techniciens : heure de début et de fin d'une session de contrôle à distance, instances de techniciens partageant des fichiers avec des utilisateurs finaux et métadonnées relatives au partage de fichiers (par exemple, le nom et l'empreinte de hachage MD5 d'un fichier transmis). La base de données du journal de chat peut être interrogée depuis le Centre d'administration.

Pour les comptes actifs, le contenu des journaux sera disponible en ligne pendant deux ans après la fin d'une session d'assistance à distance et archivé pendant les deux années suivantes.

Pour faciliter l'intégration avec les systèmes de gestion de la relation client (GRC), Rescue peut publier les détails de la session sur une URL et les administrateurs peuvent choisir d'exclure le texte du chat de ces détails. Le texte du chat est inclus par défaut, mais les Clients peuvent modifier ce paramètre dans le centre d'administration. De plus, tous les enregistrements de textes de chat entre les techniciens et les utilisateurs finaux peuvent être automatiquement omis des détails de la session stockés dans un centre de données de Rescue. Rescue permet aux techniciens d'enregistrer dans un fichier vidéo les événements qui se produisent au cours d'une session d'affichage du bureau ou de contrôle à distance. Les enregistrements sont stockés dans un répertoire spécifié par le technicien.

# 11 Détection et intervention sur les terminaux

Un logiciel de détection et d'intervention sur les terminaux avec enregistrement d'audit est déployé sur tous les serveurs GoTo afin de minimiser les interruptions ou les conséquences sur les performances du service. En cas de détection d'une activité suspecte, des enquêtes de sécurité seront lancées conformément à nos procédures de réponse aux incidents, si cela s'avère approprié et nécessaire. Voir la section 17 pour plus d'informations sur le Centre des opérations de sécurité de GoTo et les procédures de réponse aux incidents.

# 12 Gestion des menaces

L'équipe de réponse aux incidents de cybersécurité (« CSIRT ») de GoTo regroupe plusieurs équipes et est responsable de la protection contre les cybermenaces. Plus précisément, l'équipe chargée du renseignement sur les cybermenaces au sein du CSIRT recueille, vérifie et diffuse des informations sur les menaces actuelles et émergentes. GoTo se tient au courant des renseignements sur les menaces et de leur atténuation en examinant des sources ouvertes et fermées comme en participant à des groupes de partage et à des affiliations industrielles (IT-ISAC, FIRST.org, etc.).

# 13 Analyse de la sécurité et des vulnérabilités et gestion des correctifs

GoTo maintient un programme formel de gestion des correctifs et, au moins chaque trimestre, effectue des activités de gestion des correctifs sur tous les systèmes, appareils, micrologiciels, systèmes d'exploitation, applications et autres logiciels pertinents qui traitent le Contenu Client. GoTo évalue et analyse les vulnérabilités des systèmes, des hôtes/réseaux internes et externes (« Systèmes »), au moins une fois par mois, ainsi qu'après tout changement matériel de ces Systèmes et remédie aux vulnérabilités découvertes conformément aux politiques documentées qui priorisent la remédiation en fonction du risque.

# 14 Contrôle d'accès logique GoTo

Des procédures de contrôle d'accès logique sont en place pour réduire le risque d'accès non autorisé aux applications et de perte de données dans les environnements d'entreprise et de production. Les salariés de GoTo se voient accorder l'accès aux systèmes, applications, réseaux et appareils spécifiés de GoTo sur la base du principe du moindre privilège. Les privilèges des utilisateurs sont séparés en fonction du rôle fonctionnel (contrôle d'accès par rôle) et de l'environnement par des contrôles, processus et/ou procédures de séparation des tâches.

# 15 Séparation des données

GoTo s'appuie sur une architecture multi-entité, logiquement séparée au niveau de la base de données, en fonction du compte GoTo de l'utilisateur ou de l'organisation. Les parties doivent être authentifiées pour accéder à un compte. GoTo a également mis en place des contrôles pour empêcher les Utilisateurs ou les Utilisateurs finaux de voir les données d'autres Utilisateurs ou Utilisateurs finaux.

# 16 Défense périmétrique et détection d'intrusion

GoTo utilise des outils, des techniques et des services de protection du périmètre pour se protéger contre le trafic réseau non autorisé entrant dans l'infrastructure du produit GoTo. Il s'agit notamment, mais pas exclusivement, des éléments suivants :

- Des systèmes de détection d'intrusion qui surveillent les systèmes, les services, les réseaux et les applications pour détecter les accès non autorisés
- Surveillance des systèmes critiques et des fichiers de configuration pour empêcher ou réduire la probabilité de modifications non autorisées
- Pare-feu d'application web (WAF) et service de prévention DDoS sur la couche application traversé par le trafic GoTo pour bloquer le trafic des serveurs malveillants
- Un pare-feu applicatif local offre une couche supplémentaire de protection contre les vulnérabilités et le trafic malveillant des applications web (OWASP top 10 et autres)
- Des pare-feu basés sur l'hôte sur les serveurs web GoTo filtrent les connexions entrantes et sortantes, y compris les connexions internes entre les systèmes GoTo.

# 17 Opérations de sécurité et gestion des incidents

Le centre d'opérations de sécurité (SOC) de GoTo est chargé de détecter les événements de sécurité et d'y répondre. Le SOC utilise des capteurs de sécurité et des systèmes d'analyse pour identifier les problèmes potentiels et a développé des procédures de réponse aux incidents, y compris un plan documenté de réponse aux incidents.

Le plan de réponse aux incidents de GoTo respecte les processus de communication critiques, les politiques et les procédures opérationnelles standard de GoTo. Il est conçu pour gérer, identifier et résoudre les événements de sécurité pertinents suspectés ou identifiés dans ses systèmes et services, y compris Rescue. Le plan de réponse aux incidents définit les mécanismes permettant aux salariés de signaler les incidents de sécurité présumés et les voies hiérarchiques à suivre le cas échéant. Les événements suspects sont documentés et transmis, le cas échéant, par des tickets d'événement normalisés et triés par criticité.

# 18 Suppression et restitution du Contenu

**Suppression et/ou restitution :** les Clients peuvent demander la restitution et/ou la suppression de leur Contenu Client en soumettant une demande par le Portail de Gestion des Droits Individuels de GoTo (« IRM »), à l'adresse support.logmeinrescue.com ou en envoyant un courriel à privacy@goto.com. Les demandes seront traitées dans les trente (30) jours suivant leur réception par GoTo. Toutefois, dans le cas improbable où plus de temps serait nécessaire, nous vous informerons dès que possible de tout retard anticipé et de la nouvelle date limite de traitement.

**Calendrier de conservation du Contenu Client :** Sauf disposition contraire de la loi applicable, le Contenu Client est automatiquement supprimé dans les cent quarante (140) jours après la résiliation, l'annulation ou l'expiration et, dans chaque cas, le déprovisionnement du dernier abonnement du Client.

Sur demande écrite, GoTo peut fournir une confirmation/certification écrite de la suppression du Contenu.

# 19 Contrôles organisationnels

## 19.1 Politiques et procédures de sécurité

GoTo maintient un ensemble complet de politiques et de procédures de sécurité périodiquement révisées et mises à jour si nécessaire pour suivre les objectifs de

sécurité de GoTo, les changements dans la loi applicable, les normes de l'industrie et les efforts de conformité.

### 19.2 Gestion du changement

GoTo maintient un processus de gestion du changement approprié et les changements apportés aux systèmes GoTo sont évalués, testés et approuvés avant d'être mis en œuvre afin de réduire le risque de perturbation des services GoTo.

### 19.3 Programmes de sensibilisation et de formation à la sécurité

Le programme de sensibilisation à la protection de la vie privée et à la sécurité de GoTo implique de former les salariés à l'importance de traiter les données personnelles et les informations confidentielles de manière éthique, responsable, dans le respect de la loi applicable et avec le soin nécessaire. Les salariés, sous-traitants et stagiaires nouvellement embauchés sont informés des politiques de sécurité et du Code de conduite et de déontologie commerciale de GoTo lors de leur intégration. Les salariés de GoTo suivent une formation de sensibilisation à la protection de la vie privée et à la sécurité au moins une fois par an. Les activités de sensibilisation se déroulent tout au long de l'année et peuvent inclure des campagnes pour la Journée de la protection des données, le Mois de la sensibilisation à la cybersécurité, des webinaires avec le Directeur de la sécurité informatique et un programme de champions de la sécurité.

Le cas échéant, les salariés peuvent également être tenus de suivre des formations spécifiques à leur rôle. En outre, tous les salariés, sous-traitants et filiales de GoTo doivent prendre connaissance des politiques de GoTo relatives à la sécurité et à la protection des données et y adhérer.

## 20 Pratiques en matière de protection de la vie privée

GoTo prend très au sérieux la protection de la vie privée de ses Clients, Utilisateurs et Utilisateurs finaux et s'engage à divulguer les pratiques de traitement et de gestion des données de manière ouverte et transparente.

### 20.1 Politique de protection de la vie privée

GoTo maintient un programme complet de protection de la vie privée qui implique la coordination de plusieurs fonctions au sein de l'entreprise, notamment la protection de la vie privée, la sécurité, la gouvernance, le risque et la conformité (GRC), le service juridique, le produit, l'ingénierie et le marketing. Ce programme de protection de la vie privée est centré sur les efforts de conformité et implique la mise en œuvre et le maintien de politiques internes et externes, de normes et d'addenda pour régir les pratiques de l'entreprise.

### 20.2 Conformité réglementaire :

#### 20.2.1 RGPD

Le Règlement Général sur la Protection des Données (RGPD) est une loi de l'Union européenne (UE) relative à la protection des données et de la vie privée des personnes au sein de l'UE. GoTo maintient un programme complet de conformité au RGPD et dans la mesure où GoTo s'engage dans le traitement des Données personnelles soumises au RGPD au nom du Client, nous le ferons en conformité avec les exigences applicables du RGPD. Pour en savoir plus, visitez https://www.goto.com/company/trust/privacy.

### 20.2.2 CCPA

La loi californienne sur la protection des consommateurs (California Consumer Privacy Act), telle que modifiée par la loi californienne sur les droits à la vie privée (California Privacy Rights Act) (collectivement appelée « CCPA »), accorde aux Californiens des droits et des protections supplémentaires concernant la manière dont les entreprises peuvent utiliser leurs données personnelles. GoTo maintient un programme de conformité complet et, dans la mesure où GoTo s'engage dans le traitement des Données personnelles soumises à la CCPA au nom du Client, nous le ferons en conformité avec les exigences applicables de la CCPA. Pour plus d'informations sur notre conformité à la CCPA, consultez la Politique de protection de la vie privée de GoTo et les Déclarations supplémentaires de la loi californienne sur la protection de la vie privée des consommateurs (California Consumer Privacy Act).

### 20.2.3 LGPD

La loi brésilienne sur la protection des données (LGPD) régit le traitement des données personnelles au Brésil et/ou des personnes situées au Brésil au moment de leur recueil. GoTo maintient un programme de conformité complet et, dans la mesure où GoTo s'engage dans le traitement des Données personnelles soumises à la LGPD au nom du Client, nous le ferons en conformité avec les exigences applicables de la LGPD. Pour en savoir plus, visitez https://www.goto.com/company/trust/privacy.

## 20.3 Addendum de Traitement des Données

GoTo propose un addendum global de traitement des données (DPA) mondial, disponible en anglais et en allemand. Ce DPA répond aux exigences des règlements RGPD, CCPA, LGPD et autres applicables et régit le traitement du Contenu Client par GoTo.

Plus précisément, notre DPA intègre plusieurs protections de la confidentialité des données axées sur le RGPD, notamment :

(a) les détails du traitement des données et les informations sur les sous-traitants, conformément à l'article 28 ;
(b) révisé (2021) Clauses contractuelles types (aussi appelé clauses types de l'UE) ; et
(c) les mesures techniques et organisationnelles spécifiques aux produits de GoTo.

En outre, pour tenir compte des exigences de la CCPA, notre DPA mondial comprend :

a) des définitions révisées en fonction de l'ACCP ;
b) les droits d'accès et de suppression ; et
c) garantit que GoTo ne vendra pas les Données personnelles de nos Clients, Utilisateurs et Utilisateurs finaux.

Notre DPA mondial comprend également des dispositions pour :

(a) traiter de la conformité de GoTo avec la LGPD ;
(b) permettre les transferts licites de Données personnelles vers/depuis le Brésil ; et
(c) veiller à ce que nos Utilisateurs bénéficient des mêmes avantages en matière de protection de la vie privée que nos autres Utilisateurs dans le monde

## 20.4 Cadres de transfert

GoTo permet les transferts internationaux licites de données dans les cadres suivants :

### 20.4.1 Clauses contractuelles types

Les clauses contractuelles types (CCT), parfois appelées clauses types de l'UE, sont des clauses contractuelles normalisées, reconnues et adoptées par la Commission Européenne, qui garantissent que toute Donnée personnelle quittant l'Espace économique européen (EEE) sera transférée conformément à la législation de l'UE en matière de protection des données. Les CCT, révisées et publiées en 2021, sont intégrées dans le DPA mondial de GoTo afin de permettre aux clients de GoTo de transférer des données hors de l'EEE en conformité avec le RGPD.

### 20.4.2 Certifications APEC CBPR et PRP

GoTo a obtenu les certifications Cross-Border Privacy Rules (CBPR) et Privacy Recognition for Processors (PRP) de l'Organisation de coopération économique Asie-Pacifique (APEC). Les cadres CBPR et PRP de l'APEC sont les premiers cadres de réglementation des données approuvés pour le transfert de Données personnelles entre les pays membres de l'APEC. Ils ont été obtenus et validés de manière indépendante par TrustArc, un prestataire tiers de conformité de protection des données approuvé par l'APEC.

## 20.5 Mesures supplémentaires

En plus des mesures spécifiées dans ces TOM, GoTo a créé une FAQ conçue pour détailler les mesures supplémentaires mises en œuvre pour permettre les transferts licites en vertu du Chapitre 5 du RGPD et pour aborder et guider toute analyse au cas par cas recommandée par la Cour européenne de justice pour l'utilisation des CCT.

## 20.6 Demandes de données

GoTo maintient des processus complets pour faciliter la réception des demandes liées à la protection des données et à la sécurité, notamment le portail IRM, l'adresse e-mail de confidentialité (privacy@goto.com) et l'assistance à la clientèle à l'adresse https://support.goto.com.

## 20.7 Déclarations relatives aux sous-traitants et aux centres de données

GoTo publie les déclarations relatives aux sous-traitants sur son site Trust & Privacy Center(https://www.goto.com/company/trust/resource-center). Ces déclarations indiquent les noms, les lieux et les objectifs de traitement des fournisseurs d'hébergement de données et d'autres tiers qui traitent le Contenu Client dans le cadre de la fourniture du Service aux clients de GoTo.

## 20.8 Données sensibles Restrictions de traitement

Sauf demande expresse de GoTo ou si le Client a reçu une autorisation écrite de GoTo, les types de données sensibles suivants ne doivent pas être envoyées à Rescue ni fournis à GoTo :

- Numéros d'identification délivrés par le gouvernement et images des documents d'identification.
- Informations relatives à la santé d'une personne, y compris, mais sans s'y limiter, les Données de santé protégées (PHI) telles qu'elles sont définies aux États-Unis

par la loi  Health Insurance Portability and Accountability Act (HIPAA), ainsi que d'autres lois et règlements applicables.

- Les informations relatives aux comptes financiers et aux instruments de paiement, y compris, mais sans s'y limiter, les données relatives aux cartes de crédit. La seule exception générale à cette disposition s'étend aux formulaires et pages de paiement explicitement identifiés utilisés par GoTo pour collecter le paiement du Service.
- Toute information particulièrement protégée par les lois et règlements applicables, notamment les informations relatives à la race, à l'origine ethnique, aux croyances religieuses ou politiques, à l'appartenance à une organisation, etc.

### 20.9 Conformité dans les environnements réglementés

Les Clients sont responsables de la mise en œuvre de politiques, de procédures et d'autres mesures de protection appropriées liées à leur utilisation de Rescue pour l'assistance sur des appareils dans des environnements réglementés.

## 21 Contrôles par des tiers de sécurité et protection de la vie privée

Avant d'engager des fournisseurs tiers qui traitent le Contenu Client ou des données confidentielles, sensibles ou relatives aux salariés, GoTo examine et analyse les pratiques du fournisseur en matière de sécurité et de protection de la vie privée par les canaux d'approvisionnement appropriés. Le cas échéant, GoTo peut obtenir et évaluer périodiquement la documentation ou les rapports de conformité des fournisseurs afin de s'assurer que leur environnement et leurs normes de contrôle restent suffisants.

GoTo conclut des accords écrits avec tous les fournisseurs tiers et utilise des modèles d'approvisionnement approuvés par GoTo ou négocie les conditions générales de ces tiers afin de respecter les normes de confidentialité et de sécurité acceptées par GoTo, lorsque cela est jugé nécessaire. Les équipes chargées des finances, des affaires juridiques, de la protection de la vie privée et de la sécurité participent au processus d'examen des fournisseurs et vérifient que ces derniers respectent les exigences spécifiques et contractuelles de traitement des données obligatoires, le cas échéant. Les politiques de GoTo en matière de risques liés aux tiers régissent les exigences en matière de confidentialité et de sécurité des fournisseurs selon le type et la durée du traitement des données et du niveau d'accès. Le cas échéant (par exemple, lorsque le Contenu Client est traité ou stocké), les accords avec les fournisseurs comprennent des exigences de « conformité à la loi applicable », un DPA ou un document similaire qui aborde des sujets tels que le RGPD, le CCPA, le LGPD et les restrictions d'utilisation et de vente, le cas échéant. De même, des addenda de sécurité prévoyant des contrôles appropriés et des exigences en matière de systèmes sont mis en place avec les fournisseurs concernés. Le DPA des fournisseurs de GoTo comporte des restrictions concernant la « vente » de données telle que définie par la CCPA.

## 22 Contacter GoTo

Les Clients peuvent contacter GoTo à l'adresse https://support.goto.com pour toute question d'ordre général. Pour toute question ou demande relative aux Données personnelles ou à la protection de la vie privée, veuillez consulter notre portail IRM ou envoyer un courriel à privacy@goto.com.