Mesures techniques et d'organisation
GoTo Meeting, GoTo Webinar, GoTo Training et GoTo Stage

Synthèse

Ce document de mesures techniques et organisationnelles (« TOM ») définit les engagements de GoTo en matière de confidentialité, de sécurité et de responsabilité pour GoTo Meeting, GoTo Webinar, GoTo Training et GoTo Stage. GoTo applique 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 des menaces et des 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) assurer la conformité aux lois et règlements applicables, y compris les lois en matière de protection des données et de la vie privée. Ces mesures comprennent notamment :

- **Chiffrement :**
  - *En transit* Transport Layer Security (TLS) ou Datagram Transport Layer Security (DTLS)
  - *Statique* Transparent Data Encryption (TDE) et Advanced Encryption Standard (AES) 256 bits pour le Contenu Client qui est chiffré au repos.
- **Centres de données :** GoTo fait appel à des fournisseurs d'hébergement dans le cloud qui prennent des mesures pour assurer une sécurité logique et physique, une disponibilité et une évolutivité élevées.
- **Audits de conformité :** GoTo Meeting, GoTo Webinar et GoTo Training ont obtenu les certifications SOC 2 Type II, C5, 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 du niveau de stockage.
- **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.
- **Rétention des données :**
  - Les Clients de GoTo Meeting, GoTo Webinar, GoTo Training et GoTo Stage 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.
  - Pour GoTo Meeting, GoTo Webinar et GoTo Training, le Contenu Client sera automatiquement supprimé entre quatre-vingt-dix et cent (90-100) jours après l'expiration de la dernière période d'abonnement payant du client.

Version 4.0 | avril 2024

Table des matières

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

Synthèse 1

Table des matières 2

1 *Présentation du produit* 3

2 *Mesures techniques* 5

3 *Architecture du produit* 5

4 *Contrôles techniques de sécurité* 7

5 *Mises à jour du programme de sécurité* 11

6 *Sauvegarde des données, reprise après sinistre et disponibilité* 11

7 *Centres de données* 11

8 *Respect des normes* 12

9 *Sécurité des applications* 12

10 *Journalisation, surveillance et alerte* 13

11 *Détection et intervention sur les terminaux* 13

12 *Gestion des menaces* 13

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

14 *Contrôle d'accès logique* 13

15 *Séparation des données* 14

16 *Défense périmétrique et détection d'intrusion* 14

17 *Opérations de sécurité et gestion des incidents* 14

18 *Suppression et restitution du Contenu* 14

19 *Contrôles organisationnels* 15

20 *Pratiques en matière de protection de la vie privée* 16

21 *Contrôles par des tiers de sécurité et protection de la vie privée* 19

22 *Contacter GoTo* 19

1 Présentation du produit

GoTo Meeting, GoTo Webinar, GoTo Training et GoTo Stage (désignés ensemble par le « Service ») sont des solutions de communication en ligne qui permettent aux individus et aux organisations d'interagir en utilisant diverses fonctionnalités, selon l'offre de service, notamment le partage d'écran d'ordinateur, la vidéoconférence, le chat et l'audio intégré. GoTo Meeting, GoTo Webinar, GoTo Training et GoTo Stage partagent une infrastructure et sont diffusés via un RDC sur des navigateurs web ou des applications installables.

- GoTo Meeting, GoTo Webinar et GoTo Training permettent aux organisateurs de planifier, de convoquer à et de modérer des sessions en ligne avec audio, webcam, partage d'écran et plus encore à l'aide des applications GoTo web, de bureau et mobiles.
- GoTo Training offre des fonctionnalités spécifiques destinées à la formation en ligne, telles que l'accès en ligne aux tests et aux documents de cours, ainsi qu'un catalogue de cours hébergé.
- GoTo Webinar fournit un support spécialement destiné à l'organisation d'événements de présentation d'informations d'un à plusieurs participants, qui peuvent être locaux ou mondiaux, par Internet.
- GoTo Stage est une extension de GoTo Webinar grâce à laquelle les organisateurs de GoTo Webinar peuvent créer des canaux personnalisables et publier les enregistrements de leurs webinaires. Les enregistrements publiés sont présentés sur la page d'accueil de GoTo Stage, triés par secteurs d'activité. À tout moment, les organisateurs peuvent dépublier leur enregistrement via GoTo Webinar, ce qui supprime la vidéo de leur page de canal et de l'écosystème GoTo Stage.

1.1 Gestion des conférences et inscription

Les organisateurs peuvent programmer des sessions directement dans le Service. Ils peuvent ajuster les différents paramètres des sessions à venir et préparer leur contenu et leurs participants.

1.2 Audio

L'audioconférence intégrée pour les sessions GoTo Meeting, GoTo Webinar et GoTo Training est disponible via le protocole de voix sur IP (VoIP) et le réseau téléphonique commuté (RTC).

1.3 Vidéo

Tous les produits offrent une vidéo par webcam de haute qualité qui s'adapte à la bande passante et à la latence de l'utilisateur.

1.4 Envoi de contenu (Webinar et Training uniquement)

Les organisateurs peuvent envoyer des fichiers et des médias à utiliser pendant les sessions, soit avant la session, soit une fois que la session a commencé.

1.5 Rapports de sessions

Les organisateurs peuvent consulter les statistiques de participation et d'autres statistiques de session dans l'historique de leur session.

1.6 Enregistrement et transcriptions

Les sessions peuvent être enregistrées localement et dans le cloud. Les administrateurs de comptes et les organisateurs de sessions peuvent choisir d'activer les enregistrements dans le cloud en plus ou à la place des enregistrements locaux. Les enregistrements locaux sont stockés sur le système de l'organisateur et ne sont pas soumis aux limites de conservation de GoTo, définies dans la section 18 (Suppression et restitution du Contenu) ci-dessous.

Les enregistrements dans le nuage sont disponibles directement dans l'historique des sessions de l'organisateur et des transcriptions sont automatiquement créées lorsque cette fonctionnalité est activée par l'administrateur. Les transcriptions des enregistrements des sessions sont créées à l'aide de la technologie GoTo Voice AI ou Google Cloud Speech-to-Text.

Avec **GoTo Meeting**, un administrateur de compte peut choisir d'activer les enregistrements et décider si ceux-ci sont stockés localement ou dans le cloud. Si les enregistrements dans le cloud sont activés, l'organisateur de la réunion peut choisir d'enregistrer une réunion donnée et de la stocker dans le cloud. Des transcriptions sont automatiquement créées pour les enregistrements dans le cloud.

Avec **GoTo Webinar**, les organisateurs peuvent choisir de transcrire automatiquement tous les enregistrements dans le cloud. Seul un organisateur peut lancer un enregistrement et si son paramètre de transcription automatique est activé, une transcription sera créée.

Avec **GoTo Training**, les administrateurs de compte peuvent contrôler si les organisateurs peuvent sauvegarder les enregistrements dans le cloud. Les administrateurs de compte ne peuvent pas empêcher les organisateurs d'enregistrer des sessions localement. Les formations ne peuvent pas être transcrites.

1.7 Messagerie d'entreprise (Meeting uniquement)

La messagerie d'entreprise est une extension de GoTo Meeting qui permet aux utilisateurs de GoTo Meeting de voir l'état de présence des autres utilisateurs de leur compte et d'échanger des messages instantanés ou partager des fichiers avec eux. L'administrateur de compte définit les possibilités de visibilité et de découverte des différents utilisateurs.

Les utilisateurs de la messagerie d'entreprise peuvent voir l'état de présence de tout autre utilisateur de leur compte dès lors qu'il figure dans leur liste de contacts. Il est possible d'échanger des messages avec tous les membres d'une équipe et avec des utilisateurs externes s'ils ont été explicitement invités par courrier électronique. Les utilisateurs externes sont des utilisateurs de la messagerie d'entreprise ne faisant pas partie de l'équipe interne du Client (par exemple, un client, un prospect ou un partenaire). Les messages peuvent être directs (entre deux participants), dans un groupe privé ou dans un groupe public.

Les utilisateurs peuvent également partager d'autres contenus dans le cadre de la messagerie d'entreprise en envoyant et en téléchargeant des fichiers. Tous les utilisateurs ayant accès aux messages d'une conversation ou d'un groupe donné peuvent télécharger les fichiers partagés.

1.8 Webcast (Webinar uniquement)

Les webcasts GoTo Webinar utilisent des passerelles de diffusion, des moteurs de streaming tiers et des réseaux de diffusion de contenu conçus pour fournir de manière fiable des médias de partage d'écran, audio et vidéo aux participants qui se connectent à partir d'un navigateur web. Les passerelles reçoivent les données multimédias des serveurs multimédias et les transcodent dans des codecs standard. Le moteur de diffusion en continu produit des flux HTTP Live Streaming (HLS) à plusieurs débits binaires afin d'offrir une diffusion adaptative aux utilisateurs dont les connexions réseau ne sont pas optimales.

1.9 GoTo Stage (Webinar uniquement)

Les vidéos publiées sur GoTo Stage peuvent être découvertes sur la page d'accueil de GoTo Stage et dans les résultats des moteurs de recherche, à moins que l'organisateur ne restreigne cette possibilité au moyen des paramètres d'administration de la page de son canal. Toute personne inscrite à GoTo Stage peut accéder aux enregistrements non proposés à la découverte par le biais d'une URL directe vers le canal ou vers la page unique « Regarder maintenant » de la vidéo. Les visiteurs s'inscrivent à GoTo Stage en utilisant leur nom et leur adresse électronique ou peuvent se connecter via certains comptes de réseaux sociaux tels que LinkedIn, Facebook et Gmail. Afin de limiter les partages non désirés, les URL permettant aux visiteurs d'accéder aux vidéos sont en ligne pour une durée limitée.

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 cette conception et l'applique dans la pratique pour GoTo Meeting, GoTo Webinar et GoTo Training.

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

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 au RGPD, au CCPA/CPRA, au LGPD et à notre propre Addendum de Traitement des Données (DPA), ainsi qu'aux politiques de GoTo et aux accords de non-divulgation applicables.

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 qui peuvent être configurées dans le service aident les administrateurs à minimiser les menaces et les risques pour le Contenu Client.

3 Architecture du produit

GoTo Meeting, GoTo Webinar, GoTo Training et GoTo Stage sont des solutions SaaS (Software as a Service) conçues pour offrir des performances, une fiabilité, une évolutivité et une sécurité élevées. Ces Services s'appuient sur des serveurs et des équipements réseau de grande capacité, dotés de contrôles de sécurité appropriés et d'une infrastructure redondante conçue pour éviter les points de défaillance uniques. Des serveurs en cluster et des systèmes de sauvegarde assurent un fonctionnement normal des processus d'application en cas de forte charge ou de défaillance du système.

Les sessions d'application/serveur sont réparties sur des clusters distribués géographiquement et conçus pour garantir des performances et un temps de latence adéquats.

L'infrastructure et les données des Services sont hébergées par des fournisseurs d'hébergement dans le cloud.

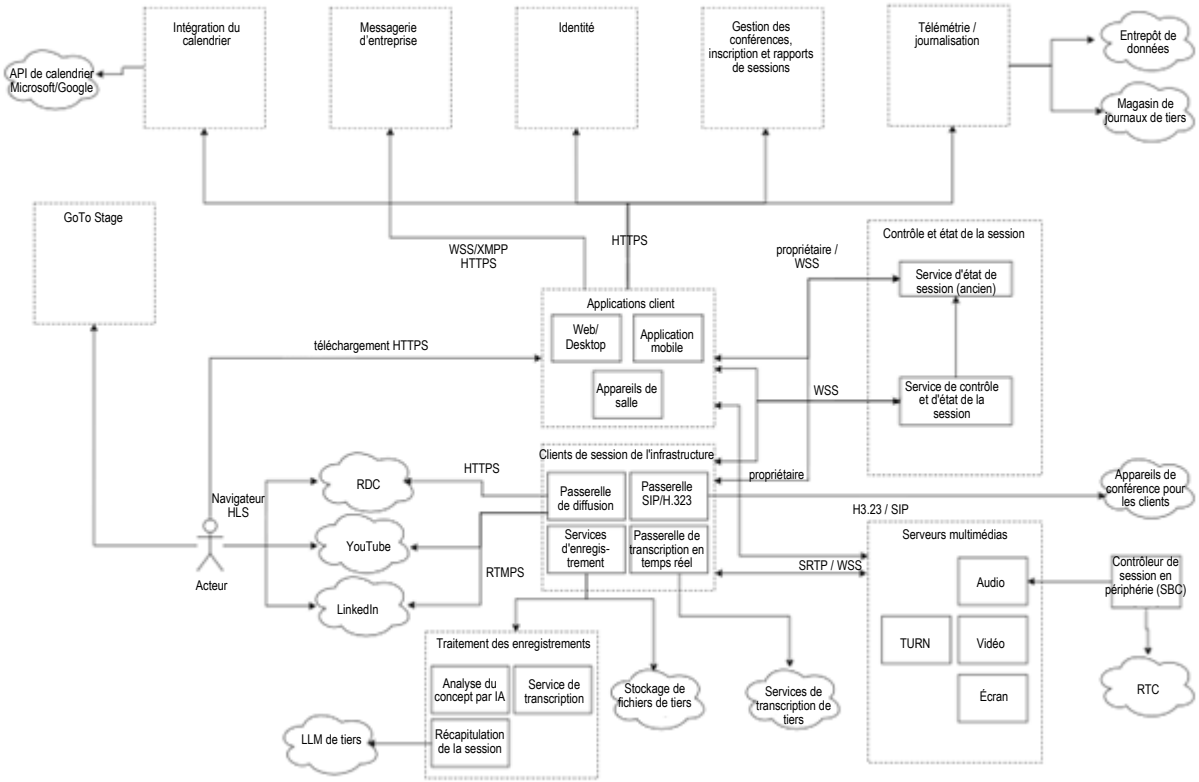

Figure 1 : Architecture Central

Applications client (les applications GoTo web, de bureau et mobiles ou « clients » ; un appareil appelé GoTo Room (Meeting uniquement)) : Les applications client fournissent les fonctionnalités du service telles qu'elles sont décrites dans la section 1 (Présentation du produit).

Services d'identité : Gère les comptes utilisateur et permet une autorisation et une connexion sécurisées et normalisées des comptes.

Services de gestion des conférences, d'inscription et de rapports de sessions : La gestion des conférences fournit des informations sur les sessions programmées et permet de programmer de nouvelles sessions et d'ajuster les sessions existantes. Les services d'inscription permettent de s'inscrire aux sessions qui le requièrent. Les rapports de sessions fournissent des informations sur les sessions passées, par exemple les enregistrements, les transcriptions, la participation et plus encore.

Messagerie d'entreprise : Gestion des canaux ainsi que de l'envoi, de la réception et du stockage des messages et des pièces jointes ; utilisée uniquement pour la messagerie hors session.

Intégration du calendrier : Permet aux utilisateurs de synchroniser leurs calendriers Microsoft Outlook ou Google pour recevoir des notifications sur les sessions GoTo.

Télémétrie/journalisation : Envoi de sondes de télémétrie ou d'entrées de journaux pour aider à recueillir des statistiques d'utilisation et à diagnostiquer les problèmes.

Services de contrôle et d'état de session : Fournit des fonctionnalités utilisées par les applications clientes pour initier et recevoir des modifications d'état de la session non liées aux médias.

Serveurs de médias : Responsables de la réception, de la modification et de la distribution des contenus audio, vidéo et de partage d'écran.

RTC : Le réseau téléphonique commuté permet aux utilisateurs de se connecter à des sessions via des téléphones physiques ou IP.

Session Border Controller : Connecte le protocole VoIP (Voix sur IP) de GoTo avec les fournisseurs de téléphonie commerciale.

Services d'enregistrement : Permet d'enregistrer le contenu des sessions audio, vidéo, de partage d'écran et de messagerie d'entreprise.

Passerelle de diffusion : Utilisée pour les webcasts de GoTo Webinar, elle prend en charge la configuration, le transcodage et la mise en paquets des flux multimédias en flux HLS, qui sont distribués via un RDC à des clients basés sur un navigateur ou envoyés vers des plateformes de diffusion en continu compatibles RTMP comme YouTube ou LinkedIn.

Passerelle SIP/H.323 : Permet la connexion à la session audio via des appareils de conférence SIP ou H.323.

Passerelle de transcription en temps réel (RTT) : Fournit une transcription en direct de la discussion entre les participants à la session.

Services GoTo Stage : Gestion du contenu vidéo des webinaires GoTo par les organisateurs ; offre une expérience de visualisation aux visiteurs.

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 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.

4.1.1 Chiffrement en transit

GoTo met en œuvre des mesures de sécurité pour les données en transit qui sont conçues pour protéger des attaques passives et actives contre la confidentialité, l'intégrité et la disponibilité. Des contrôles de sécurité des communications sont mis en œuvre pour le partage d'écran et de vidéo, la VoIP, la vidéo par webcam, le contrôle du clavier et de la souris, les informations de chat textuel et d'autres données de session.

GoTo utilise les protocoles TLS standard de l'Internet Engineering Task Force (IETF) pour protéger la communication TCP entre les points de terminaison.

HTTPS et WSS sont utilisés pour protéger les données non multimédias, tandis que les données multimédias en cours de session sont protégées par SRTP, WSS ou DTLS.

En interne, GoTo utilise également l'authentification par certificat mutuel (mTLS) sur les serveurs qui traitent les données multimédias.

4.1.1.1 Sécurité audio et vidéo

Un protocole SRTP utilisant des mécanismes de chiffrement standard qui s'appuient sur AES128 au minimum est utilisé pour protéger la confidentialité et l'intégrité des connexions VoIP entre les terminaux et les serveurs.

4.1.1.2 Sécurité des sites web, des API et des services web internes

Toutes les connexions aux sites web du Service, aux API et aux services web internes sont protégées par TLS. Cela comprend l'envoi de contenu, les rapports de session, les enregistrements et les transcriptions, etc.

4.1.1.3 Messagerie d'entreprise

Les mises à jour de présence, les messages et les fichiers sont transférés via un canal sécurisé par TLS vers les services de chat, puis vers les utilisateurs. Le contenu est fourni via des URL signées cryptographiquement qui renvoient au contenu.

4.1.1.4 Sécurité webcast (Webinar uniquement)

Les passerelles de diffusion de webcast transmettent le trafic au moteur de diffusion via SRTP, le tout au sein du réseau interne sécurisé de GoTo. Les RDC extraient les données du moteur de diffusion en continu en toute sécurité via HTTPS. Les clients extraient également des données en toute sécurité à partir des RDC via HTTPS.

4.1.2 Chiffrement au repos

4.1.2.1 Données du profil

Le contenu est stocké dans une base de données relationnelle avec un chiffrement AES 256 bits.

4.1.2.2 Gestion des conférences, inscription et rapports de sessions

Le contenu est stocké dans une base de données relationnelle avec un chiffrement AES 256 bits.

4.1.2.3 Envoi de contenu

Le contenu envoyé et les métadonnées correspondantes sont stockés dans AWS S3, Amazon Aurora et Amazon Dynamo DB, avec un chiffrement AES 256 bits. En outre, les métadonnées sont stockées dans Apache Cassandra sans chiffrement au repos.

4.1.2.4 Enregistrements et transcriptions

Les enregistrements dans le cloud sont stockés dans AWS S3. Les fichiers sont chiffrés au repos à l'aide d'un chiffrement côté serveur avec AES256.

Les fichiers audio destinés à la transcription sont chiffrés à l'aide de la norme AES256 et supprimés immédiatement une fois le processus de conversion de la parole en texte terminé.

4.1.2.5 Sécurité de la messagerie d'entreprise

Les messages sont stockés dans une base de données AWS Aurora et les fichiers partagés sont stockés dans AWS S3, tous deux avec un chiffrement AES 256 bits au repos.

4.1.2.6 GoTo Stage

Le contenu envoyé et les métadonnées correspondantes sont stockés dans AWS S3 avec un chiffrement AES 256 bits. Les métadonnées sont stockées dans Apache Cassandra et l'index de recherche dans Elasticsearch, tous deux non chiffrés au repos.

4.2 Compatibilité des pare-feu et des proxies

Le Service intègre une gestion des connexions et une logique de détection de proxy qui permet d'automatiser l'installation de logiciels, d'éviter la (re)configuration complexe du réseau et d'optimiser la productivité des utilisateurs. Les pare-feu et les proxies déjà présents dans le réseau d'un utilisateur n'ont généralement besoin d'aucune configuration spéciale pour permettre l'utilisation du Service.

Pour plus de détails, et pour connaître les domaines, IP et ports exacts utilisés, veuillez consulter les pages d'assistance respectives pour Meeting, Webinar et Training.

4.3 Fonctionnalités de sécurité du client installable

Les clients installables sont dotés de fonctions de sécurité appropriées et utilisent des mesures de chiffrement solides, notamment des logiciels signés et des connexions « client uniquement ».

4.3.1 Logiciel signé pour points de terminaison

Les exécutables du Service sont signés numériquement afin d'assurer la protection de l'intégrité et l'authenticité. Le logiciel d'application client de GoTo suit des procédures appropriées de contrôle de la qualité, des procédures de gestion de la configuration et un modèle de cycle de développement sécurisé (SDL) durant le développement et le déploiement.

4.3.2 Connexions « client uniquement »

Pour réduire le risque que des systèmes distants puissent les cibler avec des logiciels malveillants et des virus, les clients installables ne sont pas configurés pour recevoir des connexions entrantes. Cela permet de protéger les utilisateurs participant à une session contre l'infection par un hôte compromis utilisé par un autre participant.

4.3.3 Mise en œuvre d'un sous-système de chiffrement

Les fonctions de chiffrement et les protocoles de sécurité mis en œuvre dans les clients installables utilisent les bibliothèques de chiffrement Open Source BoringSSL ou OpenSSL. Aucune API externe n'est exposée : cela permettrait à d'autres logiciels d'accéder aux bibliothèques de chiffrement intégrées dans le client.

L'application web utilise les bibliothèques de chiffrement du navigateur. L'utilisateur final ne peut configurer aucun paramètre de chiffrement, ce qui permet d'éviter les erreurs de configuration accidentelles ou intentionnelles.

4.4 Authentification des utilisateurs

L'autorisation basée sur les rôles et les contrôles d'accès appropriés dépendent de la capacité à identifier et à authentifier les utilisateurs. Pour garantir que les organisateurs et les participants disposent des privilèges appropriés, des fonctions d'authentification des comptes et des sessions sont incorporées dans le Service.

4.4.1 Connexion au compte

Les sites Web du service proposent les méthodes de connexion suivantes :

- connexion directe avec nom d'utilisateur et mot de passe ;
- connexion par l'intermédiaire d'un fournisseur de compte de réseau social ou autre en utilisant LastPass, Google, Facebook, LinkedIn, Microsoft ou Apple (https://support.goto.com/fr/meeting/help/connect-your-social-or-other-account-for-sign-in) ; et
- l'authentification unique basée sur SAML.

Pour la connexion directe, tous les mots de passe sont soumis à des exigences minimales en matière de caractères et de complexité. Des mécanismes sont en place pour protéger des attaques par force brute et détecter les activités de connexion inhabituelles.

GoTo ne stocke pas les mots de passe des comptes en clair. Au contraire, les mots de passe sont stockés à l'aide d'une fonction de hachage cryptographique renforcée conçue pour résister aux attaques par dictionnaire et par force brute. Les mots de passe sont transmis via des connexions sécurisées (TLS).

4.4.2 Authentification des participants aux sessions

Pour permettre la tenue de sessions à participation restreinte, chaque session reçoit un ID unique et aléatoire. Les organisateurs peuvent également choisir d'exiger un mot de passe pour que les participants puissent se joindre à une session.

Pour participer à une session, les participants doivent fournir l'ID unique, soit en cliquant sur une URL qui contient l'ID, soit en saisissant manuellement cette valeur dans un formulaire présenté par le Service. En cas d'appel téléphonique, les participants doivent composer l'ID sur leur pavé numérique. Si l'ID est valide, chaque participant reçoit un jeton de rôle qui est présenté aux serveurs de communication lors du processus de connexion.

4.4.3 Contrôle d'accès par rôles

La possibilité d'attribuer des rôles définis par l'application aux utilisateurs du Service permet aux Clients d'appliquer les politiques d'accès de l'entreprise relatives à l'utilisation du Service et des fonctionnalités. Les utilisateurs peuvent accéder aux contrôles et aux privilèges en fonction du rôle qui leur a été attribué :

Les **organisateurs** (ou les formateurs dans le cas de GoTo Training) sont autorisés à planifier des réunions, des webinaires et des sessions de formation. L'organisateur configure chaque session, invite des participants, lance et met fin à la session et désigne les présentateurs.

Les **participants** sont les personnes invitées aux sessions. Les participants peuvent voir l'écran partagé du présentateur, chatter avec d'autres participants et consulter la liste des participants.

Les **présentateurs** sont des participants qui peuvent partager leur écran avec d'autres participants. Les présentateurs peuvent également permettre à d'autres participants de partager le contrôle de leur clavier et de leur souris.

Les **administrateurs** sont des individus autorisés à gérer un compte multi-utilisateurs. Les administrateurs peuvent configurer les fonctionnalités du compte, autoriser les organisateurs et accéder à divers outils de création de rapports.

Les **administrateurs internes de GoTo** sont des membres du personnel de GoTo autorisés à gérer les services et les comptes GoTo Meeting, GoTo Webinar et GoTo Training au nom de nos clients.

4.5 Contrôle de l'accès aux enregistrements

Les organisateurs peuvent facilement partager les enregistrements avec les participants à l'issue d'une session via des liens uniques et directs, et les participants peuvent alors lire l'enregistrement dans leur navigateur web.

Avec GoTo Webinar, les URL de partage n'expirent pas tant que l'enregistrement est disponible. Pour désactiver l'accès à un enregistrement, les organisateurs peuvent supprimer ce dernier à tout moment.

Avec GoTo Meeting, les enregistrements peuvent être partagés via des URL qui utilisent un jeton aléatoire à validité limitée. Il est possible de limiter le partage à des parties spécifiques du contenu et de le rendre accessible à toute personne ayant accès à l'URL ou uniquement aux utilisateurs dont l'adresse électronique est configurable. Ces restrictions peuvent être modifiées même après le partage de l'URL.

5 Mises à jour du programme de sécurité

GoTo révise 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.

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 en utilisant les centres de données des fournisseurs d'hébergement dans le cloud.

Pour des informations détaillées sur les fournisseurs du centre de données et sur les emplacements, veuillez consulter le document Sub-Processor Disclosure (Déclaration de sous-traitance) dans le Trust and Privacy Center de GoTo.

Tous les centres de données font l'objet d'une surveillance des conditions environnementales et sont dotés de mesures de sécurité physique permanentes.

7.1 Sécurité physique des centres de données

Les fournisseurs d'hébergement dans le cloud assurent la sécurité physique et les contrôles environnementaux des systèmes et des serveurs qui contiennent 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

Les fournisseurs d'hébergement dans le cloud limitent l'accès physique aux centres de données de production aux seules personnes autorisées. L'accès aux salles de serveurs nécessite une demande par le système de gestion de tickets approprié et l'approbation du responsable concerné, ainsi que l'examen et l'approbation. Tous les accès physiques aux centres de données et aux salles de serveurs sont réduits au minimum, consignés et examinés par les fournisseurs 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, 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, veuillez consulter notre article de blog.
- **Certifications TRUSTe APEC CBPR/PRP** pour le transfert de contenu client entre les pays membres de l'APEC obtenues et validées de manière indépendante par l'intermédiaire de TrustArc, une tierce partie leader approuvée par l'APEC en matière de conformité à la protection des données. Pour en savoir plus sur nos certifications APEC, cliquez ici.
- Rapport d'attestation de l'American Institute of Certified Public Accountants (AICPA) **Service Organization Control (SOC) 2 Type II** avec **BSI Cloud Computing Catalogue (C5)**
- 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 répondre en temps opportun. GoTo enregistre le trafic anormal ou suspect identifié dans les journaux de sécurité pertinents des systèmes de production concernés.

11 Détection et intervention sur les terminaux

Un logiciel de détection et d'intervention sur les terminaux (EDR) 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 sur une base trimestrielle, effectue des activités de gestion des correctifs sur tous les systèmes, appareils, micrologiciels et systèmes d'exploitation pertinents qui traitent le Contenu Client. GoTo évalue et analyse les vulnérabilités des systèmes, des hôtes/réseaux (« 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

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 se voient accorder l'accès aux systèmes, applications, réseaux et appareils GoTo spécifiés 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 de voir les données d'autres Utilisateurs.

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 ;
- une surveillance des systèmes critiques et des fichiers de configuration ;
- des pare-feu du réseau cloud qui filtrent les connexions entrantes et sortantes, y compris les connexions internes entre les systèmes GoTo ; et
- une segmentation du réseau interne.

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 Central et Pro. 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.goto.com ou en envoyant un e-mail 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 marqué pour suppression dans les quatre-vingt-dix (90) jours et supprimé avec succès dans les cent (100) jours suivant 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.

Les délais susmentionnés s'appliquent à tous les Services, et les délais de suppression supplémentaires spécifiques aux Services sont indiqués ci-dessous :

GoTo Meeting

Pendant la durée de l'abonnement : L'historique des sessions GoTo Meeting et les enregistrements dans le cloud seront automatiquement supprimés par roulement d'un (1) an pendant la durée de l'abonnement actif du Client, pour les comptes payants et gratuits.

Après la durée de l'abonnement : À la fin d'un abonnement payant à GoTo Meeting, les comptes du Client qui incluent une licence gratuite redeviendront des comptes gratuits et le Contenu sera conservé. Pour les comptes qui n'incluent pas de licence gratuite ou qui sont explicitement annulés ou résiliés, le Contenu sera automatiquement marqué pour suppression dans les quatre-vingt-dix (90) jours et supprimé avec succès dans les cent (100) jours suivant la résiliation, l'annulation ou l'expiration et, dans chaque cas, le déprovisionnement de l'abonnement final du Client. En outre, les comptes GoTo Meeting gratuits seront automatiquement supprimés après deux (2) ans d'inactivité de l'utilisateur (par exemple, aucune connexion).

Suppression d'un utilisateur d'un compte payant : Si un utilisateur est supprimé ou retiré d'une autre manière d'un compte payant actif, les sessions planifiées sont automatiquement marquées pour être supprimées après quatre-vingt-dix (90) jours et supprimées avec succès dans les cent (100) jours suivant la suppression de l'utilisateur.

GoTo Stage : Les utilisateurs de GoTo Stage ayant un abonnement actif à GoTo Webinar peuvent à tout moment dépublier/supprimer un webinaire publié, soit via le libre-service dans l'environnement des services GoTo Webinar, soit en soumettant une demande d'assistance à GoTo.

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 déontologique, 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 vie privée de ses clients, utilisateurs et autres personnes qui utilisent les services GoTo (« Utilisateurs finaux ») et s'engage à divulguer les pratiques de traitement et de gestion des données pertinentes 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 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 (également appelées 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 Cadre de protection des données

Les cadres de protection des données UE-États-Unis et Suisse-États-Unis (DPF) ainsi que l'extension britannique du DPF UE-États-Unis sont des cadres volontaires qui fournissent des mécanismes permettant aux entreprises de transférer des données personnelles, respectivement, de l'UE, de la Suisse et du Royaume-Uni vers les États-Unis dans le

respect des règles de protection des données en vigueur dans ces juridictions. GoTo se conforme à chacun de ces cadres concernant la collecte, l'utilisation et la conservation des données personnelles, respectivement, de l'UE, de la Suisse et du Royaume-Uni. Pour en savoir plus sur le DPF et consulter la certification de GoTo, veuillez visiter le site Web du DPF.

20.4.3 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.

20.4.4 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.

20.5 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.

20.6 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 précisent 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.

20.7 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 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.

20.8 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 GoTo Resolve 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. Par exemple, la DPA des fournisseurs de GoTo comporte des restrictions concernant la « vente » de données telle que définie par la CCPA. 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.

22 Contacter GoTo

Les Clients peuvent contacter GoTo à l'adresse support.goto.com pour toute question d'ordre général. Pour toute question ou demande relative à la protection des données ou à la sécurité, veuillez consulter notre portail IRM ou envoyer un courriel à privacy@goto.com.