

INTRODUCTION

En tant que multinationale dédiée à faciliter l'informatique et les communications professionnelles, GoTo propose des produits tels que GoTo Resolve, LogMeIn Rescue et GoTo Connect pour contribuer à une assistance et à une connexion en toute sécurité des entreprises à ce qui est le plus important : leurs équipes et leurs clients. Nous gérons un programme mondial de confidentialité des données conçu pour protéger et permettre le transfert légal des données qui nous sont confiées par nos clients et leurs utilisateurs finaux.

Ce document vise à répondre à certaines des questions les plus fréquentes concernant les pratiques de GoTo pour le transfert de données personnelles en dehors de l'Union Européenne (« UE »), l'Espace Économique Européen (« EEE ») et le Royaume Uni (« RU »), notamment :

- Mécanismes de transfert de données (par exemple Clauses Contractuelles Types) ;
- Données de transparence sur les lieux et les moyens de traitement ;
- Informations visant à aider à toute analyse d'impact de transfert demandée ;
- Informations sur les pratiques de confidentialité et de sécurité de GoTo ; et
- Mesures supplémentaires de protection des données.

FOIRE AUX QUESTIONS (FAQ)

Quelles sont les catégories de données personnelles que GoTo recueille et traite pour ses clients ?

GoTo fait tout pour limiter les types et les catégories de données personnelles recueillies auprès de ses clients et ensuite traitées à ce qui est strictement nécessaire pour l'atteinte de la ou les finalités de prestation et d'exploitation des Services de GoTo. Finalement, les types d'informations fournies par GoTo à ses clients et traitées par GoTo dépendent du Service et des scénarios d'utilisation spécifiques de chaque client de GoTo.

De plus, il est important de noter que les données personnelles traitées par GoTo lors de la prestation de nos Services le sont conformément aux instructions de l'utilisateur, qui, sauf accord contraire par écrit séparé, prennent la forme des Conditions d'utilisation des Services de GoTo (y compris tout Addendum de Traitement des Données signé conjointement avec elles). Des informations supplémentaires concernant les catégories et les types d'informations que GoTo peut traiter peuvent se trouver dans les Conditions juridiques d'utilisation des Services de GoTo et l'Addendum de Traitement des Données à l'adresse www.goto.com/company/legal, ainsi que dans la documentation des Mesures Techniques et d'Organisation (« TOM ») applicables à l'adresse www.goto.com/company/trust.

Où se trouvent les centres de données de GoTo ?

Pour assurer la disponibilité du Service et la redondance nécessaire pour la meilleure satisfaction de notre clientèle mondiale, GoTo tire parti d'une combinaison de sites physiques d'hébergement mutualisé et de prestataires d'hébergement dans le cloud en Australie, au Brésil, en Allemagne, en Inde, au Royaume Uni, aux États-Unis et à Singapour. De même, GoTo a des salariés et/ou des sites d'exploitation en Australie, au Brésil, au Canada, au Guatemala, en Allemagne, en Hongrie, en Inde, au Mexique, au Royaume-Uni et aux États-Unis. Mais cela ne signifie pas que les données personnelles seront hébergées, traitées ou accessibles dans toutes ces régions – les centres de données spécifiques de chaque Service sont identifiés dans la Déclaration de Sous-traitants applicable située dans la section [Ressources produit](#) de notre centre Trust & Privacy Center à l'adresse www.goto.com/company/trust.

Où puis-je trouver des informations sur les sous-traitants de GoTo ?

Les déclarations spécifiques du Service concernant les régions des centres de données et des sous-traitants tiers utilisés pour la prestation de nos Services se trouvent dans la Déclaration de Sous-traitants correspondante dans la section [Ressources produit](#) de notre centre Trust & Privacy Center (www.goto.com/company/trust). De même, GoTo publie une déclaration de ses filiales en pleine propriété, qui se trouve dans la [Déclaration de filiales](#) disponible sur le centre Trust and Privacy Center de GoTo.

Transferts de Données personnelles dans l'UE

Qu'est-ce qu'un transfert de données personnelles international ?

Un transfert de Données personnelles international ou « transfrontalier » survient quand des données personnelles sont fournies par une partie située dans un pays (ou soumise à certaines lois) à une autre partie située dans un pays différent. Certaines lois sur la protection de la vie privée régissent ces transferts de données personnelles. Par exemple, le RGPD interdit ces transferts à moins qu'un mécanisme de transfert reconnu par la loi ne soit mis en place, notamment que : a) le destinataire se trouve dans un pays dont les lois de protection des données personnelles ont été formellement reconnues par la Commission Européenne comme substantiellement comparables au RGPD ou « adéquates » ; b) certaines conditions s'appliquent, par exemple les destinations vers lesquelles la personne consent au transfert ; ou c) il existe des protections appropriées, par exemple quand le destinataire se trouve aux États-Unis et a été certifié selon le Cadre de Protection des Données, ou quand le destinataire ne se trouve pas dans un pays dont les lois ont été « considérées comme adéquates », si les parties ont convenu de certains engagements contractuels sur la façon de traiter les données, par exemple les Clauses Contractuelles Types de l'UE (CCT de l'UE).

GoTo transfère-t-il des données personnelles en dehors de l'UE et du Royaume-Uni ?

Oui. GoTo a une présence dans de nombreux pays, avec la prestation de Services auprès de millions de personnes et d'entreprises du monde entier. Selon le Service spécifique, GoTo peut héberger et/ou traiter des données en dehors de l'UE/EEE et du Royaume-Uni. Pour ces transferts, GoTo a pris des mesures pour s'assurer d'une protection adéquate des données personnelles conformément aux lois de protection des données applicables, notamment le RGPD.

Notre [Addendum de Traitement des Données](#) (« ATD »), associé à nos [Conditions d'utilisation des Services](#), explique comment GoTo, dans son rôle de prestataire de service et de sous-traitant de données, traite les données personnelles pour la prestation et l'exploitation de nos Services. Pour en savoir plus sur la localisation des filiales et des sous-traitants de GoTo, veuillez consulter les Déclarations de filiales de GoTo et les Déclarations de sous-traitant applicables dans son centre [Trust & Privacy Center](#).

Quelles méthodes légales utilise GoTo selon le Chapitre 5 du RGPD pour effectuer ces transferts ?

Le 10 juillet 2023, la Commission Européenne a adopté sa décision sur l'adéquation du Cadre de protection des données UE - États-Unis (« DPF »), concluant que les États-Unis assurent un niveau adéquat de protection des données personnelles transférées depuis l'UE/EEE vers les sociétés des États-Unis certifiées selon le DPF UE-États-Unis sans avoir à mettre en place des protections supplémentaires des données. GoTo a fait certifier notre conformité au [DPF UE-États-Unis, à l'extension du DPF au Royaume-Uni et au DPF Suisse-UE](#) par le Département du Commerce des États-Unis.

En plus de cette certification, le DPA de GoTo incorpore les [CCT](#) de l'UE et de l'[Addendum RU](#) aux CCT de l'UE. Ces CCT s'appliquent si l'étendue de nos certifications DPF ne couvre pas le transfert des données personnelles de l'UE, du Royaume-Uni et de la Suisse vers GoTo et s'appliqueront automatiquement à tous les transferts de données applicables si le DPF est invalidé. GoTo gère un accord de traitement des données du groupe qui incorpore les exigences nationales en matière de transfert de données, y compris les Clauses Contractuelles Types de l'UE et documente l'obligation pour chaque entité du groupe GoTo de se conformer à la loi de protection des données personnelles applicable lors du Traitement des Données personnelles qui lui sont transférées par une autre entité du groupe GoTo.

De plus, il est important de noter qu'un client achetant des Services GoTo depuis l'UE/EEE* signe un contrat avec la filiale irlandaise de GoTo, GoTo Technologies Ireland Unlimited Company, et que le contrat de Services est soumis à la loi irlandaise (État membre), y compris les lois de protection des données applicables (telles que le RGPD et le Data Protection Act 2018), et que les données ainsi traitées seraient donc protégées selon les lois en vigueur en Irlande.

*Les clients du Royaume-Uni signent un contrat avec GoTo Technologies UK Limited, et le contrat est soumis aux lois du Royaume-Uni et du Pays de Galles.

Quelles mesures dois-je prendre si mon organisation transfère des données vers GoTo sur la base des CCT ?

GoTo a mis à jour son DPA pour inclure les CCT les plus récentes et a pré-signé des versions prêtes à signer disponibles en ligne à l'adresse www.goto.com/legal.

Les sous-traitants de GoTo sont-ils liés par les CCT ?

Oui. La politique de GoTo est de signer des Addenda de Traitement des Données contenant les clauses exigées par la loi applicable et des protections au moins aussi protectrices que celles de notre DPA. Si nécessaire, nos addenda de traitement des données par les fournisseurs incorporent les CCT de l'UE et l'addendum du Royaume-Uni au service des transferts de données personnelles vers des pays tiers. Vous trouverez des informations sur les sous-traitants de GoTo et leurs localisations [ici](#).

Quelles mesures techniques et d'organisation GoTo a-t-il mis en place pour protéger les données personnelles ?

Dans le cadre de l'engagement de GoTo en faveur de la confidentialité et de la sécurité des données, nous avons mis en place et nous gérons des mesures techniques de sécurité et de confidentialité des données, notamment de chiffrement, allant au-delà des exigences minimales des CCT. Chacune de nos offres de produit a mis en place ses propres mesures techniques et d'organisation spécifiques du produit, notamment mais sans limitation :

- **Chiffrement** : recours au chiffrement Transport Layer Security (« TLS ») v1.2 pour protéger et réduire le risque d'espionnage ou d'interception des données en transit (par exemple communications pendant un appel « Computer Audio » ou « VoIP »).
- **Principes de sécurité et de protection des données** : un programme de cycle de vie de développement sécurisé (« SDL ») au niveau de l'entreprise qui prend en compte les principes de sécurité et de protection des données dans les phases pertinentes de la procédure de développement pour soutenir les développeurs dans leur création de logiciel de haute sécurité, en faveur de la conformité aux exigences de sécurité et de la réduction des coûts de développement.
- **Confidentialité par conception « Privacy by Design » (PbD)** : nous gérons des normes et des exigences PbD, ainsi que des normes globales de Sécurité et de Confidentialité technique pour s'assurer que nos produits prennent en compte les directives de protection et de sécurité dans les domaines pertinents de notre exploitation d'entreprise.
- **Cadres/évaluations de sécurité et de confidentialité** : les programmes de sécurité et/ou de confidentialité de GoTo sont, le cas échéant, régulièrement évalués selon des normes testées et validées par des tiers, notamment :

- Rapport de contrôle d'organisation de service N°2 de l'American Institute for Certified Public Accountants (« AICPA ») (« SOC2 ») Type II
- Rapport de contrôle d'organisation de service N°3 de l'AICPA (« SOC3 ») Type II
- Bundesamt für Sicherheit in der Informationstechnik (« BSI ») Cloud Computing Compliance Controls Catalogue (« C5 »)
- ISO 27001 (pour GoTo Resolve, LogMeIn Rescue, GoToAssist Remote Support v5 et Miradore)
- Certification de confidentialité TRUSTe Enterprise
- APEC Cross Border Privacy Rules (« CBPR ») et Privacy Recognition for Processors (« PRP »)

Les normes de sécurité mentionnées ci-dessus incluent de robustes contrôles et procédures d'accès, ainsi que de chiffrement, de gestion des accès, de confidentialité et de sécurité.

- **Programmes robustes de conformité interne et réglementaire** : ces programmes, supervisés par des experts et des professionnels formés des groupes Juridique, de Sécurité et de Gouvernance, risque et Conformité (« GRC ») de GoTo, nous aident à gérer des politiques, des procédures et des opérations permettant de s'assurer que GoTo reste au courant et conforme aux règles et règlements de protection des données applicables. Les équipes internes de GoTo évaluent régulièrement et cherchent à améliorer nos programmes de confidentialité et prennent des mesures pour notamment, mais sans limitation, effectuer des audits internes annuels de confidentialité (pour valider la conformité au RGPD, au CCPA et aux autres lois de protection des données applicables) au service de cet objectif.

Vous trouverez des informations détaillées et spécifiques du produit sur ces mesures techniques de sécurité et de confidentialité supplémentaires dans la documentation des Mesures Techniques et d'Organisation de GoTo (« TOM ») disponible dans la section « Ressources Produit » de notre centre Trust & Privacy Center (www.goto.com/company/trust).

Évaluations d'impact de transfert

Qu'est-ce qu'une évaluation d'impact de transfert (TIA) ?

Suite à la décision de la Cour de Justice Européenne C-311/18, souvent appelée « Invalidation du Privacy Shield » ou « Schrems II », la Commission Européenne a publié des révisions des CCT et le Comité européen de la protection des données (« EDPB ») a publié ses [recommandations finales](#) sur les mesures supplémentaires pour assurer la conformité aux lois de protection des données lors du transfert des données personnelles en dehors de l'UE/EEE. En conséquence, il a été recommandé aux « exportateurs de données » (par exemple un client de GoTo) de vérifier au cas par cas si les lois du pays tiers offrent aux données personnelles un niveau de protection essentiellement équivalent aux protections de l'UE/EEE. Si ce n'est pas le cas, l'exportateur de données devra vérifier si des mesures supplémentaires appropriées ont été mises en place par l'« importateur de données » (par exemple GoTo) pour s'assurer du niveau de protection exigé.

GoTo a conçu ses programmes de protection et de sécurité des données pour assurer un niveau approprié de protection des données, conforme à la loi applicable, et nous avons décrit les mesures et protections supplémentaires prises pour fournir ces assurances dans cette FAQ (voir « *Quelles mesures techniques et d'organisation GoTo a-t-il mis en place pour protéger les données personnelles ?* » ci-dessus, ainsi que les politiques, procédures et la documentation mentionnées juste ci-dessous).

Quelles autres ressources GoTo fournit-il à ses clients pour une évaluation TIA ?

Les ressources suivantes peuvent aider les clients de GoTo dans la conduite d'une évaluation TIA associée à nos Services :

- [Trust & Privacy Center](#)
- [Recommandations de l'EDPB sur les mesures supplémentaires 01/2020](#)
- [Déclarations de sous-traitants](#)
- [Ressources produit](#)
- [Politique relative aux demandes des autorités](#)
- [Livre blanc RGPD](#)
- [U.S. Dept. of Justice Whitepaper Re: Schrems II Decision](#)
- [Addendum de Traitement des Données de GoTo](#)
- [Programme du Cadre de protection des données](#)

Demandes des autorités

GoTo est-il soumis au 50 U.S. Code § 1881a (« FISA 702 ») ou est-il autrement soumis aux exigences de l'Executive Order 12333 ?

GoTo est soumis aux lois et règlements applicables de chaque pays où il est présent. Il est important de noter que, bien que le siège social de GoTo puisse se trouver aux États-Unis, les clients basés dans l'UE signent un contrat et acceptent les clauses de protection des données avec une entité GoTo basée dans un État membre (par exemple avec GoTo Technologies Ireland Unlimited Company*). C'est pourquoi toutes les demandes reçues des autorités ou des forces de l'ordre des États-Unis, que ce soit dans le cadre des clauses ci-dessus, de la loi U.S. Cloud Act ou autre, devraient être reconnues comme valides dans et selon les lois de la République d'Irlande ou de l'État membre applicable. Des informations supplémentaires sur le traitement par GoTo des demandes d'accès aux données par les autorités sont disponibles dans la section [Politique relative aux demandes des autorités](#).

*Les clients du Royaume-Uni signent un contrat avec GoTo Technologies UK Limited, et toutes les demandes devraient être reconnues comme valides dans et selon les lois du Royaume-Uni ou du Pays de Galles.

Quelle est la politique de GoTo concernant les demandes d'accès aux données par les autorités ?

GoTo a publié une [Politique concernant les demandes des autorités](#), conçue pour offrir plus de transparence sur les règles utilisées par GoTo pour savoir comment et quand nous traiterons les demandes reçues des forces de l'ordre, de la sécurité nationale et autres instances réglementaires (« Autorités ») concernant nos clients, leurs salariés, et/ou leurs utilisateurs. GoTo étudiera toutes les demandes d'autorités internationales au cas par cas et pays par pays, de façon à prendre en compte et comparer nos obligations légales locales à nos engagements de promotion de la sécurité et de la confidentialité des utilisateurs. La politique de GoTo est de ne fournir aucune donnée de client à toute entité gouvernementale, à moins que la partie demanderesse n'ait l'autorité appropriée pour demander ces informations dans le cadre de la loi applicable et ait fourni à GoTo un mandat, une assignation, une ordonnance ou décision judiciaire valable.

Qui devrais-je contacter si j'ai des questions sur les pratiques de protection des données de GoTo ?

Veillez vous adresser à privacy@goto.com pour toutes les questions supplémentaires concernant les pratiques de protection des données de GoTo. Remarquez que GoTo ne peut pas fournir de conseil juridique à ses clients et leur recommande de consulter leur propre conseil juridique pour toutes questions concernant la légalité de leurs propres programmes de conformité à la protection des données.