CLOUDFLARE

LIVRE BLANC

Les politiques de Cloudflare en matière de confidentialité des données et de traitement des demandes émanant des forces de l'ordre

Publication le 28 janvier 2021

Vue d'ensemble

Le réseau et l'activité de Cloudflare reposent intégralement sur la confiance de nos clients. Nous aspirons à continuellement gagner et entretenir cette confiance en développant et en déployant des produits qui contribuent à améliorer la sécurité de nos systèmes, qui chiffrent les données au repos ou en transit et qui permettent à nos clients de déterminer de quelle manière le trafic est inspecté dans différents endroits du monde.

Cependant, l'ingénierie ne permet pas de relever tous les défis. C'est pourquoi nous disposons également de politiques et de procédures qui guident notre façon de gérer les données des clients et des utilisateurs finaux sur nos systèmes, ainsi que notre façon de traiter les demandes de données émanant d'instances gouvernementales et d'autres autorités.

Ce document décrit ces politiques et fournit des liens vers des informations plus détaillées concernant les différentes facettes de notre approche de la confidentialité et de la conformité des données. Plus précisément, il présente :

- Notre point de vue concernant l'évolution de l'environnement de la protection des données
- Nos politiques en matière de confidentialité des données et de traitement des demandes de données

L'environnement changeant de la confidentialité des données

L'explosion des services cloud (et le fait que les données puissent être stockées hors des pays de résidence des personnes qui les ont générées) constitue un défi pour les instances gouvernementales qui mènent des enquêtes dans le cadre de l'application de la loi. Les fournisseurs de services en ligne de toute sorte constituent souvent un point d'accès à ces documents électroniques.

Pour les prestataires de services comme Cloudflare, ces demandes de données peuvent être lourdes de conséquences. Le travail qu'accomplissent les forces de l'ordre et les autres instances gouvernementales est important. Cependant, les données que cherchent à obtenir les forces de l'ordre et les autres instances gouvernementales ne nous appartiennent pas. En utilisant nos services, nos clients nous ont accordé leur confiance au regard du traitement de ces données. La préservation de cette confiance est fondamentale pour notre entreprise et nos valeurs.

Ces tensions sont aggravées par le fait que différents gouvernements ont adopté différentes politiques en matière de protection des données personnelles. Les États-Unis, par exemple, interdisent aux entreprises de divulguer le contenu des communications, notamment à des gouvernements autres que le gouvernement des États-Unis, excepté dans certaines circonstances définies par la loi. L'Union européenne (UE), qui a longtemps considéré la confidentialité des communications et la protection des données personnelles comme des droits de l'homme fondamentaux, protège toutes les données personnelles au sein de l'UE par le biais du Règlement général sur la protection des données (RGPD). Bien que ces protections se chevauchent à certains égards, elles diffèrent à la fois au regard de leur portée et des entités qu'elles protègent.

Les différences entre ces cadres juridiques sont importantes, notamment lorsqu'il s'agit de déterminer si les demandes juridiques d'informations émanant de gouvernements étrangers peuvent être considérées comme conformes aux exigences en matière de confidentialité. Ces dernières années, par exemple, la Cour de justice de l'Union européenne (CJUE) a conclu à plusieurs reprises que les restrictions juridiques américaines en matière de collecte de données, ainsi que certains engagements volontaires tels que le Bouclier de protection des données (« Privacy Shield ») ou son prédécesseur, la Sphère de sécurité (« Safe Harbor ») États-Unis-UE, ne sont pas suffisants pour assurer la conformité aux exigences de l'UE en matière de protection de la confidentialité, en grande partie à cause des lois américaines qui permettent aux instances juridiques de collecter des informations sur des citoyens non américains pour le renseignement étranger. En effet, le Conseil européen de protection des données (CEPD) a pris position en déclarant qu'une demande de données au titre du droit pénal américain (en dehors d'un recours juridique, où les pays de l'UE conservent un certain contrôle sur les informations présentées) ne constitue pas un fondement légitime au transfert de données personnelles couvertes par le RGPD.

Fondamentalement, l'objet de ces querelles est de déterminer dans quelles circonstances il est approprié qu'un gouvernement recoure à des ordonnances juridiques ou emploie d'autres recours juridiques pour accéder à des données concernant les citoyens d'un autre pays. Et ces querelles n'ont pas uniquement lieu en Europe. Bien que leurs réponses en termes de politiques ne soient pas cohérentes, un nombre croissant de pays considèrent désormais l'accès aux données de leurs citoyens comme un problème de sécurité nationale.

Les politiques de Cloudflare en matière de confidentialité des données et de traitement des demandes de données

Cloudflare dispose depuis longtemps de politiques conçues pour répondre aux préoccupations en matière d'accès aux données personnelles. Si c'est le cas, c'est parce que c'est ce que nous pensons être juste et parce que les conflits de lois que nous constatons aujourd'hui paraissaient inévitables. Ces politiques couvrent :

- Nos engagements publics concernant la manière dont nous traitons les données privées et les demandes de données émanant des forces de l'ordre
- Comment nous informons nos clients au sujet des demandes de données.

En règle générale, lorsqu'un conflit survient entre deux normes juridiques différentes, nous optons par défaut pour celle qui protège le mieux la confidentialité. Et nous exigeons toujours un recours juridique, car lorsque l'on entrouvre la porte qui permet d'accéder aux données, il peut être difficile de la refermer.

Nos engagements publics concernant les données privées et les demandes émanant des forces de l'ordre

Depuis notre tout premier rapport de transparence, dans lequel étaient détaillées les demandes de données émanant des forces de l'ordre en 2013, nous avons pris des engagements publics concernant notre façon de traiter les demandes de données, et nous avons effectué des déclarations publiques concernant les choses que nous n'avons jamais faites. Nous appelons ces déclarations publiques des « warrant canaries », l'idée étant qu'elles permettent d'adresser un signal au monde extérieur.

Ces « warrant canaries » ont deux fonctions. Premièrement, elles constituent une déclaration publique indiquant que nous n'effectuerions pas ces actions de notre plein gré. Deuxièmement, elles peuvent être un mécanisme de transmission d'informations (par le retrait de la déclaration du site) que nous ne pourrions peut-être pas divulguer autrement.

Les entités réglementaires ont commencé à reconnaître la valeur des engagements en matière de confidentialité, en particulier lorsqu'ils peuvent être mis en œuvre par voie contractuelle. En effet, les engagements que nous incluons depuis des années dans nos rapports de transparence sont exactement les types d'engagements que la Commission européenne a recommandé d'inclure dans son projet de clauses contractuelles types pour la conformité au RGPD.

Voici quelques exemples essentiels de nos engagements à la date de publication de ce document :

- **Nous n'avons jamais installé de logiciels ou d'équipements des forces de l'ordre sur notre réseau, ni fourni un flux des contenus transitant sur notre réseau** : en tant qu'entreprise spécialiste de la sécurité, nous savons qu'il est absolument impératif de préserver le contrôle des accès à nos réseaux. C'est pourquoi notre équipe de sécurité s'est concentrée sur les contrôles d'accès, la journalisation et la surveillance, et se soumet chaque année à plusieurs évaluations par des tiers. Nous voulons nous assurer que nos clients comprennent que ces contrôles ne comportent aucune exemption pour les forces de l'ordre ou les instances gouvernementales. C'est pourquoi nous déclarons que Cloudflare n'a jamais installé de logiciels ou d'équipements des forces de l'ordre sur son réseau et n'a jamais fourni, à quelque organisation gouvernementale que ce soit, un flux des contenus de nos clients transitant sur notre réseau.
- **Nous n'avons jamais diffusé de clés de chiffrement ou d'authentification :** Cloudflare considère qu'un chiffrement fort (aussi bien pour les contenus que pour les métadonnées) est nécessaire à la protection de la confidentialité en ligne. Si un pays cherche à empêcher un autre gouvernement d'accéder aux données personnelles de ses citoyens, la première étape doit être le chiffrement de ces données personnelles. Cependant, les clients et les régulateurs doivent également avoir la certitude que le chiffrement lui-même est digne de confiance. C'est pourquoi nous avons pris les engagements de n'avoir jamais transmis à quiconque nos clés de chiffrement ou d'authentification, ni les clés de chiffrement ou d'authentification de nos clients, et de n'avoir jamais affaibli, compromis ou subverti notre chiffrement à la demande des forces de l'ordre ou de tout autre tiers.
- **Nous n'avons jamais modifié les contenus ou les requêtes DNS de nos clients :** nous ne croyons pas que nos systèmes doivent être exploités pour diriger les personnes vers des sites qu'elles n'avaient pas l'intention de consulter, ni pour modifier les contenus auxquels elles accèdent en ligne. Nous avons donc déclaré publiquement que nous n'avons jamais modifié, à la demande des forces de l'ordre ou de quelque autre tiers, les contenus de clients ou la destination prévue des réponses DNS.
- **Transparence au regard d'éventuelles remises en cause de nos engagements** : nous nous engageons à contester devant un tribunal, si nécessaire, toute ordonnance juridique cherchant à nous faire revenir sur ces engagements. Notre objectif était d'être très clairs (aussi bien envers nos clients qu'envers les gouvernements du monde entier) au regard des limites que nous établissions.

Si notre philosophie générale en matière de protection des données est restée inchangée depuis la création de notre entreprise, nous adaptons occasionnellement nos engagements de manière à refléter les dernières modifications apportées à nos produits et à l'environnement de nos politiques. Une liste définitive et actualisée de ces engagements est disponible sur la page du rapport de transparence.

Informer nos clients en cas de demandes émanant du gouvernement

Cloudflare considère depuis longtemps que ses clients méritent d'être informés lorsqu'une entité (notamment un organisme des forces de l'ordre ou toute autre instance gouvernementale) emploie un recours juridique pour demander leurs données. Cette information permet à nos clients de contester la demande s'ils ont des inquiétudes à son sujet.

En effet, nous avons toujours eu pour politique d'informer nos clients, et ce, depuis la fondation de notre entreprise. En janvier 2013, lorsque nous avions moins de 30 employés, le FBI s'est présenté dans nos bureaux avec une lettre de sécurité nationale (c'est-à-dire une assignation administrative émise à des fins de sécurité nationale) sollicitant des informations sur un client, en nous interdisant d'en parler à quiconque d'autre que nos avocats. À l'époque, les lettres de sécurité nationale n'étaient soumises à pratiquement aucun contrôle, pouvaient être rédigées et mises en application par une branche unique du gouvernement américain et interdisaient indéfiniment à leurs destinataires de les évoquer.

Nous reconnaissons que dans certaines circonstances, les forces de l'ordre peuvent légitimement restreindre temporairement la divulgation, afin de préserver la viabilité d'une enquête. Cependant, nous pensons également que le gouvernement devrait être tenu de justifier toute disposition de non-divulgation, et que toute disposition de non-divulgation devrait être explicitement limitée dans le temps à la durée minimale nécessaire pour l'objectif concerné. C'est pourquoi nous avons collaboré avec Electronic Frontier Foundation pour contester cette lettre en justice. Le procès qui en a résulté a duré plusieurs années, et nous avons eu l'interdiction d'en parler jusqu'en 2017. Mais finalement, le FBI a révoqué la lettre.

Les tribunaux américains ayant laissé entendre que les ordonnances de non-divulgation avec une durée indéterminée soulevaient des problèmes constitutionnels, le ministère américain de la Justice a publié en 2017 des directives enjoignant les procureurs fédéraux à limiter à un an la durée maximale des ordonnances de non-divulgation, sauf dans des circonstances exceptionnelles. Cela n'a cependant pas empêché toutes les instances des forces de l'ordre américaines de solliciter des ordonnances de non-divulgation avec une durée indéterminée. À la date de publication de ce document, depuis 2017, nous avons reçu pas moins de 28 ordonnances de non-divulgation ne comportant pas de date de fin. En collaboration avec l'Union américaine pour les libertés civiles (ACLU, American Civil Liberties Union), Cloudflare a brandi la menace de poursuites judiciaires lorsque nous avons reçu ces ordonnances de non-divulgation avec une durée indéterminée. Dans chaque cas, le gouvernement a ensuite ajouté des limites de temps aux exigences de non-divulgation de ces ordonnances, ce qui nous a permis d'informer nos clients de ces demandes.

Traitement des conflits de lois

Maintenir la conformité à des législations telles que le RGPD, en particulier en présence d'ordonnances qui pourraient nous mettre dans la position difficile d'être obligés de les enfreindre, nécessite l'implication des tribunaux. Un fournisseur de services tel que Cloudflare peut demander à un tribunal d'annuler des demandes juridiques en raison d'un conflit de législations, et nous nous sommes engagés, tant dans nos déclarations publiques que contractuellement, dans notre addendum relatif au traitement des données, à prendre cette disposition si nécessaire, afin d'éviter un tel conflit. Nous considérons que le conflit doit être remis à sa juste place : entre les deux gouvernements qui se querellent pour savoir qui devrait avoir l'autorisation d'accéder à des informations.

Conclusion

Cet article ne constitue qu'une introduction à nos engagements généraux et approfondis en matière de confidentialité des données.

Pour plus d'informations sur ces engagements, veuillez consulter :

- **Notre politique de confidentialité globale** : couvre les données que nous collectons, la manière dont nous les utilisons, les données que nous communiquons et d'autres questions courantes relatives à la confidentialité.
- **Notre rapport de transparence** : des informations actualisées concernant les demandes de divulgation d'informations sur nos clients que nous avons reçues de la part d'instances juridiques.
- **Notre page d'accueil consacrée à la confidentialité et à la conformité des données** : les dernières annonces concernant la réponse qu'apportent nos politiques et nos produits aux demandes en matière de confidentialité et de conformité.

En définitive, gérer un réseau mondial qui protège les données des clients et des utilisateurs finaux (et se conforme aux différentes législations relatives à la confidentialité à travers le monde) implique de revenir aux valeurs que nous défendons depuis les débuts de notre entreprise : faire preuve de principes et de transparence, respecter la confidentialité, exiger la vigilance et informer vos clients afin qu'ils puissent prendre leurs propres décisions.

01 73 01 52 44 | enterprise@cloudflare.com | cloudflare.com/fr-fr

RÉV. : BDES-5987.2024JUL29