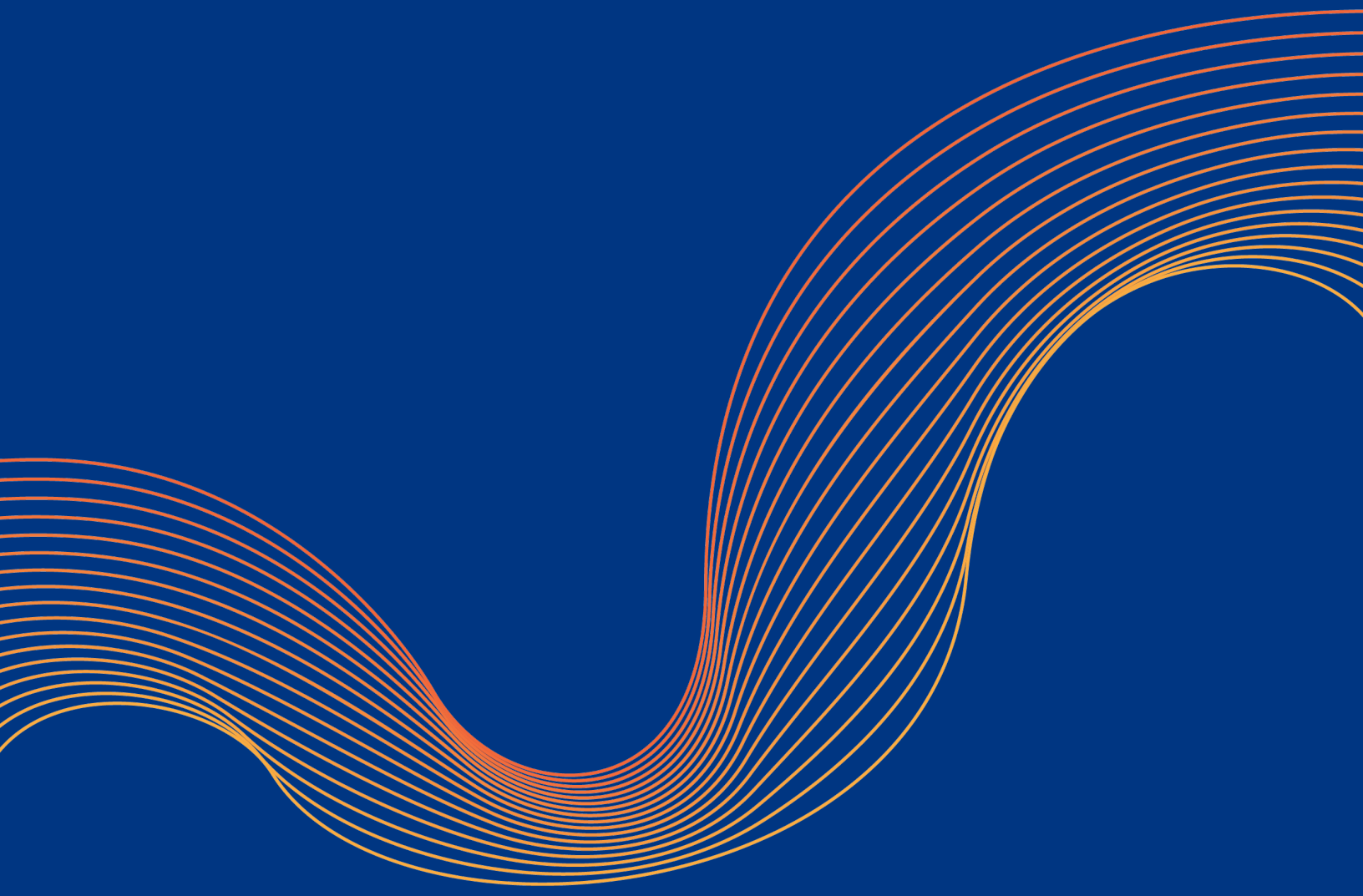
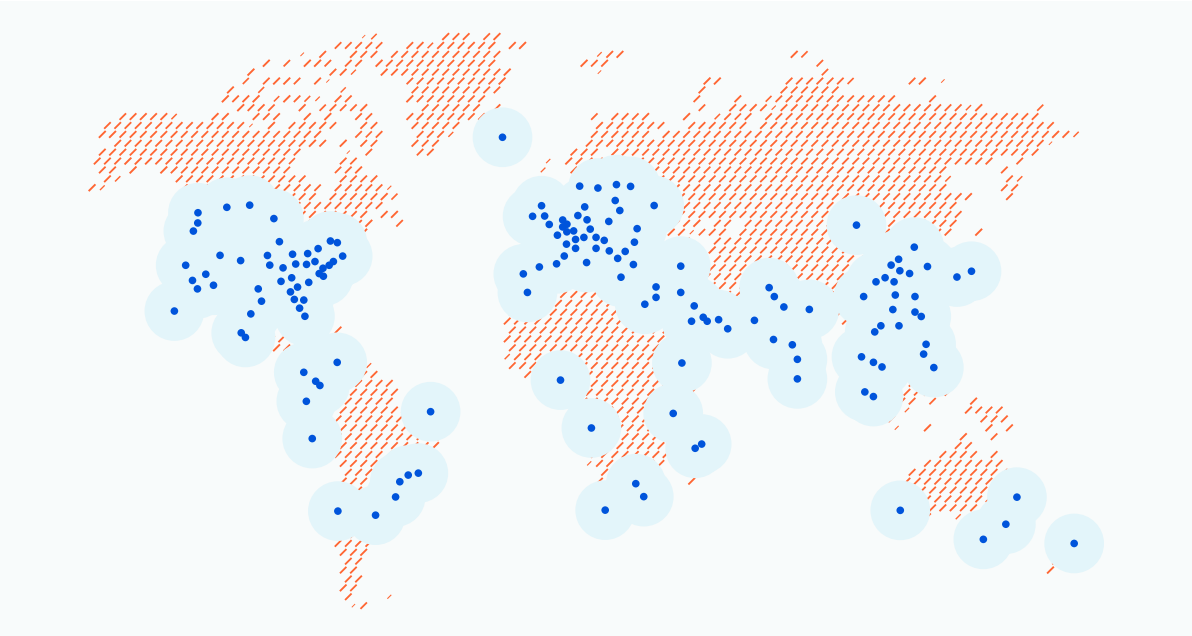
LIVRE BLANC

CLOUDFLARE

# Comment Cloudflare aide à répondre aux obligations européennes en matière de confidentialité et de localisation des données



+33 75 7 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr



*Le réseau Cloud mondial unique de Cloudflare compte plus de 200 points de présence physique répartis dans plus de 100 pays. Cloudflare fournit des outils qui vous aident à gérer la façon dont vos données confidentielles sont acheminées entre ces datacenters, afin que vous puissiez personnaliser votre trafic pour répondre à vos besoins de sécurité, de confidentialité ou encore de performance.*

## Cloudflare et la confiance des clients

Cloudflare a pour objectif de développer un meilleur Internet. Nous fournissons aux particuliers et aux entreprises de toutes tailles, partout dans le monde, une plate-forme Cloud globale offrant une vaste gamme de services réseau. Le réseau Cloudflare et son portefeuille croissant de produits renforcent la sécurité, améliorent les performances et la fiabilité de tout ce qui est connecté à Internet. En plus de servir ses clients, Cloudflare se donne également pour mission d'aider à améliorer Internet afin d'avoir un Internet toujours opérationnel et rapide, toujours sécurisé et privé, et disponible pour tous.

Le réseau Cloudflare, sa communauté de développeurs et ses activités reposent tous sur la confiance des clients. Nous aspirons à continuellement gagner et entretenir la confiance des clients en partageant clairement nos engagements en matière de confidentialité des données et la manière dont nous gérons les données des clients et des utilisateurs finaux sur nos systèmes. Nous bâtissons également la confiance en créant et en déployant des produits qui : (i) aident à améliorer la sécurité de nos systèmes, (ii) chiffrent les données au repos ou en transit et (iii) permettent à nos clients de déterminer de quelle manière et où le trafic est inspecté à différents endroits à travers le monde. Enfin, nous avons la confiance des clients en obtenant et en conservant les certifications définies par l'industrie (telle que. : SSAE 18 SOC 2 Type II) et en fournissant des mécanismes détaillant nos processus (par ex. : accords de traitement des données) qui communiquent notre modèle de responsabilité partagée avec nos clients afin de garantir la confidentialité.

## Cloudflare en Europe

Aujourd'hui, plus de 25 millions de propriétés Internet dans le monde entier utilisent Cloudflare. Parmi elles, les plus grandes entreprises européennes, les plus dynamiques d'Europe, notamment Eurovision, L'Oréal, AO.com, AllSaints et de nombreuses autres marques bien connues. Elle comprend également une liste croissante de grandes institutions européennes telles que l'INSEAD, Börse Stuttgart, l'IATA et Great Rail Journeys. À l'heure où Internet constitue une plate-forme vitale permettant aux entreprises et aux organisations de toutes tailles de servir leurs clients, leurs employés et leurs partenaires, celles-ci adoptent rapidement des réseaux Cloud sécurisés et fiables tels que Cloudflare pour les aider à protéger leurs applications et leur infrastructure Internet, ainsi que leur personnel, contre les menaces de toutes sortes.

La plate-forme Cloudflare est conçue pour soutenir les secteurs les plus réglementés et sensibles à la confidentialité des données d'Europe, tels que les services financiers, le secteur public, l'énergie, les services publics, la grande distribution, l'industrie des jeux et le secteur de la santé. Cloudflare développe ses produits afin de répondre aux normes les plus strictes en matière de sécurité et de protection de la vie privée des utilisateurs, et nous travaillons en étroite collaboration avec chacun de nos clients européens pour les aider à respecter les obligations en matière de protection des données associées à leur zone géographique et à leur secteur d'activité spécifiques.

## L'engagement unique de Cloudflare en matière de confidentialité

Cloudflare est conçu pour vous aider à améliorer votre sécurité et celle de vos clients sur Internet. Notre réseau et tous nos produits sont construits pour garantir la protection des données. Nous sommes une entreprise axée sur la confidentialité. Dans notre Politique de confidentialité, nous nous engageons à ne pas commercialiser les données personnelles que nous traitons en votre nom, ni à les utiliser à d'autres fins que la fourniture de nos services. Nous n'avons jamais trahi cette promesse depuis la création de notre entreprise. En réalité, notre politique de confidentialité a été mise en place bien avant que les gouvernements ne commencent à établir des réglementations en matière de confidentialité des données contraignant de nombreuses autres entreprises technologiques à mettre à jour leurs pratiques afin de prendre en compte la protection de la vie privée des clients et des utilisateurs. Nous ne générons pas de revenus issus de la publicité, et nous opposons donc par construction à la collecte et la conservation des données personnelles que nous traitons en votre nom.

En tant que responsable du traitement des données et fournisseur de services, Cloudflare traite les données des fichiers de log des utilisateurs finaux pour le compte de nos clients lorsque ces derniers accèdent à nos services, conformément à l'autorisation fournie par nos clients. Les données des fichiers de log ainsi traitées peuvent inclure, des adresses IP, des informations de configuration du système ainsi que d'autres informations sur le trafic à destination et en provenance de sites Web, appareils, applications et/ou réseaux de nos clients. Notre Politique de confidentialité décrit les informations que nous recueillons et comment nous utilisons les informations collectées. En outre, dans ce rôle de contrôleur de données, Cloudflare collecte et stocke les données et les logs d'activité des serveurs et du réseau dans le cadre de l'exploitation du service et effectue des observations et des analyses des données du trafic (nous nommons ces données « indicateurs de performance »). Nous pouvons citer, comme exemples d'indicateurs de performance; les mesures de continuité et de disponibilité des services, les volumes de requêtes, les taux d'erreur, les fréquences d'accès au cache et les scores de menace d'adresses IP.

Lorsque nous collectons et stockons des données d'activité sur notre réseau, nous le faisons uniquement dans le but d'améliorer nos produits pour nos clients ou pour la communauté Internet dans son ensemble. Nous ne cherchons pas à monétiser ces données de manières qui, selon nous, pourraient vous déconcerter. Par exemple, nous pouvons temporairement stocker et analyser les données de trafic réseau de l'ensemble de nos clients à travers le monde afin de permettre l'acheminement intelligent du trafic des utilisateurs finaux sur les chemins les moins encombrés et les plus fiables sur Internet. Nous pouvons également stocker et analyser les données réseau afin de détecter et d'identifier des vecteurs de menaces émergents que nous pouvons immédiatement utiliser pour mettre à jour la protection qu'offrent nos produits aux propriétés Internet de nos clients. Enfin, nous pouvons agréger des données réseau provenant d'agrégations de taille importante de nos clients (mais en aucun cas ceux d'utilisateurs ou de clients identifiables individuellement) pour aider la communauté Internet à comprendre les informations, les menaces et les tendances actuelles (voir Cloudflare Radar). Au final, les données réseau que nous collectons et stockons sont utilisées dans le seul but d'améliorer notre réseau et nos produits pour nos clients ou de partager les tendances Internet globales avec la communauté Internet dans son ensemble.

Nous présentons ci-dessous certains des engagements que nous prenons en matière de confidentialité et qui nous différencient de nombreux autres fournisseurs de services de Cloud :

- Cloudflare ne commercialise pas de données personnelles.
- Cloudflare ne suit pas l'activité des utilisateurs finaux de nos clients sur les propriétés Internet.
- Cloudflare ne procède pas au profilage des utilisateurs finaux de nos clients dans le but de vendre des publicités.
- Cloudflare ne conserve les données personnelles que lorsque c'est nécessaire pour fournir ses services à ses clients.
- Cloudflare n'a jamais fourni à quelques tiers ou gouvernements les clés de chiffrement de ses clients ou un flux de contenu clients transitant sur son réseau. Cloudflare est engagé depuis longtemps à employer tous les recours juridiques possibles avant de nous conformer à une telle requête.
- Cloudflare s'est publiquement engagé à déposer des recours juridiques pour contester toute requête du gouvernement américain concernant les données que nous identifions comme étant soumises à la réglementation RGPD.
- La politique de Cloudflare est d'informer nos clients de toute procédure juridique demandant leurs informations avant la divulgation de ces informations, sauf en cas de stricte interdiction légale.

## Fonctionnalités des produits Cloudflare conçues pour protéger les données

Nos clients européens utilisent souvent les fonctionnalités suivantes pour configurer leur déploiement de Cloudflare pour les aider à respecter leurs obligations légales en matière de traitement des données :

***Sécurité du tableau de bord et des portails :***
Le tableau de bord Cloudflare fournit une interface utilisateur simple d'utilisation, permettant aux clients de configurer et gérer l'ensemble des produits qui s'exécutent sur le réseau Cloudflare qu'ils utilisent. Les clients se connectent au tableau de bord Cloudflare via les portails Web sécurisés de Cloudflare. Pour aider les clients à garantir un accès sécurisé et autorisé aux comptes et données Cloudflare de nos clients, nous avons intégré des fonctionnalités de sécurité standard à nos portails et nos tableaux de bord. Nous avons constaté que de nombreuses entreprises et organisations rencontrent des difficultés pour sécuriser l'accès à l'ensemble de leurs différents appareils, produits et services. À l'inverse, les produits Cloudflare reposent sur une plate-forme unique, unifiée et sécurisée, de sorte que les clients Cloudflare bénéficient d'un accès homogène et fortement sécurisé aux comptes de tous leurs produits de sécurité, de performance et de fiabilité.

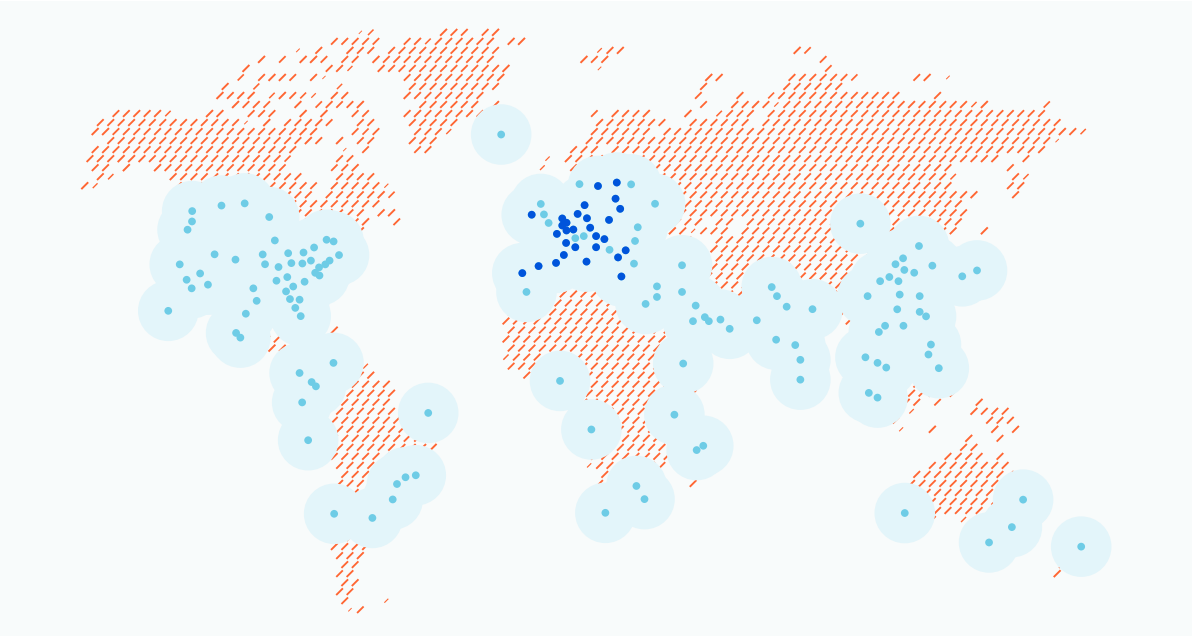
- **L'authentification à deux facteurs** (2FA) renforce la sécurité des comptes en exigeant une deuxième information pour valider l'identité de l'utilisateur lors de la connexion. La fonctionnalité Cloudflare 2FA prend en charge les jetons matériels et les applications mobiles TOTP.
- Les fonctionnalités **Single Sign-On** (authentification unique), lorsqu'elles sont activées, permettent aux clients d'avoir recours à un fournisseur d'identité sur site ou hébergé dans le Cloud pour le contrôle d'accès. Consultez la liste complète des fournisseurs pris en charge ici.
- **Les journaux d'audit** résument l'historique des accès et des modifications apportées à la configuration Cloudflare d'un client. Les journaux d'audit incluent les actions au niveau des comptes comme la connexion et la déconnexion, ainsi que les modifications des fonctionnalités DNS, Crypto, Pare-feu, Speed, Caching, Page Rules, Réseau et Trafic, etc. Les journaux d'audit sont disponibles dans tous les types de plans et sont enregistrés pour les utilisateurs individuels comme pour les organisations multi-utilisateurs.

***Chiffrement :***
le chiffrement constitue un moyen de crypter les données afin que seules les parties autorisées puissent comprendre les informations. Les données peuvent être chiffrées « au repos » lorsqu'elles sont stockées ou « en transit » lorsqu'elles sont transmises ailleurs. Le chiffrement des données transmises sur un réseau nécessite l'utilisation d'une clé de chiffrement, à savoir un ensemble de valeurs mathématiques que l'expéditeur et le destinataire d'un message chiffré connaissent.

Le chiffrement empêche les parties non autorisées (qu'il s'agisse d'auteurs d'attaques, de réseaux publicitaires, de fournisseurs d'accès Internet ou encore d'acteurs étrangers hostiles) d'intercepter et de lire les données confidentielles. Les communications chiffrées permettent aux parties communicantes d'échanger des données confidentielles sans risquer de les divulguer. Le chiffrement permet également d'éviter les comportements malveillants, tels que les attaques intermédiaires. De nombreuses réglementations industrielles et gouvernementales exigent que les entreprises gérant les données des utilisateurs maintiennent le chiffrement de ces données. Les exemples de normes réglementaires et de conformité exigeant un chiffrement incluent : HIPAA, PCI-DSS et la réglementation RGPD.

Cloudflare offre les produits réseaux et services les plus sûrs et performants, car nous acheminons via un proxy la totalité de votre trafic directement depuis la périphérie de notre réseau. En tant que proxy autorisé de votre trafic, nous effectuons une inspection sécurisée de ce dernier afin d'identifier les menaces de sécurité et d'assurer son acheminement depuis n'importe quel emplacement de notre réseau global. Cloudflare vous confère un contrôle complet sur l'endroit où a lieu l'inspection du trafic et la manière dont elle est réalisée. Cloudflare est l'un des seuls fournisseurs de Cloud à être conçu comme une plate-forme mondiale unifiée, pouvant également être configurée pour répondre à des exigences régionales spécifiques.

*Les* services régionaux permettent aux organisations de contrôler l'endroit où a lieu l'inspection de leur trafic. Lorsque les services régionaux sont activés, le trafic de contenu est ingéré sur le réseau Anycast mondial de Cloudflare à l'emplacement le plus proche du client. Au lieu d'être inspecté au niveau de ce point de présence (PoP), ce trafic est transmis de manière sécurisée aux PoP Cloudflare situés dans la région (ou les régions) sélectionnée(s) par le client, où il est ensuite traité. Si Geo Key Manager est également appliqué, les clés TLS du client sont uniquement stockées et utilisées pour gérer le trafic de contenu dans ces régions. Les services régionaux aident les clients qui souhaitent conserver un contrôle local sur leur trafic tout en conservant les avantages de sécurité d'un réseau mondial. Par exemple, un client Cloudflare en Allemagne pourrait permettre aux services régionaux de restreindre les services à l'UE. Ses clients utilisateurs finaux se connecteront à l'emplacement Cloudflare le plus



proche, où qu'il soit dans le monde, mais si cet emplacement est situé en dehors de l'UE, le trafic est transféré vers un emplacement de Cloudflare dans l'UE avant d'y être inspecté. Le client bénéficie toujours de notre réseau mondial, à faible latence et à haut débit, capable de résister même aux attaques DDoS les plus vastes. Néanmoins, les services régionaux fournissent également aux clients un contrôle local : seuls les datacenters situés dans l'UE disposent de l'accès nécessaire pour appliquer les politiques de sécurité. Cette approche permet à Cloudflare de sélectionner l'itinéraire le plus rapide vers l'UE et le point de présence disponible le plus proche pour le traitement.

En plus d'indiquer l'endroit où a lieu d'inspection du trafic, Cloudflare aide les entreprises à protéger les utilisateurs et les données en recourant à des techniques et des technologies de chiffrement les plus avancées. Geo Key Manager et Keyless SSL fournissent aux clients un contrôle total de l'emplacement de stockage des clés et des PoP qui ont accès à ces clés.

Keyless SSL permet à un client de stocker et gérer ses propres clés privées SSL pour les utiliser avec Cloudflare. Les clients peuvent utiliser de nombreux systèmes différents pour leur système de gestion de clés, notamment des modules de sécurité matérielle (« HSM »), des serveurs virtuels ainsi que du matériel exécutant Unix/Linux et Windows hébergé dans des environnements contrôlés par les clients. Keyless SSL fait appel à plusieurs méthodes pour créer une connexion sécurisée pour la transmission de la clé du client à Cloudflare, et fournit une persistance de session qui accélère généralement la vitesse de la transaction SSL globale.

Geo Key Manager fournit aux clients un contrôle granulaire de l'emplacement de stockage de leurs clés. Par exemple, un client peut choisir que les clés privées soient uniquement accessibles à l'intérieur des PoP situés dans l'UE.

Avec Cloudflare, les clients disposent, d'une part, d'un contrôle étendu de l'emplacement de stockage des clés privées, mais également de l'endroit où est réellement inspecté le trafic pour la détection des menaces de sécurité. Si un client en fait le choix, seuls les PoP situés dans les États membres de l'UE permettent l'inspection du trafic.

## Certifications de sécurité mondiales et européennes de Cloudflare

Cloudflare répond aux normes les plus strictes de l'industrie en matière de sécurité et de confidentialité, et valide chaque année ces engagements avec des auditeurs tiers. Cloudflare est conforme aux normes ISO 27001/27002, Payment Card Industry Data Security Standards (PCI DSS) et SSAE 18 SOC 2 Type II. Nous avons signé des accords de partenariat et sommes en mesure de soutenir les entreprises soumises à la loi américaine Health Insurance Portability and Accountability Act of 1996 (HIPAA). Ces validations fournissent une assurance aux organisations qui transfèrent leurs données les plus confidentielles via nos services, et les aident également à garantir le respect de leurs propres obligations en matière de conformité.

En plus des évaluations régulières effectuées par des tiers conformément aux normes de l'industrie, Cloudflare est considéré comme un « opérateur de services essentiels » en vertu de la directive européenne sur la sécurité des réseaux et des systèmes d'information (directive NIS). En plus d'être enregistré, en vertu de cette directive, auprès de l'ICO et de l'Ofcom au Royaume-Uni, du BSI en Allemagne et du CNCS au Portugal, Cloudflare a également été évalué conformément à des exigences régionales spécifiques, telles que la loi BSI en Allemagne (BSIG). Nous sommes attachés à nos relations et travaillons en étroite collaboration avec les régulateurs régionaux européens en matière de conformité, et nous fournissons des informations sur la manière dont nous répondons aux exigences en matière de protection des données.

Sur le plan pratique, la réglementation décisive RGPD (Règlement général sur la protection des données) européenne incarnait une codification de bon nombre des mesures que nous prenions déjà :

- Cloudflare collecte uniquement les données personnelles dont elle a besoin pour fournir le service qu'elle propose.
- Cloudflare ne vend pas de données personnelles.
- Cloudflare fournit aux individus la possibilité de consulter, corriger ou supprimer leurs données personnelles.
- Conformément à son rôle de responsable du traitement des données, Cloudflare offre aux clients le contrôle des informations qui, par exemple, sont mises en cache sur son réseau de diffusion de contenu (CDN), stockées dans le magasin de valeurs de clés Workers ou capturées par son pare-feu d'applications Web (WAF).

Vous pouvez consulter notre FAQ sur la réglementation RGPD ici : cloudflare.com/gdpr/introduction.

Parce que nous nous soucions de la protection des données, nous ne limitons pas nos audits aux seuls aspects requis par la loi ou par la disponibilité de certifications. Notre équipe de sécurité effectue des tests d'intrusion interne et externe rigoureux, nous avons mis en place un programme de primes pour la recherche de bugs via HackerOne et nous engageons des auditeurs tiers pour valider nos engagements en matière de confidentialité. Des exemples probants sont les audits axés sur la confidentialité, comme celui que nous avons réalisé plus tôt cette année en relation avec nos engagements relatifs à notre résolveur DNS public 1.1.1.1. Nous sommes toujours ouverts à l'obtention de validations supplémentaires qui fourniront une assurance concernant notre programme de confidentialité, nos politiques et nos pratiques en matière de traitement et de stockage des données personnelles au sein de l'UE.

## Les mécanismes de transfert de données de Cloudflare

Les types de données personnelles que Cloudflare traite pour le compte d'un client dépendent des services Cloudflare mis en œuvre. La grande majorité des données qui transitent par le réseau Cloudflare demeurent sur les serveurs de périphérie de Cloudflare, tandis que les données des journaux relatifs à cette activité peuvent être traitées pour le compte de nos clients dans notre datacenter principal situé aux États-Unis – même lorsque les clients activent les services régionaux.

Certaines de ces données de journaux incluent des informations sur les visiteurs et les utilisateurs autorisés des domaines, réseaux, sites Web, interfaces de programmation d'application (« API ») ou applications de nos clients. Ces métadonnées contiennent des données personnelles extrêmement limitées, le plus souvent sous forme d'adresses IP. Nous traitons ce type d'informations pour le compte de nos clients dans notre datacenter principal situé aux États-Unis, pendant une période limitée.

Étant donné que certaines données personnelles limitées sont transférées vers les États-Unis, nous avons facilité la tâche des entreprises qui souhaitent maintenir un mécanisme de transfert de données valide lors de l'utilisation des services de Cloudflare. Notre accord de traitement des données standard (DPA) est intégré à notre accord de service pour entreprises, et l'accord DPA intègre les clauses contractuelles standard de l'UE (SCC) relatives aux données soumises à la réglementation RGPD. Ensemble, les conditions de Cloudflare garantissent un niveau de protection des données personnelles équivalent à celui garanti par la réglementation RGPD. Vous trouverez plus d'informations concernant notre engagement au regard de la réglementation RGPD et sur notre accord DPA ici.

Le 16 juillet 2020, la Cour de justice de l'Union européenne (« CJUE ») a rendu une décision invalidant le paradigme du « Privacy Shield » (bouclier de protection des données) UE-États-Unis dans l'affaire « Schrems II ». En conséquence, certains de nos clients traitant les données de résidents de l'UE nous ont demandé ce que cette décision signifiait au regard de la légalité du transfert des données traitées par Cloudflare en leur nom vers les États-Unis. Tout d'abord, l'invalidation du Privacy Shield ne modifie pas les solides mesures de protection de la confidentialité des données mises en place par Cloudflare pour les données personnelles que nous traitons pour le compte de nos clients, et nous continuerons à observer les principes de protection des données que nous nous sommes engagés à honorer lors de notre certification en vertu du Privacy Shield.

En vertu de la décision Schrems II, les SCC approuvés par l'UE demeurent un mécanisme de transfert valide dans le cadre de la réglementation RGPD, où des garanties supplémentaires sont également mises en œuvre pour les données transférées vers les États-Unis. Cloudflare continuera à utiliser le mécanisme des SCC pour les transferts de données, et nous avons mis à jour notre accord DPA client standard afin d'incorporer des garanties supplémentaires sous forme d'engagements contractuels. Par exemple, nous nous engageons à déposer des recours légaux pour contester toute requête éventuelle des autorités américaines concernant les données que nous identifions comme étant soumises à la réglementation RGPD, et nous nous engageons à informer nos clients de toute procédure juridique demandant leurs informations avant la divulgation de ces informations, sauf en cas d'interdiction légale. Vous pouvez consulter les garanties supplémentaires que nous avons ajoutées sous forme d'engagements contractuels à la section 7 de notre accord DPA.

Les réglementations et directives en matière de protection des données évoluent continuellement, et nous surveillons de près le paysage réglementaire et législatif. Nous prêtons continuellement attention aux orientations émergentes afin de nous assurer que nos clients et partenaires puissent continuer à profiter des avantages offerts par Cloudflare dans toute l'Europe.

## Opportunités et responsabilités partagées

Parce que nous savons que toutes les organisations européennes doivent intégrer les principes de confidentialité et de sécurité à chaque phase de leurs activités, nous avons préparé ce tableau pour vous permettre de comprendre facilement qui a la responsabilité de ces exigences fréquemment demandées en matière de confidentialité :

| Principe | Responsabilité | Détails de la responsabilité |
|---|---|---|
| Protection des données intrinsèque | Partagée | Cloudflare est responsable de la fourniture de produits et de services conçus pour respecter la confidentialité. L'équipe chargée de la protection des données fournit des études, des évaluations et des formations pour garantir que la confidentialité est indissociable de notre méthode de travail.<br><br>Les clients sont responsables de leur utilisation et de la configuration de leurs services Cloudflare, et doivent périodiquement les évaluer pour confirmer que les principes de protection des données ont été pris en compte dans la conception et la mise en œuvre. |
| Demande d'accès du sujet des données | Partagée | Cloudflare fournit aux personnes concernées le droit d'accès, de rectification et de suppression des données personnelles, quelle que soit leur juridiction de résidence. Les demandes des personnes concernées peuvent être envoyées à l'adresse sar@cloudflare.com.<br><br>Si nous recevons une requête de la part d'une personne apparaissant être un utilisateur final de l'un de nos clients, nous demandons à cette personne de contacter directement notre client. |

| Principe | Responsabilité | Détails de la responsabilité |
|---|---|---|
| Sécurité | Partagée | Cloudflare gère un programme de sécurité conforme aux normes de l'industrie. Le programme de sécurité inclut la gestion de politiques et de procédures de sécurité formelles, l'établissement de contrôles d'accès logiques et physiques appropriés, la mise en œuvre de garanties techniques au sein des environnements d'entreprise et de production (notamment l'établissement de configurations sécurisées, la transmission et les connexions sécurisées, la journalisation et la surveillance), ainsi que la mise en place de technologies de chiffrement adéquates pour les données personnelles.<br><br>Les clients sont responsables de l'examen du niveau de sécurité de leurs fournisseurs de Cloud, tels que Cloudflare, et peuvent le faire en étudiant nos validations et nos rapports de conformité. Nous encourageons également nos clients à examiner les paramètres de sécurité de leur tableau de bord afin de s'assurer qu'ils sont conformes à leurs politiques et procédures de sécurité. |
| Fondement juridique du traitement | Partagée | Cloudflare traite les données conformément aux instructions de nos clients (les contrôleurs de données) et opère en tant que responsable du traitement des données conformément à la réglementation RGPD.<br><br>Il incombe aux clients de s'assurer qu'ils disposent d'un fondement juridique approprié pour le traitement des données de leurs utilisateurs finaux. |
| Violations de données personnelles | Partagée | Cloudflare informera les clients dès qu'elle aura connaissance d'une quelconque violation de la sécurité entraînant la perte, la divulgation non autorisée ou l'accès à des données personnelles traitées par Cloudflare ou ses sous-traitants. Cloudflare a également la responsabilité de fournir à ses clients une coopération et une assistance raisonnables en cas de découverte d'une violation, et notamment en fournissant aux clients les informations raisonnables que détient Cloudflare concernant les circonstances de la violation et les données personnelles concernées.<br><br>Les clients sont tenus de se conformer aux exigences réglementaires ou contractuelles requérant d'informer leurs utilisateurs finaux et/ou les autorités gouvernementales de toute violation des données personnelles. |

## Un réseau de Cloud mondial fondé sur la confiance des clients

La priorité de Cloudflare est de gagner et de maintenir la confiance des clients. Nous comprenons que la transparence concernant les engagements de confidentialité de Cloudflare, ainsi que notre approche de l'intégration des protections en matière de confidentialité et de localisation des données sur notre réseau et dans nos produits, aide les clients à satisfaire à leurs propres obligations. Nous comprenons également que les certifications sectorielles de Cloudflare et que les mécanismes d'attribution de contrats pertinemment conçus nous aident à établir une relation de confiance solide avec nos clients européens.

Les équipes chargées de la protection des données et de la sécurité de Cloudflare se tiennent prêtes à collaborer avec vous, afin de répondre aux exigences les plus strictes auxquelles vous pourriez être confronté(e) dans votre pays, région ou secteur. Nos chargés de compte, nos responsables Customer Success et nos ingénieurs commerciaux expérimentés s'associent régulièrement à nos équipes chargées de la conformité en matière de confidentialité et de sécurité pour aider nos clients à configurer les produits Cloudflare qu'ils utilisent, afin de répondre à leurs obligations spécifiques en matière de conformité. Si vous souhaitez une démonstration ou une session spécialisée consacrée à la configuration de vos services afin de répondre à vos obligations uniques, contactez-nous dès aujourd'hui. Veuillez nous envoyer un e-mail à l'adresse suivante : privacyquestions@cloudflare.com ou security@cloudflare.com.

## EN SAVOIR PLUS

1. **Comprendre les services de journaux Cloudflare**
2. **Gestion et analyse des journaux**
3. **FAQ sur les journaux**
4. **Contactez-nous** pour activer les services régionaux