WHITEPAPER

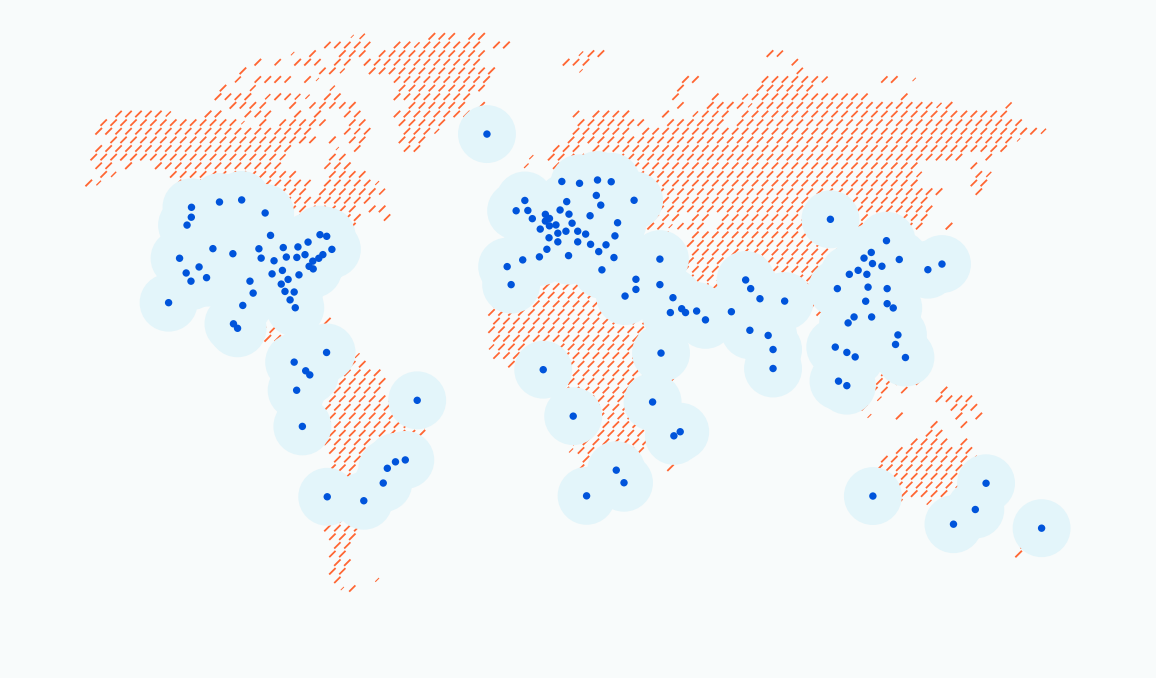
CLOUDFLARE

Protection et régionalisation des données en Europe : Cloudflare contribue à aider ses clients à répondre à cette obligation

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

SYNTHÈSE

- Dès sa création, Cloudflare a eu pour objectif de faire bénéficier ses clients d'une meilleure sécurité sur Internet. Nous avons à cœur la confidentialité des données de nos clients, et c'est dans cet esprit que nous avons conçu notre réseau, ainsi que l'ensemble de nos produits et services.
- Cloudflare met en œuvre un nombre important de protections légales et contractuelles, qui sont conformes au règlement général sur la protection des données (RGPD) de l'Union européenne.
- Cloudflare propose, à ses clients qui ne souhaitent pas que leurs données quittent l'Europe, une suite de produits technologiques de pointe.



Avec des datacenters présents dans plus de 250 villes dans plus de 100 pays, Cloudflare offre à ses clients un réseau unique. Cloudflare vous fournit les outils qui vous permettent de gérer de quelle manière vos données sont acheminées au sein de ces datacenters, vous permettant ainsi de librement choisir l'endroit où est inspecté votre trafic, d'une manière qui répond à vos besoins en matière de sécurité, de confidentialité et de performances.

À propos de Cloudflare

La mission de Cloudflare est de contribuer à bâtir un Internet meilleur. Nous proposons une plateforme de Cloud mondiale, qui fournit une vaste gamme de services réseau aux particuliers et aux entreprises de toute taille, et ce, dans le monde entier. Le réseau de Cloudflare et son portefeuille croissant de produits améliorent la sécurité, la confidentialité, les performances et la fiabilité de tous les équipements connectés à Internet. En plus de servir ses clients, Cloudflare se donne pour mission de contribuer à améliorer l'Internet lui-même – toujours actif, toujours rapide, toujours sécurisé, toujours privé et accessible à tous.

Le réseau, la communauté de développeurs et l'activité de Cloudflare se fondent sur la confiance que nous portent nos clients. Nous aspirons à continuellement gagner et conserver cette confiance en expliquant clairement nos engagements en matière de confidentialité des données et comment nous gérons les données des clients et des utilisateurs finaux qui transitent au sein de nos systèmes. Par ailleurs, nous concevons et déployons des produits qui (i) contribuent à améliorer la sécurité de nos systèmes, (ii) chiffrent les données au repos ou en transit et (iii) permettent à nos clients de déterminer comment le trafic est inspecté dans différents endroits du monde. Enfin, comme garant de notre pacte de confiance, nous travaillons à obtenir et maintenir les plus importantes certifications imposées par l'industrie (par exemple, ISO 27001 et 27701, SSAE 18 et SOC 2 Type II) et à fournir des mécanismes contractuels (par exemple, des accords relatifs au traitement des données), permettant de communiquer notre modèle de responsabilité partagée avec nos clients en matière de protection de la confidentialité des données.

Cloudflare en Europe

Aujourd'hui, des millions de propriétés Internet dans le monde utilisent Cloudflare. Cette liste inclut un nombre important d'entreprises figurant parmi les plus dynamiques et iconiques d'Europe telles que L'Oréal, ainsi qu'Eurovision, L'Oréal, AO.com, C&A et AllSaints. Elle comprend également un nombre croissant d'institutions européennes renommées parmi lesquelles

l'INSEAD, Börse Stuttgart, IATA et Telefónica. De plus en plus d'entreprises et organisations, du grand groupe à la startup en passant par les PME et ETI, considèrent l'Internet comme une plateforme essentielle pour servir leurs clients, leurs utilisateurs et leurs intervenants ; elles adoptent rapidement des réseaux de Cloud sécurisés et fiables, tels que Cloudflare, pour améliorer la protection de leurs applications, leurs infrastructures et leurs collaborateurs connectés à Internet contre toutes sortes de menaces.

Nous sommes conscients que la protection des données en Europe présente des défis uniques. Certains de ces défis résultent du Règlement général sur la protection des données (RGPD) de l'Union européenne et de la décision de la Cour de justice de l'Union européenne dans l'affaire « Schrems II » (affaire C-311/18, Commissaire à la protection des données contre Facebook Ireland et Maximillian Schrems), cette dernière ayant entraîné des exigences supplémentaires pour les entreprises qui transfèrent des données personnelles hors de l'UE. En outre, un certain nombre de secteurs fortement réglementés exigent que des catégories spécifiques de données personnelles restent à l'intérieur des frontières de l'UE.

À ce titre, la plateforme Internet de Cloudflare est conçue pour fournir des services aux secteurs européens les plus réglementés et les plus exigeants quant à la confidentialité des données, notamment les services financiers, le secteur public, l'énergie, les commodités, la vente au détail, les jeux et la santé. Chez Cloudflare, nous concevons nos produits pour répondre aux normes les plus strictes en matière de sécurité et de confidentialité des données des utilisateurs. Pour ce faire, nous travaillons en étroite collaboration avec chacun de nos clients européens pour les aider à respecter les obligations de protection des données associées à leur région et leur secteur d'activité spécifiques. Nous y parvenons par différents moyens, notamment:

- Notre engagement global en faveur de la confidentialité des données
- Le maintien de certifications de sécurité mondiales et européennes
- Le maintien de mécanismes de transfert de données conformes au règlement RGPD
- La mise en œuvre de fonctionnalités et de produits prenant en charge la régionalisation des données

Ce document développe en détail les moyens mis à votre disposition.

L'engagement unique de Cloudflare en faveur de la confidentialité des données

Le réseau Cloudflare a été conçu pour vous aider, vous et vos clients, à bénéficier d'une meilleure sécurité sur Internet. La confidentialité est au cœur de nos préoccupations : notre réseau et l'ensemble de nos produits sont conçus dans l'optique de la protection des données. Nous nous engageons, dans notre politique de confidentialité, à ne pas revendre les données personnelles que nous traitons pour votre compte et à ne pas les utiliser à d'autres fins que la mise en œuvre des services que nous vous proposons. Tout au long de notre histoire, nous n'avons jamais trahi cette promesse. En réalité, nous avons défini notre engagement concernant la confidentialité des données bien avant que les gouvernements ne commencent à mettre en place des réglementations relatives à la confidentialité des données. Ces nouvelles exigences ont contraint de nombreuses entreprises technologiques à actualiser leurs pratiques, afin de privilégier en conséquence la confidentialité des données de leurs clients et leurs utilisateurs. Nous ne générons aucun revenu de la publicité (et nous ne créons pas de profils des utilisateurs finaux de nos clients ou de leurs données à quelque fin que ce soit), et nous ne procédons donc, par défaut, à aucune opération de collecte et de conservation des données personnelles que nous traitons en votre nom.

Vous trouverez ci-dessous quelques exemples des engagements que nous prenons pour préserver la confidentialité des données. Il s'agit d'un point important qui nous différencie de nombreux autres fournisseurs de services de Cloud :

- Cloudflare ne revend pas de données personnelles.
- Cloudflare ne trace pas les utilisateurs finaux de ses clients sur les propriétés Internet.

- Cloudflare ne crée pas de profils des utilisateurs finaux de ses clients en vue d'obtenir des revenus publicitaires.
- Cloudflare conserve uniquement les données personnelles dans la mesure requise pour fournir les offres de Cloudflare à ses clients.
- Cloudflare n'a jamais fourni à un tiers ou à un gouvernement les clés de chiffrement de ses clients ou un flux de contenu d'un client transitant sur notre réseau, et l'entreprise s'est engagée de longue date à épuiser tous les recours juridiques disponibles avant d'accéder à une telle demande.
- Cloudflare s'est publiquement engagée à exercer des recours juridiques pour contester toute demande du gouvernement américain concernant des données que nous identifions comme étant concernées par le règlement RGPD.
- La politique de Cloudflare prévoit, sauf interdiction légale, d'informer ses clients de toute procédure juridique requérant leurs informations avant de divulguer ces dernières.

Les certifications de sécurité mondiales et européennes de Cloudflare

En matière de sécurité et de confidentialité des données, Cloudflare se conforme aux normes les plus strictes de l'industrie, et fait appel chaque année à des auditeurs tiers pour valider ces engagements.

Cloudflare a été certifiée conformément à une nouvelle norme internationale de confidentialité des données encadrant la protection et la gestion du traitement des données personnelles, ISO/IEC 27701:2019. Cette norme a moins de deux ans et adapte le concept existant de système de management de la sécurité de l'information dans la création d'un système de management de la protection de la vie privée (PIMS). La norme comporte des exigences visant à assurer que ce système de management de la protection de la vie privée est robuste, et qu'il fait l'objet d'améliorations continues, afin d'atteindre les objectifs définis. La norme est conçue de telle manière que les exigences auxquelles doivent satisfaire les organisations pour être certifiées sont très étroitement alignées sur les exigences du règlement RGPD.

En termes simples, la certification ISO 27701 assure à nos clients que nous disposons d'un programme de confidentialité des données évalué par un tiers, conforme à une norme internationale de l'industrie alignée sur le règlement RGPD, et que ce programme nous contraint à continuellement maintenir la conformité de notre programme de confidentialité des données. Cette certification, en plus de l'Addenda relatif au traitement des données (« ATD ») que nous mettons à la disposition de nos clients depuis le tableau de bord, assure de différentes manières à nos clients que toutes les données personnelles traitées par Cloudflare seront gérées d'une manière conforme aux exigences du RGPD.

En outre, Cloudflare est conforme aux normes ISO 27001/27002, Payment Card Industry Data Security Standards (PCI DSS) et SSAE 18 SOC 2 Type II. Ces validations offrent une assurance aux organisations qui sollicitent nos services pour transférer leurs données les plus sensibles, et les aident également à respecter et maintenir leurs propres obligations en matière de conformité.

Outre les évaluations régulières effectuées par des tiers conformément aux normes de l'industrie, Cloudflare est considérée 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 de s'être enregistrée conformément à cette directive auprès des organisations ICO et Ofcom au Royaume-Uni, BSI en Allemagne et CNCS au Portugal, Cloudflare a également été évaluée conformément à des exigences régionales spécifiques, telles que la législation BSIG en Allemagne. Nous cultivons 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, le règlement RGPD a constitué une codification des nombreuses mesures que nous mettions déjà en œuvre.

- Cloudflare collecte uniquement les données personnelles nécessaires à la fourniture du service que nous proposons.
- Cloudflare ne revend pas de données personnelles.
- Cloudflare offre aux personnes la possibilité de consulter, corriger ou supprimer leurs données personnelles.
- Conformément à son rôle de responsable du traitement des données, Cloudflare donne aux clients le contrôle des informations qui, par exemple, sont mises en cache sur son réseau de diffusion de contenu (CDN), stockées dans le référentiel clé-valeur de Workers ou capturées par notre pare-feu d'applications web (WAF).

Vous pouvez en apprendre davantage sur notre engagement envers la conformité au règlement RGPD ici :

https://www.cloudflare.com/trust-hub/gdpr/.

Parce que la protection des données nous tient à cœur, nous ne nous contentons pas d'effectuer des audits lorsque la loi nous y oblige ou lorsque des certifications sont disponibles. Notre équipe de spécialistes de la sécurité exécute des tests de pénétration internes et externes rigoureux, nous gérons un programme de primes aux bugs par l'intermédiaire de HackerOne et nous faisons appel à des auditeurs tiers pour valider nos engagements en matière de confidentialité des données. Les audits priorisant la confidentialité des données, à l'image de celui que nous avons réalisé conformément à nos engagements pour notre résolveur DNS public 1.1.1.1, en sont des exemples pertinents. Nous sommes toujours prêts à obtenir des validations supplémentaires susceptibles d'offrir une assurance concernant notre programme de protection de la confidentialité des données, nos politiques et nos pratiques relatives au traitement et au stockage des données personnelles au sein de l'UE.

Les données que traite Cloudflare

Cloudflare traite les données de logs des utilisateurs finaux des clients lorsque les utilisateurs finaux accèdent à ses services conformément à l'autorisation des clients. Ces données de logs peuvent inclure, sans s'y limiter, des adresses IP, des informations sur la configuration des systèmes et d'autres informations sur le trafic vers et depuis les sites web, les appareils, les applications et/ou les réseaux des clients. Par ailleurs, Cloudflare collecte et stocke des données et des logs d'activité de serveurs et de réseaux dans le cadre de l'exploitation de ses produits, et réalise également des observations et des analyses des données du trafic. Notre politique de confidentialité décrit plus spécifiquement les informations que nous collectons et la manière dont nous utilisons les informations collectées.

Lorsque nous collectons et stockons des données provenant de l'activité sur notre réseau, elle le fait uniquement pour améliorer nos produits pour vous, pour nos autres clients ou pour la communauté Internet au sens large. Nous ne cherchons pas à monétiser ces données d'une manière qui pourrait vous surprendre. Par exemple, nous pouvons stocker temporairement et analyser les données du trafic réseau de tous nos clients internationaux, afin d'acheminer intelligemment les requêtes sur les chemins Internet les plus efficaces. Nous pouvons également stocker et analyser des données réseau, afin de détecter et d'identifier des vecteurs de menaces émergentes que nous pouvons immédiatement utiliser pour améliorer nos outils de sécurité. Enfin, nous pouvons agréger des données réseau provenant de segments de clientèle de taille significative (mais jamais d'utilisateurs ou de clients individuellement identifiables), afin d'aider la communauté Internet à comprendre les tendances et les menaces sur Internet (voir Cloudflare Radar).

Mécanismes de transfert de données de Cloudflare

Dans le cas où Cloudflare, en tant que responsable du traitement des données, transfère des données à caractère personnel hors de l'UE, cela est fait conformément à notre accord standard relatif au traitement des données (ATD), incorporé dans notre contrat de service Enterprise, ainsi que dans notre contrat d'abonnement libre-service. Notre ATD intègre les clauses contractuelles types (CCT) de l'UE (telles que mises à jour en 2021) pour les données soumises au règlement RGPD. Prises ensemble, les conditions de Cloudflare assurent un niveau de protection des données personnelles équivalent à celui garanti par le règlement RGPD. Vous trouverez plus d'informations sur notre engagement envers le règlement RGPD et sur notre ATD ici.

Conformément à la décision Schrems II, les CCT approuvées par l'UE restent un mécanisme de transfert valide, conformément au règlement RGPD, lorsque des garanties supplémentaires sont également en place pour les données transférées vers les États-Unis. Cloudflare continuera à utiliser le mécanisme des CCT pour les transferts de données, et nous avons mis à jour notre ATD standard pour nos clients afin d'intégrer des garanties supplémentaires sous la forme d'engagements contractuels. Par exemple, nous nous engageons à exercer des recours juridiques afin de contester toute demande du gouvernement américain concernant des données que nous identifions comme étant soumises au règlement RGPD, et nous nous engageons à informer nos clients au sujet de toute procédure juridique demandant leurs informations avant la divulgation de ces informations, sauf interdiction légale. Vous pouvez consulter les mesures de protection supplémentaires que nous avons ajoutées sous la forme d'engagements contractuels dans la section 7 de notre ATD.

Les réglementations et directives en matière de protection des données évoluent continuellement, et nous surveillons de près l'environnement réglementaire et législatif. Nous examinons continuellement les orientations émergentes afin de nous assurer que nos clients et partenaires puissent continuer à profiter des avantages de Cloudflare dans toute l'Europe.

Pour les clients qui doivent s'assurer que Cloudflare ne transfère pas leurs données personnelles, nous proposons une solution complète, Cloudflare Data Localization Suite (DLS).

Fonctionnalités de produits de Cloudflare conçues pour prendre en charge la localisation des données

Cloudflare s'engage à aider ses clients à conserver les données personnelles au sein de l'UE. Avec Data Localization Suite, nous permettons aux clients de maîtriser l'endroit où leurs données sont inspectées et conservées.

Data Localization Suite comporte trois éléments :

1. Gestion des clés de chiffrement (Geo Key Manager et SSL sans clé)
2. Isolement géographique de l'inspection des charges utiles (services régionaux)
3. Isolement géographique des métadonnées du client

Gestion des clés de chiffrement:

La confidentialité des données n'est possible qu'avec un Internet sécurisé, ce que permet en grande partie un chiffrement efficace.

Le chiffrement des données transmises sur un réseau nécessite l'utilisation de clés de chiffrement, c'est-à-dire d'ensembles de valeurs mathématiques que connaissent à la fois l'expéditeur et le destinataire d'un message chiffré. SSL/TLS, un protocole cryptographique qui rend possibles les communications chiffrées, utilise une paire de clés : une clé publique et une clé privée. Pour s'assurer que leurs clés privées ne quittent pas l'UE, les clients de Cloudflare peuvent choisir entre deux fonctionnalités :

- La fonctionnalité SSL sans clé permet aux clients de stocker et gérer leurs propres clés privées afin de les utiliser avec Cloudflare. Les clients peuvent utiliser différents systèmes pour leur

magasin de clés, notamment des modules de sécurité matérielle (HSM), des serveurs virtuels et des équipements exécutant Unix/Linux et Windows, hébergés dans des environnements contrôlés par les clients. La fonctionnalité SSL sans clé est uniquement « sans clé » du point de vue de Cloudflare : Cloudflare ne voit jamais la clé privée du client, mais le client peut accéder à celle-ci et l'utiliser. Pendant ce temps, la clé publique est toujours utilisée côté client, comme à l'accoutumée.

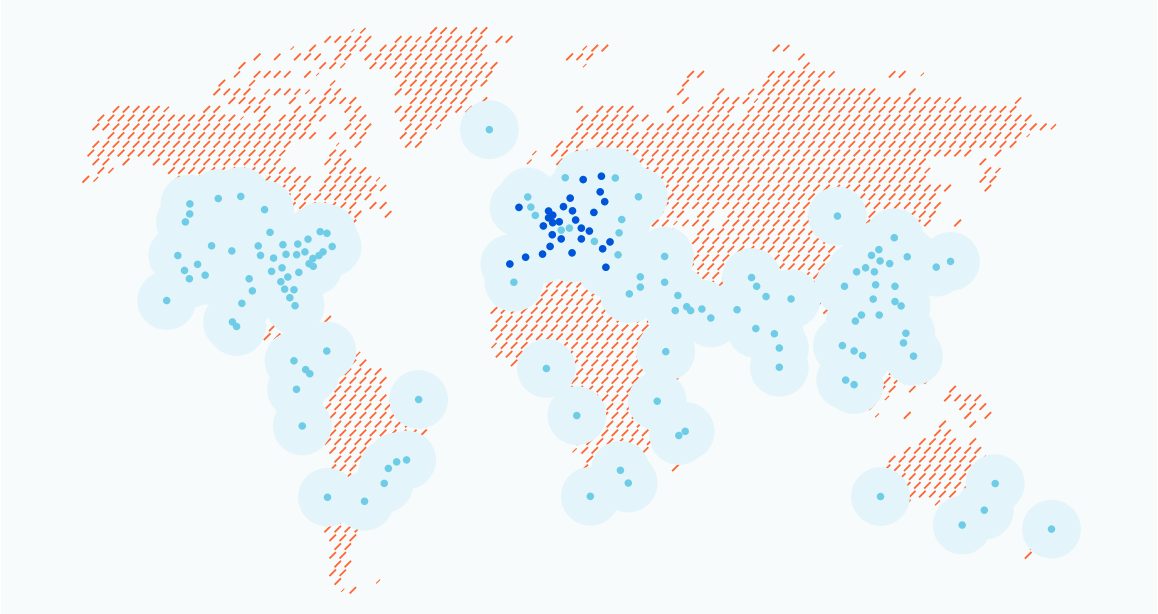
- Geo Key Manager offre aux clients un contrôle granulaire sur les datacenters dans lesquels sont stockées leurs clés privées. Par exemple, un client peut souhaiter que les clés privées soient uniquement accessibles dans des datacenters situés dans l'UE. Cette approche soulage les clients de la complexité inhérente au déploiement de la fonctionnalité SSL sans clé et de la maintenance de leur propre magasin de clés.

Isolement géographique de l'inspection des charges utiles (payload) :

Cloudflare propose les services réseau les plus sûrs et performants grâce à un proxy pour l'ensemble de votre trafic depuis la périphérie de notre réseau. En tant que proxy autorisé de votre trafic, nous déployons des services qui inspectent votre trafic en toute sécurité, afin d'identifier les menaces de sécurité et de l'acheminer depuis n'importe quel endroit sur notre réseau mondial. Cloudflare est l'un des seuls fournisseurs de Cloud dont l'architecture propose une plateforme mondiale unifiée pouvant également être configurée pour répondre à des besoins régionaux spécifiques. Cette architecture offre aux clients de Cloudflare un contrôle intégral de l'endroit et de la manière où se déroule l'inspection du trafic.

Les services régionaux de Cloudflare permettent aux clients de choisir, sur le réseau Cloudflare, l'endroit où se terminent leurs connexions TLS. Par exemple, un client peut choisir que ces connexions se terminent dans l'UE, afin que le déchiffrement et l'inspection du contenu du trafic HTTP se déroulent exclusivement au sein de l'UE. Cette restriction s'applique à tous nos services d'application en périphérie, notamment :

- Le stockage et la récupération de données à partir du cache ;
- Le blocage de messages HTTP malveillants avec le pare-feu d'applications web (WAF) ;
- La détection et le blocage d'activités suspectes avec la solution de gestion des bots ;
- L'exécution de scripts Workers.



Un scénario d'utilisation hypothétique serait celui d'un client de Cloudflare en Allemagne utilisant les services régionaux pour restreindre ses services à l'UE. Ses clients utilisateurs finaux se connectent au point de présence de Cloudflare le plus proche, où qu'il soit dans le monde, mais si cet endroit se trouve hors de l'UE, le trafic est transmis au un site point de présence de Cloudflare dans l'UE avant d'être inspecté. Le client bénéficie toujours de notre réseau mondial à faible latence et à haut débit, capable de résister aux attaques DDoS les plus importantes. Toutefois, les services régionaux offrent 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, ainsi que le point de présence disponible le plus proche aux fins du traitement.

Isolement géographique des métadonnées de clients :

L'isolement géographique des métadonnées de clients de Cloudflare assure que les métadonnées sur le trafic susceptibles de permettre l'identification d'un client restent dans l'UE.

Le mot « métadonnées » peut paraître un peu effrayant, mais son concept s'avère plutôt simple : il signifie tout simplement « données sur les données ». En d'autres termes, il s'agit de la description d'une activité survenue sur notre réseau. Tous les services sur Internet collectent des métadonnées sous une forme ou une autre, et celles-ci sont essentielles à la sécurité des utilisateurs et à la disponibilité du réseau.

Le réseau de Cloudflare se compose de dizaines de services, parmi lesquels notre pare-feu, notre cache, notre résolveur DNS, nos systèmes de protection contre les attaques DDoS, Workers et bien d'autres encore. Chaque service émet des messages de log structurés, qui contiennent des champs tels que des informations d'horodatage, des URL, l'utilisation des fonctionnalités de Cloudflare, ainsi que l'identifiant du compte et de la zone du client.

Cloudflare utilise des métadonnées concernant l'utilisation de ses produits à différentes fins :

- La diffusion de données analytiques du trafic via nos tableaux de bord et nos API ;
- Le partage de logs avec nos clients
- Le blocage de menaces telles que les bots ou les attaques DDoS
- L'amélioration des performances de notre réseau ;
- La préservation de la fiabilité et de la résilience de notre réseau.

Les métadonnées ne renferment pas le *contenu* du trafic des clients et ne contiennent donc **pas** de noms d'utilisateurs, de mots de passe, d'informations personnelles, ni d'autres détails privés sur les utilisateurs finaux du client. Toutefois, ces logs d'événements peuvent contenir les adresses IP des utilisateurs finaux, c'est-à-dire des informations considérées comme des données personnelles au sein de l'UE.

Lorsque l'isolement géographique des métadonnées est activé pour un client, notre périphérie réseau s'assure que les messages de log susceptibles de permettre l'identification d'un client (c'est-à-dire les messages contenant l'ID de compte de ce client) ne sont pas envoyés hors de l'UE. Ces messages seront uniquement envoyés à notre datacenter principal situé dans l'UE, et non à notre datacenter principal aux États-Unis.

Pratiquement toutes les métadonnées d'utilisateurs finaux sont couvertes par l'isolement géographique des métadonnées du client. Cela inclut toutes les données d'utilisateurs finaux dont Cloudflare est responsable du traitement, comme énoncé dans la politique de confidentialité de Cloudflare, pour les services couverts. Vous pouvez consulter ici la liste la plus récente des types de données et des services Cloudflare couverts par l'isolement géographique des métadonnées de clients.

Opportunités et responsabilités partagées

Nous savons que toutes les organisations européennes doivent intégrer les principes de confidentialité et de sécurité dans chaque phase de leur activité ; nous avons donc préparé ce tableau pour vous permettre de comprendre facilement à qui incombe la responsabilité de ces exigences de confidentialité fréquemment demandées :

Principe	Responsabilité	Détails de la responsabilité
Protection intrinsèque des données	Fonctionnalités	Cloudflare est responsable de la mise en œuvre de produits et de services conçus pour protéger la confidentialité des données. L'équipe chargée de la confidentialité des données effectue des examens et des évaluations et anime des formations pour s'assurer que la confidentialité des données fait partie intégrante de nos méthodes de travail. Les clients sont responsables de l'utilisation et de la configuration de leurs services Cloudflare et sont invités à examiner périodiquement l'utilisation et la configuration de ces services, afin de confirmer que les principes de protection des données ont été pris en compte lors de la conception et la mise en œuvre.
Demande d'accès de personnes concernées	Fonctionnalités	Cloudflare fournit aux personnes concernées un droit d'accès, de rectification et de suppression de leurs informations personnelles, quelle que soit leur juridiction de résidence. Les demandes d'accès de personnes concernées peuvent être adressées à sar@cloudflare.com. Si nous recevons une demande d'une personne qui semble être un utilisateur final de l'un de nos clients, nous invitons cette personne à contacter directement notre client.

Principe	Responsabilité	Détails de la responsabilité
Sécurité adéquate	Fonctionnalités	Cloudflare gère un programme de sécurité conforme aux normes de l'industrie. Ce programme de sécurité inclut le maintien de politiques et de procédures de sécurité formelles, l'établissement de contrôles d'accès logiques et physiques appropriés et la mise en œuvre de mesures de protection techniques dans les environnements d'entreprise et de production (notamment l'établissement de configurations, de transmissions et de connexions sécurisées, la journalisation et la surveillance), ainsi que le déploiement de technologies de chiffrement adéquates pour les données personnelles. Les clients sont responsables de l'examen de la posture de sécurité de leurs fournisseurs de Cloud, tels que Cloudflare, et peuvent le faire en consultant 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	Fonctionnalités	Cloudflare traite les données conformément aux instructions de ses clients (les contrôleurs de données) et agit comme un responsable du traitement des données conformément au règlement RGPD. Il incombe aux clients de s'assurer qu'ils disposent d'un fondement juridique approprié pour traiter les données de leurs utilisateurs finaux.
Violations de données personnelles	Fonctionnalités	Cloudflare informera les clients dès qu'elle aura connaissance d'une éventuelle violation de sécurité entraînant la perte, la divulgation non autorisée ou la consultation de données personnelles traitées par Cloudflare ou ses sous-traitants. Il incombe également à Cloudflare d'offrir à ses clients une coopération et une assistance raisonnables suite à la faille, notamment en fournissant aux clients les informations raisonnables que détient Cloudflare concernant les circonstances de la violation et les données personnelles concernées. Il incombe aux clients de se conformer aux exigences réglementaires ou contractuelles afin d'informer leurs utilisateurs finaux et/ou les autorités gouvernementales de toute violation de données personnelles.

Un réseau de Cloud mondial fondé sur la confiance des clients

Chez Cloudflare, notre priorité absolue est de gagner et conserver la confiance de nos clients. Nous sommes conscients que la transparence des engagements de Cloudflare concernant la confidentialité des données (ainsi que notre approche d'intégration de la régionalisation des données et des garanties de confidentialité des données dans notre réseau et nos produits) aide les clients à respecter leurs propres obligations. Nous sommes également conscients que nos certifications industrielles et nos mécanismes contractuels contribuent à créer une solide relation de confiance avec nos clients européens.

Les équipes de spécialistes de la confidentialité des données et de la sécurité de Cloudflare sont là pour collaborer avec vous et vous aider à répondre aux exigences les plus strictes que peut imposer votre pays, votre région ou votre secteur d'industrie. Nos équipes expérimentées de chargés de compte, responsables Customer Success et ingénieurs commerciaux collaborent régulièrement avec notre département en charge de la conformité en matière de confidentialité des données et de sécurité pour vous aider à configurer les produits Cloudflare en fonction de vos obligations de conformité spécifiques. Si vous souhaitez bénéficier d'une démonstration ou d'une session spécialisée consacrée à la configuration de vos services pour répondre à vos obligations spécifiques, contactez-nous dès aujourd'hui. Écrivez-nous à l'adresse privacyquestions@cloudflare.com ou security@cloudflare.com.