WHITEPAPER

CLOUDFLARE

Cómo Cloudflare ayuda a satisfacer los requisitos relacionados con la protección y la localización de datos en Europa

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

RESUMEN EJECUTIVO

- Cloudflare se fundó para ayudaros a ti y a tus clientes a estar más seguros en Internet. Somos una empresa que prioriza la privacidad, y nuestra red y todos nuestros productos se diseñan teniendo en cuenta la protección de datos.
- Cloudflare garantiza un amplio conjunto de protecciones legales y contractuales que cumplen con el RGDP de la UE.
- Ofrecemos un conjunto de funciones de producto y protecciones técnicas a los clientes de Cloudflare que no quieren que sus datos se transfieran fuera de Europa.

La exclusiva red global en la nube de Cloudflare está integrada por centros de datos en más de 250 ciudades en más de 100 países. Cloudflare te ofrece las herramientas para gestionar cómo se enrutan tus datos a través de estos centros de datos para que puedas personalizar dónde se inspecciona tu tráfico con el fin de satisfacer tus necesidades en materia de seguridad, privacidad y rendimiento.

Acerca de Cloudflare

La misión de Cloudflare es ayudar a mejorar Internet. Ofrecemos una plataforma global en la nube que proporciona una amplia gama de servicios de red a particulares y empresas de todos los tamaños en todo el mundo. La red de Cloudflare y su creciente cartera de productos mejoran la seguridad, la privacidad, el rendimiento y la fiabilidad de todos los recursos que se conectan a Internet. Además de atender las necesidades de nuestros clientes, la misión de Cloudflare es ayudar a mejorar Internet para conseguir una red siempre activa, rápida, segura, privada y disponible para todos.

La red, la comunidad de desarrolladores y el negocio de Cloudflare se basan en última instancia en la confianza de los clientes. Intentamos ganar y mantener continuamente dicha confianza a través de la transparencia en lo relativo a nuestros compromisos con la privacidad de los datos y la forma en la que gestionamos los datos de los clientes y de los usuarios finales en nuestros sistemas. También fomentamos confianza desarrollando e implementando productos que (i) ayudan a mejorar la seguridad de nuestros sistemas, (ii) cifran los datos en reposo o en tránsito y (iii) permiten a nuestros clientes determinar cómo se inspecciona el tráfico en diferentes lugares del mundo. Por último, nos ganamos la confianza de los clientes obteniendo y manteniendo las certificaciones definidas por el sector (p. ej. ISO 27001 y 27701, SSAE 18 y SOC 2 tipo 2) y a través de mecanismos de contratación (p. ej., acuerdos de procesamiento de datos) que dan a conocer nuestro modelo de corresponsabilidad con nuestros clientes para garantizar la privacidad.

Cloudflare en Europa

En la actualidad, millones de propiedades de Internet a nivel mundial utilizan Cloudflare. Esta lista incluye muchas de las empresas más importantes y de crecimiento más rápido de Europa, como Eurovision, L'Oreal, AO.com, C&A, AllSaints y muchas más marcas conocidas. Incluye también un creciente número de importantes instituciones europeas, como INSEAD, Börse

Stuttgart, IATA y Telefónica. Empresas y organizaciones de todos los tamaños confían cada vez más en Internet como una plataforma fundamental para prestar servicios a sus clientes, usuarios y partes interesadas, de ahí que estén acelerando la adopción de redes en la nube seguras y fiables como Cloudflare para ayudar a proteger sus aplicaciones, infraestructuras y usuarios con conexión a Internet de amenazas de todo tipo.

Reconocemos que la protección de datos en Europa presenta desafíos únicos. Algunos de estos retos tienen su origen en el Reglamento general de protección de datos (RGPD) de la Unión Europea y en la decisión del Tribunal de Justicia de la Unión Europea en el caso "Schrems II" (Caso C-311/18, *Comisario de protección de datos contra Facebook Ireland y Maximillian Schrems*). Este último dio lugar a nuevos requisitos para las empresas que transfieren datos personales fuera de la UE. Además, varios de sectores de regulación más estricta requieren que tipos específicos de datos personales permanezcan dentro de las fronteras de la UE.

Por ello, la plataforma de Internet de Cloudflare está diseñada para apoyar a los sectores más regulados y más conscientes de la privacidad de Europa, tales como los servicios financieros, el sector público, la energía, los servicios públicos, el comercio minorista, los videojuegos y la sanidad. En Cloudflare, desarrollamos nuestros productos para cumplir con las normas más estrictas de seguridad y privacidad de los usuarios, y cooperamos estrechamente con cada uno de nuestros clientes europeos para ayudarles a cumplir con sus obligaciones en materia de protección de datos asociadas a su ubicación y segmento industrial específicos. Y lo logramos de diversas formas, como:

- Nuestro compromiso corporativo global con la privacidad.
- Certificaciones de seguridad globales y europeas
- Mecanismos de transferencia de datos que cumplen con el RGDP
- Funciones de producto que promueven la localización de datos

En este documento se explican cada una de ellas en detalle.

Compromiso único de Cloudflare con la privacidad

Cloudflare se creó para ayudarte a ti y a tus clientes a estar más seguros en Internet. Somos una empresa que prioriza la privacidad, y nuestra red y todos nuestros productos se diseñan teniendo en cuenta la protección de datos. En nuestra política de privacidad nos comprometemos a no vender los datos personales que procesamos en tu nombre ni a utilizarlos para fines distintos de aquellos que no sean el de ofrecerte nuestros servicios. A lo largo de nuestra trayectoria, nunca hemos incumplido esta promesa. De hecho, nuestra postura sobre la privacidad se definió mucho antes de que los gobiernos empezaran a regular la privacidad de forma que obligaron a muchas otras empresas tecnológicas a actualizar sus prácticas para priorizar de forma adecuada la privacidad de los clientes y los usuarios. No generamos ingresos por publicidad ni perfiles con los datos de los usuarios finales de nuestros clientes para ningún fin y, por tanto, no recabamos ni conservamos los datos personales que procesamos en tu nombre.

A continuación, se detallan algunos de los compromisos de privacidad que asumimos y que nos diferencian de muchos otros proveedores de servicios en la nube:

- No vendemos datos personales.
- No rastreamos a los usuarios finales de nuestros clientes a través de propiedades de Internet.
- No generamos perfiles de los usuarios finales de nuestros clientes con fines publicitarios.
- Solo conservamos los datos personales en caso necesario para ofrecer nuestras soluciones a nuestros clientes.
- Nunca hemos facilitado a terceros o gobiernos las claves de encriptación de nuestros clientes ni el contenido de los clientes que transita por nuestra red. Además, mantenemos

desde hace tiempo el compromiso de que agotaremos todos los recursos legales a nuestro alcance antes de cumplir con una solicitud de este tipo.

- Nos hemos comprometido públicamente a que recurriremos a medidas legales para impugnar cualquier solicitud por parte del Gobierno estadounidense de datos que comprobemos que son objeto del RGDP.
- Nuestra política es notificar a nuestros clientes sobre cualquier proceso legal que solicite su información antes de divulgarla, salvo prohibición legal.

Certificaciones de seguridad globales y europeas de Cloudflare

Cloudflare cumple con los estándares líderes del sector en materia de seguridad y privacidad, y valida esos compromisos con auditores externos anualmente.

Cloudflare ha recibido la certificación ISO/IEC 27701:2019, una nueva norma internacional en materia de privacidad para proteger y gestionar el procesamiento de datos personales. Esta norma tiene menos de dos años, y adapta el concepto actual del Sistema de gestión de seguridad de la información (SGSI) a la creación de un Sistema de gestión de información de privacidad (PIMS). Existen requisitos para asegurarse de que este sistema de gestión de privacidad es sólido y mejora continuamente para cumplir con sus objetivos establecidos. La norma está diseñada de tal manera que los requisitos que las organizaciones deben cumplir para obtener la certificación están muy alineados con los requisitos del RGPD.

Dicho de otro modo, la certificación ISO 27701 garantiza a nuestros clientes que contamos con un programa de privacidad que ha sido evaluado por terceros para cumplir con una norma internacional del sector alineada con el RGDP, y que nos obliga a mantener nuestro programa de privacidad en continuo cumplimiento. Esta certificación, además del Anexo de procesamiento de datos (DPA) que ponemos a disposición de nuestros clientes en el panel de control, ofrece a nuestros clientes varias capas de garantía de que cualquier dato personal que Cloudflare procese se gestionará de manera que cumpla con los requisitos del RGPD.

Además, Cloudflare cumple con la norma ISO 27001/27002, los estándares de seguridad de datos del sector de las tarjetas de pago (PCI DSS) y SSAE 18 SOC 2 tipo 2. Estas validaciones ofrecen garantías a las organizaciones que transfieren sus datos más confidenciales a través de nuestros servicios, y también les ayudan a cumplir y mantener sus propias obligaciones de conformidad.

Además de las evaluaciones periódicas de terceros con respecto a las normas del sector, Cloudflare es considerado un "operador de servicios esenciales" en el marco de la directiva de la UE en materia de seguridad de las redes y los sistemas de información (directiva NIS). Además de registrarse de acuerdo con esta directiva con el ICO y Ofcom en el Reino Unido, BSI en Alemania, y CNCS en Portugal, Cloudflare también ha sido evaluado respecto a requisitos regionales específicos, como la ley BSI en Alemania (BSIG). Promovemos nuestras relaciones y trabajamos estrechamente con los organismos reguladores regionales europeos en materia de conformidad, y proporcionamos información sobre cómo estamos abordando los requisitos de protección de datos.

A nivel práctico, el RGDP fue una codificación de muchos de los pasos que ya estábamos dando:

- Cloudflare solo recaba los datos personales que necesitamos para prestar los servicios que ofrecemos.
- No vendemos información personal.
- Damos a los usuarios la posibilidad de acceder, corregir o eliminar su información personal.

- En consonancia con nuestro papel como procesador de datos, Cloudflare cede a los clientes el control sobre la información que, por ejemplo, se almacena en la memoria caché de nuestra red de entrega de contenido (CDN), en el almacén clave-valor de Workers o en nuestro firewall de aplicaciones web (WAF).

Puedes leer más sobre nuestro compromiso con el RGDP aquí:

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

Debido a nuestra preocupación por la protección de datos, no solo realizamos auditorías cuando nos lo exige la ley o cuando hay certificaciones disponibles. Nuestro equipo de seguridad lleva a cabo rigurosas pruebas de penetración internas y externas, gestionamos un programa de recompensas por errores a través de HackerOne y contratamos a auditores externos para que validen nuestros compromisos en materia de privacidad. Algunos ejemplos importantes son las auditorías centradas en la privacidad como la que realizamos en relación con nuestros compromisos para nuestro solucionador de DNS público 1.1.1.1. Siempre estamos dispuestos a obtener validaciones adicionales que ofrezcan garantías sobre nuestro programa de privacidad, políticas y prácticas de procesamiento y almacenamiento de datos personales de la UE.

Los datos que Cloudflare procesa

Cloudflare procesa los datos de registro de los usuarios finales de nuestros clientes cuando estos acceden a nuestros servicios de conformidad con la autorización de nuestros clientes. Estos datos de registro pueden incluir, entre otros, direcciones IP, información de configuración del sistema y otra información sobre el tráfico hacia y desde los sitios web, dispositivos, aplicaciones o redes de nuestros clientes. Además, Cloudflare recopila y almacena datos y registros de la actividad del servidor y de la red mientras nuestros productos están activos, y realiza observaciones y análisis de los datos de tráfico. Nuestra política de privacidad describe de forma más específica la información que recopilamos y el uso que hacemos de ella.

Cuando recopilamos y almacenamos datos de la actividad en nuestra red, lo hacemos únicamente con el fin de mejorar los productos que te ofrecemos a ti, a otros de nuestros clientes o a la comunidad de Internet en general. No pretendemos monetizar estos datos de ninguna manera que creamos que pueda resultar extraña. Por ejemplo, podemos almacenar y analizar temporalmente los datos de tráfico de red de todos nuestros clientes globales para dirigir de manera inteligente las solicitudes a través de las rutas de Internet más eficientes. También podemos almacenar y analizar datos de la red para detectar e identificar vectores de amenazas emergentes que podemos utilizar de inmediato para mejorar nuestras herramientas de seguridad. Por último, podemos añadir datos de red de segmentos de grandes clientes (pero nunca de usuarios o clientes que se pueden identificar de manera individual) para ayudar a la comunidad de Internet a comprender las tendencias y las amenazas en toda la red (véase Cloudflare Radar).

Mecanismos de transferencia de datos de Cloudflare

En el caso de que Cloudflare, como procesador de datos, transfiera datos personales fuera de la UE, lo hacemos en virtud de nuestro acuerdo de procesamiento de datos (DPA) estándar, que se incorpora a nuestro acuerdo de servicio Enterprise, así como a nuestro acuerdo de suscripción de autoservicio. Nuestro acuerdo de procesamiento de datos incorpora las cláusulas contractuales estándar de la UE (actualizadas en 2021) para los interesados al RGDP. En su conjunto, los términos de Cloudflare garantizan un nivel de protección de los datos personales equivalente al que garantiza el RGDP. Puedes consultar más información sobre nuestro compromiso con el RGDP y nuestro DPA aquí.

En virtud de la decisión de Schrems II, las cláusulas contractuales tipo (CCT) aprobadas por la UE siguen siendo un mecanismo de transferencia válido en virtud del RGPD cuando también se aplican salvaguardias adicionales para los datos transferidos a los Estados Unidos. Cloudflare seguirá utilizando el mecanismo de las CCT para las transferencias de datos, y hemos actualizado nuestro DPA estándar de clientes para incorporar salvaguardas adicionales como compromisos contractuales. Por ejemplo, nos comprometemos a recurrir a medidas legales para impugnar cualquier solicitud del Gobierno estadounidense de datos que comprobemos que son objeto del RGDP, y nos comprometemos a notificar a nuestros clientes cualquier proceso legal que solicite su información antes de divulgarla, salvo prohibición legal. Puedes consultar las salvaguardias adicionales que hemos añadido como compromisos contractuales en la sección 7 de nuestro DPA.

La normativa y las directrices sobre protección de datos están en constante evolución, y llevamos a cabo un seguimiento exhaustivo del panorama normativo y legislativo. Nos adelantamos continuamente a las nuevas directrices para garantizar que nuestros clientes y socios puedan seguir disfrutando de las ventajas de Cloudflare en toda Europa.

Para los clientes que necesitan asegurarse de que Cloudflare no está transfiriendo ningún dato personal, ofrecemos un conjunto de medidas técnicas conocidas como Data Localization Suite.

Funciones de los productos de Cloudflare diseñadas para fomentar la localización de datos

Cloudflare se compromete a ayudar a nuestros clientes a mantener los datos personales en la UE. Ofrecemos nuestra solución Data Localization Suite, que permite a los clientes controlar dónde se inspeccionan y almacenan sus datos.

Data Localization Suite tiene tres elementos:

1. Gestión de claves de cifrado (Geo Key Manager y SSL sin clave)
2. Límite de inspección de carga útil (Regional Services)
3. Límite de metadatos del cliente

Gestión de claves de cifrado:

La privacidad de los datos no es posible sin la seguridad de Internet, que se consigue en gran parte mediante una encriptación eficaz.

La encriptación de los datos transmitidos a través de una red requiere el uso de claves de cifrado, o conjuntos de valores matemáticos que tanto el emisor como el receptor de un mensaje cifrado conocen. SSL/TLS, un protocolo criptográfico que hace posible la comunicación cifrada, utiliza un par de claves: una pública y otra privada. Los clientes de Cloudflare pueden optar por utilizar dos funciones para garantizar que sus claves privadas no salgan de la UE:

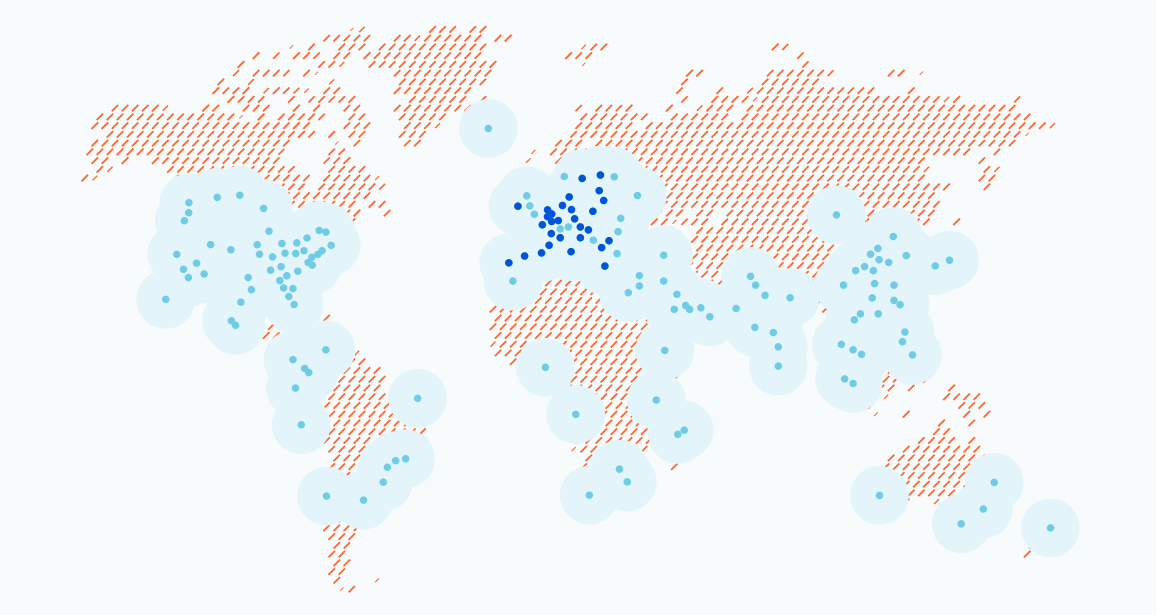
- SSL sin clave permite a los clientes almacenar y gestionar sus propias claves privadas para utilizarlas con Cloudflare. Los clientes pueden utilizar distintos sistemas para el almacenamiento de sus claves, tales como módulos de seguridad de hardware (“HSM”), servidores virtuales y hardware que ejecuta Unix/Linux y Windows alojado en entornos que los clientes controlan. SSL sin clave solo es sin clave desde el punto de vista de Cloudflare. Nunca vemos la clave privada del cliente, que es quien la mantiene y la usa. Por otro lado, la clave pública se sigue utilizando con normalidad en el lado del cliente.
- Geo Key Manager ofrece a los clientes un control granular sobre los centros de datos en los que se almacenan sus claves privadas. Por ejemplo, un cliente puede elegir que las claves privadas solo sean accesibles dentro de los centros de datos ubicados en la UE. Este enfoque evita a los clientes la complejidad que supone la implantación de SSL sin clave y el mantenimiento de su propio almacén de claves.

Límite de inspección de carga útil:

Cloudflare ofrece los productos de red como servicio más seguros y eficientes porque redireccionamos mediante proxy todo tu tráfico desde el perímetro de nuestra red. Como proxy autorizado de tu tráfico, nuestros servicios inspeccionan de forma segura tu tráfico para identificar las amenazas a la seguridad y enrutarlo desde cualquier lugar de nuestra red global. Cloudflare es uno de los únicos proveedores de soluciones en la nube cuya arquitectura es una plataforma global unificada que también se puede configurar para satisfacer requisitos regionales específicos. Esta arquitectura ofrece a nuestros clientes un control total sobre dónde y cómo se inspecciona el tráfico.

Nuestra función Regional Services permite a los clientes elegir en qué lugar de la red de Cloudflare terminan sus conexiones TLS. Por ejemplo, un cliente puede elegir que dichas conexiones terminen en la UE, de modo que el descifrado y la inspección del contenido del tráfico HTTP solo se produzcan dentro de la UE. Esta restricción se aplica a todos nuestros "servicios de aplicación" del perímetro, incluidos:

- Almacenamiento y recuperación del contenido de la memoria caché.
- Bloqueo de cargas HTTP malintencionadas con el Firewall de aplicaciones web (WAF).
- Detección y bloqueo de actividades sospechosas con la Gestión de bots.
- Ejecución de scripts Workers.



Un caso de uso hipotético sería el de un cliente de Cloudflare en Alemania que habilita Regional Services para limitar el servicio a la UE. Sus usuarios finales se conectarán a la ubicación de Cloudflare más cercana en cualquier parte del mundo, pero si esa ubicación está fuera de la UE, el tráfico pasará a una ubicación de Cloudflare en la UE antes de ser inspeccionado. El cliente sigue beneficiándose de nuestra red global eficiente y de baja latencia, que es capaz de soportar incluso los mayores ataques DDoS. Sin embargo, Regional Services también ofrece a los clientes un control local. Solo los centros de datos dentro de la UE tendrán el acceso necesario para aplicar las políticas de seguridad. Este enfoque permite a Cloudflare seleccionar la ruta más rápida hacia la UE y el punto de presencia disponible más cercano para el procesamiento.

Límite de metadatos del cliente:

Esta función mantiene los metadatos de tráfico del usuario final que pueden identificar a un cliente dentro en la UE.

“Metadatos” puede ser un término que asusta, pero es un concepto sencillo. Simplemente significa “datos sobre los datos”. En otras palabras, es una descripción de la actividad que ocurrió en nuestra red. Todos los servicios de Internet recopilan metadatos de alguna forma, y son esenciales para la seguridad de los usuarios y la disponibilidad de la red.

La red perimetral de Cloudflare se compone de docenas de servicios, tales como nuestro firewall, memoria caché, solucionador de DNS, sistemas de protección contra DDoS, entorno de ejecución de Workers y mucho más. Cada servicio emite mensajes de registro estructurados que contienen campos, como marcas de tiempo, URL, uso de las funciones de Cloudflare y el identificador de la cuenta y zona del cliente.

En Cloudflare, utilizamos los metadatos sobre el uso de nuestros productos con varios fines:

- Ofrecer análisis a través de nuestros paneles de control y las API
- Compartir los registros con los clientes
- Detener amenazas contra la seguridad, como bots o ataques DDoS
- Mejorar el rendimiento de nuestra red
- Mantener la fiabilidad y la resistencia de nuestra red

Dado que los metadatos no incluyen el *contenido* del tráfico de los clientes, **no** contienen nombres de usuario, contraseñas, información personal y otros detalles privados de los usuarios finales de los clientes. Sin embargo, los registros de servicio pueden contener las direcciones IP de los usuarios finales, que se consideran datos personales en la UE.

Cuando se activa el límite de metadatos para un cliente, nuestro perímetro garantiza que cualquier mensaje de registro que identifique a ese cliente (es decir, que contenga el Id. de cuenta de ese cliente) no se transfiera fuera de la UE. Solo se enviará a nuestro centro de datos principal en la UE, no a nuestro centro de datos principal en Estados Unidos.

Casi todos los metadatos del usuario final están cubiertos por el límite de metadatos del cliente. Incluye todos los datos del usuario final que Cloudflare procesa, tal y como se define en la política de privacidad de Cloudflare, para los servicios cubiertos. Consulta aquí la lista más actualizada de tipos de datos y servicios de Cloudflare cubiertos por el Límite de metadatos del cliente.

Oportunidades y responsabilidades compartidas

Sabemos que todas las organizaciones europeas necesitan integrar los principios de privacidad y seguridad en cada fase de su negocio, por eso hemos preparado este cuadro para que te resulte fácil entender quién es responsable de estos requisitos de privacidad más solicitados:

Principio	Responsabilidad	Detalles de la responsabilidad
Protección de datos desde el diseño	Compartida	Cloudflare es responsable de ofrecer productos y servicios teniendo en cuenta la privacidad. El equipo de privacidad proporciona revisiones, evaluaciones y formación para garantizar que la privacidad se inculca en nuestra forma de trabajar. Los clientes son responsables del uso y la configuración de sus servicios de Cloudflare, y deben revisar periódicamente su uso y configuración para validar que los principios de protección de datos se han tenido en cuenta en el diseño y la implementación.
Solicitud de acceso del interesado	Compartida	Cloudflare proporciona a los interesados el derecho de acceso, corrección y eliminación de la información personal independientemente de su jurisdicción de residencia. Las solicitudes de los interesados se pueden enviar a sar@cloudflare.com. Si recibimos una solicitud de alguien que parece ser un usuario final de uno de nuestros clientes, le pondremos en contacto con nuestro cliente directamente.

Principio	Responsabilidad	Detalles de la responsabilidad
Seguridad adecuada	Compartida	Cloudflare mantiene un programa de seguridad de acuerdo con los estándares del sector. El programa de seguridad incluye el mantenimiento de políticas y procedimientos de seguridad formales, el establecimiento de controles de acceso lógico y físico adecuados, la implementación de garantías técnicas en entornos corporativos y de producción (tales como el establecimiento de configuraciones seguras, transmisión y conexiones seguras, el registro, la supervisión), y tecnologías de encriptación adecuadas para datos personales. Los clientes son responsables de revisar la postura de seguridad de sus proveedores de soluciones en la nube como Cloudflare, y pueden hacerlo revisando nuestras validaciones e informes de conformidad. También animamos a nuestros clientes a que revisen la configuración de seguridad de su panel de control para asegurarse de que se adhieren a sus políticas y procedimientos de seguridad.
Base legal para el procesamiento	Compartida	Cloudflare procesa los datos de acuerdo con las instrucciones de nuestros clientes, que son los controladores de datos, y opera como un procesador de datos que cumple con el RGDP. Los clientes son responsables de garantizar que cuentan con las bases jurídicas adecuadas para procesar los datos de sus usuarios finales.
Fuga de datos personales	Compartida	Cloudflare notificará a los clientes tan pronto como tengamos certeza de cualquier fuga de seguridad que provoque la pérdida, la divulgación no autorizada o el acceso a los datos personales procesados por Cloudflare o sus subprocesadores. Cloudflare también es responsable de ofrecer a nuestros clientes cooperación y soporte razonables en caso de fuga, lo que incluye facilitar a los clientes la información razonable de que disponga Cloudflare sobre las circunstancias de la fuga y los datos personales afectados. Los clientes son responsables de cumplir con los requisitos reglamentarios o contractuales para notificar a sus usuarios finales o a las autoridades gubernamentales cualquier fuga de datos personales.

Red global en la nube basada en la confianza de los clientes

La prioridad de Cloudflare es ganar y mantener la confianza de los clientes. Entendemos que la transparencia en los compromisos de privacidad de Cloudflare, y en nuestro enfoque para desarrollar la localización de los datos y las salvaguardias de privacidad en nuestra red y productos, ayuda a los clientes a cumplir con sus propias obligaciones. También entendemos que nuestras certificaciones del sector y nuestros mecanismos de contratación bien diseñados nos ayudan a crear una sólida relación de confianza con nuestros clientes europeos.

Los equipos de privacidad y seguridad de Cloudflare están aquí para ayudarte a satisfacer los requisitos más estrictos de tu país, región o sector. Nuestros expertos ejecutivos de cuentas, gestores de Customer Success e ingenieros de ventas trabajan de forma periódica con nuestros equipos de conformidad de privacidad y seguridad para ayudar a nuestros clientes a configurar sus productos de Cloudflare de modo que cumplan con sus obligaciones de conformidad específicas. Si deseas ver una demostración o programar una sesión especializada sobre la configuración de tus servicios para cumplir con tus obligaciones, ponte en contacto con nosotros hoy mismo. Envíanos un correo electrónico a privacyquestions@cloudflare.com o security@cloudflare.com.