Dropbox

Privacidad y protección de los datos

Introducción

Los datos personales desempeñan un papel muy importante en la sociedad y la economía. Cada vez es más frecuente que las personas busquen obtener mayor control y claridad sobre cómo las organizaciones con las que interactúan utilizan y protegen sus datos personales.

En Dropbox, la confianza es la base de nuestra relación con millones de personas y de empresas en todo el mundo. Valoramos la confianza que has depositado en nosotros y asumimos con seriedad la responsabilidad de proteger tus datos personales.

Nuestros compromisos contigo

Nos comprometemos a proteger tus datos personales. Las Condiciones de uso de Dropbox describen tus responsabilidades al usar nuestros servicios. Nuestra Política de privacidad describe nuestros compromisos de privacidad con los usuarios y explica cómo recopilamos, usamos y manejamos tus datos personales cuando utilizas nuestros servicios. Si resides en América del Norte (Estados Unidos, Canadá y México) Dropbox Inc. actúa como tu proveedor de servicio. Para el resto de los usuarios, Dropbox International Unlimited Company actúa como controlador de tus datos personales.

Si eres usuario de Dropbox para empresas o Dropbox Education, tu organización actúa como controlador de los datos personales proporcionados a Dropbox en relación con el uso de Dropbox para empresas o Dropbox Education. El Controlador de datos determina los propósitos y los medios para el tratamiento de los datos personales.

Dropbox actúa como el procesador de datos. Procesa datos en nombre de tu organización cuando usas Dropbox para empresas o Dropbox Education, y nuestro Acuerdo de negocios incluye compromisos relacionados con el procesamiento de datos y la transferencia internacional de datos.

Nuestra trayectoria: el cumplimiento

El cumplimiento es una manera eficaz de validar la confiabilidad de un servicio. Alentamos y nos complace proporcionar una verificación independiente de que nuestras prácticas de seguridad y privacidad cumplen con las normas y regulaciones más ampliamente aceptadas; tales como ISO 27001, ISO 27017, ISO 27018, ISO 27701, HIPPA/HITECH, y SOC 1, 2 y 3.

Además, fuimos uno de los primeros proveedores de servicios en la nube en lograr la certificación ISO 27018, el estándar reconocido internacionalmente para las prácticas líderes en privacidad en la nube y protección de datos. Nuestros auditores externos independientes prueban nuestros controles y proporcionan sus informes y opiniones. Podemos compartirlos contigo siempre que sea posible. Por favor, ten en cuenta que, aunque el alcance de nuestras certificaciones y los informes de auditoría suelen referirse a Dropbox para empresas y Dropbox Education, la mayoría de nuestros controles también se aplican a los usuarios de Dropbox Basic, Plus y Professional. Además, Dropbox ahora se adhiere al Código de Conducta en la Nube de la UE. Puedes encontrar más información sobre los estándares que cumplimos y cómo verificamos nuestras prácticas en nuestra página web de cumplimiento.

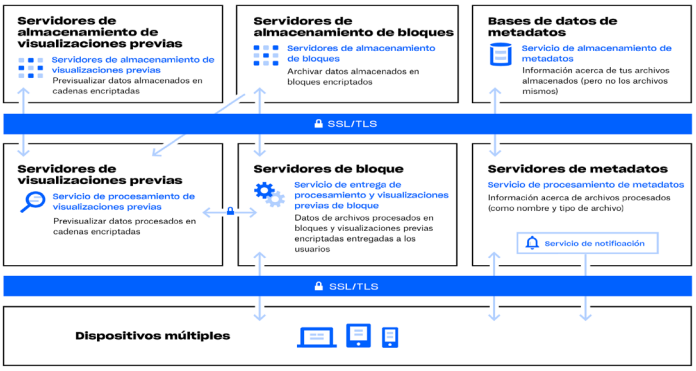
Dropbox

Infraestructura de Dropbox: protección de los datos personales

En Dropbox, creemos que la protección de tus datos personales comienza por mantener los datos seguros. Con ese objetivo, Dropbox está diseñado con múltiples capas de protección, incluidos los controles de la transferencia segura de datos de archivos, cifrado y controles de la aplicación que se distribuyen a través de una infraestructura escalable y segura.

Nuestra infraestructura: Archivos

La infraestructura para archivos de Dropbox consiste en los componentes que se detallan en el siguiente diagrama:



Servidores de metadatos

Determinada información básica sobre los datos de los usuarios, llamada metadatos, se mantiene en su propio servicio de almacenamiento discreto y actúa como índice de los datos de las cuentas de los usuarios. Los metadatos incluyen información básica de la cuenta y del usuario, como la dirección de correo electrónico, el nombre y los nombres de los dispositivos. Los metadatos también incluyen información básica sobre los archivos, incluidos los nombres y tipos de archivos, lo que ayuda a admitir características, como el historial de versiones, la recuperación y la sincronización.

Base de datos de metadatos

Los metadatos de los archivos se almacenan en un servicio de base de datos basado en MySQL y se comparten y replican según sea necesario, para cumplir con los requisitos de rendimiento y alta disponibilidad.

Servidores en bloque

El diseño de Dropbox proporciona un mecanismo de seguridad único que va más allá del cifrado tradicional para proteger los datos del usuario. Los servidores en bloque procesan archivos de las aplicaciones de Dropbox dividiendo cada archivo en bloques, cifrando cada bloque de archivos con un potente cifrado y sincronizando solo los bloques que se modificaron entre revisiones. Cuando una aplicación de Dropbox detecta un nuevo archivo o cambios en un archivo existente, la aplicación notifica a los servidores en bloque del cambio, y los bloques de archivos nuevos o modificados se procesan y transfieren a los servidores de almacenamiento.

Servidores de almacenamiento en bloque

El contenido efectivo de los archivos de los usuarios se almacena en bloques cifrados a través de los servidores de almacenamiento en bloque. Antes de la transmisión, el cliente de Dropbox divide los archivos en bloques de archivos a fin de prepararlos para el almacenamiento. Los servidores de almacenamiento en bloque funcionan como un sistema de memoria asociativa (CAS), en el que cada bloque de archivos cifrado se recupera en función de su valor hash.

Servidores de vistas previas

Los servidores de vistas previas son responsables de generar vistas previas de archivos. Las vistas previas son una representación del archivo de un usuario en un formato de archivo diferente que es más adecuado para una visualización rápida en el dispositivo de un usuario final. Los servidores de vistas previas recuperan bloques de archivos desde los servidores de almacenamiento en bloque para generar vistas previas. Cuando se solicita una vista previa de un archivo, los servidores de vistas previas recuperan la vista previa almacenada en caché desde los servidores de almacenamiento de vistas previas y la transfieren a los servidores en bloque. En última instancia, los servidores en bloque proporcionan vistas previas a los usuarios.

Servidores de almacenamiento de vistas previas

Las vistas previas almacenadas en caché se guardan en un formato cifrado en los servidores de almacenamiento de vistas previas.

Servicio de notificación

Este servicio independiente está dedicado a supervisar si se implementaron cambios en las cuentas de Dropbox. Aquí no se almacenan ni transfieren archivos ni metadatos. Cada cliente establece una conexión de sondeo de larga duración con el servicio de notificación y espera. Cuando se produce un cambio en un archivo en Dropbox, el servicio de notificación envía una señal de cambio al cliente correspondiente; para ello, cierra la conexión de sondeo de larga duración. El cierre de la conexión indica que el cliente debe conectarse a los servidores de metadatos de forma segura para sincronizar los cambios.

Dropbox

Nuestra infraestructura: Paper

Dropbox Paper (Paper) es una característica de Dropbox. Sin embargo, Paper utiliza un conjunto de sistemas muy distinto dentro del entorno de infraestructura de Dropbox. La infraestructura de Paper consiste en los componentes que se detallan en el siguiente diagrama:

Servidores de la aplicación Paper

Los Servidores de aplicación de Paper procesan las solicitudes de usuario, devuelven al usuario los resultados de los documentos de Paper editados y llevan a cabo servicios de notificación. Los Servidores de aplicación de Paper llevan las ediciones entrantes de usuarios a las bases de datos de Paper, donde se almacenan de forma duradera. Las sesiones de comunicación entre los Servidores de la aplicación Paper y las bases de datos de Paper se cifran con un código seguro.

Bases de datos de Paper

El contenido efectivo de los documentos de Paper de los usuarios, así como determinados metadatos sobre dichos documentos, se cifran en un almacenamiento duradero dentro de las bases de datos de Paper. Esto incluye información sobre un documento de Paper (como el título, membresías y permisos compartidos, asociaciones de carpetas y proyectos, etc.), así como contenido que se encuentre dentro del documento de Paper como tal, incluidos comentarios y tareas. Las bases de datos de Paper se comparten y replican según sea necesario para cumplir con los requisitos de rendimiento y alta disponibilidad.

Servidores de almacenamiento de imágenes de Paper

Las imágenes cargadas a los documentos de Paper se almacenan y cifran en el resto de los Servidores de imágenes de Paper. La transmisión de los datos de imagen entre la aplicación Paper y los Servidores de imágenes de Paper se lleva a cabo en una sesión cifrada.

Servidores de vistas previas

Los servidores de vistas previas brindan vistas previas de imágenes cargadas en los documentos de Paper y de hipervínculos incrustados en los documentos de Paper. Para las imágenes cargadas en los documentos de Paper, los servidores de vistas previas hacen uso de los datos de imagen almacenados en los servidores de almacenamiento de imágenes de Paper por medio de un canal cifrado. Para los hipervínculos incrustados en los documentos de Paper, los servidores de vistas previas hacen uso de los datos de imagen y brindan una vista previa de la imagen mediante cifrado, según se especifique en el vínculo de origen. Finalmente, los servidores en bloque proporcionan vistas previas a los usuarios.

Servidores de almacenamiento de vistas previas

Paper utiliza los mismos servidores de almacenamiento de vistas previas que se describen en el diagrama de infraestructura de Dropbox para almacenar vistas previas de imágenes almacenadas en caché. Las porciones de vistas previas en caché se almacenan en un formato cifrado en los servidores de almacenamiento de vistas previas.

Dropbox

Controles de Dropbox: Nuestras prácticas internas

Tomamos medidas exhaustivas para proteger nuestra infraestructura, red y aplicaciones. Algunas de las medidas de seguridad que implementamos incluyen cifrado en reposo, cifrado en tránsito y eliminación permanente de archivos. También ofrecemos una sólida capacitación en privacidad y seguridad para todos nuestros empleados, para construir una cultura en la que ser digno de confianza sea una prioridad. A continuación, se describen detalles de algunos de nuestros controles:

Capacitación

Parte de la seguridad de los datos personales de nuestros usuarios implica construir y desarrollar una cultura de conocimiento de la seguridad y la privacidad. Antes de que se les otorgue acceso a los sistemas, los empleados de Dropbox deben aceptar las políticas de seguridad, lo que incluye una política de privacidad de datos de usuarios. Solo los empleados con una necesidad específica tienen acceso a esos sistemas. Los empleados también participan en la capacitación obligatoria sobre seguridad y privacidad anualmente.

Cifrado en tránsito

Para proteger los datos de archivos en tránsito entre un cliente de Dropbox (actualmente, de escritorio, móvil, API o web) y los servidores finales de Dropbox, se negocia una conexión cifrada para garantizar la entrega de datos segura. De la misma manera, la conexión cifrada se negocia para proteger los datos de los documentos de Paper en tránsito entre un cliente de Paper (actualmente, móvil, API o web) y el servicio alojado. Estas conexiones se cifran utilizando el protocolo de capa de sockets seguros (SSL)/seguridad de la capa de transporte (TLS) para crear un túnel seguro protegido por el estándar de cifrado avanzado (AES) de 128 bits o superior.

Cifrado en reposo

Los archivos cargados por el usuario se almacenan en los servidores de almacenamiento de Dropbox como bloques de archivos discretos. Cada bloque se cifra utilizando el estándar de cifrado avanzado (AES) de 256 bits o superior.

Solamente se sincronizan los bloques que se modificaron entre revisiones. De la misma manera, los datos de archivos de Paper almacenados en las bases de datos de Paper también se cifran en reposo utilizando el estándar de cifrado avanzado (AES) de 256 bits.

Eliminación definitiva de archivos y documentos de Paper

Cuando algún usuario de Dropbox o un administrador de un equipo de Dropbox para empresas o Dropbox Education marcan un archivo para su eliminación permanente, se activa un proceso para eliminarlo permanentemente. Del mismo modo, cuando un usuario o un administrador de un equipo de Dropbox para empresas o Dropbox Education marcan un documento de Paper para su eliminación permanente, hay un proceso similar para eliminar permanentemente los datos del documento de Paper y de la imagen.

Solicitudes de acceso a datos personales

Para acceder a los datos personales más allá de los archivos y documentos de Paper que se almacenan en Dropbox, los usuarios pueden iniciar sesión en el sitio web e ir a sus páginas de cuenta. La página de cuenta mostrará información, como el nombre y la dirección de correo electrónico asociada a la cuenta. Los usuarios también pueden ver las direcciones IP de las sesiones conectadas, las computadoras y los dispositivos móviles, así como las aplicaciones conectadas a sus cuentas desde la página de seguridad y la página de aplicaciones conectadas.

Los usuarios de Dropbox también tienen la opción de solicitar acceso o eliminar otros datos personales que Dropbox haya recopilado sobre ellos. Puedes encontrar más información sobre este proceso en el Centro de ayuda de Dropbox.

Gobernanza de la privacidad en Dropbox

El Equipo de privacidad es responsable de operar el Programa de privacidad de Dropbox. Implementa nuestras iniciativas de privacidad clave y promueve la privacidad desde el diseño en nuestro ciclo de vida de los datos. El programa de privacidad de Dropbox cuenta con el respaldo de varios subequipos legales multifuncionales. Estos subequipos ofrecen la experiencia adicional necesaria para operar y supervisar las tareas diarias del programa de privacidad.

El equipo del Oficial de protección de datos (DPO) opera de forma separada de las demás funciones de privacidad y sirve de cumplimiento y supervisión de la privacidad apoyando directamente al oficial de protección de datos en el desempeño de sus funciones. Puedes comunicarte con el Oficial de protección de datos (DPO) mediante privacy@dropbox.com.

Dropbox

Principios para solicitudes de datos del gobierno

Entendemos que, cuando los usuarios nos confían sus datos personales, esperan que mantengamos la confidencialidad de esos datos. Como la mayoría de los servicios en línea, Dropbox suele recibir solicitudes de gobiernos que buscan información sobre los usuarios.

Los siguientes principios describen cómo gestionamos las solicitudes de datos del gobierno que recibimos.

Ser transparentes

Creemos que los servicios en línea deberían tener permiso para publicar la cantidad y los tipos de solicitudes gubernamentales recibidas, así como notificar a las personas cuando se solicita información sobre ellas. Este tipo de transparencia fortalece a los usuarios, ya que los ayuda a comprender mejor las instancias y patrones de alcance excesivo del gobierno. Continuaremos publicando información detallada sobre estas solicitudes y abogaremos por el derecho a proveer este tipo de información.

Luchar contra las peticiones demasiado amplias

Las solicitudes de datos de gobierno se deben limitar a la información que buscan y adaptar estrictamente a personas concretas e investigaciones legítimas. Nos resistiremos a las solicitudes generales y demasiado amplias.

Proporcionar servicios de confianza

Los gobiernos nunca deben instalar software de puerta trasera en los servicios en línea ni comprometer la infraestructura para obtener datos del usuario. Continuaremos trabajando para proteger nuestros sistemas y modificar las leyes a fin de dejar en claro que este tipo de actividad es ilegal.

Proteger a todos los usuarios

Las leyes que otorgan a los individuos diferentes tipos de protección con base en el lugar donde viven o su ciudadanía son obsoletas y no reflejan la naturaleza global de los servicios en línea. Continuaremos abogando por la reforma de dichas leyes.

Estos principios, junto con nuestro informe anual de transparencia, están disponibles públicamente en el sitio web de Dropbox, en https://www.dropbox.com/transparency.

Para obtener más detalles sobre nuestros controles y nuestro enfoque para proteger tus datos personales, consulta el Informe técnico de seguridad de Dropbox para empresas.

Terceros que trabajan para y junto a Dropbox

Dropbox gestiona la mayoría de las actividades relacionadas con la prestación de nuestros servicios. Sin embargo, confiamos en ciertos proveedores externos en relación con nuestros servicios (por ejemplo, proveedores de servicios de asistencia al cliente y servicios de TI). Estos terceros solo accederán a tu información para realizar tareas en nuestro nombre de conformidad con nuestra Política de privacidad, y seguiremos siendo responsables de su gestión de tu información de acuerdo con nuestras instrucciones.

Cada tercero se somete a un riguroso proceso de investigación, incluidas revisiones de seguridad y privacidad y revisiones contractuales periódicas, para evaluar su capacidad de cumplir con nuestros compromisos de protección de datos. Según este proceso de selección, Dropbox confirma que sus terceros de confianza se comprometen a cumplir con la legislación de protección de datos de la UE aplicable en relación con el procesamiento de datos personales en nombre de Dropbox. Los clientes pueden supervisar a los terceros de confianza de Dropbox revisando las certificaciones de normas ISO 27001 y 27018 y, en virtud de las obligaciones de confidencialidad adecuadas, revisar el informe SOC 2 Tipo II de Dropbox. En particular, los clientes pueden supervisar a terceros de confianza de Dropbox examinando los controles y los resultados de auditoría de Dropbox para los Criterios de Servicios de Confianza P6.1, P6.4 y CC.9.2 del Informe SOC 2 Tipo II.

Dropbox

Transferencias internacionales de datos

Cuando se transfieren datos desde la Unión Europea, el Área Económica Europea, el Reino Unido y Suiza, Dropbox usa diversos mecanismos legales, incluidos contratos con nuestros clientes y filiales, cláusulas contractuales estándares y las decisiones de aptitud de la Comisión Europea sobre determinados países, según corresponda.

Dropbox cumple los marcos de privacidad de datos UE-EE. UU. y Suiza-EE. UU., así como la extensión del Reino Unido al marco de privacidad de datos UE-EE. UU., según lo establecido por el Departamento de Comercio de EE. UU. en relación con el tratamiento de datos personales transferidos desde la Unión Europea, el Espacio Económico Europeo, el Reino Unido y Suiza a Estados Unidos. Dropbox ha certificado al Departamento de Comercio de EE. UU. que se adhiere a estos Marcos de privacidad de datos con respecto a dichos datos, pero esto no incluye las partes de DocSend o Formswift de los Servicios.

Para obtener más información sobre el Marco de privacidad de datos y ver la certificación de Dropbox, visita www.dataprivacyframework.gov.

Las reclamaciones y litigios relacionados con el cumplimiento de nuestro Marco de Privacidad de Datos se investigan y resuelven a través de JAMS, un tercero independiente. Para obtener más información, consulta nuestra Política de privacidad.

RGPD: El Reglamento General de Protección de Datos

El Reglamento General de Protección de Datos o RGPD es un reglamento de la Unión Europea que establece un nuevo marco para la protección de los datos personales de los titulares de datos de la UE. El RGPD es la parte más importante de la legislación europea de protección de datos desde la Directiva de Protección de Datos de la Unión Europea de 1995 y muchas empresas, incluida Dropbox, que realizan sus operaciones en Europa han realizado importantes inversiones en pos del cumplimiento del RGPD. El RGPD armoniza las leyes de protección de datos en toda Europa y las pone al día con el rápido cambio tecnológico de las últimas dos décadas. Este reglamento se basa en pasados marcos legales de la Unión Europea, lo que incluye la Directiva de Protección de Datos de la Unión Europea e introduce nuevas responsabilidades y obligaciones para las organizaciones que gestionan datos personales, así como nuevos derechos para las personas con respecto a sus datos personales. Las organizaciones establecidas en la UE, así como las organizaciones que procesan datos personales de los titulares de datos de la UE, están obligadas a cumplir con el RGPD.

El camino de Dropbox hacia el cumplimiento del RGPD

En Dropbox, nos comprometemos a cumplir con las disposiciones del RGPD. El respeto por la privacidad y seguridad se incorporó a nuestra empresa desde su concepción y, si bien nos expandimos, la forma en que procesamos y protegemos los datos que nos confían nuestros clientes sigue siendo una prioridad para nosotros. Dropbox es conocido por estar siempre a la vanguardia de la curva de cumplimiento. Como se describió anteriormente, fuimos uno de los primeros proveedores de servicios en la nube que obtuvo la certificación ISO 27018 por nuestros usuarios comerciales. Dada esta sólida base, Dropbox considera el cumplimiento de la normativa del RGPD como una evolución de nuestras prácticas y controles actuales, y representa un conjunto de iniciativas continuas y en evolución para garantizar que los datos personales de nuestros usuarios estén siempre protegidos. El camino de Dropbox hacia el cumplimiento del RGPD comenzó con la adopción de la reglamentación en 2016. El primer paso fue formar un equipo interdisciplinario de especialistas en protección de datos compuesto por asesores legales, profesionales de seguridad y cumplimiento, e ingenieros de productos y de infraestructura. Luego, el equipo realizó una evaluación completa de nuestras prácticas actuales de seguridad y protección de datos en función de los requisitos del RGPD.

El siguiente paso consistió en realizar una evaluación de nuestras actividades de procesamiento de datos personales y hacer un seguimiento del ciclo de vida de los datos personales a través de nuestros sistemas. Estos ejercicios a veces se conocen como Mapeos de datos y Evaluaciones de impacto de protección de datos.

Desde entonces, hemos seguido desarrollando nuestros procesos y procedimientos internos existentes para garantizar que cumplimos con los principios de responsabilidad conforme a los requisitos del RGPD, incluido el mantenimiento de registros de procesamiento de acuerdo con el artículo 30 del RGPD. Esto es importante, ya que el RGPD otorga una gran importancia a la documentación de decisiones y prácticas relativas a los datos personales.

Dropbox

Fortalecer a nuestros usuarios en su camino hacia el RGPD

Dropbox proporciona características de control y visibilidad para que puedas gestionar tus obligaciones de protección de datos con mayor facilidad, incluidas las obligaciones de cumplimiento del RGPD. Obviamente, el cumplimiento del RGPD en toda la organización no comienza ni termina con la relación con los proveedores, como Dropbox. Si bien las características te ayudan a administrar las obligaciones, estas no pueden garantizar el cumplimiento por sí mismas. El cumplimiento del RGPD requiere pensar más ampliamente en la manera en que los datos se mueven y están protegidos en la organización. Cada organización debe seguir sus propios pasos para lograr el cumplimiento, y los proveedores deben ser socios importantes en ese camino.

Minimización de datos

Un elemento importante del requisito de privacidad de diseño del RGPD es que las organizaciones deben diseñar sus servicios de tal manera que se minimicen los datos. Esto significa tener una buena visibilidad y control de los datos dentro de la organización para poder administrarlos. El panel de administración de Dropbox para empresas es una herramienta útil en este sentido, ya que te permite supervisar la actividad del equipo, ver los dispositivos conectados y auditar la actividad de archivos compartidos. Trabajamos para integrar los principios de la privacidad por diseño en nuevos productos y características.

Protección y restauración de datos

La protección para dispositivos perdidos, el historial de versiones y la recuperación de archivos brindan protección contra la pérdida, el daño o la destrucción accidental de los datos personales, y contribuyen a restaurar la disponibilidad y el acceso a datos personales de manera oportuna ante un incidente. La autenticación de dos factores es otra medida importante que recomendamos para mantener protegidos los datos.

Mantenimiento de registros

El RGPD también aumenta las obligaciones de las organizaciones de mantener registros detallados de sus actividades de procesamiento. Nuestros registros de auditoría y nuestros registros de actividad pueden ayudarte a comprender mejor tus actividades de procesamiento para respaldar el mantenimiento de los registros.

Administración del acceso

Dentro del panel de administración de Dropbox para empresas, puedes administrar fácilmente el acceso de los miembros del equipo a archivos, carpetas y documentos de Paper. En cuanto a los vínculos de archivos compartidos, nuestra característica de permisos de vínculo te permite proteger con contraseña los vínculos compartidos, establecer fechas de caducidad para otorgar accesos temporales y limitar el acceso a ellos dentro de la organización. En caso de que las responsabilidades cambien entre los usuarios, la herramienta de transferencia de cuenta te permite transferir fácilmente archivos y la propiedad de los documentos de Paper de un usuario a otro.

Los administradores tienen la posibilidad de inhabilitar el acceso de un usuario a su cuenta y conservar sus datos y relaciones de uso compartido para proteger la información de tu organización. Por último, la característica de borrado remoto te permite borrar archivos y documentos de Paper de dispositivos perdidos o robados.

Infraestructura de la UE

Si bien el RGPD no exige que los datos personales se alojen dentro de la UE, Dropbox ofrece a los clientes calificados de Dropbox para empresas y Dropbox Education la capacidad de almacenar archivos (bloques) en la UE. El almacenamiento de archivos basado en la UE se proporciona en la infraestructura de Amazon Web Services (AWS). Para obtener más información sobre nuestra infraestructura de la UE, comunícate con nuestro equipo de ventas.

Para obtener más detalles sobre las características y políticas de seguridad de Dropbox, revisa el Informe técnico de seguridad de Dropbox para empresas o escribe a sales@dropbox.com.

Trabajamos juntos para proteger tus datos personales

Dropbox trabaja con los usuarios para proteger sus datos personales. Tomamos medidas exhaustivas para proteger nuestra infraestructura, nuestra red y nuestras aplicaciones; capacitamos a nuestros empleados en prácticas de seguridad y privacidad; y forjamos una cultura en la que ser confiable es la mayor prioridad. Asimismo, sometemos a nuestros sistemas y prácticas a rigurosas pruebas y auditorías de terceros.

No obstante, los usuarios también desempeñan un papel fundamental en la protección de sus datos personales. Dropbox te permite configurar, usar y supervisar tu cuenta de formas que cumplan con las necesidades de privacidad, seguridad y cumplimiento de tu organización. Nuestra guía de responsabilidad compartida puede ayudarte a comprender mejor lo que hacemos para proteger tu cuenta y lo que puedes hacer para mantener la visibilidad y el control de tus datos personales.

Resumen

Todos los días, millones de usuarios depositan su confianza en Dropbox. Para ser dignos de esa confianza, desarrollamos y seguiremos desarrollando Dropbox con énfasis en la seguridad y la privacidad. Nuestro compromiso de proteger los datos personales de nuestros usuarios está en el centro de cada decisión que tomamos. Para obtener más información, envía un correo electrónico a privacy@dropbox.com. Para obtener más información sobre el RGPD, también puedes visitar nuestro centro de orientación sobre el RGPD.