Dropbox

Privacidad y protección de los datos

Introducción

Los datos personales juegan un papel muy importante en la sociedad y la economía. Cada vez más personas desean tener mayor control y claridad sobre la manera en que las organizaciones con las que interactúan utilizan y protegen sus datos personales, a la vez que buscan organizaciones que les ofrezcan pautas claras para proteger los 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 total seriedad la responsabilidad de proteger tus datos personales.

Nuestros compromisos contigo

Estamos comprometidos 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 la Unión Europea (UE), los datos personales se controlan mediante Dropbox International Unlimited Company, con sede en Irlanda.

Si eres usuario de Dropbox Business o de Dropbox Education, tu organización actúa como controlador de datos para cualquier dato personal proporcionado a Dropbox en relación con tu uso de Dropbox Business o Dropbox Education. El controlador de datos determina los propósitos y los medios para procesar los datos personales. Dropbox actúa como procesador de datos procesando los datos en nombre de tu organización cuando utilizas Dropbox Business o Dropbox Education, y nuestro Acuerdo de negocio 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. Nos complace proporcionar verificación independiente de que nuestras prácticas de seguridad y privacidad cumplen con la mayoría de los estándares y las regulaciones ampliamente aceptados, como ISO 27001, ISO 27017, ISO 27018, BSI C5 de Alemania, y SOC 1, 2 y 3. Por ejemplo, fuimos uno de los primeros proveedores de servicios en la nube para lograr certificación con ISO 27018, el estándar internacionalmente reconocido para prácticas líderes de privacidad y protección de datos en la nube. Nuestros auditores externos independientes prueban nuestros controles y proporcionan sus informes y opiniones. Podemos compartirlos contigo siempre que sea posible.

Ten en cuenta que, si bien el alcance de nuestras certificaciones e informes de auditoría comúnmente se refieren a Dropbox Business y a Dropbox Education, la mayoría de los controles también pueden aplicarse para los usuarios de Dropbox Basic, Plus y Professional. En nuestra página web de cumplimiento encontrarás más información sobre los estándares que cumplimos y la forma en que verificamos nuestras prácticas.

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

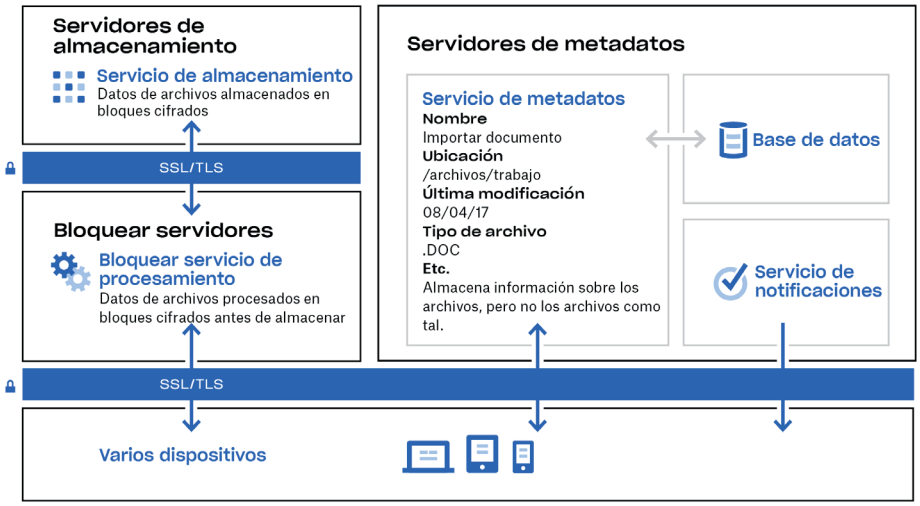
Dropbox

Dropbox Architecture: 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: los archivos

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



Servidores de bloques

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 de bloques 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 de bloques del cambio, y los bloques de archivos nuevos o modificados se procesan y transfieren a los servidores de almacenamiento.

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 cualquiera en Dropbox, el servicio de notificación envía una señal de cambio al cliente que corresponda; para ello, cierra la conexión de sondeo de larga duración. El cierre de la conexión indica al cliente que debe conectarse al servicio de metadatos de forma segura a fin de sincronizar los cambios.

Servidores de metadatos

Cierta información básica acerca de los datos de los usuarios se conserva en su propio servicio de almacenamiento exclusivo y funciona como un índice para los datos en las cuentas de los usuarios. Los metadatos de Dropbox se almacenan en un servicio de base de datos con copia de seguridad de MySQL, y se comparten y replican según sea necesario para cumplir con los requisitos de rendimiento y alta disponibilidad. Los metadatos incluyen información básica sobre la cuenta y el usuario, como la dirección de correo electrónico, el nombre del usuario y el nombre de los dispositivos. Los metadatos también incluyen información básica acerca de los archivos, como los nombres y los tipos de archivos, lo que ayuda a admitir características, como el historial de versiones, la recuperación y la sincronización.

Servidores de almacenamiento

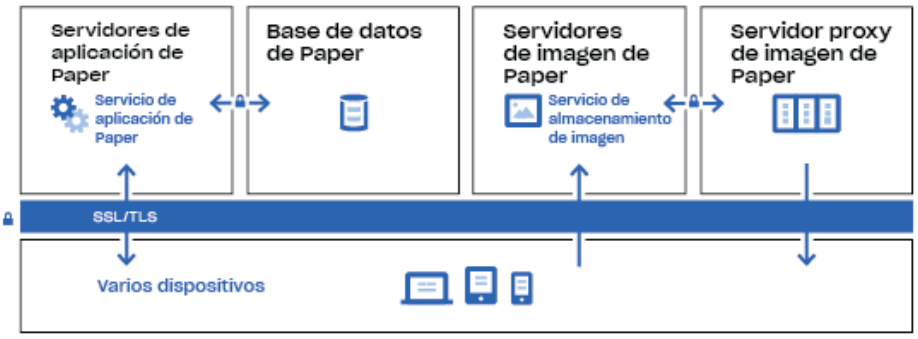
Una vez que los archivos se dividieron en bloques y se cifraron mediante los servidores de bloques, el contenido actual de estos bloques de archivos se almacena en los Servidores de almacenamiento. Los Servidores de almacenamiento funcionan como un sistema de memoria asociativa (CAS), en el que cada bloque de archivos cifrado se recupera en función de su valor hash.

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

Dropbox

Nuestra infraestructura: los archivos

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 aplicación de 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 aplicación de Paper y las bases de datos de Paper se cifran con un código seguro.

Servicio proxy de imagen de Paper

El Servicio proxy de imagen de Paper brinda vistas previas de imagen, tanto de imágenes cargadas en los documentos de Paper como de hipervínculos incrustados en los documentos de Paper. Para las imágenes cargadas en los documentos de Paper, el Servicio proxy de imagen de Paper hace uso de los datos de imagen almacenados en los Servidores de imágenes de Paper por medio de un canal cifrado. Para los hipervínculos incrustados en los documentos de Paper, el Servicio proxy extrae los datos de imagen del vínculo de origen y brinda una vista previa de la imagen mediante HTTP o HTTPS, según se especifique en el vínculo de origen.

Bases de datos de Paper

El contenido real de los usuarios de los documentos de Paper, así como determinados metadatos acerca de estos 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, 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 imagen de Paper

Las imágenes cargadas en 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 de Paper y los Servidores de imágenes de Paper se lleva a cabo en una sesión cifrada.

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

Dropbox

Controles de Dropbox: nuestras prácticas internas

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 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, incluida una política de privacidad de datos de usuarios. Los empleados también participan en capacitaciones obligatorias sobre seguridad y privacidad cuando ingresan, así como en capacitaciones de seguimiento anuales. Finalmente, también reciben capacitación periódica en conciencia sobre la seguridad a través de correos electrónicos informativos, charlas y presentaciones, así como recursos disponibles en nuestra intranet.

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 permanente de archivos y documentos de Paper

Cuando un usuario de Dropbox o un administrador de un equipo de Dropbox Business o Dropbox Education marcan un archivo para su eliminación definitiva, se desencadena un proceso para eliminar el archivo definitivamente. Del mismo modo, cuando un usuario o un administrador de un equipo de Dropbox Business o Dropbox Education marcan un documento de Paper para su eliminación definitiva, hay un proceso similar para eliminar definitivamente los datos de documento y datos de imágenes de Paper.

Solicitudes de acceso a datos personales

Para obtener información más allá de los archivos y documentos de Paper que se almacenan con Dropbox, los usuarios pueden iniciar sesión en el sitio web e ir a sus páginas de cuenta. La página de la 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 sesiones, computadoras y dispositivos móviles conectados, así como aplicaciones conectadas a sus cuentas de la página de seguridad y la página de las aplicaciones conectadas.

Los usuarios de Dropbox también pueden solicitar acceso a otra información personal que pudiéramos haber recopilado de ellos, o a eliminarla. Para obtener más información acerca de este proceso, consulte el Centro de Ayuda de Dropbox.

Para obtener más detalles sobre las características y políticas de seguridad de Dropbox, revisa el Informe técnico de seguridad de Dropbox Business o escribe a sales@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 entender mejor las instancias y los patrones de extralimitación gubernamental. Continuaremos publicando información detallada sobre estas solicitudes y abogaremos por el derecho a proveer más información relevante como esta.

Luchar contra las solicitudes extralimitadas

Las solicitudes de datos del gobierno deberían limitarse a la información que buscan y ajustarse estrictamente a personas específicas e investigaciones legítimas. Nos opondremos a las solicitudes extralimitadas y generalizadas.

Prestar servicios de confianza

Los gobiernos nunca deben instalar software de puerta trasera en los servicios en línea ni poner en riesgo la infraestructura para obtener datos de 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 las personas 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 el informe de transparencia anual, están disponibles públicamente en el sitio web de Dropbox, en: https://www.dropbox.com/transparency.

Para obtener más detalles sobre los controles y nuestro enfoque para proteger los datos personales, consulta el Documento técnico de seguridad de Dropbox Business.

Terceros que trabajan para 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 TI). Estos terceros podrán acceder a tu información exclusivamente para realizar tareas en nuestro nombre y de conformidad con esta Política de privacidad, y seremos los únicos responsables de su gestión de tu información de acuerdo con nuestras instrucciones. Cada tercero pasa por un riguroso proceso de verificación, que incluye revisiones de seguridad y revisiones contractuales habituales, con el fin de evaluar su capacidad para cumplir con nuestros compromisos de protección de datos.

Transferencias internacionales de datos

Dropbox confía en diversos mecanismos legales para su transferencia internacional de datos personales desde la UE hasta los Estados Unidos. Contamos con la certificación de los programas del Escudo de la Privacidad UE-EE. UU. y Suiza-EE. UU. con respecto a la recopilación, el uso y la retención de datos personales y su transferencia desde la UE y Suiza hasta los Estados Unidos. Además del Escudo de Privacidad, Dropbox también brinda sólidas garantías contractuales en torno a la privacidad de sus servicios, y confía en las Cláusulas Contractuales Modelo de la UE para cubrir sus transferencias internacionales de datos.

Dropbox

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 el manejo y la protección de los datos personales de los ciudadanos 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 compañías —incluida Dropbox— que realizan sus operaciones en Europa han realizado importantes inversiones en pos del cumplimiento del RGPD.

Uno de los objetivos del RGPD es armonizar y hacer que las leyes de privacidad de datos en Europa se adapten al rápido cambio tecnológico de las últimas dos décadas. Este reglamento se basa en el marco legal de la Unión Europea, 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 Unión Europea, así como las que procesan datos personales de residentes de la UE, deben 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. Dadas estas bases sólidas, en Dropbox consideramos el cumplimiento del RGPD una evolución de nuestras prácticas y controles existentes.

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 continuado desarrollando nuestros procesos y procedimientos internos existentes para garantizar que cumplimos con los principios de rendición de cuentas de conformidad con los requisitos 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.

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

Dropbox

Cómo 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 nuevo requisito del RGPD en relación con la Privacidad de diseño 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 es una herramienta muy útil en este sentido, ya que te permite supervisar la actividad del equipo, ver los dispositivos conectados y auditar la actividad de archivos compartidos.

Protección y restauración de datos

La protección de 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, 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 mientras conservan sus datos y relaciones de uso compartido para mantener protegida la información de la compañía. 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 requiere que se alojen datos personales dentro de la Unión Europea (UE) en la mayoría de los casos, Dropbox ofrece a los clientes calificados de Dropbox Business y Dropbox Education la capacidad para 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 acerca de 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 Business o escribe a sales@dropbox.com.

Dropbox

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; forjamos una cultura en la que ser confiable es la mayor prioridad; y sometemos los sistemas y las prácticas a pruebas y auditorías rigurosas de terceros.

Sin embargo, los usuarios también juegan un rol clave en la protección de sus datos personales. Dropbox te permite configurar, usar y supervisar tu cuenta de manera que cumpla con las necesidades de privacidad, seguridad y cumplimiento de tu organización. Nuestra guía de responsabilidad compartida te ayudará a comprender mejor lo que hacemos para mantener tu cuenta segura, 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 continuaremos desarrollando Dropbox centrándonos en la seguridad y la privacidad. Nuestro compromiso de proteger los datos personales de nuestros usuarios guía 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 de RGPD.

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