Dropbox

Privacidad y protección de datos

Introducción

Los datos personales constituyen una parte importante en la sociedad y la economía. Cada vez más, las personas buscan un 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 empresas en todo el mundo. Valoramos la confianza que has depositado en nosotros y nos tomamos en serio la responsabilidad de proteger tus datos personales.

Nuestros compromisos contigo

Nos comprometemos a proteger sus datos personales. Los términos de Dropbox de Servicio resumen 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 servicios.

En el caso de los demás usuarios, Dropbox International Unlimited Company oficia como el controlador de tus datos personales.

Si tú eres un usuario de Dropbox Business o de Dropbox Education, tu organización actúa como el 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 de procesamiento de datos personales. Dropbox actúa como el procesador de datos, procesando datos en nombre de tu organización cuando utilizas Dropbox Business o Dropbox Education, y nuestro acuerdo comercial incluye compromisos relacionados con el procesamiento de datos y la transferencia de datos internacionales.

Nuestro historial de rastreo: cumplimiento

El cumplimiento es una forma efectiva de validar la confianza de un servicio. Alentamos y nos complace proporcionar una verificación independiente de que nuestras prácticas de seguridad y privacidad cumplen con los estándares y las regulaciones más ampliamente aceptadas, como ISO 27001, ISO 27017, ISO 27018, HIPAA/HITECH, Alemania BSI C5 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 brindan sus informes y sus opiniones. Podemos compartir esto contigo siempre que sea posible.

Tenga en cuenta que, si bien el alcance de nuestras certificaciones e informes de auditoría generalmente se refiere a Dropbox Business y Dropbox Education, la mayoría de nuestros controles también se aplican a los usuarios de Dropbox Basic, Plus y Professional. Puedes encontrar más información sobre los estándares que cumplimos y cómo verificamos nuestras prácticas en nuestra página web de cumplimiento.

Para obtener más detalles sobre las características y las políticas de seguridad de Dropbox, revisa Dropbox Business Security Whitepaper o ponte en contacto con sales@dropbox.com

Dropbox

Arquitectura de Dropbox: protección de tus datos personales

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

Nuestra infraestructura: archivos

La infraestructura de Dropbox para archivos se compone de los componentes que se muestran en el siguiente diagrama.

Servidores de metadatos

Cierta información básica sobre los datos del usuario, llamada metadatos, se mantiene en su propio servicio de almacenamiento discreto y actúa como un índice para los datos en 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 archivos, incluidos nombres y tipos de archivos, que ayuda a admitir funciones como el historial de versiones, la recuperación y la sincronización.

Bases de datos de metadatos

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

Servidores de bloques

Por diseño, 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 los archivos de las aplicaciones de Dropbox al dividir cada archivo en bloques, encriptar cada bloque de archivos utilizando un cifrado seguro y sincronizar solo los bloques que se han modificado entre revisiones. Cuando una aplicación de Dropbox detecta un nuevo archivo o cambia a un archivo existente, la aplicación notifica a los servidores de bloques el cambio, y los bloques de archivos nuevos o modificados se procesan y se transfieren al servidor de almacenamiento.

Servidores de almacenamiento en bloque

El contenido real de los archivos de los usuarios se almacena en bloques cifrados con los servidores de almacenamiento de bloques. Antes de la transmisión, el cliente de Dropbox divide los archivos en bloques de archivos en preparación para el almacenamiento. Los servidores de almacenamiento en bloque actúan como un sistema de almacenamiento direccionable por contenido (CAS), con cada bloque de archivo cifrado individual recuperado en función de su valor de hash.

Servidores de vistas previas

Los servidores de vistas previas son responsables de producir 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 de los servidores de almacenamiento de bloques para generar vistas previas. Cuando se solicita una vista previa del archivo, los servidores de vistas previas recuperan la vista previa en caché de los servidores de almacenamiento de vistas previas y la transfieren a los servidores de bloque. En última instancia, los servidores de bloque proporcionan las vistas previas a los usuarios.

Servidores de almacenamiento de vistas previas

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

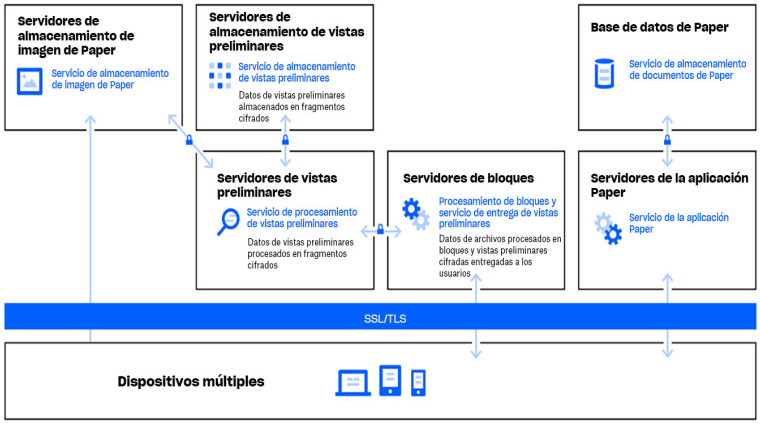
Servicio de notificaciones

Este servicio separado está dedicado a monitorear si se han realizado cambios en las cuentas de Dropbox o no. Aquí no se almacenan ni se transfieren archivos ni metadatos. Cada cliente establece una larga conexión de sondeo al servicio de notificación y espera. Cuando se produce un cambio en cualquier archivo en Dropbox, el servicio de notificación señala un cambio a los clientes relevantes al cerrar la conexión de sondeo larga. Cerrar la conexión indica que el cliente debe conectarse a los servidores de metadatos de forma segura para sincronizar cualquier cambio.

Para obtener más detalles sobre las características y las políticas de seguridad de Dropbox, revisa Dropbox Business Security Whitepaper o ponte en contacto con sales@dropbox.com

Nuestra infraestructura: Paper

Dropbox Paper (Paper) es una característica del producto Dropbox. Sin embargo, Paper utiliza un conjunto de sistemas en su mayoría distintos dentro del entorno de infraestructura de Dropbox. La infraestructura de Paper está compuesta por los componentes descritos en el diagrama a continuación.



Servidores de aplicaciones de Paper

Los servidores de aplicaciones de Paper procesan las solicitudes de los usuarios, representan los documentos de Paper editados para que puedan verlos los usuarios y ejecutan los servicios de notificaciones. Los servidores de la aplicación Paper escriben ediciones de usuario entrantes en las bases de datos de Paper, donde se colocan en un almacenamiento persistente. Las sesiones de comunicación entre los servidores de aplicaciones y las bases de datos de Paper se encriptan mediante un potente cifrado.

Bases de datos de Paper

El contenido real de los documentos de Paper de los usuarios, además de algunos metadatos relacionados con estos documentos, se encripta en un almacenamiento persistente en las bases de datos de Paper. Esto incluye información acerca de los documentos de Paper (por ejemplo, el título, los permisos y la membresía compartida, las asociaciones de carpetas y proyectos, y otros datos), además del contenido del documento mismo, incluso los comentarios y las tareas. Las bases de datos de Paper se comparten y se replican según sea necesario para cumplir con los requisitos de rendimiento y de alta disponibilidad.

Servidores de almacenamiento de imágenes en Paper

Las imágenes cargadas a documentos de Paper se almacenan y se encriptan en los servidores de imágenes de Paper. La transmisión de datos de imágenes entre los servidores de imágenes y de aplicaciones de Paper se realiza mediante una sesión encriptada.

Servidores de vistas previas

Los servidores de vistas previas producen vistas previas tanto para imágenes cargadas en documentos de Paper como para hipervínculos incrustados en documentos de Paper. Para las imágenes cargadas en documentos de Paper, los servidores de vistas previas obtienen datos de imágenes almacenados en los servidores de almacenamiento de imágenes de Paper a través de un canal cifrado. Para los hipervínculos incrustados en los documentos de Paper, los servidores de vistas previas obtienen los datos de la imagen y presentan una vista previa de la imagen mediante el cifrado según lo especificado por el enlace de origen. En última instancia, los servidores de bloque proporcionan las vistas previas a los usuarios.

Servidores de almacenamiento de vistas previas

Paper utiliza los mismos servidores de almacenamiento de vista previa descritos en el diagrama de infraestructura de Dropbox para almacenar las vistas previas de imágenes en caché. Los fragmentos de las 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 integrales para proteger nuestra infraestructura, nuestra red y nuestras aplicaciones. Algunas de las medidas de seguridad que tenemos implementadas incluyen el cifrado en reposo, el cifrado en tránsito y la eliminación permanente de archivos. También ofrecemos una sólida capacitación en privacidad y seguridad para todos nuestros empleados a fin de construir una cultura en la que ser dignos de confianza sea una prioridad. Los detalles de algunos de nuestros controles se describen a continuación:

Capacitación

Parte de la protección de los datos personales de nuestros usuarios implica construir y desarrollar una cultura de seguridad y conciencia de la privacidad. Los empleados de Dropbox deben aceptar las políticas de seguridad, incluida una política de privacidad de datos del usuario, antes de que se les otorgue acceso a los sistemas. Solo aquellos empleados con una necesidad específica tienen acceso a dichos sistemas.

Los empleados también participan anualmente en capacitación obligatoria sobre seguridad y privacidad.

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 principales de Dropbox, se negocia una conexión cifrada para garantizar una entrega segura. Del mismo modo, se negocia una conexión encriptada para proteger los datos de documentos de Paper en tránsito entre un cliente de Paper (actualmente móvil, API o web) y el servicio alojado. Estas conexiones se encriptan usando Secure Sockets Layer (SSL)/Transport Layer Security (TLS) para crear un túnel seguro protegido por encriptación de Estándar de cifrado avanzado (AES) de 128 bits o superior.

Cifrado en reposo

Los archivos cargados por los usuarios se almacenan en los servidores de almacenamiento de Dropbox como bloques de archivos discretos. Cada bloque se cifra con el Estándar de cifrado avanzado (AES) de 256 bits. Solo los bloques que se han modificado entre revisiones se sincronizan. Del mismo modo, los datos de documentos 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 en Paper

Cuando algún usuario de Dropbox o un administrador de un equipo de Dropbox Business o Dropbox Education marca 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 Business o Dropbox Education marca 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 datos personales más allá de los archivos y documentos de Paper almacenados con Dropbox, los usuarios pueden iniciar sesión en el sitio web e ir a las páginas de sus cuentas. La página de la cuenta mostrará información como el nombre y la dirección de correo electrónico asociados con 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 eliminación de otros datos personales que Dropbox haya recopilado sobre ellos.

Puedes encontrar más información sobre este proceso en el Centro de Ayuda de Dropbox.

Gestión de la privacidad en Dropbox

El equipo del Programa de privacidad es responsable de operar el Programa de privacidad de Dropbox. Implementa nuestras iniciativas de privacidad clave y defiende la privacidad por diseño en el ciclo de vida de nuestros datos. El Programa de privacidad de Dropbox cuenta con el respaldo de varios subequipos legales multifuncionales. Estos subequipos brindan la experiencia adicional requerida para operar y supervisar las tareas diarias del Programa de Privacidad.

El equipo DPO opera por separado de las otras funciones de privacidad y sirve como cumplimiento y supervisión de la privacidad, apoyando directamente al oficial de protección de datos en la ejecución de sus funciones. El oficial de protección de datos (DPO) es el representante local de la UE y se puede contactar en privacy@dropbox.com.

Para obtener más detalles sobre las características y las políticas de seguridad de Dropbox, revisa Dropbox Business Security Whitepaper o ponte en contacto con sales@dropbox.com

Dropbox

Principios sobre solicitudes de datos del gobierno

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

Los principios a continuación describen cómo manejamos las solicitudes de datos gubernamentales que recibimos.

Ser transparentes

Creemos que los servicios en línea deberían poder publicar el número y los tipos de solicitudes gubernamentales que reciben, y notificar a las personas cuando se haya solicitado información sobre ellos. Este tipo de transparencia empodera a los usuarios, al ayudarlos a comprender mejor de extralimitación del gobierno. Continuaremos publicando información detallada sobre estas solicitudes y abogaremos por el derecho a proporcionar más de esta información importante.

Combatir las solicitudes demasiado amplias.

Las solicitudes de datos del gobierno deben limitarse en la información que buscan y ajustarse estrechamente a personas específicas e investigaciones legítimas. Resistiremos las solicitudes generales y excesivamente amplias.

Prestar 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. Seguiremos trabajando para proteger nuestros sistemas y modificar las leyes a fin dejar en claro que este tipo de actividad es ilegal.

Proteger a todos los usuarios

Las leyes que protegen a las personas de forma diferente según el lugar donde residen o su nacionalidad son obsoletas y no reflejan el carácter mundial de los servicios en línea. Seguiremos abogando por la reforma de estas leyes.

Estos principios, junto con nuestro informe anual de transparencia, se ponen a disposición del público en el sitio web de Dropbox en: https://www.dropbox.com/transparency.

Para obtener detalles adicionales sobre nuestros controles y nuestro enfoque para proteger tus datos personales, consulta nuestro Dropbox Business Security Whitepaper.

Otros trabajando para y con Dropbox

Dropbox gestiona la mayoría de las actividades relacionadas con la prestación de nuestros servicios; sin embargo, utilizamos algunos terceros de confianza en relación con nuestros servicios (por ejemplo, proveedores de atención al cliente y servicios de TI). Estos terceros situaciones y patrones solo accederán a tu información para realizar tareas en nuestro nombre de conformidad con nuestra política de privacidad, y seguiremos siendo responsables del manejo 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 periódicas, para evaluar su capacidad de cumplir con nuestros compromisos de protección de datos.

Transferencias internacionales de datos

Dropbox se basa en una variedad de mecanismos legales para su transferencia internacional de datos personales de la UE a los Estados Unidos. Estamos certificados bajo Privacy Shield Programs de UE-EE. UU. y Suiza-EE. UU. relacionados con la recopilación, el uso y la retención de datos personales y su transferencia de la UE y Suiza a los Estados Unidos. Además de Privacy Shield, Dropbox también ofrece fuertes garantías contractuales en torno a la privacidad de sus servicios y ha implementado cláusulas contractuales modelo de la UE para cubrir sus transferencias internacionales de datos.

Dropbox

GDPR: el Reglamento general de protección de datos

El Reglamento general de protección de datos, o GDPR, es un reglamento de la UE que establece un marco legal para proteger los datos personales de los interesados de la UE.

El GDPR es la parte más importante de la legislación europea de protección de datos desde la Directiva de protección de datos de la UE de 1995, y muchas compañías, incluida Dropbox, que hacen negocios en Europa han invertido mucho en el cumplimiento del GDPR.

El GDPR armoniza las leyes de protección de datos en toda Europa y las pone al día con el rápido cambio tecnológico que se ha producido en las últimas dos décadas.

Se basa en marcos legales anteriores en la UE, incluida la Directiva de protección de datos de la UE, e introduce nuevas obligaciones y responsabilidades para las organizaciones que manejan datos personales, así como nuevos derechos para las personas con respecto a sus datos personales.

datos personales. Las organizaciones establecidas en la UE, así como las organizaciones que procesan datos personales de los interesados de la UE, deben cumplir con el GDPR.

La forma en que Dropbox cumple con el RGPD

Dropbox está comprometido con el cumplimiento de GDPR. El respeto a la privacidad y la seguridad se incorporó a nuestro negocio desde el principio, y a medida que hemos crecido, nuestro enfoque en el manejo y protección de datos que nuestros usuarios nos confían ha seguido siendo una prioridad. Dropbox tiene un historial de mantenerse por delante de la curva de cumplimiento, como se describió anteriormente, fuimos uno de los primeros proveedores de servicios en la nube en lograr la certificación ISO 27018 para nuestros usuarios comerciales. Dada esta sólida base, Dropbox considera que el cumplimiento del GDPR es una evolución de nuestras prácticas y controles existentes, y representa un conjunto continuo y en evolución de iniciativas para garantizar que los datos personales de nuestros usuarios estén siempre protegidos.

El viaje de Dropbox hacia el cumplimiento de GDPR comenzó tan pronto como se adoptó la regulación en 2016. Nuestro primer paso fue formar un equipo multifuncional de especialistas en protección de datos compuesto por asesores legales, profesionales de seguridad y cumplimiento e ingenieros de productos e infraestructura. Luego, nuestro equipo realizó una evaluación completa de nuestras prácticas actuales de seguridad y protección de datos con respecto a los requisitos del GDPR.

Nuestro siguiente paso fue realizar una evaluación de nuestras actividades de procesamiento de datos personales y rastrear el ciclo de vida de los datos personales a través de nuestros sistemas. Estos ejercicios a veces se los mencionan como realizar asignaciones de datos y completar evaluaciones de impacto de protección de datos.

Asignaciones de datos y completar Evaluaciones de impacto de protección de datos.

Desde entonces, hemos seguido construyendo sobre nuestros procesos y procedimientos internos existentes para garantizar que cumplamos con los principios de responsabilidad bajo los requisitos de GDPR. Esto es importante ya que el GDPR se centra cada vez más en documentar las decisiones y prácticas que afectan los datos personales.

Para obtener más detalles sobre las características y las políticas de seguridad de Dropbox, revisa Dropbox Business Security Whitepaper o ponte en contacto con sales@dropbox.com

Dropbox

Empoderar a nuestros usuarios en sus viajes GDPR

Dropbox proporciona funciones de control y visibilidad que pueden ayudarte a administrar tus obligaciones de protección de datos, incluidas las obligaciones de cumplimiento de GDPR, más fácilmente. Por supuesto, el cumplimiento de GDPR en toda tu organización no comienza ni termina con la relación con tus proveedores, como Dropbox. Si bien nuestras funciones pueden ayudarte a administrar tus obligaciones, no pueden garantizar el cumplimiento en sí mismas. El cumplimiento de GDPR requiere pensar de manera más amplia acerca de cómo se mueven los datos y cómo están protegidos en tu organización. Cada organización debe emprender sus propios pasos para alcanzar el cumplimiento, con proveedores como socios importantes en ese viaje.

Minimización de datos

Un elemento importante del requisito de Privacidad por diseño del GDPR es que las organizaciones deben diseñar sus servicios de manera que minimicen los datos. Esto significa tener una buena visibilidad y control de los datos dentro de tu organización para ayudarte a administrarlos. El panel de administración de Dropbox Business es una herramienta útil para ayudar con esto, ya que te permite monitorear la actividad del equipo, ver los dispositivos conectados y auditar la actividad de intercambio. Trabajamos para incorporar los principios de Privacidad por diseño en nuevos productos y características.

Protección y restauración de datos

La protección de dispositivo perdido, el historial de versiones y la recuperación de archivos pueden ayudar a proteger contra la pérdida accidental, daño o destrucción de datos personales, y pueden ayudar con la capacidad de restaurar la disponibilidad y el acceso a los datos personales de manera oportuna en caso de un incidente. La autenticación de dos factores es otra medida importante que recomendamos para ayudar a proteger tus datos.

Mantenimiento de registros

El GDPR 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 tu mantenimiento de registros.

Administración de acceso

Dentro del panel de administración de Dropbox Business, puedes administrar fácilmente el acceso de los miembros del equipo a archivos, carpetas y documentos en Paper. Para vínculos de archivos compartidos, nuestra función de permisos de vínculos te permite proteger con contraseña los vínculos compartidos, establecer fechas de vencimiento para otorgar acceso temporal y limitar el acceso a aquellos dentro de tu organización. En caso de que las responsabilidades cambien entre los usuarios, nuestra herramienta de transferencia de cuentas te permite transferir fácilmente archivos y la propiedad de documentos de Paper de un usuario a otro.

Los administradores también tienen la capacidad de deshabilitar el acceso de un usuario a su cuenta mientras preservan sus datos y comparten relaciones para mantener segura la información de tu organización. Por último, la función de borrado remoto te permite borrar archivos y documentos en Paper de dispositivos perdidos o robados.

Infraestructura de la UE

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

Para obtener más detalles sobre las características y las políticas de seguridad de Dropbox, revisa Dropbox Business Security Whitepaper o ponte en contacto con sales@dropbox.com

Dropbox

Trabajar juntos para proteger tus datos personales

Dropbox trabaja con sus usuarios para proteger sus datos personales. Tomamos medidas integrales para proteger nuestra infraestructura, red y aplicaciones, capacitar a los empleados en prácticas de seguridad y privacidad, construir una cultura en la que la mayor prioridad sea ser dignos de confianza, y someter nuestros sistemas y prácticas a rigurosas pruebas y auditorías de terceros.

Sin embargo, los usuarios también juegan un papel clave en la protección de sus datos personales. Dropbox te permite configurar, usar y monitorear tu cuenta en formas que satisfacen las necesidades de privacidad, seguridad y cumplimiento de tu organización. Nuestra guía de responsabilidad compartida puede ayudarte a comprender más sobre lo que hacemos para mantener tu cuenta segura y lo que puedes hacer para mantener la visibilidad y el control sobre tus datos personales.

Resumen

Todos los días, millones de usuarios confían en Dropbox. Para ser dignos de esa confianza, creamos y seguiremos haciendo crecer Dropbox con énfasis en la seguridad y la privacidad. Nuestro compromiso de proteger los datos personales de nuestros usuarios es el núcleo de cada decisión que tomamos. Para obtener más información, envíe un correo electrónico a privacy@dropbox.com. Para obtener más información sobre GDPR, también puedes visitar nuestro Centro de orientación de GDPR.