Dropbox

Privacidad y protección de datos

Introducción

Los datos personales juegan un papel fundamental en la sociedad y la economía. Las personas buscan cada vez más control y claridad con respecto a cómo usan y protegen sus datos personales las organizaciones con las que interactúan.

En Dropbox, la confianza es la base de nuestra relación con millones de personas y negocios de todo el mundo. Valoramos mucho la que depositas en nosotros y nos tomamos muy en serio la responsabilidad de proteger tus datos personales.

Nuestro compromiso contigo

Estamos comprometidos con la seguridad de tus datos personales. Los Términos de servicio de Dropbox detallan tus responsabilidades al usar nuestros servicios. Nuestra Política de privacidad describe nuestro compromiso con la privacidad de los usuarios y explica cómo recopilamos, usamos y gestionamos tus datos personales cuando usas nuestros servicios. Si vives en Norteamérica (Estados Unidos, Canadá y México), Dropbox Inc. actúa como tu proveedor de servicios. Para los usuarios del resto del mundo, Dropbox International Unlimited Company es el encargado de la protección de datos.

Si eres usuario de Dropbox para empresas o Dropbox Education, tu organización actúa como encargada de la protección de datos para los datos personales proporcionados a Dropbox en relación con tu uso de Dropbox para empresas o Dropbox Education. El encargado de la protección de datos determina los propósitos y medios del tratamiento de datos.

Dropbox actúa como el responsable del tratamiento de datos, procesando los datos en nombre de tu empresa cuando utilices Dropbox para empresas o Dropbox Education, y nuestro Acuerdo de Dropbox para empresas incluye los compromisos adoptados con relación al tratamiento de datos y las transferencias de datos internacionales.

Nuestro registro: cumplimiento

La conformidad normativa es una manera muy efectiva que tienen las empresas de demostrar que sus servicios son dignos de confianza. Te animamos a que nos solicites la verificación independiente que demuestra que nuestras prácticas de seguridad y privacidad cumplen con las normas y regulaciones más aceptadas, tales como ISO 27001, ISO 27017, ISO 27018, ISO 27701, HIPPA/HITECH y SOC 1, 2 y 3. Estaremos encantados de proporcionarte dicha verificación.

Además, fuimos uno de los primeros proveedores de servicios en la nube que obtuvo la certificación ISO 27018, el estándar reconocido internacionalmente sobre prácticas líderes en privacidad en la nube y protección de datos. Nuestros auditores independientes llevan a cabo evaluaciones sobre nuestros controles y proporcionan informes y opiniones. Trataremos de compartirlos contigo cuando sea posible. Ten en cuenta que, aunque la mayoría de las certificaciones e informes de auditoría se refieren a Dropbox para empresas y Dropbox Education, la mayoría de los controles pueden aplicarse también a usuarios de Dropbox Basic, Plus y Professional. Además, Dropbox ahora se adhiere al Código de conducta en la nube de la UE. Encontrarás más información sobre los estándares que cumplimos y cómo verificamos nuestras prácticas en nuestra página web sobre el cumplimiento.

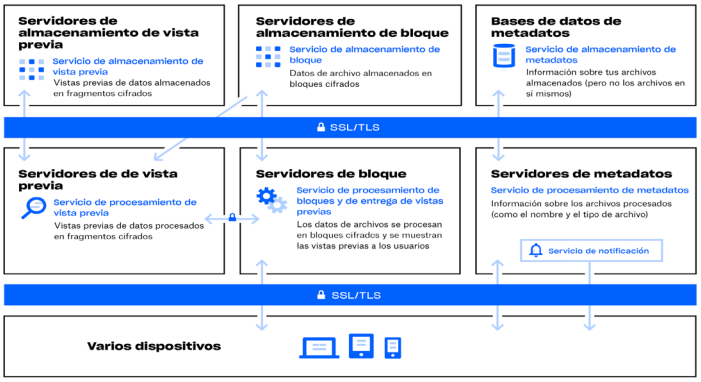
Dropbox

Arquitectura de Dropbox: protegemos tus datos personales

En Dropbox, creemos que el primer paso para proteger tus datos personales es mantenerlos a salvo. Para conseguirlo, Dropbox se ha diseñado con varias capas de protección que incluyen transferencia de datos segura, cifrado y controles a nivel de aplicación. Todas estas capas están distribuidas en una infraestructura segura y ampliable.

Nuestra infraestructura: Archivos

En el caso de los archivos, la infraestructura de Dropbox se compone de los elementos que se exponen en el diagrama que se presenta a continuación.



Servidores de metadatos

Los metadatos, es decir la información básica sobre los usuarios, se conserva en un servicio de almacenamiento propio y discreto que actúa como un índice para los datos de las cuentas de los usuarios. Entre los metadatos, se incluye información básica del usuario y la cuenta, como la dirección de correo electrónico, el nombre y los nombres de los dispositivos. También se incluye información básica sobre los archivos como el nombre y el tipo de archivo, lo que hace que se puedan usar funciones como el historial, la recuperación y la sincronización de versiones.

Bases de datos de metadatos

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

Servidores de bloque

Gracias a su diseño, Dropbox proporciona un mecanismo de seguridad único que no se limita al cifrado tradicional para proteger los datos de los usuarios. Los servicios de cifrado procesan archivos de las aplicaciones de Dropbox dividiéndolos en bloques, cifrando cada bloque con códigos seguros y sincronizando únicamente aquellos que se hayan modificado entre una revisión y otra. Cuando una aplicación de Dropbox detecta un archivo nuevo o cambios en un archivo existente, notifica el cambio a los servidores de bloque y los bloques de archivo nuevos o modificados se procesan y se transfieren a los servidores de almacenamiento.

Servidores de almacenamiento de bloques

Los verdaderos contenidos de los archivos de los usuarios se almacenan en bloques cifrados mediante los servidores de almacenamiento de bloque. Antes de la transmisión, el cliente de Dropbox divide los archivos en bloques a modo de preparación para el almacenamiento. Los servidores de almacenamiento de bloque actúan como un sistema de almacenamiento de contenido direccionable (en inglés, Content-Addressable Storage o CAS) y cada bloque de archivo cifrado se recupera según su valor de hash.

Servidores de vista previa

Los servidores de vista previa son los responsables de ofrecer las vistas previas de los archivos. Estas previsualizaciones consisten en una renderización del archivo de un usuario en un formato de archivo diferente y más adecuado para mostrarse rápidamente en el dispositivo del usuario final. Los servidores de vista previa recuperan los bloques de archivo de los servidores de almacenamiento de bloque para generar vistas previas. Cuando se solicita la vista previa, los servidores de vistas previas recuperan la vista previa almacenada en caché de los servidores de almacenamiento de vistas previas y la transfieren a los servidores de bloque. Los servidores de bloque son los que muestran finalmente las vistas previas a los usuarios.

Servidores de almacenamiento de vistas previas

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

Servicio de notificación

Este servicio independiente supervisa si se han realizado cambios o no en las cuentas de Dropbox. Aquí no se almacenan ni transfieren archivos ni metadatos. Cada cliente establece una conexión prolongada de consulta con el servicio de notificación y espera. Cuando se produce un cambio en cualquier archivo de Dropbox, el servicio de notificación señala un cambio a los clientes pertinentes cerrando la sesión de consulta. Cada cliente establece una conexión prolongada de consulta con el servicio de notificación y espera.

Para obtener información detallada sobre las políticas y las funciones de seguridad de Dropbox, consulta el Informe técnico de seguridad de Dropbox para empresas o ponte en contacto con sales@dropbox.com.

Dropbox

Nuestra infraestructura: Paper

Dropbox Paper (también conocido como Paper) es una función del producto Dropbox. Sin embargo, Paper hace uso de un conjunto de sistemas diferentes dentro del entorno de infraestructura de Dropbox. En el caso de los archivos, la infraestructura de Paper se compone de los elementos que se exponen a continuación en el diagrama.

Servidores de la aplicación de Paper

Los servidores de la aplicación de Paper procesan solicitudes de usuario, devuelven el resultado de documentos de Paper editados al usuario y llevan a cabo los servicios de notificación. Los servidores de la aplicación de Paper escriben las ediciones entrantes del usuario en las bases de datos de Paper y, una vez allí, se colocan en un almacenamiento persistente. Las sesiones de comunicación entre los servidores de la aplicación de Paper y las bases de datos de Paper se cifran utilizando un cifrado sólido.

Bases de datos de Paper

Los contenidos reales de los documentos de Paper de los usuarios, así como ciertos metadatos de estos documentos de Paper, se cifran en un almacenamiento persistente en las bases de datos de Paper. Esto incluye información sobre un documento de Paper (como el título, pertenencia y permisos compartidos, asociaciones de carpetas y proyectos, y otro tipo de información), así como contenido dentro del propio documento de Paper, como comentarios y tareas. Las bases de datos de Paper se fragmentan y replican tanto como se necesite para cumplir los requisitos de rendimiento y alta disponibilidad.

Servidores de almacenamiento de imagen de Paper

Las imágenes subidas a los documentos de Paper se almacenan y cifran en reposo en los servidores de Paper Images. La transmisión de datos de imagen entre la aplicación de Paper y los servidores de imagen de Paper tiene lugar en una sesión cifrada.

Servidores de vista previa

Los servidores de vistas previas ofrecen vistas previas de imágenes subidas a documentos de Paper, así como de los hiperenlaces incrustados dentro de documentos de Paper. Para las imágenes subidas a documentos de Paper, los servidores de vistas previas capturan los datos de imagen almacenados en los servidores de almacenamiento de imágenes de Paper a través de un canal cifrado. En el caso de los hiperenlaces incrustados en documentos de Paper, los servidores de vistas previas buscan los datos de imagen en el enlace de la fuente e interpretan una vista previa de la imagen mediante cifrado, tal y como especifique el enlace de la fuente. Los servidores de bloque son los que muestran finalmente las 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 las vistas previas de imágenes en caché. Los fragmentos de vistas previas almacenadas 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, redes y aplicaciones. Algunas de las medidas de seguridad que hemos aplicado incluyen el cifrado en reposo, cifrado en tránsito y la eliminación permanente de los archivos. También ofrecemos formación en materia de privacidad y seguridad para todos nuestros empleados con el fin de desarrollar una cultura donde ser digno de confianza sea una prioridad. A continuación, describimos algunos de los controles que llevamos a cabo.

Formación

Parte de nuestro trabajo a la hora de proteger los datos personales de nuestros usuarios implica desarrollar y contribuir al crecimiento de una cultura en la que la seguridad y la privacidad sean muy importantes. Nuestros empleados deben estar de acuerdo con las políticas de seguridad para trabajar con nosotros, lo cual incluye una política de privacidad de datos del usuario, antes incluso de darles acceso al sistema. Solo estos empleados con una necesidad específica necesitan acceso a dichos sistemas. Además, participan en una formación obligatoria sobre seguridad y privacidad anualmente.

Cifrado en tránsito

Para proteger los datos en tránsito entre el cliente de Dropbox (actualmente de escritorio, móvil, API o web) y los servidores front-end de Dropbox, se negocia una conexión cifrada para asegurar una entrega segura. De forma similar, se negocia una conexión cifrada para proteger los datos de documentos de Paper en tránsito entre el cliente de Paper (actualmente de escritorio, móvil, API o web) y el servicio hospedado. Estas conexiones se cifran con Secure Sockets Layer (SSL)/Transport Layer Security (TLS) para crear un túnel seguro protegido por un cifrado con Advanced Encryption Standard (AES) de 128 bits o superior.

Cifrado en reposo

Los archivos que suben los usuarios se almacenan en los servidores de almacenamiento de Dropbox como bloques de archivo discretos. Cada bloque se cifra usando el estándar Advanced Encryption Standard (AES) de 256 bits.

Solo se sincronizan los bloques que se hayan modificado desde la versión anterior. De forma similar, los datos de los documentos de Paper de las bases de datos de Paper también se cifran en reposo usando un estándar Advanced Encryption Standard (AES) de 256 bits.

Borrado permanente de archivos y documentos de Paper

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

Solicitudes de acceso a datos personales

Para obtener más información sobre cómo se almacenan los archivos y documentos de Paper con Dropbox, los usuarios pueden iniciar sesión en la web y visitar la página de su cuenta. Allí encontrarán más detalles como el nombre y el correo electrónico asociado a su cuenta. Además, pueden ver las direcciones IP de las sesiones conectadas, los ordenadores y los dispositivos móviles, así como aplicaciones conectadas a sus cuentas, concretamente en las páginas de seguridad y aplicaciones conectadas.

Los usuarios de Dropbox también tienen la posibilidad de solicitar el acceso o la eliminación de otros datos personales que podamos haber recopilado sobre ellos. Hay más información al respecto en el Centro de ayuda de Dropbox.

Gobierno de la privacidad en Dropbox

El equipo de privacidad es responsable de gestionar el programa de privacidad de Dropbox. Implementa nuestras principales iniciativas de privacidad y aboga por la privacidad de forma expresa en nuestro ciclo de vida de los datos. El programa de privacidad de Dropbox está respaldado, además, por varios subequipos jurídicos de distintas disciplinas. Estos subequipos aportan los conocimientos especializados adicionales que se necesitan para gestionar y supervisar las tareas del día a día del Programa de privacidad.

El equipo DPO trabaja de forma independiente a otras funciones de privacidad y funciona como cumplimiento de la privacidad, supervisando directamente al responsable de la protección de datos en la ejecución de sus tareas. Puedes contactar con el equipo responsable de la protección de datos (DPO, por sus siglas en inglés) escribiendo a privacy@dropbox.com.

Para obtener información detallada sobre las políticas y las funciones de seguridad de Dropbox, consulta el Informe técnico de seguridad de Dropbox para empresas o ponte en contacto con sales@dropbox.com.

Dropbox

Datos gubernamentales

Principios relativos a las solicitudes

Creemos que, si los usuarios nos confían sus datos personales, esperan de nosotros confidencialidad absoluta. Como muchos servicios online, Dropbox recibe a menudo solicitudes por parte de los gobiernos en referencia a los datos de nuestros usuarios.

Estos principios detallados a continuación describen cómo gestionamos las solicitudes gubernamentales que recibimos.

Ser transparentes

Creemos que nuestros servicios online deberían obtener permiso para publicar el número y tipos de solicitudes gubernamentales recibidas y notificar a los interesados cuando se ha solicitado información sobre ellos mismos. Este tipo de transparencia capacita a los usuarios ayudándoles a entender mejor las instancias y patrones de abuso por parte del gobierno. Continuaremos publicando información detallada sobre estas solicitudes y defenderemos el derecho a ofrecer este tipo de información tan importante.

Luchar contra las solicitudes de información demasiado amplias

Las peticiones de datos por parte de los gobiernos deberían limitarse a la información que buscan y a una serie de personas específicas e investigaciones legítimas. Nos oponemos a las peticiones arbitrarias y de carácter amplio.

Ofrecer servicios de confianza

Los gobiernos no deberían instalar "puertas traseras" en servicios de Internet ni poner en peligro las infraestructuras para obtener datos de los usuarios. Seguiremos esforzándonos para proteger nuestros sistemas y cambiar las leyes vigentes con el fin de dejar claro que estas actividades son ilegales.

Proteger a todos los usuarios

Las leyes que otorgan protección a las personas según dónde residan o dónde tengan su ciudadanía están anticuadas y no reflejan la naturaleza global de los servicios online. Seguiremos defendiendo la reforma de estas leyes.

Estos principios, así como nuestro informe anual de transparencia, están publicados en la web de Dropbox: https://www.dropbox.com/transparency.

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

Terceros que trabajan para Dropbox y con Dropbox

Dropbox gestiona la mayoría de las actividades relacionadas con el aprovisionamiento de nuestro servicios; sin embargo, contamos con terceras partes de confianza a la hora de ofrecer nuestros servicios (por ejemplo, proveedores que nos ofrecen atención al cliente y servicio de TI). Estas terceras partes solo tendrán acceso a tu información para llevar a cabo tareas en nuestro nombre y en cumplimiento con nuestra Política de privacidad. En este caso, nosotros seguiremos siendo responsables del tratamiento de tu información de acuerdo con nuestras propias instrucciones.

Estos terceros pasan por un proceso de investigación rigurosa, que incluye revisiones de seguridad y privacidad, y revisiones contractuales habituales, para evaluar su capacidad de cumplir nuestros compromisos de protección de datos. Según este proceso de investigación, Dropbox afirma que sus terceros de confianza se comprometen con la ley de protección de datos aplicable en la UE en relación con el procesamiento de datos en nombre de Dropbox. Los clientes pueden supervisar a los terceros que cuentan con la confianza de Dropbox revisando las certificaciones ISO 27001 y 27018 de Dropbox. Además, de conformidad con las pertinentes obligaciones de confidencialidad, pueden revisar el informe SOC 2 Tipo II de Dropbox. En particular, pueden supervisar la actividad de estos terceros examinando los resultados de los controles y auditorías de Dropbox en relación con los criterios de confianza de los servicios P6.1, P6.4 y CC.9.2 del informe SOC 2 Tipo II.

Dropbox

Transferencias internacionales de datos

Al transferir los datos desde la Unión Europea, el Espacio Económico Europeo, el Reino Unido y Suiza, Dropbox cuenta con diferentes mecanismos jurídicos, como contratos con nuestros clientes y entidades afiliadas, cláusulas contractuales tipo y las decisiones de adecuación de la Comisión Europea sobre ciertos países, si procede.

Dropbox cumple con los marcos de privacidad de datos EU-EE. UU. y Suiza-EE. UU., así como con la extensión para el Reino Unido del marco de privacidad de datos EU-EE. UU., como establece el Departamento de Comercio de Estados Unidos respecto al tratamiento de los datos personales que se transfieran 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 ajusta a estos marcos de privacidad de datos con respecto a dichos datos, pero esto no incluye la parte de los Servicios de DocSend y Formswift.

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

Las reclamaciones y disputas relacionadas con el cumplimiento de nuestro marco de privacidad de datos se investigan y resuelven a través de JAMS, un tercero de carácter independiente. Puedes consultar más información echando un vistazo a nuestra Política de privacidad.

RGPD: 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 marco legal para proteger los datos personales de los residentes de la Unión Europea. El RGPD es la regulación europea en materia de datos más importante desde la Directiva de protección de datos de la UE de 1995. Muchas empresas que llevan a cabo su actividad comercial en Europa, incluida Dropbox, han invertido mucho para poder cumplir con el RGPD. El RGPD trata de armonizar y ofrecer un marco legal sobre protección de datos en Europa para sincronizarse con el cambio tecnológico que se ha producido en las últimas dos décadas. Se ha desarrollado a partir de marcos legales previos de la UE, incluida la Directiva de protección de datos, e incluye nuevas obligaciones y responsabilidades para empresas que tratan datos personales, así como nuevos derechos para los individuos en relación con sus datos personales. Las empresas que están establecidas en la UE, así como las organizaciones que procesan datos personales de individuos residentes en la UE, están obligadas a cumplir con el RGPD.

Cómo cumple Dropbox con el RGPD

En Dropbox estamos comprometidos con el cumplimiento del RGPD. El respeto por la privacidad y la seguridad siempre ha estado presente en nuestra organización y, a medida que hemos crecido, hemos priorizado la gestión y protección de los datos que los usuarios nos han confiado. Dropbox siempre se ha mantenido un paso por delante en lo relativo al cumplimiento. Tal y como mencionábamos anteriormente, fuimos uno de los primeros proveedores en conseguir la certificación ISO 27018 para nuestros usuarios de empresa. A partir de estas sólidas bases, Dropbox considera el cumplimiento con el RGPD como una evolución de las prácticas y controles que ya llevábamos a cabo, y representa un conjunto de iniciativas continuas en constante evolución que ayudan a garantizar que los datos personales de nuestros usuarios siempre estén protegidos. El camino hacia el cumplimiento de Dropbox empezó cuando se aprobó la normativa en 2016. Nuestro primer paso fue contar con un equipo multidisciplinar de especialistas en protección de datos compuesto por profesionales expertos en asesoría, seguridad y cumplimiento, así como ingenieros de producto e infraestructura. Después, llevaron a cabo una evaluación completa para ver hasta qué punto nuestras prácticas de seguridad y protección de datos cumplían con los requisitos del RGPD.

Nuestro próximo paso fue llevar a cabo una evaluación de nuestras actividades relativas al procesamiento de los datos personales para trazar el ciclo de vida de los datos personales en nuestros sistemas. En ocasiones, estos ejercicios consisten en llevar a cabo asignaciones de datos y completar evaluaciones del impacto de la protección de datos. Desde entonces, hemos seguido desarrollando nuestros procesos y procedimientos internos para asegurarnos de cumplir con los principios de responsabilidad de acuerdo a los requisitos del RGPD, incluidos los que se refieren al mantenimiento de registros para el procesamiento en base al artículo 30 del RGPD. Esto resulta clave ya que el nuevo reglamento se centra especialmente en documentar las decisiones y prácticas que implican datos personales.

Dropbox

Ayudar a nuestros usuarios en su cumplimiento con el RGPD

Dropbox ofrece funciones de control y visibilidad que pueden ayudarte a gestionar fácilmente tus obligaciones de protección de datos, incluidas las relativas al RGPD. Por supuesto, el cumplimiento con el RGPD en tu empresa no empieza o termina en la relación con tus proveedores de servicio, como es el caso de Dropbox. Nuestras funciones pueden ayudarte a gestionar tus obligaciones, pero no aseguran el cumplimiento por sí mismas. El cumplimiento del RGPD exige una concepción más amplia sobre cómo se transportan y se protegen los datos en tu empresa. Cada organización debería llevar a cabo sus propios pasos para alcanzar el cumplimiento, teniendo en cuenta a los proveedores como una pieza clave para cumplir este objetivo.

Minimización de los datos

Un elemento a tener en cuenta dentro de los requisitos del RGPD relativos a la privacidad por diseño es que las organizaciones deberían diseñar servicios de forma que se minimice el tratamiento de datos. Esto implica tener una buena visibilidad y control sobre los datos en tu empresa para poder gestionarlos. El panel de administrador de Dropbox para empresas resulta muy útil a este respecto, pues te permite monitorizar la actividad del equipo, ver los dispositivos conectados y auditar la actividad relativa al contenido compartido. Nos esforzamos por incorporar los principios de privacidad por diseño en nuevos productos y funciones.

Protección y restauración de los datos

La protección para los dispositivos perdidos, el historial de versiones y la recuperación de archivos pueden ayudarte a protegerte ante pérdidas, daños o destrucción de datos personales de carácter accidental, y pueden ayudar con la posibilidad de restaurar la disponibilidad y el acceso a los datos personales de forma puntual en caso de incidente. La doble autenticación es otra medida importante que recomendamos a la hora de proteger los datos.

Mantenimiento de registros

El RGPD también aumenta las obligaciones a la hora de mantener un registro de las actividades de procesamiento de datos por parte de las empresas. Nuestro registro de auditoría y registro de actividades pueden ayudarte a entender mejor tus actividades de procesamiento y facilitarte el mantenimiento de un registro.

Administración del acceso

Dentro del panel de administración de Dropbox para empresas puedes gestionar fácilmente el acceso de los miembros del equipo a archivos, carpetas y documentos de Paper. En el caso de los enlaces compartidos de archivo, nuestra función de permisos de enlace te permite proteger con contraseña los enlaces compartidos, establecer fechas límites para conceder acceso temporal y limitar el acceso a los usuarios que decidas dentro de la empresa. En caso de que cambien las responsabilidades entre los usuarios, nuestra herramienta de transferencia de cuenta te permite realizar transferencias fácilmente, así como traspasar la propiedad de documentos de Paper de un usuario a otro.

Los administradores también pueden desactivar el acceso de un usuario a su cuenta y proteger al mismo tiempo sus datos y las relaciones de uso compartido para mantener segura la información de tu empresa. Por último, la función de borrado remoto permite borrar los archivos y documentos de Paper en los dispositivos que se pierdan o hayan sido robados.

Infraestructura de la UE

Aunque el RGPD no exige guardar los datos personales dentro de la UE, en muchas circunstancias, Dropbox ofrece a los clientes que cumplan los requisitos de Dropbox para empresas y Dropbox Education la posibilidad de almacenar archivos (bloques) en la UE. La infraestructura Amazon Web Services (AWS) ofrece el servicio de almacenamiento de archivos en la UE. Para obtener más información sobre la infraestructura de la UE, ponte en contacto con nuestro equipo de ventas.

Para obtener información detallada sobre las políticas y las funciones de seguridad de Dropbox, consulta el Informe técnico de seguridad de Dropbox para empresas o ponte en contacto con sales@dropbox.com.

Trabajar juntos para proteger tus datos personales

Dropbox trabaja codo con codo con sus usuarios para proteger sus datos personales. Adoptamos medidas integrales para proteger nuestra infraestructura, nuestra red y nuestras aplicaciones; formamos a nuestros empleados en las prácticas de seguridad y privacidad; y creamos una cultura en la que ser digno de confianza es la máxima prioridad.

Además, sometemos a nuestros sistemas y prácticas a una evaluación y auditoría rigurosas por parte de terceros.

Sin embargo, los usuarios juegan un papel fundamental a la hora de proteger sus datos personales. Dropbox te capacita para configurar, usar y supervisar tu cuenta de forma que cumpla con las necesidades de privacidad, seguridad y cumplimiento. Nuestra guía de responsabilidad compartida puede ayudarte a entender mejor todo lo que hacemos para proteger tu cuenta y qué puedes hacer para mantener la visibilidad y el control sobre tus datos personales.

Resumen

Cada día, millones de usuarios confían en Dropbox. Para merecernos esa confianza, hemos desarrollado una plataforma que crece priorizando la seguridad y la privacidad. Nuestro compromiso con la protección de nuestros datos personales se refleja en cada decisión que tomamos. Para obtener más información, envíanos un correo a privacy@dropbox.com. Para obtener más información sobre el RGPD, puedes visitar nuestro centro de ayuda del RGPD.