Reglamento General de Protección de Datos

El Reglamento General de Protección de Datos (RGPD) es una regulación de la Unión Europea (EU) que establece un nuevo marco para el manejo y la protección de datos personales de los ciudadanos en la UE.

Presenta nuevas obligaciones y responsabilidades para todas las organizaciones que manejan datos personales y nuevos derechos para las personas con relación a cómo se recopilan, procesan y almacenan sus datos personales.

Impacto del RGPD

Si tu organización debe cumplir con el RGPD, hay varios factores que deben considerarse. Recomendamos encarecidamente buscar asesoramiento legal para determinar los requisitos en función de cada situación particular.

1. Comprensión de los datos

Proteger los datos adecuadamente significa comprender cómo se tratan en tu organización, es decir, la manera en que se manejan, comparten, utilizan, archivan y eliminan los datos personales. Comprender qué son tus datos, y cómo se utilizan y almacenan, es un requisito clave para desarrollar la estrategia del RGPD de tu negocio.

2. Determinación de propiedad y responsabilidad

Es importante identificar a un propietario responsable del cumplimiento de la protección de datos. En algunas organizaciones, es obligatorio designar a un oficial de protección de datos. El RGPD también introdujo un nuevo "principio de responsabilidad", que requiere que las organizaciones adopten un programa para el cumplimiento de la protección de datos. Las organizaciones deberán desarrollar políticas internas de protección de datos y capacitar al personal.

3. Aseguramiento de una base legal para el procesamiento

Otro componente del RGPD cuya documentación deben garantizar las compañías son los fundamentos legales para procesar los diferentes tipos de datos personales que se manejan. Por ejemplo, si se utiliza el consentimiento como base para el procesamiento, se deberá considerar cómo obtenerlo, además de poder demostrar claramente cómo y cuándo se brindó.

4. Comprensión de los derechos de los sujetos de datos.

Asegúrate de comprender los derechos que tienen los individuos en relación con sus datos personales para poder garantizar que los procedimientos se adapten a ellos. Por ejemplo, los sujetos de datos tienen derecho a acceder a sus datos personales, así como a corregirlos, borrarlos o exportarlos electrónicamente. En determinadas circunstancias, los usuarios también tienen el derecho de oponerse a la toma de decisiones y a la elaboración de perfiles de manera automatizada.

5. Aseguramiento de la privacidad desde el diseño

La privacidad desde el diseño es un requisito legal explícito por primera vez, por lo que es importante comenzar a considerar cómo integrarla en los procesos del negocio. En algunas circunstancias, también es necesario evaluar el impacto en la privacidad.

6. Preparación para la gestión de filtraciones

Asegurarse de que las políticas y los procesos relacionados con la gestión de filtraciones de datos estén actualizados y evaluados es crucial para contar con un programa de protección de datos sólido. El RGPD exige la detección de filtraciones y su informe a las autoridades correspondientes de manera oportuna, ya que se pueden imponer multas si se reportan fallas o brechas.

7. Comunicación de información esencial

Asegurarse de que las políticas de privacidad en línea de la organización y otros avisos estén actualizados y abarquen las prácticas de protección de datos. Los nuevos requisitos incluyen detallar la base legal para el procesamiento e informar a los usuarios sobre la autoridad a la que pueden presentar sus reclamos.

8. Trabajo con los proveedores

El cumplimiento de las obligaciones del RGPD va más allá de las políticas propias de cada organización individual. Cualquier tercero que procese datos personales en tu nombre también deberá cumplir con los estándares necesarios para la protección de datos. Algunas preguntas que se pueden realizar a los proveedores incluyen lo siguiente:

- ¿Tienen prácticas sólidas de seguridad de red e información, privacidad y protección de datos?
- ¿Se adaptan a los estándares aceptados internacionalmente y verifican su cumplimiento?
- ¿Cómo pueden demostrar una cultura sólida de confianza y seguridad? ¿Qué controles ofrecen para ayudar a administrar tus datos y para cumplir con tus obligaciones como controlador?

Dropbox: protegemos tus datos

La confianza es la base de nuestra relación con millones de personas y de empresas en todo el mundo.

Valoramos la confianza que depositas en nosotros y asumimos la responsabilidad de proteger tu información con total seriedad. Para hacernos merecedores de tu confianza, desarrollamos y continuaremos desarrollando Dropbox con énfasis en la seguridad, el cumplimiento y la privacidad.

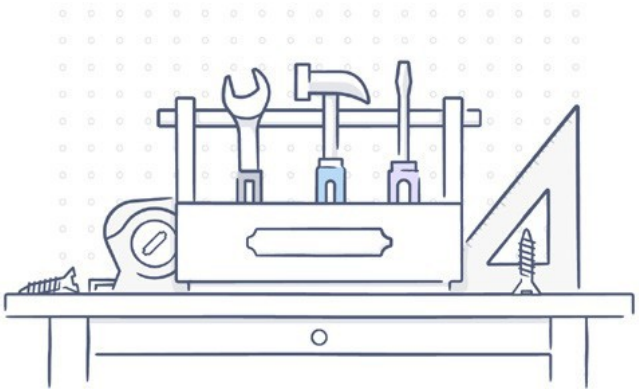
Seguridad: protección y control

Protección: arquitectura y seguridad de la información

Dropbox está diseñado con una infraestructura segura y distribuida, y cuenta con múltiples capas de protección, que incluyen transferencia segura de datos, cifrado, configuración de red y controles a nivel de aplicación distribuidos en una infraestructura escalable y segura. Nuestro sólido marco de gestión para la seguridad de la información está diseñado para evaluar los riesgos y crear una cultura de seguridad en Dropbox. Regularmente revisamos y actualizamos las políticas de seguridad, proporcionamos a nuestros empleados capacitaciones de seguridad, realizamos pruebas de seguridad de aplicaciones y redes (incluidas las pruebas de penetración), realizamos evaluaciones de riesgo y monitoreamos el cumplimiento de las políticas de seguridad. Los detalles completos se pueden encontrar en el Informe de Dropbox sobre seguridad en la empresa.

Control: empoderamiento de los administradores de TI

Dropbox proporciona las características de control y de visibilidad que necesitan los administradores de TI, lo que te ayuda a gestionar tus obligaciones de cumplimiento con mayor facilidad. Nuestro panel de administración te permite monitorear la actividad del equipo, ver los dispositivos conectados y auditar la actividad de intercambio. Puedes crear grupos para administrar fácilmente el acceso de los miembros del equipo a carpetas específicas, y el gestor de la carpeta del equipo te brinda visibilidad y control sobre estas carpetas, incluida la administración de la sincronización. La característica de permisos por vínculos te permite proteger con contraseña los vínculos compartidos, establecer fechas de caducidad para otorgar acceso temporal y limitar el acceso a aquellos en tu organización. Con nuestra herramienta de transferencia de cuenta, puedes transferir fácilmente archivos de un usuario a otro cuando cambian las responsabilidades. El borrado remoto te permite borrar archivos de dispositivos perdidos o robados.



Cumplimiento: confianza y verificación

El cumplimiento es una forma efectiva de validar la confianza de un servicio. Te alentamos a comprobar que nuestras prácticas de seguridad cumplen con las regulaciones y las normas más aceptadas en el mundo, como ISO 27001 y SOC 1, 2 y 3. Nuestros auditores externos independientes prueban nuestros controles y brindan sus informes y opiniones, los que compartimos contigo siempre que es posible. Puedes encontrar más información sobre los estándares con los que cumplimos y la manera en que verificamos las prácticas de seguridad en nuestra página de cumplimiento.

Privacidad: nuestro compromiso

Tú eres propietario de tus datos, y, ya sea información personal o de trabajo, tomamos la confianza de nuestros usuarios con mucha seriedad y trabajamos arduamente para garantizar la protección de todos los datos en nuestros sistemas. Nuestra política de privacidad claramente describe cómo administramos y protegemos tu información. Publicamos un informe de transparencia y nuestros principios para solicitudes de datos del gobierno, a fin de compartir con qué frecuencia recibimos, analizamos y respondemos estas solicitudes. Además, intentamos reformar las leyes para que protejan nuestra privacidad de manera más eficiente.

Trabajo en conjunto para mantener tus datos seguros

Dropbox trabaja con sus clientes comerciales para mantener sus datos seguros. Tomamos medidas integrales para proteger infraestructura, red y aplicaciones, capacitamos a los empleados en prácticas de seguridad y de privacidad, construimos una cultura donde ser digno de confianza es la prioridad principal, y hacemos que terceros prueben y auditen rigurosamente nuestros sistemas y prácticas. Los clientes también desempeñan un papel fundamental al garantizar que sus equipos y sus datos estén protegidos y seguros. Dropbox te permite configurar, usar y monitorear tu cuenta de manera que cubra las necesidades de seguridad, privacidad y cumplimiento de tu organización. Nuestra guía de responsabilidad compartida puede ayudarte a comprender mejor lo que hacemos para mantener tu cuenta segura y lo que puedes hacer para mantener la visibilidad y el control sobre los datos de tu equipo.