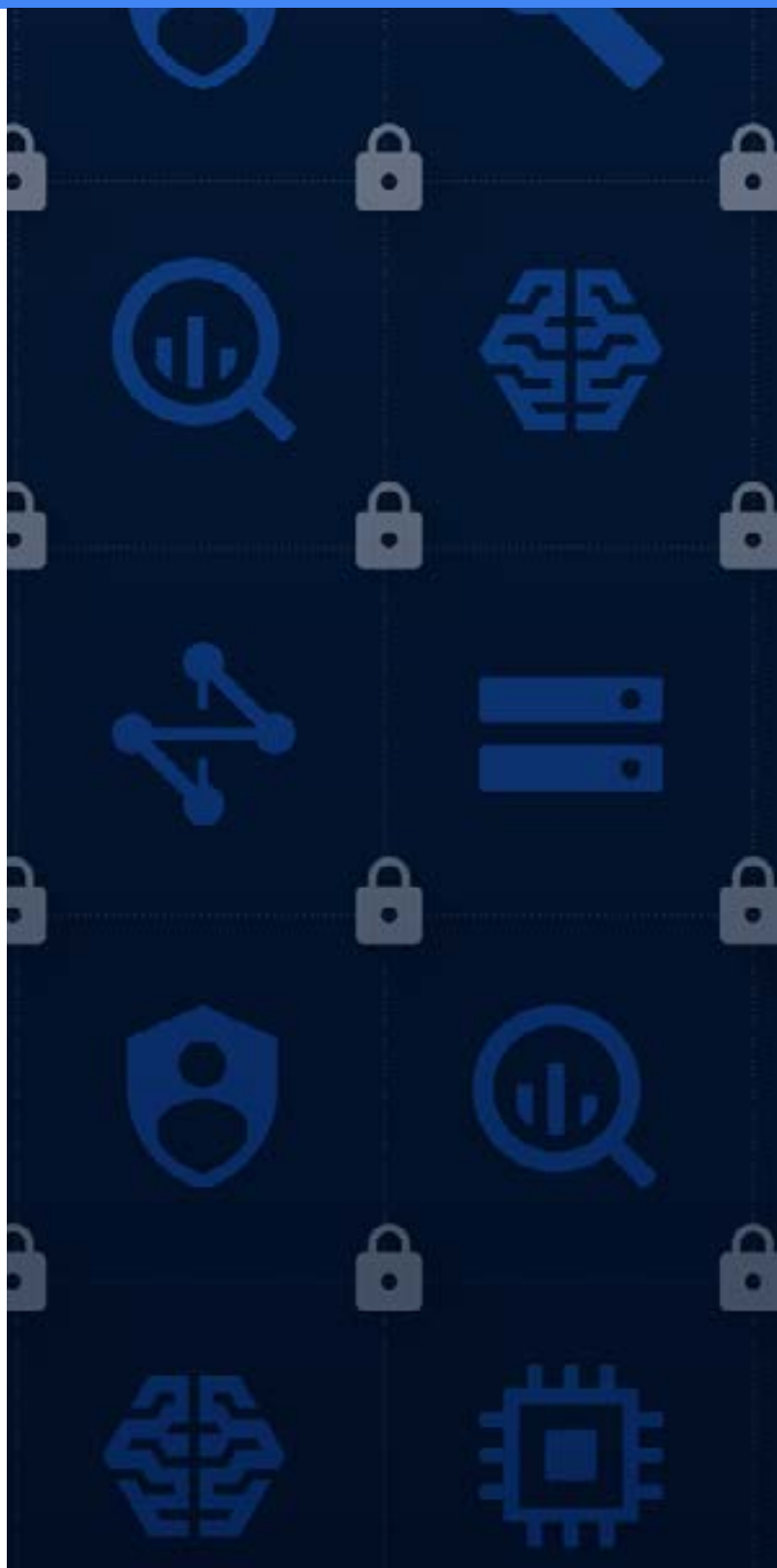
Google Cloud

Reglamento General de Protección de Datos (RGPD)



INTRODUCCIÓN

Reglamento General de Protección de Datos (RGPD)

La normativa europea más importante en materia de protección de datos de los últimos veinte años entrará en vigor el 25 de mayo del 2018. El Reglamento General de Protección de Datos (RGPD) reemplazará a la actual Directiva de Protección de Datos 95/46/CE. El RGPD refuerza los derechos de los individuos en lo que respecta a sus datos personales y busca unificar las leyes de protección de datos en Europa con independencia del lugar en el que se procesen los datos.

Puedes tener la seguridad de que nos comprometemos a cumplir el RGPD en los servicios de Google Cloud Platform. También nos comprometemos a ayudar a nuestros clientes en su proceso de adaptación al RGPD con las potentes medidas de seguridad y privacidad que hemos integrado en nuestros servicios y en nuestros contratos a lo largo de los años.

QUÉ PUEDES HACER

¿Cuáles son tus responsabilidades como cliente?

Normalmente, los clientes de G Suite[1] y de Google Cloud Platform actúan como controladores de los datos personales que proporcionan a Google con el objetivo de usar sus servicios. Los controladores determinan las finalidades del tratamiento de los datos personales, así como los medios con que se llevará a cabo. En cambio, la tarea de los encargados consiste en tratar los datos en nombre de los controladores. Google es un encargado del tratamiento de los datos que procesa los datos personales en nombre del controlador cuando este utiliza G Suite o Google Cloud Platform. Los responsables del tratamiento de los datos deben implementar las medidas técnicas y organizativas apropiadas para garantizar y demostrar que todos los procesos relacionados la información personal se llevan a cabo de acuerdo con el RGPD. Las obligaciones de estos responsables están relacionadas con principios como la licitud, lealtad y transparencia, la limitación de la finalidad, la minimización de los datos y la exactitud de estos, así como con facilitar los derechos de los interesados con respecto a sus datos.

Si eres un responsable del tratamiento de los datos, puedes obtener más información sobre las responsabilidades que implica el RGPD en tu caso en el sitio web de la autoridad de protección de datos nacional o competente relacionada con este reglamento (según corresponda)[2]. Te recomendamos que también consultes con frecuencia las publicaciones de las asociaciones dedicadas a la privacidad, como la **asociación internacional de profesionales de la privacidad (IAPP)**.

También deberías buscar asesoramiento legal independiente para conocer tu estado y tus obligaciones en relación al RGPD, ya que solo un abogado puede ofrecerte el asesoramiento legal más adecuado para tu situación. El objetivo de este sitio web no es ofrecerte asesoramiento legal ni debería usarse en sustitución de este.

¿Por dónde deberías empezar?

Si eres cliente de Google Cloud o lo vas a ser dentro de poco, este es un buen momento para empezar a prepararte para el RGPD. Estos consejos te ayudarán:

- Familiarízate con las disposiciones del RGPD y presta especial atención a las diferencias que pueda haber con tus obligaciones de protección de datos actuales.
- Plantéate crear un inventario actualizado de los datos personales que manejas. Puedes usar algunas de nuestras herramientas para identificar y clasificar los datos más fácilmente.
- Repasa los controles, las políticas y los procesos que sigues para determinar si cumplen los requisitos del RGPD y elabora un plan para poner remedio a los aspectos que estén en disonancia.
- Piensa en cómo puedes aprovechar las funciones de protección de datos con las que cuentas actualmente en Google Cloud como parte de tu propio marco de trabajo de cumplimiento normativo. Revisa los materiales de la auditoría externa y de la certificación de G Suite o de Google Cloud Platform para descubrir cómo pueden ayudarte en este aspecto.
- Consulta el material de asesoramiento sobre la normativa actualizada en cuanto esté disponible y ponte en contacto con un abogado para obtener un asesoramiento legal que se adapte a las circunstancias específicas de tu empresa.

1 G Suite incluye G Suite Business y G Suite para Centros Educativos.

2 Te recomendamos que recurras a un servicio externo de asesoramiento legal para determinar qué autoridad de protección de datos nacional o competente se aplica en tu caso.

QUÉ ESTAMOS HACIENDO

Compromisos con el RGPD de G Suite y Google Cloud Platform

Los responsables del tratamiento de los datos están obligados, entre otras cosas, a garantizar la implementación de medidas técnicas y organizativas apropiadas de acuerdo con los requisitos del RGPD. A continuación encontrarás algunos aspectos que podrías tener en cuenta a la hora de llevar a cabo la evaluación de tus servicios de G Suite y Google Cloud Platform.

LOS CONOCIMIENTOS, LA FIABILIDAD Y LOS RECURSOS DE UN EXPERTO

Experiencia en la protección de datos

Google emplea a profesionales en el ámbito de la seguridad y de la privacidad, entre los que se encuentran algunos de los mayores expertos del mundo en materia de seguridad de la información, de aplicaciones y de redes. Este equipo se dedica a mantener los sistemas de defensa de la empresa, a desarrollar los procesos de evaluación de seguridad, a crear la infraestructura de seguridad y a implementar las políticas de seguridad de Google. Google también cuenta con un nutrido equipo de abogados, expertos en el cumplimiento normativo y especialistas de políticas públicas que se encargan de preservar el cumplimiento de la privacidad y de la seguridad de Google. Estos equipos están en contacto con los clientes y actores de la industria, así como con las autoridades de supervisión con el fin de modelar nuestros servicios de G Suite y de Google Cloud Platform de forma que nuestros clientes puedan cumplir con sus obligaciones.

COMPROMISOS DE PROTECCIÓN DE DATOS

Contratos de tratamiento de datos

Los contratos de tratamiento de datos de G Suite y Google Cloud Platform exponen con claridad los compromisos que hemos adquirido con nuestros clientes en lo que respecta a la privacidad. A lo largo de los años, hemos cambiado estas condiciones gracias a los comentarios de nuestros clientes y de los organismos reguladores. Hace poco, las hemos actualizado específicamente para que reflejen el RGPD y las hemos puesto a disposición de los clientes con suficiente antelación antes de que el reglamento entre en vigor para facilitar la valoración de su cumplimiento y su disposición en relación al RGPD cuando usen los servicios de Google Cloud.
Ahora, los clientes pueden aceptar estas condiciones de tratamiento de datos actualizadas a través del proceso de participación que se describe aquí para la enmienda sobre tratamiento de datos de G Suite y aquí para los términos y condiciones de seguridad y de tratamiento de datos de Google Cloud Platform. La actualización de las condiciones surtirá efecto a partir del 25 de mayo del 2018 (inclusive), cuando el RGPD entrará en vigor.

Tratamiento basado en instrucciones

Los datos que introducen nuestros clientes y sus usuarios en nuestros sistemas se tratarán única y exclusivamente de acuerdo con sus instrucciones, tal y como se describe en nuestros contratos de tratamiento de datos de RGPD actuales y actualizados.

Compromiso de confidencialidad del personal

Todos los empleados de Google deben aceptar un acuerdo de confidencialidad y realizar cursos sobre la confidencialidad y la privacidad, así como recibir nuestra formación sobre el ***Código de Conducta.*** *En el código de conducta de Google se incluyen de forma específica las responsabilidades y el comportamiento que se espera de nuestros empleados en relación con la protección de la información.*

USO DE ENCARGADOS DEL TRATAMIENTO

Las empresas del grupo Google llevan a cabo la mayor parte de las actividades de tratamiento de datos necesarias para poder ofrecer los servicios de G Suite y de Google Cloud Platform. No obstante, colaboramos con terceros que ofrecen asistencia para estos servicios. Estos proveedores se someten a un exigente proceso de selección para garantizar que cuentan con los conocimientos técnicos necesarios y que son capaces de ofrecer el nivel adecuado de seguridad y de privacidad.

Puedes consultar la información sobre los subencargados del tratamiento de datos del grupo Google que ofrecen asistencia para los servicios de G Suite y Google Cloud Platform, así como sobre los subencargados de terceros involucrados en estos servicios. También incluimos compromisos relacionados con los subencargados en nuestros acuerdos actuales y actualizados de tratamiento de datos.

SEGURIDAD DE LOS SERVICIOS

Según el RGPD, el controlador de los datos y el encargado de su tratamiento deben implementar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad acorde al riesgo.

En Google contamos con una infraestructura global diseñada para ofrecer una seguridad puntera durante todo el ciclo de tratamiento de la información. Esta infraestructura se ha desarrollado para garantizar la seguridad de nuestros usuarios en todos los procesos: la implementación de servicios, el almacenamiento de datos con medidas de privacidad para el usuario final, las comunicaciones entre servicios, las comunicaciones seguras y privadas con los clientes a través de Internet y las operaciones seguras de los administradores. G Suite y Google Cloud Platform se ejecutan en esta infraestructura.

Hemos diseñado la seguridad de nuestra infraestructura en capas que se sustentan recíprocamente, desde la seguridad física de los centros de datos hasta las medidas de seguridad de nuestros hardware y software, pasando por los procesos que utilizamos para aumentar la seguridad operativa. Gracias a esta protección por capas, conseguimos unos sólidos cimientos en materia de seguridad para todas las acciones que realizamos.

Puedes encontrar una descripción detallada de nuestra infraestructura de seguridad en el **informe técnico sobre el diseño de la infraestructura de seguridad de Google.**

Disponibilidad, integridad y resistencia

Diseñamos los componentes de nuestra plataforma para que sean altamente redundantes. Los centros de datos de Google están distribuidos geográficamente para minimizar los efectos de las interrupciones del servicio regionales (como desastres naturales o problemas locales) en los productos que funcionan en todo el mundo. Si se produce un fallo en el hardware, en el software o en la red, los servicios se trasladan de una instalación a otra de forma automática e instantánea, de modo que las operaciones pueden continuar sin interrumpirse. Nuestra infraestructura es altamente redundante, lo que protege a los clientes frente a las pérdidas de datos.

Pruebas

Cada año, llevamos a cabo pruebas relacionadas con la recuperación tras fallos con el objetivo de ofrecer un espacio coordinado para que los equipos de Infraestructura y Aplicaciones comprueben los planes de comunicación, las situaciones de conmutación por error, la transición operacional y otras respuestas de emergencia. Todos los equipos que participan en el ejercicio de recuperación tras fallos desarrollan planes de pruebas y análisis posteriores, en los que se deja constancia de los resultados y de las lecciones extraídas de las pruebas.

Encriptado

Google utiliza el encriptado para proteger los datos, tanto los que están en tránsito como los que están en reposo. Los datos en tránsito con destino a G Suite están protegidos mediante HTTPS (esta opción está activada de forma predeterminada para todos los usuarios). Los servicios de G Suite y de Google Cloud Platform encriptan el contenido en reposo que los usuarios hayan almacenado mediante uno o varios mecanismos de encriptado, sin que estos tengan que realizar ninguna acción. Puedes encontrar una descripción detallada de cómo encriptamos los datos en nuestro **informe técnico sobre el encriptado.**

Controles de acceso

Los derechos y niveles de acceso de los empleados de Google se basan en la función que desempeñan en su puesto de trabajo. Se aplican según los conceptos de asignación del menor grado de privilegios preciso y de información en el caso exclusivo de que sea necesario, de modo que los derechos de acceso se asignan en función de las responsabilidades definidas. Las peticiones para obtener más derechos de acceso siguen un proceso formal en el que es necesario que el propietario del sistema o de los datos, el administrador u otros directivos (tal y como dictan las políticas de seguridad de Google) aprueben la petición.

Administración de las vulnerabilidades

Buscamos vulnerabilidades en el software mediante una combinación de herramientas disponibles para el público general y herramientas internas específicas; pruebas de penetración exhaustivas, tanto manuales como automáticas; procesos de control de calidad; revisiones de seguridad de software y auditorías externas. La comunidad investiga cuestiones de seguridad de un modo más amplio, por lo que también valoramos enormemente su labor a la hora de identificar las vulnerabilidades de G Suite, de Google Cloud Platform y de otros productos de Google. Nuestro Vulnerability Reward Program anima a los usuarios a informarnos de problemas relacionados con el diseño y el despliegue de nuestros productos que podrían poner en peligro los datos de los clientes.

Seguridad de los productos: G Suite

Los clientes de G Suite pueden utilizar las funciones y las opciones de configuración de nuestros productos para mejorar la protección de sus datos personales ante cualquier tratamiento no autorizado o ilegal:

- *La verificación en dos pasos reduce en gran medida el riesgo de accesos no autorizados al pedir a los usuarios más pruebas que demuestren su identidad cuando inician sesión. El uso obligatorio de la llave de seguridad añade otra capa de protección a las cuentas de los usuarios al precisar de una llave física.*
- *Las alertas de inicio de sesión sospechoso permiten detectar inicios de sesión de este tipo mediante funciones de aprendizaje automático muy potentes.*
- *La seguridad aumentada para el correo electrónico hace que todos los mensajes deban firmarse y encriptarse a través de extensiones seguras multipropósito de correo de Internet (S/MIME).*
- *La prevención de la pérdida de datos (DLP) sirve para evitar que la información confidencial incluida en Gmail y Drive pueda compartirse sin autorización. Puedes encontrar más información en nuestro informe técnico sobre la DLP.*
- *Gracias a la administración de derechos de la información de Drive, puedes inhabilitar la descarga, la impresión y la copia de archivos desde el menú de uso compartido avanzado, así como establecer fechas de vencimiento para el acceso a los archivos.*
- *La gestión de dispositivos móviles te permite supervisar el sistema de forma continua y recibir alertas si se detecta actividad sospechosa en los dispositivos.*

Si quieres obtener más información, visita esta página web

Seguridad de los productos: Google Cloud Platform

Los clientes de Google Cloud Platform pueden utilizar las funciones y opciones de configuración de nuestros productos para mejorar la protección de sus datos personales ante cualquier tratamiento no autorizado o ilegal:

- *La verificación en dos pasos reduce en gran medida el riesgo de que se produzca un acceso no autorizado al pedir a los usuarios más pruebas que demuestren su identidad cuando inicien sesión. El uso obligatorio de la llave de seguridad añade otra capa de protección a las cuentas de los usuarios al precisar de una llave física.*
- *La gestión de identidades y accesos de Google Cloud (Cloud IAM) te brinda la posibilidad de crear y administrar al detalle los permisos de acceso y modificación de los recursos de Google Cloud Platform.*
- *La API Data Loss Prevention te permite identificar y supervisar el tratamiento de categorías especiales de datos personales para desplegar los controles adecuados.*
- *Stackdriver Logging y Stackdriver Monitoring te ofrecen la opción de integrar el almacenamiento de registros, la supervisión, las alertas y los sistemas de detección de anomalías en Google Cloud Platform.*
- *Cloud Identity-Aware Proxy (Cloud IAP) controla el acceso a las aplicaciones en la nube que se ejecutan en Google Cloud Platform.*
- *Cloud Security Scanner busca y detecta vulnerabilidades comunes en las aplicaciones de Google App Engine.*

Si quieres obtener más información, visita esta página web

DEVOLUCIÓN Y ELIMINACIÓN DE DATOS

Durante el periodo de vigencia del acuerdo, los administradores pueden exportar los datos de los clientes en cualquier momento mediante la funcionalidad específica de los servicios de G Suite o de Google Cloud Platform. Los compromisos relacionados con la exportación de datos han estado presentes en nuestras condiciones de tratamiento de datos desde hace varios años (y seguiremos ofreciéndolos después de que el RGPD entre en vigor). También trabajamos sin descanso para mejorar la solidez de las funciones de exportación de datos de los servicios de G Suite, así como de todos los servicios de Google Cloud Platform (consulta la documentación de Google Cloud Platform para obtener más información).

Además, la funcionalidad específica de los servicios de G Suite y Google Cloud Platform te permite eliminar los datos de clientes en cualquier momento. Cuando nos indicas que quieres que nos deshagamos de algo por completo (por ejemplo, cuando un mensaje de correo electrónico borrado ya no se puede recuperar de la papelera), eliminamos todos los datos relevantes del cliente de todos nuestros sistemas en un máximo de 180 días, a menos que se apliquen obligaciones de retención de datos.

ASISTENCIA AL RESPONSABLE

Derechos del interesado

Los controladores de los datos pueden utilizar las consolas de administración de G Suite o de Google Cloud Platform, así como la funcionalidad incluida en sus servicios, para rectificar o eliminar los datos que ellos mismos o sus usuarios hayan introducido en nuestros sistemas, así como para acceder a ellos o restringir su tratamiento. El Reglamento General de Protección de Datos (RGPD) otorga ciertos derechos a las personas a quienes se refieren los datos, por lo que los controladores de los datos encontrarán esta funcionalidad muy útil para responder a las peticiones de estas personas y cumplir sus obligaciones.

Equipo de protección de datos

Nuestros clientes tienen a su disposición un equipo específico al que pueden acudir con sus consultas relacionadas con la protección de datos de G Suite y de Google Cloud Platform.

Notificaciones de incidentes

Desde hace años, hemos contraído compromisos contractuales relacionados con la notificación de incidentes en G Suite y Google Cloud Platform. Seguiremos informándote lo antes posible de los incidentes relacionados con los datos de tus clientes de acuerdo con las condiciones correspondientes incluidas en nuestros acuerdos actuales y en las condiciones actualizadas que se aplicarán a partir del 25 de mayo del 2018 (inclusive), cuando el RGPD entre en vigor.

TRANSFERENCIAS INTERNACIONALES DE DATOS

El RGPD ofrece varios mecanismos para facilitar la transferencia de datos personales fuera de la Unión Europea (UE). Estos mecanismos se han establecido para comprobar que el nivel de protección sea el adecuado o para garantizar la implementación de las medidas de seguridad pertinentes a la hora de transferir los datos personales a un país que no pertenezca a la UE. Este nivel de seguridad se puede alcanzar mediante las cláusulas contractuales tipo. Es posible ratificar que el nivel de protección es el adecuado mediante decisiones de constatación como las del marco Escudo de la privacidad UE-EE. UU. En nuestros contratos actuales sobre el tratamiento de datos, nos comprometemos a mantener un mecanismo que facilite la transferencia de datos personales fuera de la UE, tal y como se estipula en la Directiva de Protección de Datos. Además, ofreceremos un compromiso correspondiente a partir del 25 de mayo del 2018 (inclusive), cuando el RGPD entrará en vigor.
La certificación de Google conforme al marco Escudo de la privacidad, tanto el que mantiene con la UE como el que ha firmado con Suiza, ***incluye a G Suite y a Google Cloud Platform****. Las autoridades de protección de datos europeas también han confirmado que nuestras cláusulas contractuales tipo cumplen los requisitos de seguridad necesarios. Esto demuestra que los compromisos contractuales de G Suite y de Google Cloud Platform cumplen la Directiva de Protección de Datos y ofrecen un marco legal para las transferencias de datos personales desde la UE hasta otros lugares del mundo.*

ESTÁNDARES Y CERTIFICACIONES

Tanto nuestros clientes como los organismos reguladores esperan que entidades independientes lleven a cabo controles relativos a la seguridad, la privacidad y el cumplimiento. G Suite y Google Cloud Platform se someten a varias auditorías externas con regularidad para poder ofrecer esta garantía.

ISO 27001 (gestión de la seguridad de la información) ISO 27001 es uno de los estándares de seguridad independientes más reconocidos y aceptados internacionalmente. Google ha obtenido la certificación ISO 27001 para los sistemas, las aplicaciones, las personas, la tecnología, los procesos y los centros de datos que componen nuestra infraestructura común compartida, así como para los productos de G Suite y de Google Cloud Platform.

ISO 27017 (seguridad en la nube) ISO 27017 es un estándar internacional de prácticas para llevar a cabo tareas de control relacionadas con la seguridad de la información. Se basa en ISO/IEC 27002 y es específico para los servicios en la nube. Google ha obtenido la certificación ISO 27017 para G Suite y para Google Cloud Platform.

ISO 27018 (privacidad en la nube) ISO 27018 es un estándar internacional de prácticas relacionadas con la protección de información personal identificable en los servicios de la nube pública. Google ha obtenido la certificación ISO 27018 para G Suite y para Google Cloud Platform.

SSAE16/ISAE 3402 (SOC 2/3) Los marcos de trabajo de auditoría SOC 2 (controles de organizaciones de servicios) y SOC 3 del instituto estadounidense de contables públicos certificados (AICPA) definen los principios de confianza y los criterios para garantizar la seguridad, la disponibilidad, la integridad del tratamiento y la confidencialidad. Google cuenta con los informes SOC 2 y SOC 3, tanto para Google Cloud Platform como para G Suite.

PREGUNTAS FRECUENTES

" ¿QUÉ ES EL RGPD? "

El Reglamento General de Protección de Datos es una nueva legislación de la UE que afecta a la protección de la privacidad y que sustituirá a la Directiva 95/46/CE sobre la protección de datos del 24 de octubre de 1995.

" ¿CUÁNDO ENTRARÁ EN VIGOR EL RGPD? "

El Reglamento General de Protección de Datos entrará en vigor el 25 de mayo del 2018 en todos los Estados miembros de la Unión Europea.

" ¿NOS OBLIGA EL RGPD A ALMACENAR LOS DATOS PERSONALES EN LA UE? "

No. Al igual que ocurre con la Directiva 95/46/CE sobre la protección de datos, el RGPD establece algunas condiciones para la transferencia de los datos personales a países que no pertenezcan a la UE. Dichas condiciones se pueden cumplir mediante mecanismos como las cláusulas del contrato modelo.

" ¿EL RGPD PERMITIRÁ A LOS CLIENTES LLEVAR A CABO AUDITORÍAS DE GOOGLE CLOUD? "

El RGPD establece que los controladores de los datos deben tener derechos de auditoría en sus contratos con los encargados del tratamiento de datos. Ofreceremos nuestros acuerdos actualizados de tratamiento de datos a partir del 25 de mayo del 2018, cuando el RGPD entre en vigor. Por tanto, se incluirán los derechos de auditoría en beneficio de nuestros clientes.

" ¿CUÁL ES LA FUNCIÓN DE LOS INFORMES EXTERNOS ISO 27001, ISO 27017, ISO 27018 Y SOC 2/3 EN EL CUMPLIMIENTO DEL RGPD? "

Los clientes pueden utilizar las certificaciones ISO y los informes de auditoría SOC 2/3, que hemos obtenido de entidades externas, para llevar a cabo sus evaluaciones de riesgos y determinar las medidas técnicas y organizativas que deben llevarse a cabo.

" ¿QUÉ OTRA INFORMACIÓN OFRECE GOOGLE SOBRE EL RGPD? "

Consulta **el sitio web de Empresas y datos de Google.**