

NORMA UE · PROTECCIÓN DE DATOS

RGPD: datos personales de la UE en Sudamérica

El RGPD (Reglamento General de Protección de Datos) se aplica también a empresas sin sede en la UE. Con más frecuencia aún le llega a través de sus clientes europeos, en cuanto usted trata datos personales por encargo de ellos.

FUENTE LEGAL	VIGENTE DESDE	CON ADECUACIÓN	AFECTA A
Reglamento (UE) 2016/679	25/05/2018	Argentina, Uruguay, Brasil	Proveedores para personas en la UE y encargados del tratamiento

En pocas palabras

El RGPD (Reglamento General de Protección de Datos) regula cómo se pueden tratar los datos personales: nombres, direcciones de correo electrónico, números de cliente, datos de ubicación, datos de salud y todo lo que pueda asociarse a una persona. Se aplica directamente en todos los Estados miembros desde el 25/05/2018.

Para las empresas de fuera de la UE hay dos vías por las que el RGPD entra en juego. La primera es el principio del lugar de mercado del artículo 3, apartado 2: quien ofrece bienes o servicios a personas en la UE o controla su comportamiento, por ejemplo mediante rastreo en un sitio web, queda sujeto directamente al RGPD. La segunda vía es más común. Una empresa de la UE le encarga a usted tratar datos por cuenta de ella, y solo puede hacerlo si existe un contrato según el artículo 28 y si la transferencia a su país está permitida por el capítulo V (arts. 44 a 50).

El capítulo V prevé varias bases. La más sencilla es una decisión de adecuación de la Comisión según el artículo 45: su país se considera seguro y los datos circulan como dentro de la UE. Si no existe, el cliente europeo necesita garantías adecuadas según el artículo 46, que en la práctica casi siempre son las cláusulas contractuales tipo de la Comisión (Decisión de Ejecución (UE) 2021/914).

Las autoridades de control pueden imponer multas de hasta 20 millones de euros o el 4 % del volumen de negocios anual mundial, lo que sea mayor (art. 83, apartado 5). Frente a empresas de fuera de la UE la ejecución es más difícil, pero frente a su cliente europeo no lo es. Por eso él revisa con cuidado a quién confía datos y se asegura por contrato responsabilidad y derechos de control. Una filtración de datos en un proveedor de Lima recae jurídicamente sobre el contratante en Madrid.

A quién afecta en Sudamérica

Están afectados directamente las tiendas en línea, los proveedores SaaS, los operadores turísticos, las escuelas de idiomas o las empresas de aplicaciones que se dirigen de forma específica a clientes en la UE. Un hotel en Cusco con una página de reservas en alemán y precios en euros entra en esta categoría. Estas empresas deben designar un representante en la UE según el artículo 27. Solo queda exceptuado el tratamiento ocasional que no incluya a gran escala datos sensibles (art. 27, apartado 2).

Afectados de forma indirecta están todos los encargados del tratamiento: un centro de contacto en Bogotá para una operadora de telecomunicaciones española, soporte de TI desde Córdoba, liquidación de sueldos, desarrollo de software con datos reales de clientes, análisis de datos, alojamiento en la nube.

PAÍS	DECISIÓN DE ADECUACIÓN DE LA UE	QUÉ NECESITA EL CLIENTE DE LA UE
Argentina	Sí, Decisión 2003/490/CE, confirmada en el informe de la Comisión del 15/01/2024	Contrato según el art. 28
Uruguay	Sí, Decisión de Ejecución 2012/484/UE, confirmada el 15/01/2024	Contrato según el art. 28
Brasil	Sí, adoptada el 26/01/2026	Contrato según el art. 28
Chile , Colombia , Perú , Ecuador , Paraguay , Bolivia	No	Contrato según el art. 28, cláusulas contractuales tipo y evaluación de impacto de la transferencia

La decisión sobre Brasil es recíproca: la autoridad brasileña de protección de datos, la ANPD, reconoció a su vez a la UE como adecuada. Abarca tanto el sector público como el privado. Para una empresa de software de Florianópolis, desde la decisión del 26/01/2026 ya no hacen falta cláusulas contractuales tipo ni evaluación de impacto de la transferencia para los datos que llegan desde la UE. Eso ahorra buena parte del papeleo que antes tenía con cada cliente de la UE.

La adecuación le ahorra las cláusulas contractuales tipo, pero no el contrato del artículo 28 ni las medidas técnicas de protección. Su cliente le seguirá pidiendo ambas cosas.

Plazos

El RGPD rige sin cambios desde 2018. Las fechas nuevas tienen que ver sobre todo con la región: la decisión de adecuación para Brasil del 26/01/2026 y nuevas leyes nacionales, por ejemplo en [Chile](#) y [Paraguay](#), que todavía no son plenamente aplicables.

En noviembre de 2025 la Comisión propuso un “Ómnibus Digital” que también modificaría partes del RGPD. Mientras la propuesta no se apruebe, el RGPD rige en su versión conocida. Por eso, planifique con el derecho vigente.

Aun así, en el día a día hay plazos. El responsable del tratamiento en la UE debe notificar una violación de la seguridad de los datos a la autoridad de control en 72 horas (art. 33). Como encargado del tratamiento, usted debe avisarle “sin dilación indebida”, y muchos contratos fijan para eso 24 o 48 horas.

Qué piden en concreto los clientes de la UE

- Un contrato de encargo del tratamiento (en inglés DPA) según el artículo 28, por lo general sobre el modelo del cliente.
- Para países sin adecuación, las cláusulas contractuales tipo, normalmente el módulo 2 (de responsable a encargado) o el módulo 3 (de encargado a subencargado).
- Una evaluación de impacto de la transferencia (Transfer Impact Assessment) que analice si las autoridades de su país pueden acceder a los datos.
- Una descripción de sus medidas técnicas y organizativas según el artículo 32.
- Una lista de sus subencargados, por ejemplo proveedores de nube y sistemas de tickets.
- Un registro de las actividades de tratamiento para los datos del cliente.
- Como respaldo de esas medidas, a menudo un certificado [ISO/IEC 27001](#), a veces complementado con ISO/IEC 27701 para privacidad.

Quien se dirige directamente a clientes en la UE necesita además una política de privacidad conforme al RGPD, una base jurídica para cada tratamiento, un procedimiento para solicitudes de acceso y supresión y, en su caso, el representante en la UE del artículo 27.

Primeros pasos

1. Determine si se dirige directamente a personas en la UE o si solo trata datos para empresas de la UE. De eso depende si necesita un representante en la UE.

2. Haga una lista de los datos personales que recibe de clientes de la UE, dónde se almacenan y quién tiene acceso.
3. Revise la legislación de su propio país. La LGPD de Brasil y las leyes de Argentina y Uruguay se parecen al RGPD; en otros países faltan varias cosas. Los detalles están en las páginas por país.
4. Prepare una descripción de sus medidas técnicas y organizativas que pueda entregar a cualquier cliente.
5. Defina un procedimiento para violaciones de seguridad de los datos, con aviso al cliente dentro del plazo contractual.
6. Haga el [diagnóstico UE](#) gratuito para ver sus brechas.

Una plataforma GRC como [Sightadel](#) ayuda a mantener al día el registro, las medidas técnicas y organizativas y los contratos para muchos clientes.

Relación con las certificaciones

El RGPD prevé certificaciones propias según el artículo 42, que en la práctica son poco frecuentes. Por eso los clientes de la UE recurren a [ISO/IEC 27001](#) para acreditar la seguridad del tratamiento según el artículo 32. Los proveedores SaaS con clientes en Estados Unidos suelen tener un [informe SOC 2](#), que muchos clientes de la UE también aceptan. Si trabaja con IA y datos personales, conviene mirar el [Reglamento de Inteligencia Artificial](#). A los proveedores de TI de bancos se les suma [DORA](#), y a muchos otros [NIS2](#).

Un certificado no reemplaza el análisis del caso concreto. Pero demuestra que los derechos de acceso, el cifrado, el registro de eventos y la gestión de incidentes están regulados y que alguien externo los revisa con regularidad. Son justamente los puntos que el cliente pregunta cuando revisa sus medidas técnicas y organizativas. Quien tiene el certificado responde con una referencia en lugar de veinte páginas de explicaciones.

FAQ

¿El RGPD se aplica a mi empresa en Sudamérica?

Sí, si ofrece bienes o servicios a personas en la UE o controla su comportamiento (art. 3, apartado 2). Si solo trata datos por encargo de una empresa de la UE, las obligaciones le llegan a través del contrato del art. 28.

¿Qué aporta la decisión de adecuación para Brasil?

Desde el 26/01/2026 las empresas de la UE pueden transferir datos personales a Brasil sin cláusulas contractuales tipo. El contrato del art. 28 y las medidas de seguridad siguen siendo necesarios. Más información en la página de [Brasil](#).

¿Necesito un representante en la UE?

Si el RGPD se le aplica directamente por el art. 3, apartado 2, por lo general sí (art. 27). Como simple encargado del tratamiento de un cliente de la UE, normalmente no.

¿Qué es una evaluación de impacto de la transferencia?

Un análisis de si el derecho del país de destino, por ejemplo las facultades de acceso de las autoridades, deja sin efecto la protección que dan las cláusulas contractuales tipo. Es habitual en países sin decisión de adecuación.

¿Qué herramienta ayuda a llevar la documentación del RGPD para varios clientes?

[Sightadel](#) trae el RGPD como marco, con plantillas para el registro de actividades de tratamiento, las medidas técnicas y organizativas y el procedimiento ante violaciones de datos. Se desarrolla y se aloja en Alemania, y el tratamiento se hace como encargo según el art. 28 del RGPD. Lo que prepara una vez lo puede entregar a cada cliente.

Fuentes · Actualizado: 11 de octubre de 2026

Reglamento (UE) 2016/679 (RGPD), EUR-Lex: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

Comisión Europea: decisiones de adecuación: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Comisión Europea: declaración conjunta de la UE y la ANPD del 28/01/2026: https://commission.europa.eu/news-and-media/news/joint-press-statement-michael-mcgrath-and-waldemar-goncalves-ortunho-junior-director-president-2026-01-28_en

Informe de la Comisión del 15/01/2024 sobre las decisiones de adecuación vigentes: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024DC0007>

Decisión de Ejecución (UE) 2021/914 (cláusulas contractuales tipo): https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

Información general, no constituye asesoramiento legal. Prevalecen los textos oficiales.

PÓNGALO EN PRÁCTICA CON HERRAMIENTAS HECHAS EN ALEMANIA



Sightadel guía a su equipo por el RGPD: plantillas, tareas, evidencias y preparación de auditorías en un solo lugar. Desarrollado y alojado en Alemania, con paquete de consultoría opcional.

[Ver Sightadel →](#)

veyrisk

veyrisk muestra lo que un atacante ve de su empresa desde fuera: servicios abiertos, certificados, vulnerabilidades conocidas. Puede presentar el informe a clientes europeos y auditores.

[Ver veyrisk →](#)

Sightadel, veyrisk y Valar son productos de neonotu GmbH, empresa que opera MercoEU.

¿Qué parte de esto aplica a su empresa?

El diagnóstico UE gratuito se lo muestra en 10 minutos, según su sector y su país.

<https://www.mercoeu.com/es/diagnostico-ue>