

Acuerdo de Tratamiento de Datos

Cómo trata Vericto los datos personales por cuenta de sus clientes. Forma parte de los Términos de Servicio.

ÚLTIMA ACTUALIZACIÓN	VERSIÓN
2026-10-04	1.1

Partes

Este Acuerdo de Tratamiento de Datos (el "**DPA**") forma parte de los Términos de Servicio o del contrato firmado entre las partes (el "**Contrato**"), entre:

- **El Cliente**, identificado en el Contrato, que actúa como **responsable del tratamiento** (en el GDPR, *controller*; en la Ley 1581 de 2012, *responsable*; en la LGPD, *controlador*); y
- **Vericto S.A.S.**, NIT 902.100.599-0, con domicilio en Bogotá D.C., Colombia ("**Vericto**"), que actúa como **encargado del tratamiento** (*processor / encargado / operador*).

Si hay contradicción entre este DPA y el Contrato en materia de protección de datos, prevalece este DPA.

1. Definiciones

Los términos "datos personales", "tratamiento", "responsable", "encargado", "titular", "subencargado" y "violación de seguridad de los datos personales" tienen el significado que les da la **Normativa Aplicable**, que incluye, según corresponda: el Reglamento (UE) 2016/679 (**GDPR**); el UK GDPR y la Data Protection Act 2018; la Ley 1581 de 2012 y el Decreto 1377 de 2013 (Colombia); la Ley 13.709/2018 (**LGPD**, Brasil); la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México, 2025); y cualquier otra norma de protección de datos que aplique al tratamiento.

"Datos del Cliente" son los datos personales que Vericto trata por cuenta del Cliente al prestar el servicio, descritos en el Anexo I.

2. Objeto y alcance

2.1. Vericto trata los Datos del Cliente únicamente para prestar el servicio descrito en el Contrato (evaluación de sentencias SQL, audit trail, dashboard, alertas y reportes) y según las instrucciones documentadas del Cliente. El Contrato, este DPA y la configuración que el Cliente elige en el dashboard son las instrucciones del Cliente.

2.2. Si Vericto considera que una instrucción infringe la Normativa Aplicable, lo informará al Cliente sin demora y podrá suspender su ejecución hasta que el Cliente la confirme o la modifique.

2.3. Vericto no vende los Datos del Cliente, no los usa para entrenar modelos de inteligencia artificial y no los trata para fines propios, salvo lo necesario para facturar, prevenir abusos y cumplir obligaciones legales.

3. Responsabilidades del Cliente

3.1. El Cliente es responsable de la licitud del tratamiento, de informar a los titulares y de contar con una base legal para que los datos lleguen a Vericto, incluidos los datos personales que puedan aparecer en los literales de las sentencias SQL.

3.2. Vericto ofrece el **modo de telemetría sanitized**: con él, los valores literales de las sentencias se reemplazan por marcadores antes de almacenarse, en todos los canales. Con el proxy TCP y la CLI, el reemplazo ocurre en la infraestructura del Cliente. El modo raw (por defecto) almacena el texto de la sentencia cifrado en reposo. El Cliente elige el modo.

3.3. El proxy TCP se ejecuta en la infraestructura del Cliente y lo opera el Cliente. Vericto no recibe ni almacena los connection strings de las bases de datos del Cliente: se configuran en el proxy, dentro de la infraestructura del Cliente.

4. Confidencialidad

Vericto garantiza que las personas autorizadas a tratar los Datos del Cliente están sujetas a una obligación de confidencialidad, contractual o legal, y solo acceden a ellos en la medida necesaria para prestar el servicio o dar soporte.

5. Seguridad

Vericto aplica las medidas técnicas y organizativas del **Anexo II**, apropiadas al riesgo. Vericto puede actualizarlas siempre que el nivel de protección no disminuya.

6. Subencargados

6.1. El Cliente autoriza de forma general a Vericto a contratar los subencargados del **Anexo III**.

6.2. Vericto avisará al Cliente con al menos **30 días** de antelación antes de agregar o reemplazar un subencargado, por email a los administradores del workspace y en esta página. El Cliente puede oponerse por motivos razonables relacionados con la protección de datos dentro de ese plazo. Si las partes no encuentran una solución, el Cliente puede terminar el servicio afectado sin penalidad.

6.3. Vericto impone a cada subencargado obligaciones de protección de datos equivalentes a las de este DPA y responde ante el Cliente por su cumplimiento.

7. Derechos de los titulares

Teniendo en cuenta la naturaleza del tratamiento, Vericto ayudará al Cliente, con medidas técnicas y organizativas apropiadas, a responder las solicitudes de los titulares (acceso, rectificación, supresión, oposición, portabilidad, entre otras). Si Vericto recibe una solicitud directamente, la remitirá al Cliente sin responderla, salvo que el Cliente lo autorice.

El Cliente dispone en el dashboard de la exportación del audit trail (CSV/JSON), su purga y la eliminación de usuarios y workspaces.

8. Violaciones de seguridad

8.1. Vericto notificará al Cliente **sin demora indebida y a más tardar dentro de las 48 horas** siguientes a tener conocimiento de una violación de seguridad que afecte a Datos del Cliente.

8.2. La notificación incluirá, en la medida en que se conozca: la naturaleza de la violación, las categorías y el número aproximado de titulares y registros afectados, las consecuencias probables, las medidas adoptadas o propuestas y un punto de contacto. La información que no esté disponible al principio se entregará por fases.

8.3. Vericto colaborará con el Cliente para que este cumpla sus obligaciones de notificación a las autoridades y a los titulares.

9. Evaluaciones de impacto

Vericto proporcionará la información razonablemente necesaria para que el Cliente realice evaluaciones de impacto o consultas previas con la autoridad de control relacionadas con el servicio.

10. Auditorías e información

10.1. Vericto pondrá a disposición del Cliente la información necesaria para demostrar el cumplimiento de este DPA: este documento, el Anexo II, la lista de subencargados y las respuestas a cuestionarios de seguridad razonables.

10.2. Vericto está en proceso de certificación SOC 2. Cuando cuente con un informe SOC 2, lo pondrá a disposición del Cliente bajo acuerdo de confidencialidad, y ese informe podrá reemplazar las auditorías del punto 10.3.

10.3. Si la información anterior no es suficiente, o si lo exige una autoridad, el Cliente puede realizar una auditoría, directamente o mediante un auditor independiente sujeto a confidencialidad: como máximo una vez cada 12 meses, salvo tras una violación de seguridad; con al menos 30 días de aviso; en horario laboral y sin afectar a otros clientes. La auditoría corre por cuenta del Cliente, salvo que revele un incumplimiento material de Vericto; Vericto le informará el costo estimado y el alcance cuando la solicite.

11. Transferencias internacionales

11.1. Vericto usa subencargados en distintos países (Anexo III). Toda transferencia internacional se hace con las garantías que exige la Normativa Aplicable:

- **Datos sujetos al GDPR:** las Cláusulas Contractuales Tipo de la Comisión Europea (Decisión (UE) 2021/914), Módulo 2 (responsable a encargado) entre el Cliente y Vericto, y Módulo 3 (encargado a encargado) con los subencargados, que se incorporan por referencia.
- **Datos sujetos al UK GDPR:** el *International Data Transfer Addendum* a esas cláusulas.
- **Datos sujetos a la LGPD:** las cláusulas contractuales estándar de la ANPD (Resolución CD/ANPD n.º 19/2024).
- **Otras jurisdicciones:** los mecanismos de transferencia que exija la normativa aplicable al Cliente.

11.2. En caso de conflicto entre esas cláusulas y este DPA, prevalecen las cláusulas de transferencia.

12. Devolución y eliminación

12.1. Durante la vigencia, el Cliente puede exportar el audit trail en cualquier momento.

12.2. Al terminar el servicio, Vericto eliminará los Datos del Cliente dentro de los **30 días** siguientes, salvo que la ley exija conservarlos. Los datos eliminados desaparecen de las copias de respaldo en un plazo máximo de 30 días; mientras tanto, las copias se mantienen cifradas y fuera de uso.

12.3. A solicitud del Cliente, Vericto confirmará por escrito la eliminación.

13. Responsabilidad, vigencia y ley aplicable

13.1. La responsabilidad de cada parte bajo este DPA está sujeta a las limitaciones del Contrato, salvo donde la Normativa Aplicable no permita limitarla.

13.2. Este DPA rige mientras Vericto trate Datos del Cliente.

13.3. Este DPA se rige por las leyes de la República de Colombia, y cualquier controversia se somete a los jueces y tribunales de Bogotá D.C., salvo cuando las cláusulas de transferencia del punto 11 o normas imperativas aplicables al Cliente exijan otra ley o jurisdicción.

13.4. Vericto puede actualizar este DPA. Los cambios que reduzcan la protección de los Datos del Cliente se notifican con 30 días de antelación; si el Cliente los rechaza, puede terminar el servicio sin penalidad. Una copia firmada conserva su versión hasta que las partes firmen otra.

Anexo I — Descripción del tratamiento

Titulares	(a) Usuarios del Cliente en Vericto (empleados o contratistas con cuenta en el dashboard). (b) Personas cuyos datos aparecen en los literales de las sentencias SQL que el Cliente envía, cuando usa el modo raw. (c) Usuarios de las aplicaciones del Cliente, en la medida en que su dirección IP quede registrada en los eventos de evaluación.
Categorías de datos	Cuenta: nombre, email, rol, idioma, zona horaria, hash de contraseña, secreto MFA cifrado, sesiones (IP y user agent). Uso del servicio: API keys (solo su hash SHA-256), configuración del workspace, reglas y políticas, registro de acciones en el dashboard (IP y user agent). Eventos de evaluación: texto de la sentencia SQL (cifrado; sanitizado en modo sanitized), hash, regla activada, decisión, latencia, IP de cliente, base de datos y dialecto. Reportes de validación: vista previa de cada sentencia (sanitizada en modo sanitized), veredictos, nombre de archivo y procedencia de CI (repositorio, commit, autor). Facturación: la gestiona Paddle como <i>merchant of record</i> ; Vericto no recibe datos de tarjetas.
Datos sensibles	Vericto no los solicita. Pueden aparecer en literales de SQL si el Cliente usa el modo raw; el Cliente puede evitarlo con el modo sanitized.
Naturaleza y finalidad	Evaluar sentencias SQL contra el ruleset del Cliente, registrar las decisiones en el audit trail, mostrar dashboards, enviar alertas, generar reportes y dar soporte.
Duración	La vigencia del Contrato más el plazo de eliminación del punto 12.
Retención durante la vigencia	Audit trail: 7 días (Free), 30 días (Builder), 90 días (Team), configurable (Enterprise). El Cliente puede purgarlo antes.

Anexo II — Medidas técnicas y organizativas

- **Cifrado en tránsito:** TLS 1.3 en las conexiones HTTP y TLS 1.2 o superior en las conexiones TCP del proxy. HSTS en los dominios de Vericto.

- **Cifrado en reposo:** AES-256-GCM para el texto de las sentencias, los secretos de webhooks y los secretos MFA, con claves derivadas por workspace (HKDF sobre una clave maestra). Las API keys se almacenan solo como hash SHA-256 y su valor en claro se muestra una única vez.
- **Minimización:** modo sanitized en todos los canales; el proxy TCP corre en la infraestructura del Cliente, y Vericto no necesita acceso de red a sus bases de datos.
- **Control de acceso:** roles por workspace (owner, admin, member, viewer), MFA (TOTP) para las cuentas, SSO/OIDC para los workspaces que lo configuran, API keys con scopes limitados y fecha de expiración, y claves de corta duración por OIDC para CI/CD.
- **Aislamiento:** cada consulta se limita al workspace del usuario o de la API key, y la base de datos aplica Row Level Security.
- **Integridad y trazabilidad:** audit trail de decisiones que los usuarios no pueden modificar; exportaciones y reportes firmados con Ed25519, verificables sin conexión; registro de eventos de seguridad de las cuentas.
- **Resiliencia:** el proxy sigue evaluando con el último ruleset sincronizado si el control plane no está disponible, y puede guardar la telemetría en disco hasta que vuelva.
- **Copias de respaldo:** el proveedor de base de datos realiza una copia de respaldo diaria, cifrada en reposo. Las copias se conservan como máximo 30 días y luego se eliminan. Vericto prueba su restauración al menos una vez al año.
- **Operación:** revisión de código y pruebas automatizadas en cada cambio; credenciales de infraestructura en un gestor de secretos (AWS SSM Parameter Store), nunca en el código. Vericto realiza, sin limitarse a ellas, pruebas de penetración, gestión de vulnerabilidades y formación del personal, y aplica una política de respuesta a incidentes.
- **Divulgación responsable:** security@vericto.com, con respuesta inicial en menos de 24 horas para vulnerabilidades críticas.

Anexo III — Subencargados

Subencargado	Servicio	Datos	Ubicación
Amazon Web Services, Inc.	Hosting del backend y la API, gestión de secretos, logs	Datos del Cliente que procesa el backend	Estados Unidos (us-east-1)
Supabase, Inc.	Base de datos PostgreSQL	Cuenta, audit trail, configuración, reportes	Estados Unidos (us-east-1)
Cloudflare, Inc.	CDN, DNS y protección DDoS	Tráfico HTTP, direcciones IP	Red global
Resend	Email transaccional	Email del destinatario y contenido del mensaje	Estados Unidos
Paddle.com Market Ltd	Pagos, como merchant of record	Nombre, email, país, datos de facturación	Reino Unido
Stripe, Inc.	Pagos de suscripciones anteriores a Paddle	Nombre, email, datos de facturación	Estados Unidos
Google LLC (Google Analytics 4)	Analítica de uso del dashboard, con IP anonimizada	Eventos de navegación, identificadores de cookie	Estados Unidos

Firmas

Este DPA se acepta al aceptar los Términos de Servicio. Si tu organización necesita una copia firmada, descarga la versión en PDF, complétala y envíala a legal@vericto.com; te la devolvemos firmada por Vericto.

Por el Cliente

Razón social:

Identificación fiscal:

Domicilio:

Nombre del firmante:

Cargo:

Fecha:

Firma

Por Vericto S.A.S.

NIT: 902.100.599-0

Domicilio: Bogotá D.C., Colombia

Nombre del representante legal:

Cargo: Representante legal

Fecha:

Firma