

Data Processing Agreement

How Vericto processes personal data on behalf of its customers. Part of the Terms of Service.

LAST UPDATED	VERSION
2026-10-04	1.1

Parties

This Data Processing Agreement (the "**DPA**") forms part of the Terms of Service or the agreement signed by the parties (the "**Agreement**"), between:

- **The Customer**, identified in the Agreement, acting as **controller** (under Law 1581 of 2012, *responsable*; under the LGPD, *controlador*); and
- **Vericto S.A.S.**, Tax ID (NIT) 902.100.599-0, registered in Bogotá D.C., Colombia ("**Vericto**"), acting as **processor** (*encargado / operador*).

If this DPA and the Agreement conflict on data protection, this DPA prevails.

1. Definitions

The terms "personal data", "processing", "controller", "processor", "data subject", "sub-processor" and "personal data breach" have the meaning given by the **Applicable Law**, which includes, as applicable: Regulation (EU) 2016/679 (**GDPR**); the UK GDPR and the Data Protection Act 2018; Law 1581 of 2012 and Decree 1377 of 2013 (Colombia); Law 13.709/2018 (**LGPD**, Brazil); Mexico's Federal Law on the Protection of Personal Data Held by Private Parties (2025); and any other data protection law that applies to the processing.

"**Customer Data**" means the personal data Vericto processes on behalf of the Customer when providing the service, described in Annex I.

2. Purpose and scope

2.1. Vericto processes Customer Data only to provide the service described in the Agreement (evaluation of SQL statements, audit trail, dashboard, alerts and reports) and on the Customer's documented instructions. The Agreement, this DPA and the configuration the Customer chooses in the dashboard are the Customer's instructions.

2.2. If Vericto believes an instruction infringes the Applicable Law, it will inform the Customer without delay and may suspend it until the Customer confirms or changes it.

2.3. Vericto does not sell Customer Data, does not use it to train artificial intelligence models and does not process it for its own purposes, except as needed for billing, abuse prevention and compliance with legal obligations.

3. Customer responsibilities

3.1. The Customer is responsible for the lawfulness of the processing, for informing data subjects and for having a legal basis for the data to reach Vericto, including any personal data that may appear in the literals of SQL statements.

3.2. Vericto offers the **sanitized telemetry mode**: with it, the literal values of statements are replaced with placeholders before they are stored, on every channel. With the TCP proxy and the CLI, the replacement happens in the Customer's infrastructure. Raw mode (the default) stores the statement text encrypted at rest. The Customer chooses the mode.

3.3. The TCP proxy runs in the Customer's infrastructure and is operated by the Customer. Vericto does not receive or store the connection strings of the Customer's databases: they are configured in the proxy, inside the Customer's infrastructure.

4. Confidentiality

Vericto ensures that the people authorised to process Customer Data are bound by a contractual or statutory duty of confidentiality and only access it as needed to provide the service or support.

5. Security

Vericto applies the technical and organisational measures in **Annex II**, appropriate to the risk. Vericto may update them as long as the level of protection does not decrease.

6. Sub-processors

6.1. The Customer gives Vericto general authorisation to engage the sub-processors in **Annex III**.

6.2. Vericto will notify the Customer at least **30 days** before adding or replacing a sub-processor, by email to the workspace administrators and on this page. The Customer may object on reasonable data protection grounds within that period. If the parties cannot find a solution, the Customer may terminate the affected service without penalty.

6.3. Vericto imposes on each sub-processor data protection obligations equivalent to those in this DPA and remains liable to the Customer for their performance.

7. Data subject rights

Taking into account the nature of the processing, Vericto will assist the Customer, through appropriate technical and organisational measures, in responding to data subject requests (access, rectification, erasure, objection, portability and others). If Vericto receives a request directly, it will forward it to the Customer without answering it, unless the Customer authorises it to.

In the dashboard, the Customer can export the audit trail (CSV/JSON), purge it, and delete users and workspaces.

8. Personal data breaches

8.1. Vericto will notify the Customer **without undue delay and no later than 48 hours** after becoming aware of a breach affecting Customer Data.

8.2. The notification will include, as far as known: the nature of the breach, the categories and approximate number of data subjects and records affected, the likely consequences, the measures taken or proposed and a contact point. Information not available at first will be provided in phases.

8.3. Vericto will cooperate with the Customer so it can meet its notification obligations to authorities and data subjects.

9. Impact assessments

Vericto will provide the information reasonably needed for the Customer to carry out impact assessments or prior consultations with the supervisory authority relating to the service.

10. Audits and information

10.1. Vericto will make available to the Customer the information needed to demonstrate compliance with this DPA: this document, Annex II, the list of sub-processors and answers to reasonable security questionnaires.

10.2. Vericto is in the process of SOC 2 certification. Once it has a SOC 2 report, it will make it available to the Customer under a confidentiality agreement, and that report may replace the audits in section 10.3.

10.3. If the information above is not sufficient, or an authority requires it, the Customer may carry out an audit, directly or through an independent auditor bound by confidentiality: at most once every 12 months, except after a breach; with at least 30 days' notice; during business hours and without affecting other customers. The audit is at the Customer's expense, unless it reveals a material breach by Vericto; Vericto will inform the Customer of the estimated cost and scope when it is requested.

11. International transfers

11.1. Vericto uses sub-processors in several countries (Annex III). Every international transfer is made with the safeguards the Applicable Law requires:

- **Data subject to the GDPR:** the European Commission's Standard Contractual Clauses (Decision (EU) 2021/914), Module 2 (controller to processor) between the Customer and Vericto, and Module 3 (processor to processor) with sub-processors, incorporated by reference.
- **Data subject to the UK GDPR:** the International Data Transfer Addendum to those clauses.
- **Data subject to the LGPD:** the ANPD standard contractual clauses (Resolution CD/ANPD No. 19/2024).
- **Other jurisdictions:** the transfer mechanisms required by the law applicable to the Customer.

11.2. If those clauses conflict with this DPA, the transfer clauses prevail.

12. Return and deletion

12.1. During the term, the Customer can export the audit trail at any time.

12.2. When the service ends, Vericto will delete Customer Data within **30 days**, unless the law requires keeping it. Deleted data disappears from the backups within 30 days at most; until then, the backups stay encrypted and out of use.

12.3. On the Customer's request, Vericto will confirm the deletion in writing.

13. Liability, term and governing law

13.1. Each party's liability under this DPA is subject to the limitations in the Agreement, except where the Applicable Law does not allow limiting it.

13.2. This DPA applies for as long as Vericto processes Customer Data.

13.3. This DPA is governed by the laws of the Republic of Colombia, and any dispute is submitted to the courts of Bogotá D.C., except where the transfer clauses in section 11 or mandatory rules applicable to the Customer require another law or jurisdiction.

13.4. Vericto may update this DPA. Changes that reduce the protection of Customer Data are notified 30 days in advance; if the Customer rejects them, it may terminate the service without penalty. A signed copy keeps its version until the parties sign another.

Annex I — Description of the processing

Data subjects	(a) The Customer's users in Vericto (employees or contractors with a dashboard account). (b) People whose data appears in the literals of SQL statements the Customer sends, when it uses raw mode. (c) Users of the Customer's applications, to the extent their IP address is recorded in evaluation events.
Categories of data	Account: name, email, role, language, time zone, password hash, encrypted MFA secret, sessions (IP and user agent). Service usage: API keys (SHA-256 hash only), workspace configuration, rules and policies, dashboard activity log (IP and user agent). Evaluation events: SQL statement text (encrypted; sanitized in sanitized mode), hash, triggered rule, decision, latency, client IP, database and dialect. Validation reports: preview of each statement (sanitized in sanitized mode), verdicts, file name and CI provenance (repository, commit, author). Billing: handled by Paddle as merchant of record; Vericto does not receive card data.
Sensitive data	Vericto does not request it. It may appear in SQL literals if the Customer uses raw mode; the Customer can avoid that with sanitized mode.
Nature and purpose	Evaluating SQL statements against the Customer's ruleset, recording decisions in the audit trail, showing dashboards, sending alerts, producing reports and providing support.
Duration	The term of the Agreement plus the deletion period in section 12.
Retention during the term	Audit trail: 7 days (Free), 30 days (Builder), 90 days (Team), configurable (Enterprise). The Customer can purge it earlier.

Annex II — Technical and organisational measures

- **Encryption in transit:** TLS 1.3 on HTTP connections and TLS 1.2 or higher on the proxy's TCP connections. HSTS on Vericto domains.
- **Encryption at rest:** AES-256-GCM for statement text, webhook secrets and MFA secrets, with per-workspace keys (HKDF over a master key). API keys are stored only as SHA-256 hashes and their plain value is shown once.
- **Minimisation:** sanitized mode on every channel; the TCP proxy runs in the Customer's infrastructure, and Vericto needs no network access to its databases.

- **Access control:** per-workspace roles (owner, admin, member, viewer), MFA (TOTP) for accounts, SSO/OIDC for workspaces that configure it, API keys with limited scopes and an expiry date, and short-lived OIDC keys for CI/CD.
- **Isolation:** every query is limited to the workspace of the user or API key, and the database enforces Row Level Security.
- **Integrity and traceability:** an audit trail of decisions users cannot modify; exports and reports signed with Ed25519, verifiable offline; a log of account security events.
- **Resilience:** the proxy keeps evaluating with the last synced ruleset if the control plane is unavailable, and can keep telemetry on disk until it is back.
- **Backups:** the database provider takes a daily backup, encrypted at rest. Backups are kept for at most 30 days and then deleted. Vericto tests restoring them at least once a year.
- **Operations:** code review and automated tests on every change; infrastructure credentials in a secrets manager (AWS SSM Parameter Store), never in code. Vericto carries out, without being limited to them, penetration testing, vulnerability management and staff training, and applies an incident response policy.
- **Responsible disclosure:** security@vericto.com, with an initial response within 24 hours for critical vulnerabilities.

Annex III — Sub-processors

Sub-processor	Service	Data	Location
Amazon Web Services, Inc.	Hosting of the backend and API, secrets management, logs	Customer Data the backend processes	United States (us-east-1)
Supabase, Inc.	PostgreSQL database	Account, audit trail, configuration, reports	United States (us-east-1)
Cloudflare, Inc.	CDN, DNS and DDoS protection	HTTP traffic, IP addresses	Global network

Sub-processor	Service	Data	Location
Resend	Transactional email	Recipient email and message content	United States
Paddle.com Market Ltd	Payments, as merchant of record	Name, email, country, billing data	United Kingdom
Stripe, Inc.	Payments for subscriptions predating Paddle	Name, email, billing data	United States
Google LLC (Google Analytics 4)	Dashboard usage analytics, with anonymised IP	Browsing events, cookie identifiers	United States

Signatures

This DPA is accepted when accepting the [Terms of Service](#). If your organisation needs a signed copy, download the PDF version, complete it and send it to legal@vericto.com; we will return it signed by Vericto.

For the Customer

Legal name:

Tax ID:

Registered address:

Signatory name:

Title:

Date:

Signature

For Vericto S.A.S.

Tax ID (NIT): 902.100.599-0

Registered address: Bogotá D.C.,
Colombia

Legal representative name:

Title: Legal representative

Date:

Signature