

Data Processing Agreement

Legal & Trust | Last updated: April 2026

This Data Processing Agreement applies when Zoveto processes Customer personal data on behalf of a Customer under an order form, subscription, pilot, statement of work, enterprise agreement, or other written agreement that references this DPA.

This DPA forms part of the applicable agreement between **Zoveto Technologies Private Limited** ("Zoveto", "we", "us") and the Customer.

Agreement and scope

This Data Processing Agreement ("DPA") governs Zoveto's processing of Customer personal data in connection with the subscribed services, including pilots, implementation services, and related support described in the applicable agreement, order form, or statement of work.

This DPA applies to personal data processed by Zoveto on behalf of Customer through the Zoveto platform and related services.

Roles of the parties

Unless otherwise agreed in writing:

- Customer determines the purposes and means of processing Customer personal data.
- Customer acts as Data Fiduciary/controller where applicable.
- Zoveto acts as Data Processor/service provider where it processes Customer personal data on Customer's instructions.
- Each party remains responsible for its own compliance obligations under applicable law.

DPDP Act 2023 alignment

Zoveto will process personal data in accordance with applicable data protection law, including India's Digital Personal Data Protection Act, 2023 where applicable.

Zoveto processes Customer personal data only on documented Customer instructions, including the agreement, order form, product configuration, support requests, and written instructions.

Zoveto will reasonably assist Customer with Data Principal rights, grievance, consent withdrawal, correction, deletion, nomination, security, breach response, and deletion/return obligations where applicable.

Zoveto will ensure authorised personnel are bound by confidentiality obligations.

Zoveto will not sell Customer personal data.

Zoveto will not process Customer personal data for unrelated advertising or unrelated profiling.

Processing purposes

Purpose	Description
Service delivery	Hosting, operating, maintaining, and improving the subscribed Zoveto services.
Account administration	Creating accounts, managing users, roles, permissions, authentication, and billing administration.
Customer support	Troubleshooting, diagnostics, issue resolution, and support communications.
Implementation and migration	Onboarding, configuration, data import, workflow setup, training, and professional services where agreed.
Security and abuse prevention	Monitoring, logging, fraud prevention, incident detection, access control, and protection of systems and data.
Analytics and product improvement	Aggregated or usage-based analysis to improve reliability, performance, usability, and product functionality.
Legal and compliance	Maintaining records required for tax, accounting, contractual, regulatory, security, and legal obligations.
Communications	Service notices, administrative messages, product updates, and customer-success communications related to the services.

Categories of personal data

Category	Examples
Account and user data	Names, work emails, phone numbers, organisation names, job titles, user IDs, roles, and permissions.
Authentication and access data	Login metadata, access timestamps, IP addresses, session information, device/browser information, and security logs.
Business operations data	Inventory, warehouse, procurement, sales/CRM, finance/GST, HR, MRO, vendor, customer, and workflow records uploaded or generated by Customer.
Support data	Support tickets, messages, diagnostics, screenshots, files, call notes, and troubleshooting information shared by Customer.
Billing and commercial data	Billing contacts, invoices, subscription plan, payment status, GST/tax details, and order-form information.
Usage and telemetry data	Product usage events, feature interactions, performance logs, error logs, and analytics data.
Communications data	Service emails, administrative messages, demo or onboarding communications, and customer-success interactions.

Categories of Data Principals

- Customer employees, workers, contractors, and authorised users.
- Customer's vendors, suppliers, distributors, and logistics partners.
- Customer's customers, leads, prospects, and business contacts.
- Customer's finance, accounting, procurement, warehouse, operations, sales, HR, and management users.
- Other individuals whose personal data is submitted to the services by or on behalf of Customer.

Customer instructions

Zoveto will process Customer personal data only according to documented Customer instructions.

Customer is responsible for ensuring it has the rights, notices, consents, authorisations, and lawful basis needed to submit Customer personal data to the services.

Zoveto may decline or suspend processing instructions that are unlawful, unsafe, technically infeasible, or outside the subscribed services.

Zoveto will inform Customer if Zoveto believes an instruction infringes applicable data protection law.

Confidentiality

Zoveto shall ensure that personnel authorized to process Customer personal data are subject to confidentiality obligations that survive termination of their employment or engagement.

Security measures

Zoveto maintains reasonable organisational and technical measures suitable for SaaS operations, including access controls, least-privilege access, encryption in transit (TLS), encryption at rest for core production systems, backup and recovery measures, logging and monitoring, and administrative safeguards.

Further security details are described at <https://zoveto.com/security>.

Business continuity and disaster recovery

Zoveto shall maintain commercially reasonable business continuity, backup, and disaster recovery measures appropriate to the nature of the Services and associated operational risks.

Security testing

Zoveto may conduct vulnerability assessments, penetration testing, security reviews, and continuous monitoring activities to maintain the security, availability, and integrity of the Services.

Security incidents

Zoveto will notify Customer without undue delay after confirming a security incident affecting Customer personal data.

Notification will include available information about the nature of the incident, affected data, likely impact, mitigation steps, and recommended customer actions where available.

Zoveto will take reasonable steps to investigate, contain, remediate, and reduce recurrence of confirmed incidents.

Customer is responsible for regulatory or Data Principal notifications where Customer is the Data Fiduciary/controller unless otherwise required by law or agreed in writing.

Subprocessors

Zoveto may use subprocessors to provide hosting, infrastructure, analytics, communications, support, security, and operational services.

The current subprocessor list is incorporated into this DPA by reference and is available at <https://zoveto.com/subprocessors>.

Zoveto remains responsible for subprocessors' performance of data protection obligations to the extent required by applicable law and contract. Zoveto will impose appropriate confidentiality and data protection obligations on subprocessors.

Current subprocessors (summary)

Provider	Purpose
Amazon Web Services (AWS)	Cloud hosting, compute, storage, networking, and infrastructure operations
Google Analytics	Website analytics and aggregate traffic insights (when analytics consent is enabled)
Microsoft Clarity	Website session replay, heatmaps, and behavioral diagnostics on the marketing site (when analytics consent is enabled)
Razorpay	Payment processing, billing workflows, and transaction records
Google (Gmail SMTP)	Transactional email delivery and account/service communication

Subprocessor changes

Zoveto may update its list of subprocessors from time to time and shall provide reasonable notice of material subprocessor additions through its subprocessor page or other commercially reasonable means.

Government and regulatory requests

Unless prohibited by applicable law, Zoveto shall promptly notify Customer of any legally binding request from a governmental authority, regulator, court, or law enforcement agency seeking access to Customer personal data and shall reasonably cooperate with Customer regarding such request.

Data minimization

Zoveto shall process only the personal data reasonably necessary to provide the Services, comply with Customer instructions, satisfy legal obligations, and maintain service security and reliability.

Commercial use restriction

Zoveto will not sell, rent, disclose for monetary consideration, or commercially exploit Customer personal data except as necessary to provide the Services or as required by applicable law.

Data export

During the subscription term and any applicable post-termination export period, Customer may request export of Customer personal data in a commercially reasonable electronic format where technically available.

Return and deletion after contract end

On expiry or termination of the applicable agreement, Customer may request export or return of Customer personal data where technically available under the subscribed plan or order form.

Unless a longer period is required by law, tax, accounting, dispute, security, backup, or legitimate business requirements, Zoveto will delete or anonymise Customer personal data from active production systems within **sixty (60) days** after contract end or written deletion request.

Residual backup copies may remain in encrypted or access-controlled backups for up to **ninety (90) days** and will be deleted or overwritten in the ordinary backup lifecycle.

Zoveto may retain limited records required for legal, tax, accounting, fraud prevention, security, dispute resolution, or contract enforcement purposes.

Deleted or anonymised data will not be restored to production systems except where required for legal, security, or disaster recovery purposes.

Data Principal requests

Customer is responsible for responding to Data Principal requests where Customer is the Data Fiduciary/controller.

Zoveto will reasonably assist Customer with access, correction, deletion, grievance, consent withdrawal, and nomination-related requests to the extent such requests relate to Customer personal data processed by Zoveto.

Zoveto may redirect a Data Principal request to Customer where the request relates to Customer-controlled data.

Audit and compliance verification

Upon reasonable written request and not more than once in any twelve-month period, Zoveto shall provide Customer with information reasonably necessary to demonstrate compliance with this DPA, including available security documentation, policies, certifications, or audit reports where applicable. Any audit activities shall be subject to reasonable confidentiality, security, operational, and scheduling requirements.

Data residency and cross-border processing

Where personal data is transferred across borders, Zoveto applies contractual and technical safeguards required by applicable law.

For production customer data where Zoveto has committed India-only data residency in the applicable order form or security documentation, Zoveto will host such production data in India, subject to approved subprocessors and lawful processing requirements.

Some metadata, support, analytics, email, payment, or communication workflows may be processed by approved subprocessors outside India as described at <https://zoveto.com/subprocessors> and <https://zoveto.com/security>.

Conflict with main agreement

If there is a conflict between this DPA and the main agreement, this DPA controls only for data protection and processing of Customer personal data.

Commercial terms remain governed by the main agreement, order form, or Master Service Agreement.

Term

This DPA remains in effect for as long as Zoveto processes Customer personal data on behalf of Customer.

Sections intended to survive termination continue as necessary, including confidentiality, deletion/return, audit records, liability, and legal compliance.

Contact

DPA and enterprise privacy requests: privacy@zoveto.com

Grievance officer details for Data Principal complaints are available in the Privacy Policy at <https://zoveto.com/privacy#grievance>.