VIZZI ANALYTICS INC.

Privacy Policy

Last Updated: 17 November 2026

Thank you for choosing Vizzi Analytics ("Vizzi"). Vizzi Analytics Inc. ("Company", "we", "our", or "us") is committed to protecting your privacy and being transparent about the limited information collected and processed through our desktop software and online License Portal. This Privacy Policy explains how we collect, use, store, protect, and retain personal information when you purchase, administer, or use Vizzi.

1. Information Collection and Local Execution

1.1. Vizzi is a locally executed desktop analytics application designed to process customer data within the user's own computing environment. During ordinary local desktop operation, we do not collect, receive, host, or store your audit datasets, imported tables, project files, workflows, or analysis results.

1.2. We collect and maintain only the limited information reasonably necessary for the following operational purposes:

A. License Portal and Subscription Administration

- Customer and organization names;
- Authorized user names and email addresses;
- License identifiers, subscription tiers, activation timestamps, and expiration dates;
- License seat assignments and reassignment records;
- Device or installation identifiers and activation records required to enforce seat and device limits (which are associated with a user or organization account and are not anonymous); and
- Administrative actions performed within the self-service License Portal.

B. Customer Support and Communications

- Billing and contact details supplied when purchasing subscriptions or requesting support;
- Support correspondence, diagnostic details, and information voluntarily provided to resolve technical issues; and
- Contact records necessary to deliver software update notices, renewal reminders, and service communications.

C. Security and System Integrity

- Authentication logs, session tokens, and access control records;
- Periodic license verification events and technical diagnostics; and
- Security events, failed login attempts, and administrative audit trails.

1.3. We do not use the License Portal or telemetry mechanisms to monitor the content of customer analytics, inspect audit results, or collect information about the datasets being analyzed locally.

2. How We Use Information

2.1. Information collected through Vizzi's licensing and support systems is used strictly for legitimate business and operational purposes, including:

- Activating, validating, and administering named-user software licenses;
- Enabling organizational administrators to manage seat assignments in the License Portal;
- Preventing unauthorized access, credential sharing, or circumvention of license limits;
- Providing technical support and responding to customer inquiries;
- Maintaining the security, availability, and integrity of our licensing infrastructure; and
- Meeting applicable tax, accounting, legal, and regulatory obligations.

2.2. We do not sell, rent, or trade personal information, nor do we use licensing or support data for third-party advertising or behavioral profiling.

3. Online License Portal and Verification

3.1. Vizzi connects to our online License Portal upon initial activation and during periodic license checks to confirm an active subscription, verify seat assignments, and enforce device limits.

3.2. Where permitted by your license configuration, Vizzi may continue operating offline for a limited grace period without an internet connection, after which online verification with the License Portal is required.

3.3. For multi-seat organizational subscriptions, designated customer administrators can view and manage user assignments and licensing records associated with their organization through role-based access controls.

4. Data Storage and Third-Party Infrastructure

4.1. We rely on trusted third-party infrastructure providers to operate our licensing, authentication, and payment workflows. Specifically, our online License Portal uses Supabase for database hosting, user authentication, and backend licensing services, alongside payment processors (such as Stripe) for subscription billing.

4.2. Information maintained in our backend infrastructure includes customer records, authorized user profiles, subscription details, seat assignments, authentication logs, and verification records. We require our service providers to maintain appropriate contractual, security, and privacy safeguards.

4.3. Depending on hosting configurations and service provider infrastructure, personal information may be processed or stored outside Canada (including in the United States) and may be subject to the lawful access laws of the jurisdiction in which it is hosted.

5. Data Retention and Deletion

5.1. We retain personal information only for as long as reasonably necessary to fulfill the purposes described in this Policy or to comply with applicable legal, tax, and accounting obligations:

- Active Account & License Records: Maintained for the duration of an active subscription and deleted or anonymized within a reasonable period after the customer relationship ends, unless retention is required for legal or accounting purposes.
- License Verification & Technical Logs: Retained for a limited rolling period reasonably necessary for security monitoring, troubleshooting, and license enforcement, then deleted or anonymized.
- Administrative Audit Logs: Retained where necessary for account accountability, security, and dispute resolution, and periodically reviewed for deletion or anonymization.

- Support Correspondence: Retained as reasonably necessary to resolve inquiries, maintain support history, and improve documentation.
- Financial & Tax Records: Invoices and transaction records are retained for the statutory periods required under Canadian tax and corporate laws.
- Encrypted Backups: Records deleted from active databases may persist temporarily in encrypted system backups until overwritten in accordance with standard backup rotation schedules.

6. Data Security

6.1. We implement reasonable technical and organizational safeguards designed to protect personal information against unauthorized access, loss, misuse, or disclosure, including:

- Encrypted TLS communications between the desktop application, License Portal, and backend databases;
- Role-based access controls and row-level security policies separating organizational accounts;
- Restricted administrative access and multi-factor authentication on core infrastructure;
- Security event monitoring, audit logging, and periodic access reviews.

6.2. While we take reasonable precautions to protect your information, no method of electronic transmission or storage is completely secure.

7. AI Functionality and External Integrations

7.1. Vizzi offers optional integrations with third-party artificial intelligence (AI) providers, cloud storage platforms, email services, and external data sources, which users configure directly (including via Bring-Your-Own-Key API credentials).

7.2. When optional AI-assisted features are invoked, your prompt and relevant workflow context or schema metadata may be transmitted directly from your device to your selected third-party AI provider. Standard AI features are not designed to automatically upload entire customer datasets; however, any data you explicitly include in prompts or route through configured integrations will be transmitted to that provider.

7.3. Customers and users are solely responsible for configuring optional integrations, avoiding the submission of unauthorized confidential or personal data in prompts, and reviewing the privacy and security policies of their chosen third-party providers.

7.4. Vizzi Analytics Inc. does not collect customer datasets or use customer data to train AI models.

8. Privacy Rights: Access, Correction, and Deletion

8.1. Depending on your jurisdiction (including under Canadian federal and provincial privacy laws such as PIPEDA and BC PIPA), you may request access to, correction of, or deletion of personal information we hold about you.

8.2. If your license is administered through an organizational subscription, certain seat or profile updates may be handled directly by your organization's License Portal administrator or coordinated with them.

8.3. We will respond to verified privacy requests within statutory timeframes, subject to legal, security, or accounting obligations requiring continued retention.

9. Changes to This Privacy Policy

9.1. We may update this Privacy Policy periodically to reflect changes in our software, licensing infrastructure, or legal requirements. The current version will be posted on our website and within the License Portal with an updated revision date.

9.2. Where material changes affect how personal information is collected, used, or disclosed, we will provide appropriate notice and obtain consent where required by applicable law.

10. Contact Information

Vizzi Analytics Inc.
British Columbia, Canada
Website: www.vizzianalytics.com
Support & Licensing: support@vizzianalytics.com