Data, Privacy & AI Standards

How Raisin protects your data, respects your donors, and uses AI responsibly

Document Version	1.2
Review Cycle	Annual
Document Owner	Product & Engineering, Raisin Software
Applies To	All Raisin platform customers, users, and their constituents
Effective Date	December 1, 2026

This document is the single public reference for how Raisin Software handles data, privacy, and artificial intelligence across the platform. It is written in plain language so that fundraising professionals — not just legal or IT teams — can understand and trust how we operate. It is incorporated by reference into the Raisin Services Agreement. Current certifications, subprocessor lists, and AI provider DPA summaries are published at https://trust.raisinsoftware.org.

Introduction

Raisin Software (A.K.A. New Media Inc.) is the digital fundraising partner to growing non-profits. The trust of our clients, their donors, and the broader charitable sector is the foundation of everything we build. This document describes the commitments we make on three interconnected topics: how we secure your data, how we protect privacy, and how we use artificial intelligence.

The Services Agreement between Raisin and your organization governs the contractual relationship. This document is incorporated by reference into that Agreement. In the event of any conflict between this document and the Services Agreement, the Services Agreement prevails.

Section 1 — Who We Are and What We're Responsible For

1.1 Raisin's Role: Data Processor

When you use the Raisin platform, your organization collects and controls donor and participant data. Raisin acts as a data processor on your behalf:

- We process data according to your instructions, as set out in our Services Agreement and this document.
- We do not own your data. We do not use it for our own commercial purposes beyond delivering the platform to you.
- We implement appropriate technical and organizational safeguards to protect it.

1.2 Your Role as a Data Controller

As a Raisin customer, you are the data controller for the donor, participant, and constituent information you collect through the platform. This means you are responsible for:

- ensuring you have a lawful basis and appropriate consent to collect personal information;
- publishing your own privacy policy to donors and participants;
- responding to data subject requests (access, correction, deletion) from your constituents; and
- complying with all applicable privacy laws in your jurisdiction.

1.3 How This Document Relates to Your Services Agreement

This document is incorporated by reference into the Raisin Services Agreement as the public-facing companion to the Data Security Schedule. The Services Agreement is the governing contractual document. This document explains our obligations in plain language and extends them to cover privacy and AI.

Section 2 — Privacy

2.1 For Donors and Participants: What You Should Know

> If you are a donor, participant, or volunteer who has interacted with a fundraising campaign powered by Raisin, this section is for you. Your personal information is controlled by the charitable organization running the campaign — not by Raisin.

When you donate to or participate in a Raisin-powered campaign:

- Your data is collected by and on behalf of the charitable organization, not by Raisin.
- Raisin does not sell, rent, or share your personal information with third parties for commercial purposes.
- Raisin does not use your name, email address, or other directly identifying personal information to train any AI model.
- Raisin does not use one organization's constituent data to generate suggestions or intelligence for any other organization.

To access, correct, or delete your personal information, contact the charitable organization directly. If you cannot reach them, contact us at privacy@raisinsoftware.org.

2.2 Privacy Principles

Raisin's data handling practices are organized around the ten PIPEDA privacy principles. The full Privacy Policy of the Raisin Platform is published at https://www.raisinsoftware.org/platform-privacy-policy. In summary:

Principle	Raisin's Commitment
Accountability	A Privacy Officer is accountable for compliance and reports to the CEO.
Identifying Purposes	Data is collected only for stated fundraising and administrative purposes.
Consent	Personal information is collected with the knowledge and consent of the individual.
Limiting Collection	We collect only what is necessary for the stated purpose.
Limiting Use & Retention	Data is not used or disclosed beyond its collected purpose. Retained only as long as necessary.
Accuracy	Licensees are responsible for keeping constituent data accurate and current.
Safeguards	Technical and organizational measures protect data at appropriate sensitivity levels.
Openness	This policy and our practices are publicly available at trust.raisinsoftware.org.
Access	Individuals may request access to their personal information through the relevant Licensee.
Challenging Compliance	Individuals may challenge compliance by contacting our Privacy Officer.

2.3 Data We Do Not Use

- We do not sell, share, or license donor or constituent data to third parties for commercial purposes.
- We do not use one organization's constituent data to generate suggestions, scoring, or intelligence for any other organization.
- We do not use donor names, email addresses, or other directly identifying personal information to train any AI model.

2.4 Retention and Deletion

Customer Data is retained for the duration of the subscription term. Raisin retains different categories of Customer Data for different periods following termination, in accordance with the Data Retention

Schedule set out in the Data Security Standards (Attachment A, Section 4A): general platform content is deleted within 1 year of termination; transaction and financial records are retained for 7 years from the date of transaction, consistent with Canada Revenue Agency (CRA) and U.S. Internal Revenue Service (IRS) requirements; and security and audit logs are retained for the longer of 7 years from creation or 3 years from termination. Upon termination, Customer Data will be made available for export for 30 days before the applicable retention periods begin. Customers should note that deletion of constituent records may affect associated fundraising totals, campaign reports, and other platform data that references or is derived from those records.

2.5 Applicable Law

Our privacy practices are designed to comply with PIPEDA and, for Quebec, Law 25 (Bill 64). For customers or constituents in the United States, we apply equivalent protections consistent with applicable state privacy laws including CCPA/CPRA (California), CDPA (Virginia), CPA (Colorado), CTDPA (Connecticut), and TDPSA (Texas).

2.6 Privacy Contact

Privacy Officer: privacy@raisinsoftware.org | 866-766-3336

A.K.A. New Media Inc. (dba Raisin Software), 2738 Dundas St W, Suite 200, Toronto, ON M6P 1Y3

Section 3 — Data Security

3.1 Security Governance

Raisin maintains IT security policies that are integral to our business and mandatory for all employees. Management maintains executive oversight, including formal governance, employee education, and compliance enforcement. Security policies are reviewed at least annually. All employees complete security and privacy education annually and certify compliance. New hires undergo mandatory employment verification including criminal background checks.

3.2 Compliance Certifications

Certification / Standard	Status
PCI DSS Level 1 Service Provider	Continuously maintained for over fifteen (15) years. Reflects independent validation of Raisin's cardholder data environment against payment card industry security requirements.
SOC 2 Type II	Actively in progress as part of Raisin's 2026 compliance roadmap. Provides independent third-party assurance that controls for security, availability, and confidentiality operate effectively on a continuous basis.
ISO/IEC 42001:2023 (AI Mgmt)	Working toward certification. International standard for AI Management Systems governing Raisin's AI governance and risk management practices.
NIST AI RMF	Applied internally. Informs Raisin's AI risk assessment and fairness testing practices.

Current certification status and third-party attestation documents are published and maintained at https://trust.raisinsoftware.org.

3.3 Access Controls

Access to Customer Data is restricted to the minimum level required. Privileged access is individual, role-based, subject to approval and regular validation, and governed by segregation of duties. Redundant and dormant accounts are identified and removed promptly.

3.4 Encryption

Customer Data is encrypted in transit (HTTPS, SFTP, FTPS) and at rest. Raisin manages cryptographic keys through documented procedures covering generation, rotation, revocation, and destruction.

3.5 Network and Infrastructure Security

Raisin maintains documented network architecture with measures designed to prevent unauthorized connections. Production and non-production environments are logically separated. Endpoint protections include firewalls, encryption, malware detection, and patch management.

3.6 Vulnerability Management

Raisin performs annual security and privacy risk assessments, annual penetration testing (including independent third-party testing), and continuous automated vulnerability scanning. Identified vulnerabilities are remediated based on risk and exploitability.

3.7 Incident Response and Breach Notification

Raisin maintains a documented Incident Response Plan. In the event of a confirmed Security Incident affecting Customer Data — including material errors caused by AI features — Raisin will notify affected customers within seventy-two (72) hours of confirmation.

3.8 Business Continuity and Disaster Recovery

Customer Data is backed up daily with encrypted off-site copies. In the event of a Force Majeure Event causing service unavailability, Raisin will restore access within fourteen (14) days using the most recent backup, with no more than twenty-four (24) hours of data loss.

3.9 Hosting

All Customer Data is hosted at secure facilities in Canada.

3.10 Subprocessors

Raisin uses third-party Subprocessors in the delivery of the Cloud Service, including payment processors, infrastructure providers, and AI providers. All Subprocessors are bound by data protection obligations no less protective than those in the Data Security Standards. A current, publicly accessible Subprocessor list — including all third-party AI providers — is maintained at https://trust.raisinsoftware.org.

3.11 Audit Rights

Upon written request, Raisin will provide customers with current certifications and attestations regarding our Technical and Organizational Measures (TOMs). Onsite audit rights are available to enterprise customers, customers with a regulatory mandate requiring such inspection, or any customer where Raisin has confirmed a Security Incident affecting their data. Full audit procedures are set out in the Data Security Standards Section 8.

Section 4 — Artificial Intelligence

4.1 Our Current AI Features

Raisin currently offers the following AI-assisted features within the platform. All are opt-in, enabled on a campaign-by-campaign basis by your administrators. AI features are clearly labelled within the platform at the campaign configuration level, and your organization's administration panel shows which AI features are enabled for each campaign at any time.

Feature	Description
Personal Story Writer (Jun 2026)	Helps P2P fundraisers draft a personal fundraising page story based on guided prompts. The fundraiser must actively choose to publish any output.
AI-Assisted Social Posts (Feb 2026)	Generates suggested social media copy across six call-to-action types and three tones. The fundraiser chooses, edits, and shares — or ignores — any suggestion.

Raisin publishes an annual AI Transparency Summary describing which AI capabilities are active, any material changes during the year, and the third-party AI providers we rely on.

4.2 What Data AI Features Use — and What They Don't

> Key Commitment: Raisin does not use donor names, email addresses, or other directly identifying personal information to train any AI model — our own or any third party's, including our current AI provider.

Current AI content features use only:

- publicly available campaign information (organization name, event name, campaign goal, website URL); and
- the fundraiser's own page content and self-entered prompts.

Raisin also collects anonymized behavioural and outcome-linked signals — such as session engagement patterns, form interaction signals, and constituent giving outcomes — and uses these to train and improve its platform intelligence capabilities, including donor scoring, engagement propensity

modelling, and campaign optimization. These signals are processed at an aggregated level designed to prevent identification of individual donors and are subject to the same access controls as all Customer Data. Where signals are linked to individual giving outcomes for scoring purposes, this is disclosed in the relevant feature documentation.

What we do not do:

- We do not use donor names, email addresses, or other directly identifying personal information in AI features or for model training.
- We do not use one organization's constituent data to generate suggestions, scoring, or intelligence for any other organization.
- We do not sell, share, or license any constituent data to third parties for their commercial purposes.

4.3 Our AI Provider Relationship

Where AI features are powered by our AI provider's API, we operate under an enterprise agreement that includes:

- a Data Processing Agreement (DPA) aligned to GDPR and PIPEDA requirements;
- a contractual prohibition on the use of Customer Data or outputs for model training or fine-tuning;
- output retention limited to thirty (30) days for quality assurance, after which data is deleted; and
- access to outputs restricted to authorized Raisin staff for QA purposes only.

A summary of our AI provider DPA and contractual protections is published at https://trust.raisinsoftware.org, which is publicly accessible without login.

4.4 Human Control and Feature Transparency

No AI-generated content in Raisin is published, sent, or actioned on behalf of a fundraiser or your organization without a human actively choosing to do so. Your organization retains final control over whether AI features are enabled, and individual fundraisers retain final control over all content they publish.

AI features are clearly labelled in the platform wherever they are available. Your organization's administration panel displays which AI features are enabled at the campaign level, giving you a verifiable, real-time view of AI feature status across your account.

4.5 Fairness and Prohibited Uses

The following uses are prohibited and technically restricted:

- Scoring, ranking, or filtering donors based on protected characteristics (race, religion, gender, national origin, disability, or sexual orientation).
- Automated decisions that deny a donor or prospective donor access to a program without human review.
- Generating communications that promote misinformation or manipulative psychological techniques.

Before deploying any AI feature that generates recommendations about donors or segments, Raisin conducts bias evaluation to identify and mitigate systematic disparities across demographic groups.

4.6 Explainability

Where AI features influence recommendations or scores visible to your team, Raisin provides a plain-language explanation of the key factors that contributed to that output. You should never see a score or recommendation without some indication of why it was generated.

4.7 AI Incident Response

If an AI feature causes a material error affecting Customer Data, donor data, or communications, Raisin will notify affected customers within seventy-two (72) hours of confirming the incident, investigate root cause, and publish a summary of corrective actions taken.

4.8 Regulatory Alignment

Framework / Standard	Relevance to Raisin
PCI DSS Level 1 Service Provider	Continuously maintained for over fifteen (15) years. Governs payment card data security across all Raisin transactions.
SOC 2 Type II	In progress (2026 roadmap). Independent attestation of continuous security, availability, and confidentiality controls.
ISO/IEC 42001:2023	Working toward certification. International standard for AI Management Systems.
NIST AI RMF	Applied internally to inform AI risk assessment and fairness testing.
PIPEDA / Quebec Law 25	Canadian federal and provincial privacy law governing personal information, including data processed by AI features.
EU AI Act (2026)	For customers with EU operations, Raisin's AI features are designed to meet transparency and human oversight requirements for limited-risk AI systems.
California's AI Transparency Act (SB 942)	Raisin is a *deployer* of a third-party AI provider's system, not the builder of one.

4.9 Customer Obligations for AI Features

Customers may use AI features to draft and improve donor communications, generate campaign insights, score and segment donors based on behavioural signals, and automate routine communications under staff supervision.

Customers may not use AI features to generate false or deceptive content, attempt to extract donor PII in bulk through AI prompts, circumvent platform access controls, or make final decisions outside the platform's scope (employment, housing, credit, etc.). The raisin platform contains various guardrails in place for prompt generation, for example.

Section 5 — Your Responsibilities as a Platform Customer

5.1 Your Obligations as a Data Controller

You are responsible for ensuring you have a lawful basis to collect and process constituent data, publishing your own privacy policy to donors and participants, and complying with all applicable privacy laws in your jurisdiction.

5.2 Data Subject Requests

If a donor or participant contacts Raisin directly to exercise their privacy rights (access, correction, deletion), Raisin will inform you and assist where technically feasible. You are responsible for fulfilling such requests as the data controller.

5.3 Reporting Concerns

If you believe an AI feature has produced a biased or unfair output, or if you identify a potential security vulnerability, contact Raisin support immediately. We investigate all such reports and publish aggregate findings in our annual AI Transparency Summary.

Section 6 — Keeping This Document Current

This document is reviewed annually and updated whenever Raisin introduces material changes to our data security, privacy, or AI practices. Customers will be notified of material changes at least thirty (30) days before they take effect.

For questions about any aspect of this document:

- Email: privacy@raisinsoftware.org
- Trust Centre: https://trust.raisinsoftware.org (publicly accessible, no login required)
- In-product: Settings → Help → Contact Support → AI & Data Policy
- Enterprise customers: through your designated Customer Success Manager

Appendix A — Personal Data Processing Details

See the Data Security Standards (Attachment A) for the full Personal Data Processing Attachment. Available at: https://www.raisinsoftware.org/data-security-standards.

Appendix B — Subprocessor List

A current, publicly accessible list of third-party Subprocessors — including all AI providers — is maintained at https://trust.raisinsoftware.org. No login is required.

Appendix C — API Terms

Access to the Raisin API is governed by the API terms set out in Attachment B of the Data Security Standards and the applicable License & Subscription Agreement.

Appendix D — AI Feature Reference

Current as of July 2026. Updated annually in the AI Transparency Summary.

Feature	Data Inputs / Outputs / Controls
Personal Story Writer (June 2026)	Inputs: Organization name, campaign name, goal, URL; fundraiser's own prompts. Output: 110–160 word story draft. Retention: 30 days. Human control: fundraiser must actively publish.
AI-Assisted Social Posts (Feb 2026)	Inputs: Campaign information, fundraiser page content. Output: Social copy across 6 CTA types × 3 tones. Retention: 30 days. Human control: fundraiser chooses, edits, and shares.