

TABKEEPER PRIVACY POLICY

Version 2.1 Effective Date: July 26, 2026 · Last Updated: August 10, 2026 Part of the Tabkeeper Legal Framework v2.0
Tabkeeper Inc. support@tabkeeper.io © 2026 Tabkeeper Inc. All Rights Reserved.

Effective Date: July 26, 2026 · Last Updated: August 10, 2026 Tabkeeper Inc., a New York corporation ("Tabkeeper," "we," "us," or "our"), respects your privacy. This Privacy Policy explains how we collect, use, disclose, retain, and protect information in connection with the Services — including the Tabkeeper websites located at tabkeeper.io and its subdomains, the Tabkeeper web and mobile applications, our bookkeeping services, and all related tools and features. This Privacy Policy is part of the Tabkeeper Legal Framework and should be read together with the Tabkeeper Terms of Service (the "Terms"). It is a statement of Tabkeeper's information practices, provided for transparency: it is not a contract and does not create warranties, representations, or obligations beyond those required by Applicable Law, as described in Section 2.2 of the Terms. Capitalized terms used but not defined in this Privacy Policy — including "Services," "Customer Content," "Financial Data," "Connected Financial Account," "AI Features," "AI Input," "AI Output," "Organization," "Workspace," "User," "Subprocessor," and "Aggregated Data" — have the meanings given to them in Section 3 of the Terms. Please read this Privacy Policy carefully. By accessing or using the Services, you acknowledge that you have read and understood this Privacy Policy. If you do not agree with our practices as described here, please do not use the Services.

1. Scope of This Privacy Policy

1.1 What This Policy Covers. This Privacy Policy applies to Personal Information and other information that Tabkeeper collects and processes when you visit our websites, create an Account, use the Services (including Personal Finance Features, where offered), engage Tabkeeper for Bookkeeping Services, communicate with us, or otherwise interact with Tabkeeper. It covers both Business Users and individuals using the Services for personal, family, or household purposes.

1.2 What This Policy Does Not Cover. This Privacy Policy does not apply to: (a) Third-Party Services, including websites, integrations, financial institutions, and platforms that you connect to or access through the Services, each of which is governed by its own privacy policy; (b) information practices of Third-Party Professionals (such as independent CPA firms) with whom you separately engage; or (c) information that has been aggregated, anonymized, or de-identified such that it no longer identifies you, which we may use as described in the Terms.

1.3 Organizations and Authorized Users. Where you use the Services as an Authorized User of an Organization (for example, as an employee, contractor, or invited accountant of a business), the Organization — not Tabkeeper — controls the Workspace, decides what Customer Content is submitted, and manages User Roles and access. In that context, Tabkeeper processes Customer Content on the Organization's behalf and at its direction, and questions about the Organization's practices, or requests to access or delete information within an Organization's Workspace, should be directed first to that Organization's Owner or Administrator. Owners and Administrators may be able to view activity within their Organization, including audit logs of actions taken by Users, where offered.

1.4 Bookkeeping Clients. Where Tabkeeper provides Bookkeeping Services under a Bookkeeping Engagement Agreement, additional confidentiality and records provisions of that agreement also apply.

2. Information We Collect We collect information in four ways: directly from you, from your Connected Financial Accounts and integrations at your direction, automatically when you use the Services, and from third parties. The specific information collected depends on which Services and features you use.

2.1 Information You Provide Directly. (a) Account and registration information, including your name, email address, password (stored in hashed form), phone number where provided, business or organization name, and Account settings and preferences. (b) Customer Content and Financial Data, including expense and revenue records; accounts payable and receivable records; vendor and customer records; receipts, invoices, bank and financial statements, and other documents, images, PDFs, and spreadsheets you upload; CSV and other files you import; budgets, savings goals, and financial plans; and other financial information you enter into the Services. (c)

Personal finance information, where you use Personal Finance Features, which may include information about your personal transactions and spending, budgets, savings, debts, loans, mortgages, credit accounts, investment, brokerage, and retirement accounts, and net worth. We treat this information as sensitive and handle it as described in Section 8. (d) Bookkeeping engagement information, where you purchase Bookkeeping Services, including the business, financial, and tax-related records and documents you provide so that we can perform those services. (e) Payment and billing information. For purchases made through an app store — such as Apple In-App Purchase in our iOS application — your payment is collected and processed by the app store provider as an independent party under its own terms and privacy policy, and Tabkeeper receives transaction confirmations and subscription status rather than your payment card details. For purchases made directly from Tabkeeper, where offered, we collect your billing name and address and limited payment details; full payment card numbers are collected and processed by our Payment Processor (such as Stripe) and are not stored by Tabkeeper. (f) Communications, including support requests, emails, chat messages, survey responses, feedback, and any other information you choose to send us. (g) AI Inputs, where you use AI Features, including prompts, questions, and the Customer Content you submit to or process with those features.

2.2 Information from Connected Financial Accounts and Integrations. Where you link a Connected Financial Account or connect a Third-Party Service, we receive information from that source at your direction, as described in Sections 13 and 14 of the Terms. Depending on the account and provider, this may include: (a) transaction history and details; (b) account balances; (c) account identifiers and related account information; (d) account holder identity information, where available and authorized; and (e) data from connected platforms such as accounting, point-of-sale, payroll, ordering, and delivery systems. Bank and financial account connections are read-only: Tabkeeper does not receive the credentials needed to move money and does not initiate transfers. Where connections are powered by a Data Aggregation Provider such as Plaid, that provider's collection and processing of your information is governed by its own privacy policy, and we encourage you to review it.

2.3 Information Collected Automatically. When you use the Services, we and our service providers automatically collect: (a) usage data, such as pages and screens viewed, features used, buttons clicked, session duration, and navigation paths; (b) device and log data, such as IP address, browser type and version, operating system, device type and identifiers, language settings, referring URLs, and timestamps; (c) approximate location inferred from your IP address (we do not collect precise GPS location); (d) diagnostic and crash data, including error reports and performance metrics; and (e) information collected through cookies and similar technologies, as described in Section 6.

2.4 Information from Other Sources. We may receive information about you from: (a) our Payment Processor (such as payment confirmation and fraud signals); (b) service providers that help us prevent fraud and secure the Services; (c) publicly available business information; and (d) other Users, for example when an Owner or Administrator invites you to an Organization and provides your name and email address.

3. How We Use Information We use the information described in Section 2 for the following purposes: (a) To provide, operate, and maintain the Services, including creating and administering Accounts, Organizations, and Workspaces; syncing and displaying Financial Data from Connected Financial Accounts; processing, categorizing, and organizing transactions; generating financial reports, dashboards, forecasts, and reminders; enabling exports; and providing customer support and onboarding. (b) To perform Bookkeeping Services for clients who engage us under a Bookkeeping Engagement Agreement. (c) To operate AI Features, where offered, including generating categorizations, reports, forecasts, answers, and insights from your AI Inputs, as further described in Section 4. (d) To process payments and manage billing, including Subscriptions, Free Trials, coupons, invoicing, and collections, through our Payment Processor. (e) To communicate with you, including transactional and Account-related messages (such as receipts, renewal notices, security alerts, and changes to the Services or the Tabkeeper Legal Framework),

responses to your inquiries, and, subject to your opt-out rights, product updates, feature announcements, educational content, and promotional communications. (f) To secure the Services and prevent misuse, including authenticating Users; detecting, investigating, and preventing fraud, money laundering, security incidents, and violations of the Terms or Acceptable Use Policy; and enforcing our agreements. (g) To improve and develop the Services, including troubleshooting, research, analytics, testing, and developing new features, using where practicable Aggregated Data rather than identifiable information. (h) To comply with legal obligations, including tax, accounting, sanctions, and regulatory requirements, and to respond to lawful requests as described in Section 54 of the Terms. (i) For other purposes with your consent or at your direction. We do not use your Financial Data or Customer Content to serve you third-party advertising, and we do not sell identifiable customer financial information, as described further in Section 5.

4. AI Features and Your Information

4.1 Processing of AI Inputs. Where you use AI Features, your AI Inputs and relevant Customer Content are processed to generate AI Outputs. This processing may be performed by Tabkeeper's own systems and by third-party AI model and infrastructure providers acting as Subprocessors, which may include, but are not limited to, OpenAI and other model providers.

4.2 Limits on AI Training. Tabkeeper does not use your identifiable Customer Content to train generalized AI models made available to other customers, except as permitted through Aggregated Data or with your consent, as described in Section 19.4 of the Terms. Our third-party AI providers are engaged under agreements that restrict them from using your Customer Content other than to provide services to Tabkeeper.

4.3 Review of AI Outputs. AI Outputs may be reviewed by Tabkeeper personnel using human, automated, or hybrid methods for quality, safety, security, and support purposes, subject to the access limits described in Section 9.3.

5. How We Share Information We do not sell your Personal Information, and we do not sell identifiable customer financial information. We share information only in the circumstances described below.

5.1 Service Providers and Subprocessors. We share information with third-party service providers that perform services on our behalf, under written agreements that impose confidentiality and data protection obligations and restrict them from using your information for their own purposes. Categories and current representative providers include, but are not limited to: (a) Cloud hosting, infrastructure, and databases — including, but not limited to, Amazon Web Services (AWS), Vercel, Supabase, Google Firebase, and Cloudflare; (b) Payment processing and billing for purchases made directly from Tabkeeper, where offered — including, but not limited to, Stripe (purchases made through an app store are processed by the app store provider as an independent party, as described in Section 2.1); (c) Bank and financial account connectivity — including, but not limited to, Plaid; (d) AI model and infrastructure providers — including, but not limited to, OpenAI or other model providers we may engage; (e) Analytics and product usage — including, but not limited to, Google Analytics, Mixpanel, and PostHog; (f) Error monitoring and diagnostics — including, but not limited to, Sentry; (g) Email and communications delivery — including, but not limited to, Resend; and (h) Customer support, onboarding, and business operations tooling. Where published, our Subprocessor List identifies the material Subprocessors that process Customer Content or Personal Information, and we may update our providers from time to time.

5.2 Within Your Organization. Information you submit within an Organization's Workspace, and activity you take there, may be visible to the Organization's Owner, Administrators, and other Users in accordance with the User Roles and permissions configured by the Organization, including through audit logs, where offered.

5.3 Third-Party Services You Connect. Where you connect a Third-Party Service or Connected Financial Account,

we exchange information with that service as needed to operate the integration you have directed. The third party's handling of your information is governed by its own terms and privacy policy.

5.4 Third-Party Professionals at Your Direction. Where you direct us to share information with a Third-Party Professional — for example, by granting your CPA access to your Workspace or asking us to coordinate with a CPA firm for tax preparation — we disclose the information you direct us to share. The professional's use of that information is governed by your engagement with them and their professional obligations.

5.5 Corporate Transactions. If Tabkeeper is involved in, or evaluates, a merger, acquisition, financing, reorganization, bankruptcy, or sale of some or all of its assets or equity, information may be disclosed to counterparties and advisors under confidentiality obligations and may be transferred as part of the transaction. If a transfer results in a material change to this Privacy Policy, we will provide notice as described in Section 15.

5.6 Legal Compliance and Protection. We may disclose information where we reasonably believe disclosure is required or appropriate to: (a) comply with Applicable Law, legal process, or a governmental request, as described in Section 54 of the Terms; (b) enforce the Tabkeeper Legal Framework and investigate potential violations; (c) detect, prevent, or address fraud, security, or technical issues; or (d) protect the rights, property, or safety of Tabkeeper, our Users, or the public.

5.7 Affiliates. We may share information with our Affiliates, if any, consistent with this Privacy Policy.

5.8 With Your Consent. We share information for any other purpose disclosed to you with your consent or at your direction.

5.9 Aggregated and De-Identified Data. We may use and share Aggregated Data for analytics, benchmarking, AI improvement, fraud detection, product improvement, and statistics, as described in Section 17 of the Terms. We will not attempt to re-identify Aggregated Data and will not publicly disclose it in a manner that identifies you or any individual.

6. Cookies and Similar Technologies

6.1 What We Use. We and our service providers use cookies, pixels, local storage, software development kits, and similar technologies to operate and improve the Services. These fall into the following categories: (a) Strictly necessary — required for core functionality such as authentication, session management, security, load balancing, and fraud prevention. These cannot be disabled through our controls. (b) Preferences — remember your settings and choices, such as display options and saved views. (c) Analytics and performance — help us understand how the Services are used (for example, through Google Analytics, Mixpanel, and PostHog) so we can improve them, and help us identify errors and performance issues (for example, through Sentry).

6.2 Your Choices. You can control cookies through your browser settings, including blocking or deleting cookies, and through any cookie preference controls we make available within the Services. Disabling certain cookies may limit functionality, and disabling strictly necessary cookies may prevent the Services from working. Where required by Applicable Law, we honor opt-out preference signals, such as the Global Privacy Control, for the browser or device on which the signal is set. Our systems do not currently respond to other "Do Not Track" browser signals, for which no common standard exists.

6.3 No Third-Party Advertising Cookies. We do not use your Financial Data for third-party advertising, and we do not permit third-party advertising networks to collect information about you through the Services for their own targeted advertising purposes. Where published, our Cookie Policy provides additional detail about the specific technologies we use.

7. Data Retention

7.1 Active Accounts. We retain Personal Information and Customer Content for as long as your Account is active and as needed to provide the Services, comply with our legal obligations, resolve disputes, and enforce our agreements.

7.2 After Deletion or Closure. Following account deletion or a verified deletion request, we delete or de-identify

Customer Content and associated Personal Information within ninety (90) days, and residual copies in routine backups are retained for up to ninety (90) days before being overwritten or deleted in the ordinary course — in each case except where longer retention is required or permitted as described in Section 33 of the Terms (for example, for legal compliance, dispute resolution, fraud prevention, or enforcement).

7.3 Records We Must Keep. Certain records may be retained for longer periods where required for legal, tax, accounting, audit, or compliance purposes — for example, billing and transaction records, and books and records relating to Bookkeeping Services, which may be retained for up to seven (7) years or as otherwise required by Applicable Law or professional standards.

7.4 Aggregated Data. Aggregated Data, which does not identify you, may be retained and used without time limitation.

7.5 Export Before You Go. You may export your Customer Content in CSV, PDF, or Excel formats, depending on data type, at any time while your Account is active, and we strongly encourage you to do so before closing your Account.

8. Personal Finance Data Where you use Personal Finance Features, we collect and process personal financial information — such as personal transactions, budgets, savings goals, debts, loans, mortgages, credit accounts, investment, brokerage, and retirement account information, and net worth — solely to provide, secure, support, and improve the Services as described in this Privacy Policy. We treat this information as sensitive: we do not sell it, we do not use it for third-party advertising, and we restrict internal access to it as described in Section 9.3. Where Applicable Law provides specific rights for sensitive personal information, Section 11 describes those rights and how to exercise them.

9. Data Security

9.1 Our Program. We maintain a security program with administrative, technical, and physical safeguards designed to protect your information and appropriate to the nature of the data we process, as described in Section 35 of the Terms and, where published, our Security Overview. These safeguards include or may include encryption of data in transit and at rest, role-based access controls, network and application security measures, logging and monitoring, routine backups, vulnerability management, personnel confidentiality obligations, and vendor security review.

9.2 Account Security Features. We may offer security features for your use, such as multi-factor authentication, where offered, and we strongly encourage you to enable available protections, use a strong unique password, and safeguard your credentials and devices.

9.3 Internal Access Limits. Tabkeeper limits access to Customer Content and Personal Information by its personnel to what is reasonably necessary for legitimate purposes — onboarding, customer support, troubleshooting and bug fixing, performance of Bookkeeping Services, customer success, security and fraud prevention, compliance, and development of features you request — subject to confidentiality obligations, role-based access controls, and logging.

9.4 No Guarantee; Incident Notification. No method of transmission or storage is completely secure, and we cannot guarantee absolute security. If we become aware of a security incident involving unauthorized access to or disclosure of your unencrypted Personal Information, we will use commercially reasonable efforts to notify you without undue delay and in accordance with Applicable Law, as described in Section 35.3 of the Terms.

10. International Data Transfers Tabkeeper is based in the United States, and the Services are hosted using cloud infrastructure located in the United States. Your information may be processed, stored, and transferred in the United States and in

other jurisdictions where our service providers operate, and those jurisdictions may have data protection laws different from those of your home jurisdiction. Where we transfer Personal Information internationally and Applicable Law requires safeguards for such transfers, we implement appropriate measures, which may include contractual protections with our service providers. By using the Services, you understand that your information will be processed in the United States and such other jurisdictions.

11. Your Rights and Choices

11.1 Rights Available to All Users. Regardless of where you live, we make the following available to you: (a) Access and portability — you may access your Financial Data within the Services and export your Customer Content in CSV, PDF, or Excel formats, depending on data type; (b) Correction — you may update your Account information within the Services or request correction of inaccurate Personal Information; (c) Deletion — you may delete individual records within the Services, disconnect Connected Financial Accounts and integrations, and request deletion of your Account and Customer Content as described in Section 33 of the Terms; (d) Marketing opt-out — you may opt out of marketing communications at any time by using the unsubscribe link in any marketing email or contacting us; transactional and legal notices will continue; (e) Notification and cookie controls — you may manage push, SMS (where offered), and cookie preferences as described in Section 6 and within the Services.

11.2 How to Exercise Rights. You may exercise these rights through in-product tools, where offered, or by emailing support@tabkeeper.io from the email address associated with your Account. We may need to verify your identity — and, for requests concerning an Organization's Workspace, your authority — before acting on a request, and we may decline requests that are prohibited by law, that would infringe the rights of others, or that we cannot verify. We will respond within the timeframe required by Applicable Law (and in any event, we aim to respond within thirty (30) days). Where a request concerns Customer Content that we process on behalf of an Organization, we may refer the request to that Organization and assist it in responding.

11.3 Authorized Agents; No Discrimination; Appeals. Where Applicable Law permits, you may designate an authorized agent to exercise rights on your behalf, subject to verification of the agent's authority. We will not discriminate against you for exercising your privacy rights. If we decline a rights request, you may appeal by replying to our response or emailing support@tabkeeper.io with the subject line "Privacy Appeal"; if your appeal is denied, you may be able to contact your state attorney general or applicable supervisory authority.

12. United States State Privacy Rights This Section 12 supplements the rest of this Privacy Policy and applies to residents of U.S. states with comprehensive privacy laws, including California, Colorado, Connecticut, Texas, Utah, Virginia, and other states with similar laws, to the extent those laws apply to Tabkeeper.

12.1 Categories of Personal Information. In the preceding twelve (12) months, we have collected the following categories of Personal Information, as described in Section 2: (a) identifiers (such as name, email address, IP address, and account identifiers); (b) commercial information (such as Subscription and transaction history with us); (c) financial information (such as the Financial Data and Connected Financial Account information you provide or authorize, and limited billing details); (d) internet and other electronic network activity (such as usage, device, and log data); (e) approximate geolocation inferred from IP address; (f) professional or employment-related information (such as business name and role within an Organization); (g) communications and other information you provide; and (h) inferences drawn from the foregoing to provide and improve the Services. We collect these categories from the sources, and for the purposes, described in Sections 2 and 3, and we disclose them to the categories of recipients described in Section 5.

12.2 Sensitive Personal Information. Certain information we collect — such as account log-in credentials and the personal financial information described in Section 8 — may be "sensitive" under some state laws. We collect and use sensitive Personal Information only to provide the Services and for the other purposes permitted by Applicable

Law, and we do not use or disclose it for the purpose of inferring characteristics about you.

12.3 No Sale; No Targeted Advertising Sharing. We do not sell Personal Information for money, and we do not share Personal Information for cross-context behavioral or targeted advertising. Because of this, we do not offer a "Do Not Sell or Share My Personal Information" mechanism; if our practices change, we will update this Privacy Policy and provide any legally required notices and opt-outs before the change takes effect. We also do not knowingly sell or share the Personal Information of anyone under eighteen (18) years of age, and we do not use Personal Information for profiling in furtherance of decisions that produce legal or similarly significant effects, as those terms are defined under applicable state laws.

12.4 Your State Rights. Depending on your state, you may have the right to: (a) know and access the Personal Information we have collected about you, including the categories collected, sources, purposes, and categories of recipients; (b) obtain a portable copy; (c) correct inaccurate Personal Information; (d) delete Personal Information, subject to exceptions; (e) limit certain uses of sensitive Personal Information; and (f) not receive discriminatory treatment for exercising your rights. You may exercise these rights, designate an authorized agent, and appeal any refusal, as described in Section 11.

12.5 California Notice at Collection. For California residents: the categories listed in Section 12.1 constitute our notice at collection; our retention practices are described in Section 7; and we do not sell or share Personal Information as described in Section 12.3. California's "Shine the Light" law permits California residents to request information about disclosures of personal information to third parties for those third parties' direct marketing purposes; we do not make such disclosures.

13. Users Outside the United States The Services are operated from the United States and are designed primarily for U.S. users, though the Software may be used worldwide as described in the Terms. If you use the Services from the European Economic Area, the United Kingdom, Switzerland, or another jurisdiction with comprehensive data protection laws, the following also applies to the extent such laws apply to our processing:

13.1 Controller; Processor. Tabkeeper is the controller of Personal Information relating to your Account, billing, communications, and use of the Services. For Customer Content processed within an Organization's Workspace, the Organization is the controller and Tabkeeper processes such information as a processor or service provider on its behalf; a Data Processing Addendum is available for eligible customers upon request.

13.2 Legal Bases. We process Personal Information on the following legal bases: (a) performance of a contract — to provide the Services under the Terms and any Bookkeeping Engagement Agreement; (b) legitimate interests — to secure and improve the Services, prevent fraud, communicate with you, and operate our business, balanced against your rights and interests; (c) consent — where required, for example for certain marketing or optional features, which you may withdraw at any time without affecting prior processing; and (d) legal obligation — to comply with Applicable Law.

13.3 Your Rights. Where applicable law provides them, you have rights of access, rectification, erasure, restriction, portability, and objection, and the right to withdraw consent. You may exercise these rights as described in Section 11. You also have the right to lodge a complaint with your local data protection supervisory authority, though we would welcome the opportunity to address your concerns first at support@tabkeeper.io.

13.4 Transfers. Personal Information will be transferred to and processed in the United States as described in Section 10, using appropriate safeguards where required.

14. Children's Privacy The Services are intended for users eighteen (18) years of age and older, and we do not knowingly collect Personal Information from anyone under eighteen (18). If we learn that we have collected Personal Information from a person under eighteen (18), we will promptly delete it. If you believe a person under

eighteen (18) has provided us Personal Information, please contact us at support@tabkeeper.io.

15. Changes to This Privacy Policy We may update this Privacy Policy from time to time to reflect changes in the Services, our practices, or Applicable Law. When we do, we will revise the "Last Updated" date at the top of this Privacy Policy and post the updated version. For material changes, we will provide reasonable advance notice — by email, by notice within the Services, or by other prominent means — before the change takes effect, consistent with Section 55 of the Terms. Your continued use of the Services after an updated Privacy Policy takes effect constitutes your acknowledgment of the updated policy; where Applicable Law requires your consent to a change, we will obtain it.

16. Contact Us

If you have questions, concerns, or requests regarding this Privacy Policy or Tabkeeper's privacy practices, contact us at: Tabkeeper Inc., Attn: James Lin, 61-26 161st St, Flushing, NY 11365. Phone: (917) 517-2100. Email: tabkeeperinc@gmail.com or support@tabkeeper.io (for privacy matters, please use the subject line "Privacy Request").

© 2026 Tabkeeper Inc. All rights reserved.

