FIXTOCK · LEGAL

Data & Privacy Policy

Version 2026-10-11 · Effective October 11, 2026 · Reedstem LLC, Aurora, Colorado, USA

This Data & Privacy Policy explains what information Reedstem LLC collects through Fixtock, how we use and share it, how long we keep it, how we protect it, and the choices and rights you have, during your subscription, after it ends, and after your account is closed.

Contents

1. Who is responsible for your data . . . 2
2. Information we collect . . . 2
3. How we use information . . . 3
4. Legal bases (users in the UK, EEA, Nigeria and similar countries) . . . 4
5. AI features . . . 4
6. How we share information . . . 4
7. Law-enforcement and government requests . . . 5
8. Data storage and international transfers . . . 6
9. Data retention . . . 6
10. During and after your subscription . . . 7
11. Inactive accounts . . . 7
12. How we protect information . . . 8
13. Your privacy rights . . . 8
14. Your choices . . . 9
15. Children . . . 9
16. Former users and Members . . . 10
17. No liability for data loss . . . 10
18. Changes to this Policy . . . 10
19. Contact us . . . 10

1. Who is responsible for your data

> ***In short:*** *We control your account data. Your business controls the business data it puts into Fixtock, including its customers' and staff's details; we process that for the business.*

Reedstem LLC, a Colorado limited liability company based in Aurora, Colorado, United States, operates Fixtock and is responsible for this Policy ("we", "us", "our").

Account and service data. For information about you as a user of Fixtock (for example your name, email, phone number, login, device and usage information, subscription and support history), we decide how and why it is used and are the "controller" (or "business") under privacy laws.

Business data. For information that a Company and its Members enter into a Company workspace, including personal data about the Company's customers, suppliers, staff and other people ("Business Data"), the Company is the controller and we act as its "processor" (or "service provider"), processing Business Data only on the Company's instructions, to provide the Service, and as described in this Policy and the Terms & Conditions. If you are a customer, supplier or employee of a business that uses Fixtock and you have a question or request about your data, please contact that business first; we will help it respond.

This Policy applies to the Fixtock apps, website and related services. It does not apply to third-party services, or to how a Company uses data outside Fixtock.

2. Information we collect

> ***In short:*** *Account details you give us, the business records your team enters, and technical information from your device.*

Account information: first and last name; email address; phone number (and whether it is verified); password (stored only in a securely hashed form by our authentication provider); profile photo, if you add one; preferred country and settings; the Companies you belong to and your role in each; invitation details.

Business Data entered by you and your Members: Company name, stores and locations; products, variants, batches, expiry dates, stock quantities, costs, prices, margins and tax rates; sales, returns, transfers, audits, adjustments and stock counts; financial events, statements and balances; customer records (such as names, phone numbers, emails, addresses, customer IDs, receivables, deposits and purchase history); supplier contact details; staff names, roles and the actions they take; notes and attachments; and AI conversations and generated reports.

Activity and audit information: what actions were taken in a Company, by which user, when, and from which store, so that Companies can see their history and audit trails.

Subscription and payment information: your plan, purchase and renewal dates, status, App Store transaction and subscriber identifiers, country and price. Payments are handled by Apple, Google or another payment processor; we do not receive or store your full card number.

Device and technical information: device model, operating system and version, app version, language, time zone, IP address, device and installation identifiers, push-notification token, crash reports, diagnostic

logs and performance data.

Usage information: features and screens used, actions taken, dates and times, and similar information about how the App is used.

Communications: messages you send us, support requests, feedback, survey answers, and records of our emails, SMS messages and notifications to you, including verification codes and whether they were delivered.

Security information: sign-in attempts, verification and password-reset requests, rate-limit records, and signals used to detect fraud or abuse.

Information from others: information a Company Owner or Admin provides about you when inviting you; information from App Stores and payment providers about your subscription; and information from our service providers (for example, delivery reports).

We do not knowingly collect sensitive data such as government ID numbers, health, biometric or precise location data, and you must not enter it into Fixtock (see the Terms & Conditions, Section 6).

3. How we use information

> ***In short:*** *To run Fixtock, keep it secure, bill subscriptions, support you, improve the product and meet legal duties. We do not sell your data.*

We use information to:

- create and manage accounts, verify email addresses and phone numbers, and authenticate users;
- provide the Service, including storing, syncing, calculating and displaying Business Data, reports, statements, analytics, notifications and AI features;
- enable collaboration within a Company, including roles, permissions, invitations and audit trails;
- manage subscriptions, plan limits, entitlements, trials, renewals, refunds and billing questions;
- communicate with you about your account, security, transactions, changes to the Service and our documents, and support requests;
- maintain, debug, test, analyse and improve the Service and develop new features, using aggregated or de-identified information where practical;
- detect, prevent and investigate fraud, abuse, security incidents, breaches of our Terms, and illegal activity;
- comply with legal obligations, respond to lawful requests, enforce our agreements, and establish, exercise or defend legal claims; and
- with your consent where required, send you marketing about Fixtock (you can opt out at any time).

We do not sell personal information, we do not share it for cross-context behavioural advertising, and we do not use Business Data to advertise to you or your customers.

4. Legal bases (users in the UK, EEA, Nigeria and similar countries)

> ***In short:*** *We process data because it's needed for our contract with you, for our legitimate interests, to meet legal duties, or with your consent.*

Where the law requires a legal basis, we rely on: performance of a contract (to provide the Service you signed up for); legitimate interests (to secure and improve the Service, prevent fraud and abuse, keep business records, and communicate about the Service, balanced against your rights); compliance with a legal obligation (for example, tax and accounting records, and responding to lawful requests); and consent (for example, optional marketing and certain device permissions). Where we rely on consent, you can withdraw it at any time, without affecting earlier processing.

For Business Data, the Company is responsible for having a valid legal basis.

5. AI features

> ***In short:*** *When you use AI features, relevant business data is sent to our AI provider to generate the answer. AI output can be wrong.*

Fixtock's AI features (such as business summaries, insights and answers to your questions) send the relevant parts of your Business Data and your prompts to a third-party AI model provider (currently Google, through Firebase / Gemini) to generate a response. The provider processes that information on our behalf under its terms. Where the provider gives us that choice, we use settings or service tiers under which your content is not used to train the provider's general models.

AI conversations and generated reports may be stored in your Company workspace so you can see them again. AI outputs are generated automatically, may be inaccurate, and are not professional advice. Do not include information in AI prompts that you do not want processed in this way.

6. How we share information

> ***In short:*** *Only with service providers that help us run Fixtock, within your Company, with App Stores for billing, when the law requires it, or in a business sale. Never sold.*

Within your Company. Business Data and your name, role and actions are visible to other Members of your Company according to their roles and permissions. The Owner and authorised Admins can see and manage the Company's data and its Members.

Service providers (processors). We share information with providers that help us run the Service, under contracts that limit their use of it, including: Google Cloud and Firebase (hosting, database, authentication, cloud functions, push notifications, storage and related services); Google's AI services (AI features); RevenueCat (subscription management); Apple and Google (App Store purchases and billing); email and SMS delivery providers (verification codes and service messages); crash-reporting and analytics tools; and customer-support tools.

Payment and App Stores. App Stores and payment processors receive information needed to process purchases, renewals, refunds and fraud checks, under their own privacy policies.

Legal requirements and safety. We may disclose information as described in Section 7, and where we believe in good faith it is necessary to protect the rights, property or safety of Reedstem LLC, our users or the public, to prevent fraud or abuse, or to enforce our agreements.

Business transfers. If we are involved in a merger, acquisition, financing, reorganisation, bankruptcy or sale of all or part of our business or assets, information may be transferred to the buyer or successor, which will be bound to handle it consistently with this Policy, or will notify you of any changes.

With your direction. We share information when you ask us to, for example when you export or share a report, or authorise a third-party integration.

Aggregated or de-identified information that cannot reasonably identify you, your Company or any person may be shared for any lawful purpose.

7. Law-enforcement and government requests

> ***In short:*** *We give user data to authorities only when legally required, such as by a court order, warrant or subpoena, and we tell you unless we're not allowed to.*

We may access, preserve and disclose information about a user, a Company or Business Data in response to a valid legal process, such as a court order, search warrant, subpoena or similar legally binding request from a court, law-enforcement agency, regulator or other government authority with jurisdiction, or where disclosure is otherwise required by applicable law.

We review each request to check that it is legally valid and reasonably limited, and we may object to or narrow requests we consider invalid, overbroad or inappropriate. We generally require requests from outside the United States to come through a recognised international legal process (such as a mutual legal assistance treaty), unless U.S. law permits otherwise.

Unless we are legally prohibited, or doing so would endanger someone, obstruct an investigation, or concern an emergency, we will try to notify the affected user (and, where appropriate, the Company Owner) before disclosing their information so they can seek legal advice or protection.

In an emergency involving a danger of death or serious physical injury, we may disclose information without legal process, to the extent permitted by law.

We may preserve information for up to 90 days (or longer if renewed or required) in response to a formal preservation request while legal process is obtained.

Requests from authorities must be sent to support@fixtock.com with the subject "Law enforcement request". We are not liable for disclosures made in good faith in response to legal process or to an emergency.

8. Data storage and international transfers

> ***In short:*** *Data is mainly stored on Google Cloud servers in the United States, and may be processed in other countries.*

Fixtock is operated from the United States. Information is stored and processed mainly on Google Cloud / Firebase infrastructure in the United States, and our service providers may process it in other countries. These countries may have data-protection laws different from those where you live.

Where the law requires it (for example, for data from the UK, the EEA, Switzerland or Nigeria), we transfer personal data using appropriate safeguards, such as the European Commission's Standard Contractual Clauses, the UK International Data Transfer Addendum, adequacy decisions, or other mechanisms recognised by the relevant regulator. By using Fixtock you understand that your information will be transferred to and processed in the United States.

9. Data retention

> ***In short:*** *We keep data while your account or Company is active, then delete or anonymise it on a schedule, except where the law requires us to keep it longer.*

We keep information only for as long as needed for the purposes in this Policy, unless a longer period is required or allowed by law. Our general schedule is:

- Account data: for as long as your account exists, then deleted or anonymised within 30 days of account deletion, except as listed below.
- Business Data in an active Company: for as long as the Company account exists, whatever plan it is on, until the Owner deletes it or the Company is closed.
- After a paid subscription ends: Business Data is kept; the Company moves to the free plan and its limits (see Section 10).
- After a Company is closed or deleted: Business Data is deleted from live systems within 30 days, and from backups within a further 90 days.
- Records of a Member who leaves a Company: kept as part of the Company's records (including the Member's name in history and audit trails) for as long as the Company keeps those records.
- Backups: kept for up to 90 days, then overwritten, and are not used to restore individual accounts except for disaster recovery.
- Subscription, purchase and billing records: up to 7 years after the transaction, for tax, accounting and legal purposes.
- Records of acceptance of our legal documents: for as long as the account exists and up to 7 years after, as evidence of agreement.
- Security, fraud-prevention and audit logs: up to 24 months, or longer if needed for an investigation.
- Verification codes and rate-limit records: up to 24 hours after expiry, unless kept for an ongoing security investigation.
- Support communications: up to 3 years after the issue is closed.

- Information subject to a legal hold, investigation, dispute or legal request: until it is resolved and any required retention period has passed.
- Aggregated or de-identified data: may be kept indefinitely.

At the end of the retention period, we delete or anonymise the information, or, where that is not technically possible (for example, in backups), we securely isolate it until deletion is possible.

10. During and after your subscription

> ***In short:*** *While you subscribe, we use your data only to provide the Service. When the subscription ends, your data stays on the free plan until you or we delete it.*

During a subscription, we process Business Data only to provide, secure, support and improve the Service and as described in this Policy.

When a paid subscription is cancelled, expires, fails or is refunded, the Company moves to the free plan. Its Business Data is not deleted because of that change, but features and limits of the free plan apply, and some data may become read-only or unavailable until the Company upgrades or reduces its usage.

We do not use Business Data after a subscription ends for any purpose other than the ones in this Policy (keeping it available to the Company, security, legal compliance, and aggregated or de-identified statistics). We will not sell it, and we will not use it to compete with your business.

You should export any data you need before closing your account or Company. After deletion under Section 9, data cannot be recovered.

11. Inactive accounts

> ***In short:*** *If an account or Company isn't used for 24 months, we may delete it after warning you.*

An account is "inactive" if no one has signed in to it for 24 consecutive months; a Company is inactive if none of its Members has signed in for 24 consecutive months and it has no active paid subscription.

We may delete an inactive account or Company and its data. Before we do, we will send a notice to the account email address (and, for a Company, the Owner's email) at least 30 days in advance. Signing in during that period keeps the account. If the email is undeliverable or ignored, deletion may proceed. We may also delete unverified accounts that have not completed registration within 90 days.

We are not liable for the deletion of inactive accounts or Companies under this Section.

12. How we protect information

> ***In short:*** *We use strong, industry-standard security, but no system is 100% secure, and we cannot guarantee absolute safety.*

We use reasonable administrative, technical and physical safeguards appropriate to the nature of the information, including: encryption in transit (TLS) and at rest provided by our cloud infrastructure; hashed passwords managed by our authentication provider; role-based access controls and security rules that keep each Company's data separate; server-side checks on sensitive operations; email and phone verification; rate limiting and abuse detection; limiting staff access to personal data to what is needed; and vetting our service providers.

However, no method of transmission over the internet or of electronic storage is completely secure. We cannot guarantee the absolute security of any information, and you use the Service at your own risk. You are responsible for keeping your password and devices secure, for the roles you grant, and for your own backups (see the Terms & Conditions, Sections 4, 5 and 16).

Data breaches. If we become aware of a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data we hold, we will investigate, take reasonable steps to contain it, and notify affected users, Companies and regulators without unreasonable delay and within the time required by applicable law.

13. Your privacy rights

> ***In short:*** *Depending on where you live, you can access, correct, delete or export your data, and object to some uses. Email us to make a request.*

Everyone. You can view and update much of your account information in the App (Profile & security). You can ask us to access, correct, export or delete your personal information, or to stop sending marketing, by emailing support@fixtock.com with the subject "Privacy request".

United States. If you live in a U.S. state with a consumer privacy law (such as California, Colorado, Connecticut, Virginia, Utah, Texas, Oregon and others), and that law applies to us, you may have the right to: know and access the personal information we hold about you; correct it; delete it; obtain a portable copy; and opt out of the "sale" of personal information, "sharing" for cross-context behavioural advertising, targeted advertising and certain profiling (we do not do these). You will not be discriminated against for exercising these rights. You can appeal our decision on a request by replying to our response with the subject "Privacy appeal"; if you are not satisfied, you may contact your state Attorney General. You may use an authorised agent, who must provide proof of authority.

UK, EEA and Switzerland. You may have the right to access, rectify, erase, restrict or object to processing of your personal data, to data portability, to withdraw consent, and to lodge a complaint with your local data-protection authority.

Nigeria. Under the Nigeria Data Protection Act 2023, you may have the right to be informed, to access, rectify, erase or port your data, to restrict or object to processing, to withdraw consent, not to be subject to decisions based solely on automated processing, and to lodge a complaint with the Nigeria Data

Protection Commission.

Other countries. You may have similar rights under your local law, and we will respond in line with that law.

How we handle requests. We will verify your identity (usually by asking you to write from your account email or to sign in) before acting on a request, and respond within the time the applicable law requires (generally within 30 to 45 days). Some requests may be refused or limited where the law allows, for example where we must keep information for legal reasons, or where it would reveal another person's data.

Business Data. Requests about Business Data (for example, from a business's customer or employee) will be referred to the Company that controls it. A Company Owner can correct or delete Business Data in the App.

Deleting your account. Deleting your personal account removes your access and your account data as described in Section 9. It does not delete Business Data belonging to a Company you were a Member of, and your name may remain in that Company's history. If you are the only Owner of a Company, deleting your account may require closing that Company, which deletes its Business Data for all Members.

14. Your choices

> ***In short:*** *You control notifications, device permissions and marketing messages.*

You can turn push notifications on or off in the App or your device settings; manage device permissions (such as camera, photos or files) in your device settings; unsubscribe from marketing emails with the link in each email; and update your profile in the App. Service and security messages (such as verification codes and account notices) cannot be turned off while you have an account.

Our apps do not use third-party advertising trackers. Our website may use essential cookies needed for it to work, and, with your consent where required, analytics cookies. We do not respond to "Do Not Track" signals, but we honour Global Privacy Control signals where the law requires.

15. Children

> ***In short:*** *Fixtock is for adults only. We don't knowingly collect data from children.*

Fixtock is a business tool intended for people aged 18 or over. It is not directed to children, and we do not knowingly collect personal information from anyone under 18 (or from children under 13 under the U.S. Children's Online Privacy Protection Act). If we learn that we have collected information from a child, we will delete it. If you believe a child has provided us with information, contact support@fixtock.com.

Companies must not enter personal data about children into Fixtock.

16. Former users and Members

> ***In short:*** *When you leave, your access ends but your actions stay in your former Company's records.*

When a Member leaves or is removed from a Company, their access ends immediately, but the records they created, and their name and actions in history and audit trails, remain part of the Company's Business Data under the Company's control. Former Members can ask us to delete their personal account (Section 13); this does not remove those Company records, because the Company has a legitimate need to keep accurate business and audit records.

If a Company closes, its Members lose access to its data, and the data is retained or deleted as described in Section 9.

17. No liability for data loss

> ***In short:*** *We take care of data, but we are not liable for data loss. Keep your own copies.*

To the maximum extent permitted by law, and as set out in the Terms & Conditions (Sections 16 and 17), Reedstem LLC is not liable for the loss, corruption, deletion or unavailability of any information, including through deletion under this Policy, inactive-account deletion, actions of Members, software errors, service interruptions, security incidents or failures of third-party providers. You are responsible for keeping your own backups and exports of information that is important to you or that you must keep by law.

18. Changes to this Policy

> ***In short:*** *We'll post updates here and tell you about important changes.*

We may update this Policy from time to time. We will post the new version with a new effective date and version number. If changes are material, we will notify you in the App or by email before they take effect and, where required by law, ask for your consent. Your continued use of Fixtock after changes take effect means you accept them, to the extent permitted by law.

19. Contact us

> ***In short:*** *For privacy questions or requests, email support@fixtock.com with the subject "Privacy request".*

Reedstem LLC, Aurora, Colorado, United States. Mailing address: available on request by email.

Email: support@fixtock.com (subject "Privacy request" for privacy matters; "Law enforcement request" for legal process from authorities).

If you are in the UK or EEA and we are required to appoint a local representative, we will publish its details here.

Acceptance. By tapping “Accept” in the Fixtock app, creating an account or using the Service, you confirm that you have read, understood and agree to this Data & Privacy Policy, version 2026-10-11. Keep a copy of this PDF for your records.