Privacy Policy

Last updated: 2026-02-17

This Privacy Policy describes how the Spending Tracker application ("Service") c
ollects, uses, stores, and deletes personal information and financial data.

1. Who We Are
- Business type: Sole proprietorship
- Service: Spending Tracker
- Contact: Replace with your support email before publishing

2. Data We Collect
- Account profile data: email address, display name, authentication settings.
- Financial connection metadata: institution name, account identifiers/masks, ac
count balances.
- Transaction data: transaction date, merchant, description, amount, category, a
ccount mapping.
- Security and operational data: login events, request identifiers, basic IP/use
r agent metadata for security auditing.

3. Data We Receive via Plaid
- We use Plaid to connect financial institutions.
- We do not collect online banking credentials directly.
- Plaid access tokens are encrypted at rest before storage.

4. How We Use Data
- Provide core features: transaction sync, categorization, budgeting, reporting.
- Improve data quality: learned category rules and user-driven category correcti
ons.
- Security and fraud prevention: authentication, logging, access controls, incid
ent response.
- Legal compliance and recordkeeping.

5. Legal Basis and Consent
- We process data based on user consent and contract performance (providing requ
ested features).
- Users are asked to authorize financial data access through Plaid Link and Data
 Transparency Messaging.

6. Data Sharing
- We do not sell personal financial data.
- Data is shared only with necessary processors/providers to operate the Service
 (for example, hosting/database and Plaid).
- We may disclose data if legally required (court order, legal process, or regul
atory obligation).

7. Data Retention
- Data is retained only as long as needed for service operation, legal obligatio
ns, and security purposes.
- Retention and deletion controls are implemented and reviewed periodically.
- Users can request deletion; account-level deletion removes associated user-sco
ped records.

8. Data Security
- TLS is used for data in transit.
- Sensitive tokens are encrypted at rest.
- Access to production systems is restricted and monitored.
- Security logging and incident response procedures are in place.

9. Your Rights
- Depending on your jurisdiction, you may have rights to access, correction, del

etion, portability, and objection/restriction.
- To exercise rights, contact: Replace with your support email before publishing
.

10. International Transfers
- If data is processed outside your jurisdiction, we use reasonable contractual and technical safeguards.

11. Children
- The Service is not intended for children under 13 (or equivalent minimum age b y jurisdiction).

12. Changes to this Policy
- We may update this policy periodically.
- Material changes will be reflected by updating the "Last updated" date and, wh ere required, direct notice.

13. Contact
- Replace with your legal business name and support email/address.