BudgetClip Inc. Privacy Policy

Version 1.16.1 · Last updated October 22, 2026

The short version

BudgetClip helps you organize your finances. We use the information you provide to run your account, show your financial records and support you. BudgetClip Inc. will not sell, rent or trade your personal or financial information for advertising or any other purpose. We will not use your financial records for targeted advertising. BudgetClip Inc. prohibits sending users' financial records to external AI services, including for development, support or product features. We use AI-assisted development tools with source code, documentation and fictional test data. We do not use advertising trackers or your financial records for marketing recommendations or household benchmarks. The public demo uses fictional finances.

BudgetClip is available by invitation. We protect the hosted service with HTTPS and authenticated access, maintain encrypted off-server backups, and test recovery in isolated environments. Managed daily production backups follow a 30-day retention schedule. Your financial records are private to your account and are not visible to other users. You can export your records or start account deletion at any time in the app. Necessary operator/provider access and retained copies are explained below; account deletion is not immediate erasure of every copy. See "How long we keep information" for the schedules and handling of retained copies.

Who is responsible

BudgetClip is operated by BudgetClip Inc., a Canadian corporation incorporated on October 18, 2026 and registered in Ontario. The **Owner and Privacy Officer** is accountable for our privacy practices and handles access requests, corrections, deletion requests and complaints. Contact **privacy@budgetclip.ca**. Please do not email passwords, bank credentials or connection tokens.

This policy covers the hosted service at budgetclip.ca, its website, waitlist, demo and support communications. People running their own copy of the software are responsible for that deployment and its handling of information.

Information we handle

Category	Information we handle	Why we use it
Account and sign-in	Email address, account identifiers, password hash, authentication and MFA records, sessions and security settings.	Create and protect your account, authenticate you and manage signed-in devices. Passwords are checked by the authentication system; connection credentials remain on the server.
Financial records	Account names and types, balances, transactions, dates, amounts, currencies, merchants, notes, categories, budgets, rules, income, bills and savings goals.	Provide the budgeting tools you request, calculate reports and save your financial settings.
Imported files and attachments	Financial files and any personal information in records or attachments you enter or upload.	Import and organize the information you provide. Supply only what is useful, and include another person's information only with authority.

Category	Information we handle	Why we use it
Support and feedback	Your message, optional reply email and technical details you choose to include.	Respond to requests, investigate reported problems and show the status of your submissions.
Waitlist and invitations	Email address, language, contact consent and invitation records.	Manage requested access invitations and waitlist communications. Joining the waitlist does not create an account.
Preferences and technical records	Browser preferences, network addresses, browser information, access events and error or security records.	Remember your choices, operate the service and detect abuse or security incidents.
Agreement and administrative records	User Agreement version and acceptance time, necessary administrative actions and minimal deletion records.	Record your choices, manage the service, resolve disputes and prevent restoration of a closed account.

Account setup and the waitlist use your email address without asking for a profile name or date of birth. Self-service deletion asks you to type the email address displayed for your account after account verification and explicit acknowledgements. Password and two-factor verification continue to protect deletion. Names you choose for financial accounts, Budgets or records remain part of your financial information. Stripe and bank-connection providers handle the billing or identity information needed for their respective services as described below.

Why we use it and your choices

We use this information to authenticate you, provide the financial tools you request, save your settings, troubleshoot problems, respond to support requests and detect abuse or security incidents. We record agreement acceptance and necessary administrative actions to manage the service and resolve disputes. Authorized operators and service providers may access information only as needed to deliver the requested service, provide support, maintain or recover the service, investigate security incidents or meet legal obligations. We do not provide end-to-end encryption that prevents authorized operator access. These limited uses do not permit the sale, rental or trading of your information.

Waitlist consent is separate from registration and is limited to beta-access contact. Joining does not create an account or connect a bank. Optional marketing is not bundled into the User Agreement. We will explain any material new use, and obtain appropriate consent before introducing it. This does not create an exception to our no-sale commitment or permit using financial records for targeted advertising.

You can use the fictional demo without providing financial records. If you withdraw permission needed for a feature, that feature may stop working; you can ask about alternatives, disconnect a feed or close your account.

Service providers and their purposes

Hosting and data storage. DigitalOcean hosts the application, financial database, private operational state and logs in Toronto, Canada. DigitalOcean’s infrastructure and operational controls are covered by independent SOC 2 Type II and SOC 3 Type II assurance reports. See DigitalOcean’s assurance reports.

Email. Our support, privacy and employee inboxes use Proton Mail, an award-winning privacy-focused email service operated by Proton AG, a Swiss company. Correspondence may be processed outside Canada. Resend delivers requested account verification, password-reset, Google-link confirmation and invitation emails. It receives recipient addresses, message contents including short-lived links or codes, and delivery metadata. These account emails contain no transactions, balances or bank credentials. Open and click tracking are disabled. Resend processes account email-service data in the United States.

Sign-in. Google or Meta processes basic identity, email and connection information when you choose its sign-in option, as described below. Your financial records are not sent to these providers for sign-in.

Bank connections. For a bank connection you authorize through Plaid, the provider processes institution and account information, balances and transactions to supply your bank feed. The authorization flow identifies the requested access. Plaid may process information outside Canada.

Subscription payments. Stripe handles subscription checkout, payment methods, invoices and the customer portal. Stripe receives billing and payment information. BudgetClip stores customer, subscription and payment-status references rather than your full card details. Your budgeting transactions and balances are not sent to Stripe. Information may be processed outside Canada.

Feedback and support. Our private, self-hosted GitLab installation stores the feedback and support tickets described below. Authorized support administrators can access the messages and optional reply information you submit.

We limit disclosures to what is needed for the stated service, your instructions, security investigations or legal requirements. The no-sale commitment and external-AI financial-record prohibition apply to these uses. Hosting and supporting providers may use infrastructure or support outside Canada, where information may be subject to that jurisdiction’s laws. Toronto application hosting does not mean every provider’s processing stays in Canada. We remain responsible for our handling of information and the providers we choose.

Provider notices include DigitalOcean, Proton Mail, Resend, Google, Meta, Plaid and Stripe. We explain material changes to the described processing before introducing them.

Feedback and support tickets

When you choose **Submit** in Contact us, BudgetClip stores your message in an encrypted queue and sends it to our private, self-hosted GitLab support project. Your message is visible to the operator and authorized project administrators, not the public. You can choose to include your account email for a reply. Technical details are selected by default for problem reports and are off by default for support requests. Feature requests do not include technical details. When selected, they show the reported browser and version, operating system, device type, screen and window dimensions, display scale, app version, page, language, theme and sync status. You can review the exact diagnostic snapshot in the form and uncheck this option before submitting. Reply email remains a separate choice. Those automatic details exclude balances, merchants, bank-account identities, credentials, full URLs and raw error messages. Please do not include sensitive financial records or secrets in your message.

Delivered queue message copies are removed after seven days, checked on startup and hourly. Undelivered messages remain queued until delivered or a failure is resolved. Minimal references and delivery receipts remain to prevent duplicate tickets and support deletion requests. Closed support tickets and correspondence have a 24-month retention target, with earlier deletion on request or through account closure where applicable. Account closure requests removal of linked active tickets and waits for confirmed cleanup before finishing; uncertain results require assistance. Copies in backups and any separate email correspondence have the retention limits described below.

Optional social sign-in

Google sign-in is optional. Choosing it opens Google's sign-in page or, in the Android app, Google's account chooser. Google receives connection information and the fact that you are using BudgetClip to sign in. We request basic identity and email, and store Google's stable account identifier, the app/client identifier, your associated BudgetClip account/email and connection time to recognize your sign-in. Provider tokens are used transiently during sign-in; they are not stored as ongoing access to your Google account. We do not send your financial records to Google for sign-in or request your Google password, contacts or posts.

Connecting an existing account requires explicit confirmation and BudgetClip authentication. You can disconnect Google in Account → Connected sign-ins and continue using your BudgetClip password. This does not delete your Google account. Google may process information outside Canada under Google's Privacy Policy. Account-verification messages, invitation requirements and agreement acceptance remain separate.

When you choose Facebook sign-in, Meta processes basic identity, email and connection information. BudgetClip stores the stable provider identifier and account binding to recognize your sign-in. The same confirmation and authentication requirements apply to account linking. Provider tokens are used transiently; your financial records are not sent to Meta for sign-in. You can disconnect the provider in Account → Connected sign-ins. Disconnecting does not delete your Facebook account. Meta may process information outside Canada under its Privacy Policy.

Cookies and browser storage

We use necessary cookies and browser storage to provide the service. We do not use advertising trackers.

Storage or session	Purpose	Duration and your controls
Account session cookies	Authenticate requests and protect account access.	Application sessions last at most 12 hours; native authentication may expire sooner. Sign out to end your current app session.
Remembered sign-in	Keep you signed in when you choose this option.	Up to 30 days; review and disconnect remembered sessions through the app's signed-in device controls.
Invitation and waitlist cookies	Support invitation and waitlist checks.	Used for the relevant checks. You can clear site cookies through your browser; doing so can interrupt those flows.
Demo session	Keep fictional demo records separate from real accounts.	Up to two hours; discarded on reset, exit or server restart.
Browser preferences	Save language, theme, localization and account order.	Stay on your device until changed or cleared. Clearing site storage resets these preferences.

Storage or session	Purpose	Duration and your controls
Android home-screen widgets	Display your selected Budget, category totals, recorded net worth and its 12-month trend, savings-goal summaries, Budget review counts and amounts, and scheduled bills, with your chosen theme.	Encrypted, backup-excluded summaries on your device. Refresh removes expired summaries after 24 hours or a Budget-month change. Android controls when background refresh runs. Signing out clears the widget account state; removing widgets removes their configuration and summaries no other widget uses.

In the Android app, choosing Remember me saves an encrypted session identifier in app-private storage protected by Android Keystore. It is excluded from app backups. The saved sign-in is removed when you sign out or the app detects an expired or rejected session. Your password, Google token and financial records are not saved with it. Clearing the app's storage also removes the saved sign-in.

Blocking necessary cookies can prevent sign-in and other account functions. Clearing browser storage does not delete your server-side account or financial records.

Widgets are optional. Their local summaries are protected with AES-256-GCM and Android Keystore, separately from the remembered sign-in. Amounts and progress are hidden by default; you can choose to display them in Appearance and the widget settings. Budget/category/goal names, review counts and bill dates can remain visible. Anyone able to view your home screen can see the displayed content, which Android and your launcher render. Remove the widget to remove that display. The net-worth widget uses the same account-inclusion settings and recorded balance history as the application. Background refresh and the widget Refresh button use your existing authorized session and shows the last successful update time; it does not initiate a bank sync.

How long we keep information

The table distinguishes automatic expiry from retention targets applied through controlled review. Historical copies are reviewed against this schedule before removal. A legal obligation, an active access request or a documented incident hold may require specific records to be kept longer. Holds are limited to necessary records and reviewed before deletion resumes.

Record or copy	Retention period	How it is handled
Active account, financial records and settings	While your account is active, unless you delete records or complete closure.	Disconnecting a feed does not remove already imported history or cancel an independent provider subscription.
Active waitlist entries	Up to 90 days.	Expiry is checked on startup and hourly. You can request earlier removal. Separate exports or backups require their own cleanup.
Active account-email jobs	Up to 24 hours.	Encrypted jobs are pruned on startup and hourly while running. Minimal delivery receipts and provider records have separate retention and review.
Reset and verification links	Password reset: 30 minutes. Account-email verification: one hour. Google account-link confirmation: five minutes.	Verification status remains until account closure or replacement. Link expiry does not itself delete separate delivery records.

Record or copy	Retention period	How it is handled
Feedback queue messages	Delivered copies: seven days. Undelivered messages: until delivery or a failure is resolved.	Delivered-copy expiry is checked on startup and hourly. Minimal references and receipts prevent duplicate tickets and support deletion.
Managed daily production backups	30-day retention schedule.	Eligible expired copies are removed after a verified replacement is available. The newest complete copy and copies awaiting verification are preserved for recovery; overruns require review.
Manual backups and deployment rollback copies	Retention target: 30 days after a verified replacement is available.	Reviewed for removal against the replacement date, recovery-key dependencies and current deletion safeguards.
Old attachments outside active records	Until associated account cleanup or the documented operational need ends.	Ownership and shared-record dependencies are reviewed monthly before removal.
Closed support tickets and correspondence	Retention target: 24 months after the request closes; earlier deletion on request or through account closure where applicable.	Open requests remain available for resolution. Required holds and minimal cleanup references are preserved.
Routine infrastructure logs	30-day retention target.	Reviewed for removal; necessary records may be preserved under a documented hold.
Security and administrative audit records	12-month retention target.	Access is restricted; required incident and legal holds apply to the necessary records.
Privacy-breach records	At least 24 months after we determine that a breach occurred.	Every personal-information breach is recorded, including the harm assessment, notification decisions and response. Longer applicable legal or hold requirements take precedence.
Agreement, completed invitation and billing records	For account administration, consent evidence or a documented accounting, dispute or legal obligation.	Necessary records are reviewed monthly and superseded personal information is removed when its purpose ends.
Minimal deletion, revocation and duplicate-prevention records	While a restorable copy or unresolved operation could reactivate an account, connection or duplicate action.	Limited to identifiers, state and timestamps; reviewed before release.

Account deletion and backup retention are handled separately. Retained copies are reviewed for deletion and any applicable retention requirement. Current deletion records must be applied before restored services reopen so recovery does not reactivate a closed account. Session and browser-storage durations are described above.

Access, correction, export and deletion

In **Account → Data & privacy**, authenticated users can download JSON records or transaction CSV after a fresh password check and MFA where enabled. Exports include supported active financial records across currencies and excluded accounts. JSON includes supported settings, attachment metadata and your active feedback queue records or delivery references; older GitLab support history can be requested from us. It does not include attachment contents, deleted records, credentials, infrastructure logs or a complete restorable backup. Contact us for requests that exceed export limits or require other records.

You can correct records through available account and financial editors or ask us for help. Changes in BudgetClip do not correct the original records at your bank. Contact the bank about those records.

You can initiate account deletion at any time in Account → Data & privacy, or contact us where assistance is required. Account closure first disconnects feeds and waits for cleanup, then requires another confirmation to delete the native account and its owned records. Administrator accounts, attachments, shared groups or uncertain cleanup results require assistance. Retained backups and logs are not erased automatically. Account closure does not delete records held independently by your bank or other providers. A minimal deletion register containing identifiers, status and timestamps stays to prevent a restored backup from reactivating a closed account; it does not contain financial values or passwords. Browser preferences may remain on your device until you clear them.

We handle personal information under applicable Canadian privacy law, including the Personal Information Protection and Electronic Documents Act (PIPEDA). For written access requests under PIPEDA, we respond within 30 days of receipt, subject to the extensions permitted by law. If an extension is necessary, we notify you within those first 30 days, explaining the reason, the new deadline and your right to complain to the Privacy Commissioner. We assist with preparing a request where needed and preserve the information covered by an access request for as long as necessary to allow available recourse.

Contact **privacy@budgetclip.ca** to request access, correction, removal, withdrawal of optional consent or an explanation of retained information. We may need proportionate identity verification. We will explain any limits that apply, including records affecting another person or legal retention requirements. You can also raise an unresolved concern with the appropriate privacy regulator, including the Office of the Privacy Commissioner of Canada.

Protecting information

We use HTTPS for the hosted service, authenticated access, server-side handling of connection secrets and controls intended to separate users' records. Financial database tables are encrypted at rest with AES-256, and internal database connections use verified TLS 1.3. TLS also protects network connections behind the public website, including routing to the application, backend APIs, sign-in and recovery services, and the operational email relay. Certificates and destination hostnames are verified. Android widget snapshots are encrypted locally with AES-256-GCM using Android Keystore. BudgetClip Inc. prohibits employees, subcontractors and other third parties from viewing your account or financial records, except for the limited service, support, security, recovery and legal purposes described in this policy. App-based two-factor authentication and signed-in device controls help you protect account access. Encrypted off-server backups and isolated recovery checks support recovery of the production service. The public demo uses fictional records in an isolated workspace.

Security incidents

If we discover a security incident, we investigate, contain it and assess the sensitivity of the information and the likelihood of misuse. Where a breach creates a real risk of significant harm, we report it to the Office of the Privacy Commissioner of Canada and notify affected individuals as soon as feasible after determining that the breach occurred, as required by PIPEDA. Notices explain the information involved, the steps taken and what affected individuals can do to reduce harm. We keep records of every personal-information breach for at least 24 months after determination, including our assessment and notification decisions, and preserve them longer where another applicable legal requirement or authorized hold applies.

Eligibility and changes

Account holders must meet the age-of-majority requirement in the User Agreement. Family budgeting may include information about dependants; provide it only where you are authorized to do so. The service is not designed for children to register independently.

We publish a dated version when this policy changes. Material changes will be brought to users’ attention, and new purposes requiring consent will be presented before use. Contact us if a change affects your choices.

If language versions of this policy differ in meaning or interpretation, the English version prevails to the extent permitted by applicable law. Mandatory language and consumer rights remain unaffected.