



ECHO PORTFOLIO

Privacy Policy

Effective date: 30 July 2026

Last updated: 1 August 2026

Echo Portfolio is provided by **Blake Kneebone** ("Echo", "we", "us", or "our"). This Privacy Policy explains how Echo Portfolio handles information when you use the Echo Portfolio mobile app, widgets, support services, and related online services (together, the "Services").

1. The short version

Echo Portfolio is designed to keep core portfolio records on your device.

- You can use manual portfolios, file imports, direct connections, public-wallet tracking, and other core portfolio features without creating an Echo account.
- Portfolio names, holdings, units, transactions, cost bases, and calculated portfolio values are normally stored locally in the app.
- To deliver market data and protect the Services, the app sends asset symbols, exchange and currency identifiers, and limited network and security information. Ordinary market-data requests do not include your units, transaction history, cost bases, or calculated portfolio values.
- An optional Echo account is used for Support and for connection-partner integrations. Those features necessarily process the information you choose to provide or connect.
- Optional app diagnostics are off unless you consent. They are not used for advertising or linked to an Echo account or stable device identifier.
- We do not sell personal information, show behavioural advertising, or track you across other companies' apps and websites.

More detail follows.

2. Information handled by the Services

2.1 Portfolio and investment information stored on your device

Depending on the features you use, the app may store:

- portfolio names and base currencies;
- asset symbols, exchanges, currencies, holdings, units, prices, cost bases, transactions, and calculated performance or portfolio values;
- public wallet addresses and transaction information obtained for those addresses;
- data imported from a file or a connected broker, exchange, or other service; and
- watchlists, preferences, widget settings, and other app configuration.

This information is normally stored locally on your device. It may also be included in an operating-system backup or device transfer, depending on your device, platform, and backup settings. Apple or Google controls those backup services under its own terms and privacy policy.

2.2 Market-data and service-security information

When the app requests prices, charts, instrument details, news, exchange rates, or other public content, we may process:

- asset symbols, exchange identifiers, currency codes, requested time periods, and similar request parameters;
- app version and build, operating system and major version, device class, and service-response information;
- IP address and standard network request information processed by our hosting, content-delivery, and security infrastructure; and
- device- or app-integrity proofs, short-lived security tokens, request timing, rate-limit information, and evidence needed to prevent abuse.

We use this information to provide requested content, protect the Services, diagnose failures, enforce reasonable limits, and maintain reliability.

2.3 Optional Echo account

If you create an Echo account using Sign in with Apple, we receive an account identifier from Apple and, if you choose to provide them, your name and email address. Apple may provide a private relay email address instead of your personal email address. We also process authentication and session information needed to secure the account.

An Echo account is not required for core local portfolio use. It is required for Support and for integrations that use a connection partner.

2.4 Optional integrations

If you choose to connect a broker, exchange, wallet, or other integration, the information handled depends on that service and the connection method. Before a connection is made, the app identifies the information requested and how the connection works.

A connection may involve:

- account identifiers and connection status;
- holdings, balances, transactions, and related account information;
- a public wallet address and public blockchain activity;
- credentials or access tokens needed to connect; and
- consent, connection, refresh, and error records.

Some integrations connect directly from your device. Credentials for those direct connections are stored in the device's secure credential storage where supported, and imported portfolio records are stored locally. Other integrations use an Echo account and a connection partner to establish and maintain the connection. In that case, the partner and our cloud services process the connection information needed to provide the feature.

We use connected information only to provide the integration, import or refresh the information you request, show it in the app, troubleshoot the connection, and meet security or legal obligations. The connected service and any connection partner handle information under their own privacy policies and terms.

2.5 Support information

If you contact Support, we process the information you submit, which may include:

- your Echo account identifier and contact details;
- support messages, request status, and conversation history;
- screenshots, images, files, or diagnostic logs that you explicitly attach;
- app version, operating-system information, and technical details relevant to the issue; and
- a push-notification token if you enable Support notifications.

Do not include passwords, access tokens, recovery phrases, private keys, or other secrets in a Support request.

2.6 Optional app diagnostics

If you consent to app diagnostics, the app may send sampled records about:

- app launches and general feature-action outcomes;
- bounded error, result, and duration categories;
- app version and build;
- iOS or Android and the operating-system major version; and
- phone or tablet device class.

These diagnostics do not include portfolio, holding, or transaction contents; asset searches; credentials; Support messages; files; quantities; portfolio values; or a stable account or device identifier. We do not join them to your Echo account, Support history, or connection information.

You can turn diagnostics off in the app. The app may send one final, identifier-free “diagnostics disabled” signal and then stops diagnostic collection and clears queued diagnostic records on the device.

2.7 Camera, photos, and files

Camera access is requested only when you choose to scan a public wallet QR code. You can enter the address manually instead. QR processing is performed for the feature you selected.

The app uses system file and photo pickers. It receives only the file or image you select, not unrestricted access to your photo library. A selected item leaves your device only when the feature requires it—for example, when you attach it to a Support request or send information to a service you chose to connect.

2.8 Information from app stores and platform services

Apple and Google may process app downloads, purchases, subscriptions if offered, crash information, device integrity, push notifications, and store interactions under their own privacy policies. We may receive limited status, transaction, or technical information needed to provide and support the app. We do not receive your full payment-card details from an app store.

3. How we use information

We use information to:

- provide portfolios, market data, charts, news, widgets, integrations, Support, and other requested features;
- authenticate accounts and maintain connection consent;
- secure the Services, detect abuse, investigate incidents, and enforce limits;
- diagnose errors, monitor reliability, and improve app functionality when you have enabled diagnostics;
- communicate with you about Support, security, service changes, and this policy;
- comply with law and respond to valid legal requests; and
- establish, exercise, or defend legal claims.

Where applicable law requires a legal basis, we rely on performance of our agreement with you, your consent, compliance with legal obligations, and our legitimate interests in operating and securing the Services. You may withdraw consent at any time, without affecting processing already carried out lawfully.

4. When we disclose information

We may disclose information:

- **To service providers.** Hosting, content-delivery, authentication, notification, security, and support providers process information for us under contractual and confidentiality obligations.
- **At your direction.** When you connect a broker, exchange, wallet, or connection partner, we exchange the information needed to perform your request.

- **To platform providers.** Apple and Google process information needed for Sign in with Apple, app integrity, system notifications, app distribution, and related platform functions.
- **For legal and safety reasons.** We may disclose information if reasonably necessary to comply with law, a valid legal process, protect a person, prevent fraud or abuse, or protect our rights and the Services.
- **For a business transfer.** Information may be disclosed as part of a merger, financing, reorganisation, sale of assets, or similar transaction, subject to appropriate confidentiality and notice requirements.

We do not sell personal information. We do not disclose personal information for cross-context behavioural advertising, and we do not use the app to track you across other companies' apps or websites.

5. Storage, retention, and deletion

We retain information only for as long as reasonably needed for the purposes described above, including security, legal, accounting, dispute-resolution, and service-continuity needs.

- **Local app data** remains on your device until you delete the relevant portfolio or app data, uninstall the app, or erase the device. Copies may remain in operating-system backups until those backups expire or you delete them using the platform's controls.
- **Echo account, Support, and connection-partner data** is kept while your account or request is active and as needed to provide, secure, and document the service. When you delete your Echo account, we delete account-owned Support content and attachments, revoke account-owned partner authorisations, remove push registrations, and delete the account profile. Content you posted on another person's Support request is anonymised where retaining the operational timeline is necessary.
- **Account-deletion safety record** is retained for 90 days after account deletion to reject old credentials and delayed messages. It records deletion state, not your deleted profile or portfolio contents.
- **Optional diagnostic event records** expire within 72 hours, plus a short processing-finalisation period. Population-level aggregates that do not identify an account or stable device may be retained to understand reliability. Because those aggregates cannot be connected to an individual, they cannot be individually retrieved or deleted.
- **Security and infrastructure records** are kept for a limited period appropriate to incident detection, investigation, abuse prevention, and legal obligations, then deleted or de-identified.

Deletion from active systems may take a reasonable time to complete. Residual copies may remain temporarily in restricted backups or disaster-recovery systems and are removed under their normal expiry schedules.

6. Your choices and rights

You can:

- use core portfolio features without creating an Echo account;
- enable or disable app diagnostics in the app;
- grant or withdraw camera and notification permission in device settings;
- disconnect an integration and remove locally imported data using the app's controls;
- delete local portfolios and other app data;
- delete your Echo account in **More → Echo account → Delete Echo account**; and
- contact us to request access, correction, deletion, restriction, or a copy of personal information we control, or to object to certain processing, where applicable law provides those rights.

Deleting an Echo account removes account-owned cloud data but does **not** automatically delete portfolio records stored locally on your device. To remove those records, delete them in the app or remove the app and manage any operating-system backups separately.

We may need to verify your identity before completing a privacy request. Some requests may be limited where retention is required by law, necessary for security or legal claims, or technically impossible for information that was never linked to you.

For an account-deletion request outside the app, visit <https://dt03nj1f3lavq.cloudfront.net/account-deletion.html> or contact echo@blake.org.au.

7. Security

We use administrative, technical, and organisational safeguards designed to protect information. These include encrypted network transport, platform secure credential storage where supported, access controls, app- and device-integrity checks, and restricted operational access. No storage or transmission method is completely secure, so we cannot guarantee absolute security.

You are responsible for protecting your device, device passcode, account credentials, wallet secrets, and credentials for services you connect.

8. International processing

We and our service providers may process information in Australia and other countries where we or they operate. Privacy laws in those countries may differ from those where you live. Where required, we use appropriate contractual or other safeguards for international transfers.

9. Children

Echo Portfolio is a financial record-keeping tool intended for adults and is not directed to children. We do not knowingly collect personal information from a child in circumstances where parental consent is legally required. If you believe a child has provided personal information, contact us so we can investigate and take appropriate action.

10. Third-party content and services

The Services may display market information, news, links, and content supplied by third parties. If you open a third-party site or connect a third-party service, that third party's privacy policy and terms apply to its handling of information. This policy does not control independent third parties.

11. Changes to this policy

We may update this policy as the Services, law, or our practices change. We will post the updated policy and change the "Last updated" date. If a change is material, we will provide additional notice where required.

12. Contact us

Privacy questions, requests, or complaints may be sent to:

Blake Kneebone

PO Box 1187, Fremantle, WA, Australia 6959

Email: echo@blake.org.au

If you make a complaint, please describe your concern and how we can contact you. We will investigate and respond within a reasonable period. You may also have the right to complain to the privacy or data-protection authority in your jurisdiction.