



POLICY · DATA PROTECTION AND PRIVACY

Data Retention and Deletion Policy

Version 2 · Approved by Jacek Janczura · 21 October 2026

Taufolio · Jacek Janczura
Adama Mickiewicza 73, 01-625 Warszawa, Poland
EU VAT: PL5253008276 · support@taufolio.com

Contents

1. Objective

2. Scope

3. Policy statement

4. Data retention guidelines

5. Document security classification

6. Non-compliance

7. Responsibilities

8. Schedule

9. Version history

1. Objective

Users of Taufolio may ask for their data to be deleted, and Taufolio must not keep data longer than it needs it. This policy sets out the retention periods Taufolio applies, how deletion requests are handled and how deletion is carried out. It supports the GDPR principle of storage limitation and the commitments made in the published Privacy Policy.

2. Scope

This policy applies to all data in Taufolio's possession that comes from its users or relates to them, in the production database and file storage, in backups, and in the subprocessors that process data on Taufolio's behalf. It also covers data collected for features that are in testing, beta or early access.

3. Policy statement

Data is retained only while there is a continued and valid reason to store or process it. Users may request deletion of their data. Requests must be authenticated and assessed for legitimacy, and deletion may be withheld only where the law requires the data to be kept or where another legitimate ground in the GDPR applies. Anonymization may be used instead of deletion where it achieves the purpose and no law or contract prevents it.

4. Data retention guidelines

4.1 General rules

- Data must be kept only for the purposes described in the Privacy Policy and only for as long as reasonably necessary: to provide the service, to maintain account history and purchased entitlements, to comply with legal, tax, accounting or reporting obligations, to resolve disputes, to enforce agreements and to investigate abuse, fraud or security incidents.
- Retention periods enforced by automated processes must be implemented in code or provider settings, not left to manual action.
- Staff members who are unsure about a deletion request or this policy must contact the Information Security Officer before acting.

4.2 Retention periods

Data	Retention
Customer brokerage credentials (tokens, API keys, secrets)	Deleted immediately when the user disconnects the broker or deletes the account

Data	Retention
Raw earnings-call transcripts and uploaded transcript files	Deleted from storage 90 days after creation by an automated retention job
Upload audit events	Deleted 90 days after creation by the same job
Error and performance monitoring records (Sentry, EU region)	90 days from collection, then deleted automatically
Screenshots and files attached to bug reports, with technical device data and the record of last steps	Kept while the case is open, deleted automatically 90 days after it is closed
Uploaded brokerage statements and files (portfolio import)	Deleted automatically 365 days after upload at the latest; kept for that time so that Taufolio can fix the importer when it skips or misreads part of a file; deleted at once when the import is cancelled and when the workspace is deleted with the account. Import screenshots are deleted right after a successful analysis, or after 7 days at the latest if the analysis fails
Product analytics events (PostHog, EU region)	Up to 1 year
Session replay recordings (PostHog)	30 days from recording
Account and workspace data	Life of the account, plus a reasonable period after closure to complete deletion, resolve disputes and meet legal obligations
Generated reports and portfolio data	Life of the account or workspace, or until the item is deleted, whichever comes first; deleted on account closure, subject to any legal hold
Billing, invoicing and accounting records	The period required by tax and accounting law (in Poland, typically 5 years from the end of the tax year)
Security, audit and anti-abuse logs	Only as long as needed to investigate incidents and abuse and for related legal purposes

Other categories are kept only for as long as reasonably necessary for the purposes above. Where this table and the published Privacy Policy differ, the Privacy Policy prevails and this document must be corrected.

4.3 Deletion requests

1. A deletion request must come from the user, through the account settings or by email to support@taufolio.com.

2. The Data Protection contact must verify the requester's identity and assess the request. A user who has closed their account or ended their subscription and asks for deletion is normally entitled to it. A request from a user with an active subscription may be fulfilled by closing the account, which ends the service, and the user must be told so before deletion proceeds.
3. Deletion may be withheld, in whole or in part, for data Taufolio must keep by law (for example invoices) or needs to establish, exercise or defend legal claims. The user must be told what is kept, why and for how long.
4. The request and its outcome must be recorded in the Taufolio issue tracker, and the user informed within the period required by law.

4.4 Account deletion

When a user deletes their Taufolio account:

- encrypted brokerage credentials are hard-deleted immediately, and the user is deleted at the connection provider (SnapTrade);
- profile data, workspace data, portfolios and generated content are deleted or irreversibly anonymized, except for records that must be retained under section 4.2;
- uploaded files and import files stored in private storage are deleted with the workspace;
- subprocessors that hold the user's data (authentication, analytics, email) must be instructed to delete it where they do not do so automatically.

Account deletion is covered by automated tests. Disconnecting a single broker deletes that connection's credentials in the same way, immediately. Data already imported from the broker stays in the user's portfolio until the user deletes it.

4.5 Backups

Backups are created automatically by the database provider. Deleted data may persist in backups until they expire under the provider's schedule. Backups must not be restored into production without re-applying deletions made since the backup was taken. Because customer credentials are encrypted at the application layer with a key held outside the database, a backup does not expose them.

4.6 Policy and document retention

Company policy documentation and its earlier versions must be kept for at least six years.

5. Document security classification

Public. This document is published in the Taufolio Trust Center. See the Data Classification Policy for the classification levels.

6. Non-compliance

Compliance with this policy is verified through code review, automated tests, provider audit logs, periodic internal reviews and feedback to the policy owner. Any staff member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or of their contractual agreement. The action depends on the extent, intent and consequences of the violation.

7. Responsibilities

The Information Security Officer is responsible for approving and reviewing this policy and the related procedures, and for ensuring that automated retention jobs run. Staff members are responsible for applying the relevant sections of this policy in their own work.

8. Schedule

This document is reviewed at least annually and whenever a significant change occurs in Taufolio's systems, processing or organization.

End of Data Retention and Deletion Policy. For the version history, see the next page.

9. Version history

Version	Change	Approved by	Date
2 (current)	Taufolio policy issued for the Taufolio service and published in the Taufolio Trust Center	Jacek Janczura, owner	21 October 2026