



POLICY · DATA PROTECTION AND PRIVACY

Data Protection Policy

Version 1 · Approved by Jacek Janczura · 18 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. Principles for processing personal data

5. Brokerage-connection data and credentials

6. Data subject rights

7. Staff training

8. Data Protection contact

9. Document security classification

10. Non-compliance

11. Responsibilities

12. Schedule

13. Version history

1. Objective

Taufolio is committed to protecting the privacy of personal information and to complying with data protection law, in particular the General Data Protection Regulation (GDPR). This policy ensures that every staff member understands their responsibilities toward the personal and sensitive information Taufolio collects and processes in the course of its operations.

2. Scope

This policy applies to all processes and operations of Taufolio within the scope of its information security management, to all staff members (employees and contractors), and to all personal data Taufolio processes, whether collected directly from users or indirectly through the providers that help deliver the service. It covers the Taufolio website and application, reports, the portfolio tracker, brokerage connections, billing and support channels.

3. Policy statement

"Personal data" means any information that relates to an identified or identifiable person. In practice it includes everything that can be assigned to an individual in any way, for example a name, email address, account identifier, IP address, portfolio holdings linked to an account, or a customer number. This policy lays down the rules for processing personal data that Taufolio collects, directly or indirectly, from the users of its service. Taufolio is the controller of this data. The categories of data, purposes, legal bases and recipients are described in the published Privacy Policy, which prevails for users.

4. Principles for processing personal data

Taufolio applies the GDPR principles to every way it collects and stores personal data. Personal data must be:

- processed lawfully, fairly and in a transparent manner;
- collected for specific, explicit and legitimate purposes, and not used in ways incompatible with them;
- adequate, relevant and limited to what is necessary (data minimization);
- accurate and, where necessary, kept up to date;
- kept in an identifiable form for no longer than necessary, as set out in the Data Retention and Deletion Policy;
- processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

4.1 Lawful bases

Every processing activity must rest on a documented lawful basis under GDPR Article 6. Taufolio relies on performance of a contract (providing the service, accounts, reports, portfolio features, subscriptions), compliance with legal obligations (tax and accounting records), legitimate interests (securing the service, preventing abuse, error monitoring), and consent where the law requires it (product analytics and session replay, which operate only after the user consents in the cookie banner). Consent must be as easy to withdraw as to give. Taufolio does not use personal data for automated decision-making or profiling that produces legal or similarly significant effects.

4.2 Processors and transfers

Personal data may be shared with a processor only under a data processing agreement and a confidentiality obligation, and only after the Information Security Officer has assessed the provider. Transfers outside the European Economic Area must rely on an adequacy decision, standard contractual clauses or an equivalent safeguard. Data sent to AI model providers must be treated as leaving the EEA, and only the data that each feature genuinely needs may be sent. Credentials, passwords, payment-card data and investor journal notes must never be sent to an AI model provider.

5. Brokerage-connection data and credentials

Users may import portfolios and connect brokerage accounts on a strictly read-only basis, through SnapTrade and through the direct tastytrade and Interactive Brokers connectors. This data receives the strictest handling Taufolio applies.

- **Data minimization at the broker.** Taufolio requests read-only scopes only: accounts, positions, balances and transactions. It must never request trading, order-placement, withdrawal or transfer permissions, and it places no orders.
- **Credentials.** OAuth client identifiers and secrets, access and refresh tokens, API keys and any provider-issued user secret are classified as Restricted. They are encrypted by the application with AES-256-GCM before they reach the database, using per-record keys derived from a master key that is held only in the hosting provider's encrypted secret store and never in the database. They live only in a dedicated, server-only table with Row Level Security enabled and forced and all public privileges revoked. See the Encryption Policy.
- **No passwords.** Taufolio never receives or stores the password or login credentials of a user's brokerage account; with SnapTrade the user signs in on the provider's portal.
- **Never logged, never shown.** Credentials must never be written to logs, error reports, analytics or AI prompts, and are never returned to the browser after they are saved. Staff members cannot view them in the admin panel.
- **Portfolio data.** Holdings, balances, transactions and dividends imported from a broker are classified as Confidential personal data. They must not be sent to error monitoring, and in session replay amounts and portfolio lists are masked.

- **Revocation and deletion.** Disconnecting a broker, or deleting the Taufolio account, hard-deletes the encrypted credentials immediately. For SnapTrade, the user is also deleted at the provider. Account deletion is covered by automated tests.

5.1 Technical and organizational measures

Taufolio applies measures appropriate to the risk of the personal data it processes, as described in the Information Security Policy and the policies it references. They include encryption at rest and in transit, role-based access with MFA for staff administrator accounts, Row Level Security on every table in the public database schema, server-only database access, and masking of sensitive values in analytics. Where the risk justifies it, additional controls such as data masking and data leakage prevention tooling must be considered.

6. Data subject rights

Taufolio honors the rights of data subjects under the GDPR:

- **Right to be informed:** clear and transparent information on how personal data is used, provided in the Privacy Policy.
- **Right of access (Article 15):** confirmation of processing and a copy of the data.
- **Right to rectification (Article 16):** correction of inaccurate or incomplete data.
- **Right to erasure (Article 17):** deletion of personal data where the GDPR provides for it.
- **Right to restriction of processing (Article 18).**
- **Right to data portability (Article 20):** data provided by the user in a structured, commonly used, machine-readable format.
- **Right to object (Article 21):** including to processing based on legitimate interests.
- **Right to withdraw consent (Article 7(3)):** at any time, without affecting earlier processing.
- **Rights related to automated decision-making and profiling (Article 22).**
- **Right to lodge a complaint** with a supervisory authority; in Poland, the President of the Personal Data Protection Office (UODO).
- **Non-discrimination:** no user may be treated unfavorably for exercising these rights.

6.1 Handling requests

Requests are received at support@taufolio.com. The Data Protection contact must:

1. log the request in the Taufolio issue tracker on the day it arrives;
2. verify the requester's identity before acting, without collecting more data than needed for verification;
3. carry out or decline the request, giving reasons for any refusal, and respond within the period required by law (one month, extendable under the GDPR in complex cases);
4. record the outcome and, where data was corrected or erased, inform the processors that hold it.

Erasure requests are carried out under the Data Retention and Deletion Policy. Exports of personal data must be stored only in encrypted storage and deleted once delivered.

7. Staff training

Staff members with regular access to personal data, who are involved in its collection or who develop tools that process it, must receive data protection training covering the content and handling of this policy before they receive such access. All staff members must acknowledge annually that they have completed the training and understand this policy.

8. Data Protection contact

The Data Protection contact leads data protection efforts at Taufolio, handles data subject requests, advises on privacy questions and is the point of contact for supervisory authorities. This role is held by the Information Security Officer. Whether a separate Data Protection Officer must be appointed under GDPR Article 37 must be assessed whenever the nature or scale of processing changes. Personal data breaches are handled under the Data Breach Notification Policy.

9. Document security classification

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

10. 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.

11. Responsibilities

The Information Security Officer is responsible for approving and reviewing this policy and the related procedures. Staff members are responsible for applying the relevant sections of this policy in their own work.

12. Schedule

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

End of Data Protection Policy. For the version history, see the next page.

13. Version history

Version	Change	Approved by	Date
1 (current)	Taufolio policy issued for the Taufolio service and published in the Taufolio Trust Center	Jacek Janczura, owner	18 October 2026