



POLICY · DATA PROTECTION AND PRIVACY

Privacy by Design 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

5. Procedures

6. Training and accountability

7. Document security classification

8. Non-compliance

9. Responsibilities

10. Schedule

11. Version history

1. Objective

This policy sets out the principles and practices for protecting the privacy of personal information in the design, development and delivery of Taufolio's products and services. Privacy by Design means protecting individuals proactively: collecting as little personal data as possible, using it only for the intended purpose, and applying strong security to prevent unauthorized access or disclosure. It implements GDPR Article 25 (data protection by design and by default).

2. Scope

This policy applies to all staff members (employees and contractors) and third-party service providers who handle personal information in the course of work for Taufolio. It applies to every new feature, integration, data flow and subprocessor, and to material changes to existing ones, including the portfolio tracker, brokerage connections, AI-assisted features, analytics and support tooling.

3. Policy statement

Taufolio is committed to safeguarding the privacy and security of personal information. Privacy considerations must be built into products, services and business processes from the earliest stage of development, not added afterwards.

4. Principles

Taufolio follows these principles.

- **Proactive, not reactive.** Privacy is considered from the initial design phase through to end of life. Risks are identified before a feature ships.
- **Privacy as the default setting.** Products are configured to collect and use the least personal data. Optional processing, such as product analytics and session replay, stays off until the user consents.
- **Privacy embedded into design.** Privacy is part of the architecture. Examples: the database is reached only by server-side code and never directly from a browser; Row Level Security is enabled on every table in the public schema; sensitive values are masked before they reach analytics; request bodies and portfolio contents are not sent to error monitoring.
- **End-to-end security.** Personal information is protected from collection through storage, use and disposal. Customer brokerage credentials are encrypted by the application before storage, are never logged or shown, and are hard-deleted when no longer needed.
- **Transparency and user control.** Taufolio explains in the Privacy Policy what it collects, why, with whom it shares it and where it is processed. Users can withdraw analytics consent at any time, disconnect a brokerage account, switch off optional emails and delete their account.

- **Respect for user privacy.** Personal information is not used for any purpose other than the one it was collected for, is not sold, and is not used to send users' account data to AI model providers beyond what a feature needs. Brokerage access is read-only and limited to the scopes required.

5. Procedures

To apply these principles, Taufolio must:

1. **Assess privacy impact.** Before building or materially changing a feature that processes personal data, document what data is used, why, where it goes and which risks arise. A formal data protection impact assessment (GDPR Article 35) must be completed where processing is likely to result in a high risk. Adding a subprocessor, an AI model provider or a brokerage connector always requires this review.
2. **Minimize data.** Collect, use and retain only what is needed for the intended feature, consistently with the Data Protection Policy and the Data Retention and Deletion Policy. Where data is only needed in aggregate or in part, only that part may be sent on, for example percentage figures instead of amounts when asking an AI model to explain a portfolio move.
3. **Keep notices accurate.** The Privacy Policy must be updated, and users informed, before a change in processing takes effect.
4. **Obtain consent where required.** Where the law requires consent, it must be obtained before the data is collected or the tracking technology runs, and withdrawal must be possible at any time.
5. **Apply technical and organizational measures.** Classify data under the Data Classification Policy, encrypt it under the Encryption Policy, restrict access to the least privilege needed, and keep credentials and personal data out of logs, error reports and prompts.
6. **Check in development.** Code review must consider privacy impact for any change that touches personal data, and changes to data handling should be covered by automated tests (for example account deletion and the absence of credentials in responses).
7. **Review and improve.** Review this policy and related procedures regularly, and after any incident or finding that shows a gap, to ensure ongoing compliance with applicable law.

6. Training and accountability

Taufolio must give staff members and service providers the training and resources they need to understand their roles under this policy. Individuals are accountable for complying with this policy and its procedures, and appropriate disciplinary action will be taken for non-compliance.

7. Document security classification

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

8. 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.

9. Responsibilities

The Information Security Officer, who also holds the Data Protection contact role, 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.

10. Schedule

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

End of Privacy by Design Policy. For the version history, see the next page.

11. 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