



POLICY · RESILIENCE AND INCIDENT RESPONSE

Data Breach Notification 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. Reporting of a suspected breach

5. Investigation of a suspected breach

6. Breach notification

7. Document security classification

8. Non-compliance

9. Responsibilities

10. Schedule

11. Version history

1. Objective

The objective of this policy is to set out the rules for notifying individuals, regulatory authorities and other relevant parties in the event of a data breach. It ensures that prompt and appropriate action is taken to mitigate the impact of a breach, to uphold the privacy and security of individuals' data, and to comply with applicable law, in particular the General Data Protection Regulation (GDPR).

2. Scope

This policy applies to all staff members (employees and contractors) and to third-party service providers who handle personal data in the course of their work for Taufolio.

3. Policy statement

Taufolio is committed to safeguarding the data it collects to deliver its services. If personal data, or other sensitive data such as brokerage credentials, is acquired, accessed, used or disclosed in a manner not permitted by law or in a manner that compromises its security or privacy, the event may be a breach.

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Breach notification procedures must be maintained to define the steps and responsibilities that ensure a quick, effective, consistent and orderly response to information security incidents that lead to a data breach. The Personal Data Breach Notification Procedure sets out those steps.

4. Reporting of a suspected breach

Any staff member who discovers a potential breach of personal or sensitive data must report it to the Information Security Officer immediately, without waiting to confirm it. Users and partners can report a suspected breach through the in-app "Report a problem" form or by email to support@taufolio.com.

5. Investigation of a suspected breach

The Information Security Officer must review the circumstances of every suspected breach to determine whether the incident was intentional or unintentional. Certain unintentional events do not constitute a reportable breach:

1. Personal data was acquired, accessed or used by a staff member in good faith and within the scope of that person's permitted activities, and there is no further unpermitted use or disclosure.
2. Personal data was inadvertently disclosed by one staff member to another staff member who is authorized to see it, and there is no further unpermitted use or disclosure.

For every other event, the Information Security Officer must assess whether the incident is likely to result in a risk, or a high risk, to the rights and freedoms of individuals, including the risk of financial, reputational or other harm. The risk assessment must be documented, together with the reasons for the conclusion. Where Taufolio concludes that no notification is required, the reasons must be recorded as well.

6. Breach notification

6.1 Supervisory authority

Taufolio's competent supervisory authority is the President of the Personal Data Protection Office (UODO) in Poland. Where a personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the Information Security Officer must notify the UODO without undue delay and, where feasible, no later than 72 hours after becoming aware of it. A notification that is not made within 72 hours must be accompanied by the reasons for the delay. Where a breach is unlikely to result in a risk to individuals, no notification to the authority is required, but the breach and the reasoning must still be documented.

6.2 Affected individuals

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, Taufolio must communicate the breach to the affected data subjects without undue delay, in clear and plain language.

6.3 Partners and customers

Where the breach affects data that Taufolio processes in connection with a partner, for example a brokerage provider such as SnapTrade, tastytrade or Interactive Brokers, Taufolio must notify that partner according to the notification duties in its contract with the partner. Where Taufolio acts as a processor for another controller, it must notify that controller without undue delay.

6.4 Documentation

Every personal data breach, whether or not it is notified, must be recorded with its facts, its effects and the remedial action taken, so that the supervisory authority can verify compliance.

6.5 Mitigation

Taufolio must mitigate, to the extent practicable, any harmful effect of a use or disclosure of data in violation of this policy or of its contractual obligations, and must act to prevent a recurrence.

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 periodic internal reviews, provider audit logs 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 is also Taufolio's data protection contact, is responsible for approving and reviewing this policy and the related procedures, and for deciding on and making breach notifications. Staff members are responsible for reporting suspected breaches immediately and for applying the relevant sections of this policy in their work.

10. Schedule

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

End of Data Breach Notification 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