



PROCEDURE · RESILIENCE AND INCIDENT RESPONSE

Personal Data Breach Notification Procedure

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. Personal data breach notification procedure

4. Document security classification

5. Non-compliance

6. Responsibilities

7. Schedule

8. Version history

1. Objective

This procedure sets out the steps to follow in the event of a personal data breach, as required by the General Data Protection Regulation (GDPR). It ensures prompt and appropriate notification of the supervisory authority and of affected individuals, so that the impact of the breach is mitigated and the rights and freedoms of individuals are upheld.

2. Scope

This procedure applies to all staff members (employees and contractors) and to data processors of Taufolio who handle or have access to personal data. It covers all breaches involving the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

3. Personal data breach notification procedure

3.1 Definitions

- **Personal data.** Any information relating to an identified or identifiable natural person, for example names, identification numbers, email addresses, account and portfolio data, and online identifiers.
- **Personal data breach.** A breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- **Supervisory authority.** The President of the Personal Data Protection Office (UODO), Poland.

3.2 Reporting a personal data breach

- Any staff member or data processor who becomes aware of a personal data breach must report it immediately to the Information Security Officer, who is also Taufolio's data protection contact, by email or directly.
- Users and partners can report a suspected breach through the in-app "Report a problem" form or by email to support@taufolio.com.
- The report should include the date and time, a description of the breach, the type of personal data involved, and any known or suspected cause.
- The moment the Information Security Officer has a reasonable degree of certainty that a breach has occurred is the moment Taufolio is considered "aware" and the 72-hour period begins. The Information Security Officer must record that time.

3.3 Assessment and investigation

1. The Information Security Officer starts the assessment immediately after receiving a report and opens an entry in the incident register, following the Incident Management Procedure.

2. The investigation must establish the nature and scope of the breach, the categories and approximate number of affected individuals and records, the potential risks to individuals' rights and freedoms, and the cause and source of the breach.
3. The risk must be rated as no risk, risk, or high risk, and the reasoning documented.
4. Provider audit logs (Vercel, Supabase, Clerk, GitHub) and monitoring data must be used as evidence, and must be preserved.

3.4 Breach notification

3.4.1 Notification to the supervisory authority

- If the breach is likely to result in a risk to the rights and freedoms of individuals, the Information Security Officer must notify the UODO within 72 hours of becoming aware of it. If the notification is made later, it must state the reasons for the delay.
- If the breach is unlikely to result in a risk, no notification is required, and the decision and its reasons must be documented.
- The notification must describe the nature of the breach, including where possible the categories and approximate number of individuals and records concerned, give the contact details of the data protection contact, describe the likely consequences, and describe the measures taken or proposed to address the breach and mitigate its effects.
- Where not all information is available within 72 hours, it may be provided in phases without further undue delay.

3.4.2 Notification to affected individuals

- If the breach is likely to result in a high risk to the rights and freedoms of individuals, Taufolio must notify the affected individuals without undue delay.
- The notification must be written in clear and plain language and must include a description of the breach, the type of personal data involved, the likely consequences, the recommended actions individuals can take to protect themselves (for example reviewing their brokerage accounts or changing passwords), and the contact details for further questions (support@taufolio.com).
- Notification may be made by email or by an in-app message, whichever reaches the users most reliably.

3.4.3 Notification to partners and processors

- Where the breach affects data shared with, or received from, a partner such as a brokerage provider, Taufolio must notify the partner as its contract requires.
- Where a subprocessor reports a breach to Taufolio, Taufolio must assess it under this procedure without waiting for further confirmation.

3.5 Mitigation and remediation

Taufolio must take immediate and appropriate action to mitigate the impact of the breach and to prevent further unauthorized access or harm. This may include:

- implementing additional security measures, such as revoking and rotating credentials and tightening access;
- recovering or restoring the personal data, as described in the Business Continuity Plan;
- coordinating with the relevant authorities, partners and subprocessors;
- offering support to affected individuals where necessary.

3.6 Record keeping and review

Every personal data breach must be documented in the incident register with its facts, effects, the remedial action and the notification decisions, whether or not a notification was made. After closure, the Information Security Officer must review the lessons learned and update controls and procedures accordingly.

4. Document security classification

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

5. Non-compliance

Compliance with this procedure is verified through periodic internal reviews, provider audit logs and feedback to the policy owner. Any staff member found to have violated this procedure 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.

6. Responsibilities

The Information Security Officer is responsible for approving and reviewing this procedure and the related policies, 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 procedure in their work.

7. Schedule

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

End of Personal Data Breach Notification Procedure. For the version history, see the next page.

8. Version history

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