Personal Data Breach Notification Procedure

Version 1 - Approved by Rishabh

Contents

1. Objective

This Personal Data Breach Notification Procedure outlines the steps to be followed in the event of a personal data breach as required by the General Data Protection Regulation (GDPR). The procedure aims to ensure prompt and appropriate notification to affected individuals and relevant authorities to mitigate the impact of the breach and uphold the rights and freedoms of individuals.

2. Scope

This procedure applies to all employees, contractors, and data processors of Superhawk AI who handle or have access to personal data. It covers all breaches involving accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data.

3. Personal Data Breach Notification Procedure

3.1 Definitions

- Personal Data: Personal data refers to any information relating to an identified or identifiable natural person, such as names, identification numbers, contact details, financial information, health data, etc.
- Personal Data Breach: A personal data breach refers to a breach of security that leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data transmitted, stored, or otherwise processed.

3.2 Reporting a Personal Data Breach

- Any employee, contractor, or data processor who becomes aware of a personal data breach must immediately report it to the designated Data Protection Officer (DPO) or the Privacy Officer.
- The report should include details such as the date, time, and description of the breach, the type of personal data involved, and any known or suspected causes.
- Reports should be submitted via email to the Privacy Officer and logged in the incident tracking system (GitHub Issues or designated internal tracker) within one hour of discovery. For urgent incidents outside business hours, reporters must also notify the on-call engineer via the internal on-call rota.

3.3 Assessment and Investigation

- The Privacy Officer will promptly initiate an assessment and investigation upon receiving a personal data breach report.
- The investigation will determine the nature and scope of the breach, assess potential risks and impacts on individuals' rights and freedoms, identify affected individuals, and establish the cause and source of the breach.
- The investigation team will include the Privacy Officer, a representative from Engineering, and a representative from IT/Security. Engineering will review relevant GitHub logs and cloud

(AWS/GCP) access logs; IT/Security will review Google Workspace access and employee device status. Findings and evidence will be recorded in the incident tracking system.

3.4 Breach Notification

3.4.1 Notification to Supervisory Authority:

- In the event of a personal data breach, where it is likely to result in a risk to the rights and freedoms of individuals, Superhawk AI will notify the relevant Supervisory Authority within 72 hours of becoming aware of the breach unless the breach is unlikely to result in a risk to individuals' rights and freedoms.
- The notification will include details of the breach, the approximate number of affected individuals, the likely consequences, and any measures taken or proposed to address the breach.
- Notifications to the Supervisory Authority will be prepared by the Privacy Officer with input from Engineering and Legal (if available) and sent via the supervisory authority's official online portal or email. The Privacy Officer is responsible for documenting the time of discovery and the time of submission to demonstrate compliance with the 72-hour requirement.

3.4.2 Notification to Affected Individuals:

- If the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, Superhawk AI will notify the affected individuals without undue delay.
- The notification will include a description of the breach, the type of personal data involved, potential risks or impacts, recommended actions for individuals to mitigate harm, and contact information for further inquiries.
- Notifications to affected individuals will be sent via Google Workspace email or alternative contact channels on file. Communications will be reviewed by the Privacy Officer and approved by the CEO or delegated executive prior to sending. If appropriate, Superhawk AI may publish a notice on its official website and provide FAQs to assist affected individuals.

3.5 Mitigation and Remediation

Superhawk AI will take immediate and appropriate actions to mitigate the impact of the personal data breach and prevent further unauthorized access or harm.

This may include but is not limited to:

- Implementing additional security measures
- Recovering or restoring the personal data
- Coordinating with relevant authorities and stakeholders
- Offering support services to affected individuals, such as identity theft protection or credit monitoring, where necessary.
- Specific remediation steps may include revoking compromised credentials, rotating keys or tokens in AWS/GCP, restoring data from vendor-managed backups, and issuing security updates. For data stored solely within third-party SaaS platforms, Superhawk AI will

coordinate with the vendor (e.g., Google Workspace, cloud providers) to leverage their incident response and recovery controls.

4. Document Security Classification

Company Internal. Please refer to the Data Classification Policy for more details.

5. Non-Compliance

Compliance with this policy shall be verified through various methods, including, but not limited to, automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, which may include termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

6. Responsibilities

The Privacy Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation. The Privacy Officer is responsible for coordinating breach response, notifying supervisory authorities and affected individuals, and maintaining the incident log. Engineering is responsible for forensic analysis of code repositories (GitHub) and cloud environments (AWS, GCP). IT/Security is responsible for employee device remediation and Google Workspace investigations. The CEO or delegated executive approves external communications. All employees and contractors must report suspected breaches immediately and cooperate with investigations.

7. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization. Reviews will be conducted by the Privacy Officer in coordination with Engineering and IT/Security. Any changes will be versioned and recorded in the Version history section.

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

Version History

	Version	Log	Date
1	Current	Policy version approved by Rishabh	13 Mar, 2026
1		New policy version created	13 Mar, 2026