Data Protection Policy

Version 1 - Approved by Rishabh

Contents

1. Objective
2. Scope
3. Policy Statement
4. Principles for Processing Personal Data
5. Security of Personal Data
6. Data Subject Rights
7. Staff Training
8. Data Protection Officer
9. Document Security Classification
10. Non-Compliance
11. Responsibilities
12. Schedule
13. Version History

1. Objective

Superhawk AI is committed to protecting the privacy of personal information and to compliance with data protection laws. The purpose of this policy is for all Superhawk AI staff members to understand their responsibilities toward protecting the privacy of personal and sensitive information that we collect and process as part of our operations.

2. Scope

This policy applies to all Superhawk AI employees, contractors, and temporary staff who process personal data as part of Superhawk AI's SaaS operations, including data stored or processed within cloud platforms (AWS and GCP) and on employee devices. It covers personal data collected from customers, users, and prospects, including PII, business and operational data, and behavioral data, across systems including GitHub (code-related data), Google Workspace (email and collaboration), and other approved third-party services used by Superhawk AI.

3. Policy Statement

"Personal Data" refers to any data that relates to an identified or identifiable individual or person. In practice, personal data includes all that can be assigned to an individual in any way. For example, personal data includes a telephone number, credit card number or identification number, account data, number plate, appearance, customer number, or address. This policy lays down guidelines to secure the processing of personal data collected by Superhawk AI, directly or indirectly from the customers and users of Superhawk AI's services.

4. Principles for Processing Personal Data

At Superhawk AI, we incorporate the following principles of data protection in the way we collect and store personal data. We ensure that the data we collect is:

- Processed lawfully, fairly, and in a transparent manner.
- Collected for specific, explicit, legitimate, and limited purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and, where necessary, kept up to date.
- Kept in an identifiable form for no longer than is necessary.
- Processed in a manner that ensures appropriate security.

5. Security of Personal Data

- Superhawk AI relies on a combination of vendor-managed and internal technical and organizational measures to protect personal data. Production data and primary storage are hosted in AWS and GCP services; encryption at rest and in transit is provided by the respective cloud provider services and configured per the Information Security Policy. Backups and high-availability are implemented using cloud provider managed services and their SLAs.

- Access to systems storing personal data is controlled via role-based access using identity and access management features in AWS, GCP, and Google Workspace. Source code and configuration are stored in GitHub with branch protection and least-privilege access. Employee devices must follow the device security requirements described in the Endpoint Security procedures (including disk encryption and approved endpoint protection).
- Where required by business commitments or regulations, Superhawk AI may deploy additional controls such as Data Loss Prevention (DLP) configured via Google Workspace and cloud provider services to monitor and restrict data exfiltration, and application-level data masking for sensitive fields within our services. Implementation of these controls follows the risk assessment and change-management processes defined in the ISMS.

6. Data Subject Rights

To adequately protect the personal data collected and processed by Superhawk AI, you must understand the rights to which data subjects are entitled. Listed below are the data subject rights that we adhere to:

- Right to be informed: The right to know how personal data is used in clear and transparent language.
- Right of access: The right to know and have access to the personal data held about an individual.
- Right to data portability: The right to receive and transfer data in a common and machine-readable electronic format.
- Right to be forgotten: The right to have personal data erased.
- Right to rectification: The right to have data corrected where it is inaccurate or incomplete.
- Right to object: The right to complain and to object to processing.
- Right to restriction of processing: The right to limit the extent of the processing of personal data according to an individual's wishes.
- Rights related to automated decision-making and profiling: The right not to be subject to decisions without human involvement.
- Right to non-discrimination: The right to not be discriminated against for an individual exercising their rights.

7. Staff Training

All Superhawk AI employees, contractors, and temporary staff with access to personal data must complete data protection and privacy training on hire and at least annually thereafter. Training covers handling PII, GDPR obligations, incident reporting, use of Google Workspace and cloud services, secure coding practices for those working on the product hosted in AWS/GCP, and acknowledgement of this Data Protection Policy. Completion is tracked centrally, and staff must attest annually to understanding and compliance.

8. Data Protection Officer

Superhawk AI appoints a Data Protection Officer (DPO) or equivalent responsible for overseeing data protection compliance. The DPO maintains the company's data protection program as defined in the Security Roles on the Sprinto platform, coordinates data subject requests, liaises with

supervisory authorities when required, and reviews data processing activities involving AWS, GCP, Google Workspace, and third-party vendors.

9. Document Security Classification

Company Internal (please refer to the Data Classification policy for more details).

10. 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.

11. Responsibilities

The Information Security 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. Responsibilities also include: the DPO for managing data subject requests and regulatory liaison; Engineering for secure handling of personal data in GitHub and cloud environments; IT/Operations for configuring cloud IAM and endpoint security; and HR for ensuring staff and contractor training and acknowledgements.

12. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization, such as onboarding of new cloud providers, major changes to data processing activities, or changes in applicable data protection law or regulatory requirements.

End of Data Protection Policy. 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