Privacy By Design Policy

Version 1 - Approved by Rishabh

Contents

1. Objective

The objective of this policy is to outline the principles and practices for protecting the privacy of personal information in the design, development, and delivery of Superhawk AI products and services. Privacy by Design is to proactively protect the privacy of individuals by minimizing the amount of personal data collected, ensuring that the data collected is used only for the intended purpose, and implementing strong security measures to prevent unauthorized access or disclosure.

2. Scope

This policy applies to all employees, contractors, temporary staff, and third-party service providers who design, develop, operate, or support Superhawk AI's SaaS products and related services that collect or process Personal Identifiable Information (PII), business and operational data, or behavioral data. It covers data processed or stored in cloud platforms (for example AWS and GCP) and on employee devices (laptops/workstations) used to access company systems.

3. Policy Statement

At Superhawk AI, we are committed to safeguarding the privacy and security of personal information. We believe in integrating privacy considerations into our products, services, and business processes from the earliest stages of development. This Privacy by Design policy outlines our commitment to protecting personal information and our approach to embedding privacy protections into our operations.

4. Principles

Our organization is committed to the following Privacy by Design principles:

- Proactive, not Reactive: Privacy considerations are integrated into all aspects of our products and services, from the initial design phase through to end-of-life.
- Privacy as the Default Setting: Our products and services are designed to minimize the collection and use of personal information and to make privacy the default setting.
- Privacy Embedded into Design: Privacy considerations are incorporated into the design and architecture of our products and services, including security measures to protect personal information from unauthorized access, use, and disclosure.
- End-to-End Security: Our products and services are designed to ensure end-to-end security of personal information, from collection to storage, use, and disposal.
- Transparency and User Control: We provide clear and concise information about our privacy practices, including how personal information is collected, used, and disclosed, and give individuals control over their personal information.
- Respect for User Privacy: We respect the privacy of individuals and do not use personal information for any purpose other than the intended purpose.

5. Procedures

To implement these principles, Superhawk AI will: - Conduct privacy impact assessments (PIAs) for new product features, integrations, and significant changes to data processing, documenting risks and mitigation plans. - Apply data minimization by default: limit collection to data strictly necessary for the feature or service, and avoid storing PII beyond its retention purpose. - Maintain and publish concise privacy notices for users and customers that explain collection, use, retention, and sharing practices; ensure notices reflect processing in AWS and GCP environments. - Where required by law or contract, obtain and record user consent; implement mechanisms to record consent decisions and to honor user opt-outs and data subject requests (access, rectification, deletion) in accordance with GDPR. - Rely on vendor-managed security and privacy controls for cloud infrastructure: use AWS and GCP native controls for encryption at rest and in transit, IAM for access control, and provider backups for infrastructure-level backups; validate vendor controls during vendor risk assessments. - Secure developer workflows and code repositories by using GitHub with enforced MFA, least-privilege access, and branch protection. Ensure secrets are not stored in repositories and are managed using approved secret management solutions. - Protect employee devices by requiring disk encryption, OS security updates, and endpoint protection per the Device Management and Acceptable Use policies. - Implement role-based access controls and periodic access reviews for systems processing personal data; logging and monitoring will be enabled to detect and investigate unauthorized access. - Ensure third-party processors (including SaaS providers) are contractually required to provide appropriate technical and organizational measures and to support data subject requests and breach notifications. - Regularly review and update privacy-related procedures following changes in law, product functionality, or vendor services; document reviews and remediation actions.

6. Training and Accountability

Superhawk AI will provide role-specific privacy and data protection training to employees and contractors during onboarding and annually thereafter. Training will cover GDPR obligations, handling of PII, secure use of AWS, GCP, GitHub, and Google Workspace, how to recognize and report incidents, and procedures for responding to data subject requests. Compliance with training requirements will be tracked and reported to the Privacy Officer.

7. Document Security Classification

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

8. 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.

9. 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 Security team is responsible for implementing technical controls in AWS and GCP and for securing GitHub repositories. Engineering managers and product owners are responsible for ensuring PIAs are completed for new features. The IT/Operations function is responsible for device management and Google Workspace configuration. Third-party vendors used to process personal data must designate a contractual point of contact for privacy matters.

10. Schedule

This document shall be reviewed annually, upon major product releases, upon changes to processing in AWS or GCP, when onboarding new third-party processors, and whenever significant changes occur in the organization.

End of Privacy By Design 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