HAWK PRIVACY STATEMENT

Data Classification	**Public**
Author	Ira Goel & External Advisor
Approver	Management
Approved Date	Jan 30, 2025
Effective From	Jan 30, 2025
Current Version	1.0

1.0 Privacy Practices

At Hawk, privacy is at the core of everything we do. As a trusted partner to financial institutions, we process sensitive financial transaction data, we understand the critical importance of maintaining the highest standards of data privacy, security, and compliance. We take data protection very seriously, both as a controller and as a processor of our customers' personal data. Our commitment to privacy by design and default ensures that every product we deliver is secure, privacy-centric, and fully aligned with privacy frameworks, including GDPR, CCPA, and financial industry regulations.

We go beyond compliance – privacy is deeply embedded in our company culture, engineering processes, and security architecture. We understand that customer trust is our lifeblood, and we safeguard it through transparency and responsible data protection practices. We believe that transparency is the foundation of trust. That is why we provide clear, easy-to-understand privacy notices, granular user controls and stringent third-party audits to ensure our customers remain in control of their data. Our commitment to privacy is an ongoing, proactive effort to protect personal information and build lasting relationships based on trust and integrity.

2.0 Data Protection Organization

We have implemented a holistic Data Privacy Management System (DPMS) at Hawk to maintain the highest standards of privacy compliance. As part of the DPMS, we have developed comprehensive privacy policies, tools and guidelines to enable the organization to put privacy into practice. At Hawk, our dedicated Privacy, Security and Compliance teams work together to ensure that privacy is not just a regulatory requirement but is integrated into our daily business as a strategic priority.

For this purpose, we have developed and implemented clear policies and procedures to ensure consistent and accountable privacy practices. A dedicated Data Protection Officer (DPO) oversees compliance and our privacy strategy whereas cross-functional privacy champions ensure best practice across all departments. To identify and mitigate potential risks, we regularly conduct privacy risk assessments and data protection impact assessments (DPIAs) as part of our data protection core process as part of our product development processes. We understand that our team is the reason we win. That is why privacy training is embedded in our culture. Every Hawk employee, regardless of role, receives in-depth privacy training to ensure data is handled with the utmost care and responsibility.

We have further implemented a structured risk management process, regular self-assessments and third-party audits. Our incident response process framework ensures rapid detection, containment and remediation in the event of a data breach. Ongoing regulatory monitoring ensures that all relevant policies, controls and guidelines are continuously adapted to evolving requirements. By continuously improving our DPMS, we ensure that our customers' personal data remains fully compliant with international standards.

3.0 Security of Processing

We are committed to ensuring the highest level of confidentiality, integrity, and availability of personal data. For us, security is not just a feature – it is a fundamental principle integrated into every layer of our operations. Security is embedded into every process through a risk-based approach, incorporating state-of-the-art encryption techniques, strict access controls, and advanced pseudonymization methods to safeguard sensitive information. Learn more about Hawk's Information Security Practices here.

4.0 Engaging Third Parties

Every service provider, sub-processor, and partner undergoes a rigorous due diligence process, ensuring that only vendors who align with our high security and privacy standards are engaged. The suitability assessment is led by experts from our privacy, security, risk and compliance teams who evaluate the specific categories of personal data being processed, the risk levels associated with data transfers and data residency, and the provider's security policies, encryption methods, and internally recognized compliance certifications, such as ISO 27001, SOC 2, and other relevant certifications. This assessment further includes an in-depth review of independent third-party audits and penetration test results to verify adherence to industry best practices. Additionally, the maturity of the provider's privacy program is assessed, ensuring they uphold data subject rights under GDPR and CCPA.

Every service provider is contractually bound to apply stringent privacy safeguards, including contractual data processing limitations, breach notification obligations, and audit rights. Our continuous monitoring program ensures that vendors are regularly reassessed to maintain compliance with our evolving security and privacy policies. We retain only those partners who demonstrate an ongoing commitment to data protection excellence.