Data Privacy Policy

*[Company Name] | Effective date: [YYYY-MM-DD] | Version: 1.0*

# 1. Purpose

This Data Privacy Policy (“Policy”) describes how we collect, use, disclose, store, and protect Personal Information.

It supports compliance with applicable laws, including the Protection of Personal Information Act, 2013 (POPIA), and, where applicable, the EU/UK General Data Protection Regulation (GDPR/UK GDPR).

# 2. Scope

This Policy applies to all employees, contractors, and third parties who process Personal Information on behalf of [Company Name].

It covers all processing activities related to customers, employees, suppliers, partners, and website/app users.

# 3. Key Definitions

"Personal Information" or "Personal Data": information relating to an identifiable natural person.

"Special Personal Information": sensitive categories such as health, biometric, religious or philosophical beliefs, union membership, political persuasion, sex life, or criminal behavior (as defined under POPIA/GDPR).

"Processing": any operation performed on Personal Information (collection, storage, use, disclosure, deletion).

"Responsible Party" / "Controller": the entity that determines the purposes and means of processing.

"Operator" / "Processor": a third party that processes Personal Information on behalf of the Responsible Party/Controller.

# 4. Roles & Responsibilities

Board & Executives: oversee privacy governance and risk.

Data Protection Officer (DPO) / Information Officer (IO): oversee compliance, handle requests and incidents | Contact: [privacy@company.com].

Managers: ensure teams follow this Policy and related procedures.

Employees & Contractors: process Personal Information lawfully and report incidents immediately.

# 5. Lawful Bases for Processing

We process Personal Information only when a lawful basis applies (e.g., consent, contract performance, legal obligation, legitimate interests, vital interests, or public task where applicable).

Where required, we conduct legitimate interests assessments to balance our interests with individual rights.

# 6. Categories of Personal Information

Identifiers (e.g., name, ID/passport number, employee number).

Contact details (e.g., email, phone, address).

Employment and HR data (e.g., job title, payroll details, performance information).

Customer and transaction data (e.g., account details, order history, support records).

Technical data (e.g., IP address, device identifiers, usage logs).

Special Personal Information (processed only with enhanced safeguards and legal bases).

# 7. Collection & Use

We collect Personal Information directly from individuals or from authorized third parties.

We use Personal Information for specified, explicit, and legitimate purposes, and we do not process it in ways that are incompatible with those purposes.

We implement data minimisation: collect only what is necessary for the stated purpose.

# 8. Sharing & Disclosures

We share Personal Information with Operators/Processors and trusted partners only under written agreements requiring confidentiality, security, and lawful processing.

We may disclose information to authorities when legally required or to protect rights, property, or safety.

We prohibit unauthorized onward disclosures.

# 9. Cross-Border Transfers

International transfers occur only where adequate safeguards exist (e.g., adequacy determinations, standard contractual clauses, binding corporate rules, or other lawful mechanisms).

We assess transfer risks and implement supplementary measures when appropriate.

# 10. Data Subject Rights

Subject to applicable law, individuals have rights of access, correction/rectification, deletion/erasure, restriction, objection, and data portability.

Requests can be submitted to [privacy@company.com]. We verify identity and respond within statutory timelines.

We maintain logs of requests and outcomes.

# 11. Security of Personal Information

We maintain appropriate technical and organisational measures, including risk-based access controls, encryption where appropriate, network and endpoint security, secure development practices, vendor security reviews, and regular training.

Employees must follow Information Security and Acceptable Use Policies and report suspected incidents immediately.

# 12. Retention & Disposal

We retain Personal Information only for as long as necessary to fulfil the purposes collected, to meet legal, tax, or regulatory requirements, or to resolve disputes.

We apply retention schedules and securely dispose of data when no longer required (e.g., secure deletion, anonymisation, destruction).

# 13. Children’s Data

We do not knowingly collect Personal Information from children without appropriate consent and safeguards as required by law.

If you believe a child’s data was provided without consent, contact [privacy@company.com].

# 14. Cookies & Tracking Technologies

Our websites and apps may use cookies, SDKs, and similar technologies for functionality, analytics, and advertising where lawful.

We provide notices and, where required, consent mechanisms and controls for cookie preferences. See our Cookie Notice.

# 15. Data Protection Impact Assessments (DPIAs)

We conduct DPIAs for high-risk processing, including large-scale processing of special categories, systematic monitoring, or new technologies with significant privacy impact.

# 16. Data Breach Response

Employees must report suspected or actual Personal Information breaches immediately to the DPO/IO at [privacy@company.com].

We follow an incident response plan: contain, assess, remediate, document, and, when required, notify regulators and affected individuals within statutory timeframes.

# 17. Third-Party Processors & Vendors

We evaluate vendors’ privacy and security controls before engagement and on a periodic basis thereafter.

Processing by vendors must be governed by a written agreement including confidentiality, security, breach notification, sub-processor control, and audit rights.

# 18. Training & Awareness

All personnel with access to Personal Information must complete privacy and security training at onboarding and annually thereafter.

Managers ensure awareness of updates to this Policy and related procedures.

# 19. Accountability & Records

We maintain records of processing activities (ROPAs), decision logs (e.g., for legitimate interests, DPIAs), and evidence of consent where applicable.

We review this Policy and associated controls periodically to ensure ongoing compliance and effectiveness.

# 20. Changes to this Policy

We may update this Policy from time to time. Material changes will be communicated through appropriate channels and the effective date will be updated.

# 21. Contact

Questions or requests regarding this Policy can be directed to the DPO/Information Officer at [privacy@company.com] or by mail: [Company Address].

# 22. Employee Acknowledgment

I acknowledge that I have read and understand this Data Privacy Policy and agree to comply with it.

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_

*This document is uncontrolled if printed. Verify the latest version on the Company policy portal.*