PIPERS ROAD

DOUGLASDALE

2191

KEPAY WEBSITE POPIA DATA PROCESSING DECLARATION

Effective Date: August 2026
Platform Owner: KePAY (Pty) Ltd ("we", "us", "our")
Statutory Compliance: Sections 19, 20, and 21 of the Protection of Personal Information Act (POPIA) No. 4 of 2013

1. OPERATIONAL POSTURING AND ASSIGNMENT OF ROLES
   KePAY (Pty) Ltd operates a proprietary, digital, hybrid zero-knowledge payslip delivery platform. In terms of South African data privacy legislation under POPIA:

- The Corporate Client (The Employer) acts as the Responsible Party, possessing sole ownership and institutional determination over workforce data parameters.
- KePAY acts strictly as an Operator, executing the ingestion, cryptographic processing, and transmission of delivery notifications solely under the explicit written instruction of the Responsible Party.

2. BIFURCATED ENCRYPTION AND PRIVACY Posturing
   To guarantee the highest standard of data privacy compliance and satisfy information security audits, our platform architecture enforces strict data bifurcation:

- Zero-Knowledge Payload Data: Granular salary metrics, income tax parameters, and banking numbers are encrypted client-side using Advanced Encryption Standard (AES-256) at the boundary of ingestion. KePAY holds no master decryption keys and remains completely blind to plaintext financials.

- Encrypted Directory Metadata: Basic routing indicators (employee numbers and cellular delivery endpoints) are stored separately, encrypted at rest, and utilized solely by automated system machine scripts to fire WhatsApp and SMS notification loops.

3. MANDATORY SECURITY AND DATA SOVEREIGNTY SAFEGUARDS
   In strict alignment with Section 19 of POPIA, KePAY maintains rigorous technical and organizational boundaries to secure data repositories against unauthorized access, exposure, or tampering:

- 100% of all primary system databases, repositories, matching tables, and point-in-time recovery archives are hosted within enterprise cloud environments located completely within the geographic borders of the Republic of South Africa.
- The development environment enforces strict Dual-Control code-merge gates, requiring multi-signature validation from the CEO before any architectural modifications push live to production servers.
- Automated retention scripts enforce a strict data-purge run, completely scrubbing or de-identifying temporary directory metadata records within a maximum of 30 to 90 days following the completion of a distribution cycle.

4. ENTERPRISE DATA PROCESSING AGREEMENT (DPA) AVAILABILITY
   We do not utilize generic or implied consent mechanisms to govern corporate data assets. Before the onboarding of any pilot workflow or commercial service line, KePAY mandates the formal execution of our comprehensive, standalone Data Processing Agreement (DPA).

This procurement-ready legal framework defines our mutual operational liabilities, notification protocols for security compromises within 24 hours, and statutory audit paths. Corporate procurement teams, legal counsels, and Chief Information Officers (CIOs) may request or download our standard, unexecuted master DPA framework directly through the KePAY Trust Centre located at www.kepay.co.za/trust-centre.

5. SECURITY INCIDENT DISCLOSURE AND CONTACT DIRECTORY
   KePAY operates a continuous vulnerability and incident monitoring desk. To report system anomalies, request data deletion under statutory rights, or interface with our compliance division, contact our appointed Information Officer directly:

Data Protection & Compliance Desk: privacy@kepay.co.za
Information Security Incident Response Team: security@kepay.co.za