



PIPERS ROAD
DOUGLASDALE
2191

KEPAY WEBSITE PRIVACY POLICY

Effective Date: 28 August 2026

Platform Owner: KePAY (Pty) Ltd ("we", "us", "our")

Compliance Standard: Protection of Personal Information Act
(POPIA) No. 4 of 2013

1. RECOGNITION OF SOVEREIGN PRIVACY

KePAY (Pty) Ltd operates a proprietary, digital, hybrid zero-knowledge payslip ingestion, encryption, and secure delivery platform (the "Platform"). We respect the privacy of every individual and organization that interacts with our digital interfaces.

This Privacy Policy outlines how we collect, store, process, and protect your Personal Information in accordance with South African law.

2. THE "TWO-BASKET" STRUCTURAL DATA BIFURCATION

To satisfy statutory transparency mandates under POPIA, our system architecture splits all personal and organizational records into two separate processing channels:

Basket 1: Zero-Knowledge Payload Data (The Payslip)

- **What it includes:** Net salaries, gross earnings, medical aid deductions, income tax metrics, hourly rates, and banking account numbers.
- **Our Posture:** This information is **100% Zero-Knowledge encrypted** using Advanced Encryption Standard (AES-256) at the point of ingestion. KePAY holds no master decryption keys. No administrator, developer, or subcontractor of KePAY can view, read, or intercept your plaintext financial figures.

Basket 2: Encrypted Directory Metadata (The Route)

- **What it includes:** Personnel numbers, corporate or personal email destinations, and mobile numbers.
- **Our Posture:** This basic matching data is required by our background scripts to route automated delivery alerts (via WhatsApp or SMS). This directory table is heavily encrypted at rest using AES-256 and used strictly to execute delivery loops.

3. LEGAL STATUS: ASSIGNMENT OF ROLES UNDER POPIA

- **The Client as Responsible Party:** For the purposes of processing workforce payroll records, your employer acts as the **Responsible Party** under POPIA. They determine the purpose of and means for processing the information.
- **KePAY as the Operator:** KePAY acts strictly as an **Operator** in terms of Section 20 and 21 of POPIA. We process personal data solely to execute the digital delivery instructions explicitly documented by your employer in a binding Master Service Level Agreement (SLA) and Data Processing Agreement (DPA).

4. PURPOSE SPECIFICATION & DATA MINIMISATION

We collect and process your basic contact details solely to fulfil the purpose of secure platform utility. KePAY covenants that we will **never**:

- Cross-reference, package, lease, sell, or trade your contact variables to external marketing agencies or credit bureaus.
- Use your payroll profiles to map out spending behaviours or generate algorithmic credit scores.
- Push third-party product advertisements or unsolicited promotions to your mobile phone or inbox.

5. LOCALIZED SOVEREIGN DATA STORAGE

Data protection requires geographical residency alignment. KePAY guarantees that 100% of primary active databases, system repositories, matching tables, and system archives are hosted within enterprise data centres located **strictly within the geographic borders of the Republic of South Africa** (AWS Cape Town/Johannesburg regions), completely satisfying local data sovereignty mandates.

6. MANDATORY ANTI-THEFT AND SYSTEM SECURITY SAFEGUARDS

In compliance with **Section 19 of POPIA**, we maintain appropriate, reasonable technical and organizational measures to secure your records against unlawful access, including:

- Strict identity access management (IAM) enforcing mandatory Multi-Factor Authentication (MFA) across all administrative boundaries.
- Multi-signature code deployment gates to prevent unauthorized alterations to the platform's backend encryption rules.
- Tamper-proof, immutable system logs capturing every interaction with our directory environments.

7. YOUR STATUTORY PRIVACY RIGHTS

Under Chapter 3 of POPIA, you possess specific, non-forfeitable rights regarding your data. To exercise these rights, you may approach your employer's designated Information Officer, who will coordinate with us to execute your mandate:

- **Right of Access:** Request confirmation of whether we hold active encrypted directory items linked to your user profile.
- **Right to Correction:** Update or correct outdated or broken notification contact numbers.
- **Right to Erasure:** Request the permanent deletion or complete de-identification of your profile records from our active cloud storage systems within 30 days of a contract expiration.

8. INFORMATION COMPLIANCE DESK

If you have any questions, strategic concerns, or system inquiries regarding KePAY's data handling protocols, please reach out directly to our appointed Information Officer at:

Email Contact: privacy@kepay.co.za

Official Web Desk: www.kepay.co.za/trust-centre