WELLTEC GROUP
POPIA
AND
DATA PRIVACY POLICY

Group-Wide Data Protection Framework

Including all FSPs, Credit Providers (CPs), Shared Services, Debt Restructuring, Debt Counselling & Collections Entities

---

DOCUMENT CONTROL / VERSION SHEET

Item	Detail
Policy Name	POPIA and Data Privacy Policy
Policy Owner	Head of Legal, Risk & Compliance
Approval Body	Welltec Group Board of Directors
Version	4.0
Approval Date	16 April 2026
Review Cycle	Annual
Next Review Date	February 2027
Classification	Confidential – Regulatory Compliance

TABLE OF CONTENTS

1. INTRODUCTION

The protection of personal information is a legal and regulatory requirement under the Protection of Personal Information Act 4 of 2013 (POPIA), supported by related legislation including the Financial Advisory and Intermediary Services Act (FAIS), the National Credit Act (NCA), the Consumer Protection Act (CPA), and governance principles under King IV.

The Welltec Group operates as a diversified financial services group comprising Financial Services Providers (FSPs), Credit Providers (CPs), shared services entities, and debt recovery and restructuring operations.

This policy establishes a unified framework to ensure lawful, responsible, and secure processing of personal information across all Group entities.

The Group recognises that the lawful processing and protection of personal information constitute a fundamental governance, regulatory, and operational obligation.

2. OBJECTIVES

This policy ensures that the Welltec Group:

- Complies with POPIA and all applicable South African legislation
- Protects the rights of data subjects (customers, employees, partners)
- Ensures transparency in data processing activities
- Implements consistent data protection standards across all Group entities
- Mitigates risk of data breaches and regulatory non-compliance

3. SCOPE

This policy applies to all personal information processed by the Group, including:

- Customers and clients
- Employees and contractors
- Credit applicants and debtors
- Service providers and third parties
- Any data processed across FSP, CP, collections, or restructuring operations

It applies to all formats of data:

- Electronic
- Physical
- Audio-visual
- Stored or archived data

4. DEFINITIONS

(Aligned to POPIA – simplified governance version)

- Act – Protection of Personal Information Act 4 of 2013
- Data Subject – Natural or juristic person to whom data relates
- Responsible Party – Welltec Group or any subsidiary determining purpose of processing
- Operator – Third party processing data on behalf of the Group
- Personal Information – Any identifiable personal or financial data

- Processing – Any operation involving personal data (collection, storage, use, transfer)
- Consent – Voluntary, informed permission to process data
- Information Regulator – South African regulator under POPIA

5. ROLES AND RESPONSIBILITIES

5.1 Board & Executive Management

- Ultimate accountability for POPIA compliance across the Group

5.2 Information Officer (Group)

- Head of Legal, Risk & Compliance
- Oversees compliance, reporting, and regulatory engagement
- Manages data subject requests and breach notifications
- Ensures alignment across FSP and CP entities

5.3 IT & Security Function

- Maintains system security, encryption, and infrastructure protection
- Conducts vulnerability testing and monitoring

5.4 Business Units (FSPs / CPs / Collections)

- Ensure operational compliance with POPIA principles
- Implement data minimisation and lawful processing

6. PROTECTION OF PERSONAL INFORMATION PRINCIPLES

The Group ensures compliance with the 8 POPIA principles:

1. Lawful and fair processing
2. Purpose specification
3. Minimal collection
4. Accuracy and integrity
5. Retention limitation
6. Data subject participation
7. Security safeguards
8. Cross-border protection adequacy

7. PERSONAL INFORMATION RISK MANAGEMENT PROCESS

7.1 Risk Identification

- Inherent and residual risk assessments conducted across all entities

7.2 Control Measures

- Role-based access control
- Encryption of sensitive data
- Password protection and authentication controls
- Staff training and awareness

7.3 Data Use Governance

- Personal information shall only be processed for specific, explicitly defined, and lawful business purposesNo informal sharing of personal information.

7.4 Data Accuracy

- Regular verification and updating of records
- Data cleansing processes implemented

8. DATA SUBJECT RIGHTS, COMPLAINTS, GOVERNANCE & REVIEW

Data subjects have the right to:

- Request access to their personal information;
- Request correction, updating, or deletion of personal information where applicable;
- Object to the processing of personal information;
- Withdraw consent where processing is based on consent;
- Lodge complaints relating to the processing or protection of personal information.

Requests and complaints may be submitted through the Group's formal complaints process available on the Group website or directly to:

compliance@welltec.co.za

Complaints may relate to:

- Access to personal information;
- Correction or deletion of information;
- Objections to processing;

- Withdrawal of consent;
- Direct marketing communications;
- Alleged unlawful processing or data privacy concerns;
- Security breaches or unauthorised disclosure of information.

All complaints shall be investigated and addressed within a reasonable timeframe in accordance with POPIA, internal governance procedures, and applicable regulatory requirements.

Where a data subject remains dissatisfied with the outcome of a complaint, the matter may be escalated to the Information Regulator of South Africa.

The Group maintains ongoing governance and monitoring measures to ensure compliance with POPIA and applicable regulatory requirements, including:

- Annual policy reviews;
- Internal audits and compliance monitoring;
- Reporting to executive governance structures;
- Staff awareness and training initiatives;
- Monitoring of operational compliance across FSP, CP, collections, restructuring, and shared services entities;
- Continuous improvement of data protection controls and security safeguards.

The Head of Legal, Risk & Compliance acts as the Group Information Officer and retains oversight responsibility for implementation, monitoring, and enforcement of this policy.

8.1 Data Protection Complaints Procedure

A complaint may be lodged where a data subject believes that:

- Personal information has been unlawfully processed;
- Information has been disclosed without authorisation;
- Security safeguards are inadequate;
- Direct marketing communications Welltec used are unlawful;
- Any right under POPIA has been infringed.

The complaint should include:

- Name and contact details;

- Nature of the complaint;
- Supporting documentation where available;
- Desired resolution.

The Information Officer or authorised delegate shall:

- Investigate the complaint;
- Assess compliance obligations;
- Implement corrective measures where necessary;
- Provide written feedback to the complainant.

Where the complainant remains dissatisfied, the matter may be escalated to the Information Regulator of South Africa.

8.2 Governance, Monitoring & Review

The Group maintains ongoing governance and monitoring measures to ensure compliance with POPIA and applicable regulatory requirements.

This includes:

- Annual policy reviews;
- Internal compliance monitoring and audits;
- Staff awareness and training;
- Reporting to executive governance structures;
- Monitoring of operational compliance across FSP, CP, collections, and restructuring entities;
- Continuous improvement of data protection controls and security measures.

The Head of Legal, Risk & Compliance serves as the Group Information Officer and retains oversight responsibility for implementation and enforcement of this policy.

9. DISCLOSURE OF INFORMATION

Personal information may only be disclosed:

- Where required by law
- To regulators (FSCA, NCR, SAPS, courts)
- To authorised operators under contract

10. DATA ACCURACY & RETENTION

- Data must be accurate, complete, and up to date
- Retention is limited to legal or business necessity
- Data is securely destroyed when no longer required
- Personal information shall only be retained for as long as:
    - Required by applicable legislation;
    - Necessary for lawful business purposes;
    - Required for contractual or regulatory obligations;
    - Required for dispute resolution or litigation purposes.
- Retention periods shall align with applicable legislation including:
    - POPIA;
    - FAIS;
    - FICA;
    - NCA;
    - Labour legislation;
    - Companies Act requirements.
- Secure destruction methods shall be applied to all records no longer required.

11. INCIDENT & BREACH MANAGEMENT

In the event of a breach:

The Group shall:

- Notify the Information Regulator as required by POPIA
- Notify affected data subjects without undue delay
- Investigate root cause and system impact
- Implement corrective and preventative controls
- Record incident in the Group risk register
- Restore system integrity

All breaches are escalated to the Head of Legal, Risk & Compliance.

12. CROSS-BORDER DATA TRANSFERS

Personal information may only be transferred outside South Africa where:

- Adequate protection exists, or
- Consent has been obtained, or
- Transfer is required by law

13. SPECIAL PERSONAL INFORMATION

The Group may process special personal information where permitted by law, including:

- Biometric information;
- Criminal behaviour information;
- Financial and credit information;
- Employment and health-related information where operationally required.

Such processing shall be subject to enhanced security controls and lawful justification under POPIA.

14. OWNERSHIP AND ACCOUNTABILITY

This policy is owned by: Welltec Group

Role: Head of Legal, Risk & Compliance
Email: compliance@welltec.co.za

Top management confirms commitment to full implementation across all regulated entities, including FSPs, CPs, and debt recovery operations.