COMPREHENSIVE PRIVACY NOTICE

For:

Entity	Registration number	Licence / registration	Principal activity
Bengil Konsultante BK	1999/301293/23	FSP 46378	Financial services, credit life and funeral
Thandabantu Finance cc	1999/027881/23	NCRCP 2202	Microloans
Flexifin Loans cc	1999/027903/23	NCRCP 186	Microloans
Thandabantu Finance IIII cc	1999/025435/23	NCRCP 2577	Microloans
Loanwize cc	2004/031522/23	NCRCP 3981	Microloans
Prime Flex Finance (Pty) Ltd	2023/238194/07	NCRCP 19963	Microloans
Cashiflex Loans (Pty) Ltd	2023/238544/07	NCRCP 19999	Microloans
Mobi Cash Loans (Pty) Ltd	2023/238478/07	NCRCP 19987	Microloans

Collectively “The Group”

Microloans | *Credit Life Insurance* | *Funeral Plan Insurance*

Document owner	Information Officer
Version	1.0
Effective date	10 July 2026
Review cycle	At least annually and after any material change
Status	External privacy notice

1. INTRODUCTION AND PURPOSE

This Privacy Notice explains how organisations within the Group collect, use, share, protect, retain and dispose of personal information. It applies to prospective, current and former clients, policyholders, beneficiaries, employees, job applicants, representatives, suppliers, service providers and other persons whose personal information is processed in connection with the Group's activities.

The Group is committed to lawful, reasonable and transparent processing in accordance with the Protection of Personal Information Act 4 of 2013 ("POPIA"), the National Credit Act 34 of 2005 ("NCA"), the Financial Advisory and Intermediary Services Act 37 of 2002 ("FAIS"), the Financial Intelligence Centre Act 38 of 2001 ("FICA"), applicable insurance legislation and other legal or regulatory requirements.

This notice should be read together with the relevant loan agreement, pre-agreement statement and quotation, insurance policy wording, mandate, application form, website terms, complaints procedure and any specific consent or disclosure provided when information is collected.

2. GROUP STRUCTURE AND RESPONSIBLE PARTIES

"The Group" is a trading and operational description used for a group of close corporations and companies under common ownership. Each entity remains a separate legal person and is ordinarily the responsible party for personal information processed for its own business activities.

The entities may use shared staff, premises, systems, service providers, policies and governance arrangements. Personal information may therefore be shared between participating entities where this is necessary for a legitimate and lawful business purpose, subject to confidentiality, access control and POPIA requirements. Common ownership does not, by itself, permit unrestricted sharing.

The entity named in a client's loan agreement, policy document, quotation, receipt or other transaction record is the primary responsible party for that transaction.

3. PERSONAL INFORMATION WE MAY COLLECT

3.1 Loan applicants, borrowers and related persons

- Identification information, including full name, identity or passport number, date of birth, nationality, marital status and copies of identity documents.
- Contact and address information, including residential, postal and email addresses, telephone numbers and proof of residence.
- Employment and income information, including employer details, occupation, period of employment, payslips, bank statements and other evidence of income.

- Financial and affordability information, including income, expenses, dependants, assets, liabilities, existing credit commitments, payment history and bank account details.
- Credit information obtained from registered credit bureaux, including credit scores, payment profiles, enquiries, judgments, adverse information and debt review or administration status where applicable.
- Loan application, quotation, agreement, repayment, settlement, collection, arrears and account administration information.
- DebiCheck mandates, debit-order information, payment instructions and transaction records.
- Information used to prevent fraud, impersonation, identity theft, money laundering, terrorist financing or other unlawful conduct.
- Correspondence, branch visit records, instructions, queries, complaints, disputes and supporting documents.
- Information about representatives, authorised persons, dependants, beneficiaries or other third parties supplied in connection with a product or transaction.

3.2 Insurance clients, policyholders, insured persons and beneficiaries

- Policy application and onboarding information, including details required to arrange, issue, administer or service credit life or funeral plan cover.
- Policy, premium, beneficiary, dependant, claim, cancellation, amendment and pay-out information.
- Health or medical information only where it is lawfully required for underwriting, claims assessment, policy administration or another permitted purpose.
- Death certificates, medical records, relationship evidence and other claim-supporting information where relevant.
- Correspondence and complaints concerning insurance products or services.

3.3 Employees, applicants, contractors and representatives

- Identity, contact, recruitment, qualification, reference and background-screening information.
- Employment, remuneration, payroll, tax, leave, performance, disciplinary, training and competency information.
- Banking information, emergency contacts, statutory records and limited health information where lawfully required.
- System access, security logs, device information and records relating to acceptable use and cybersecurity.

3.4 Suppliers, service providers and business contacts

- Names and contact details of directors, members, employees, representatives and authorised signatories.

- Company registration, ownership, banking, tax, contracting, invoice, due-diligence and regulatory information.
- Performance, access, security, incident, audit and correspondence records.

4. HOW PERSONAL INFORMATION IS COLLECTED

Most microloan applications are initiated and completed with clients who visit a branch. Branch staff collect information directly from the client, inspect or receive supporting documents and capture or upload the information to the Mobiloan loan management system.

- Directly from the data subject in person, by telephone, email, electronic form, website enquiry, written application or correspondence.
- From documents provided during a loan, insurance, claim, complaint, employment or supplier process.
- From registered credit bureaux, banks, payment service providers, employers, fraud-prevention services, public registers, regulators and law-enforcement bodies where lawful.
- From another Group entity where the information is required for a shared or related service and the disclosure is lawful.
- From authorised representatives, family members, beneficiaries, employers or other third parties where the data subject has authorised the disclosure or the law permits it.
- Automatically through business systems, website logs, cookies or similar technologies, where applicable.

Important: Telephone calls made or received through the Group's Mobiloan and Excalibur systems — including calls to clients, client references, employers and other relevant third parties in connection with loan enquiries, applications, verification, account servicing and collections — are recorded and stored as part of those systems' standard functionality. Each call is logged against a specified call purpose for compliance and indexing purposes. Call recordings and call purpose records constitute personal information and are used for purposes that may include verification of employment and references, quality assurance, staff training, evidencing instructions and mandates, dispute resolution, fraud prevention, and compliance with the Group's legal and regulatory obligations. Recordings are retained, secured and disposed of in accordance with this Privacy Notice's security and retention provisions. Where a telephone line or communication channel is used that does not involve routine recording, and recording is later introduced for that channel, a separate notice will be given before recording begins.

5. PURPOSES AND LAWFUL BASES FOR PROCESSING

Personal information is processed only where there is a lawful justification. Depending on the circumstances, processing may be necessary to conclude or perform a contract, comply with a legal obligation, pursue a legitimate interest, protect a lawful interest of the data subject or a third party, or act with consent where consent is required. Consent is not treated as the sole basis where another lawful basis applies.

5.1 Microloan and credit-provider activities

- Receiving and assessing loan applications and verifying identity, employment, income and supporting information.
- Conducting the affordability assessment and credit bureau enquiry required to evaluate creditworthiness and prevent reckless lending.
- Preparing pre-agreement statements, quotations and credit agreements, and explaining applicable terms, costs and repayment obligations.
- Opening, administering and servicing loan accounts; paying loan proceeds; receiving and allocating repayments; issuing statements; and processing settlements or refunds.
- Creating and administering DebiCheck or other lawful payment mandates and reconciling collections.
- Managing arrears, payment arrangements, debt collection, handover, legal recovery and enforcement of contractual rights.
- Preventing and investigating fraud, identity theft, misrepresentation and other unlawful conduct.
- Complying with the NCA, FICA where applicable, consumer-protection requirements, tax laws, court orders, regulator requirements and statutory recordkeeping duties.
- Managing queries, complaints, disputes, ombud or regulator referrals, audits and legal proceedings.
- Producing aggregated management information, risk analysis and operational reporting.

5.2 Insurance and financial-services activities

- Providing information about, arranging and administering applicable credit life and funeral plan insurance products.
- Completing policy applications, issuing or facilitating policy documentation, collecting or allocating premiums and maintaining policy records.
- Processing policy changes, cancellations, claims, beneficiary information, benefits and pay-outs.
- Communicating with insurers, underwriting managers, cell-captive partners, claims administrators and other authorised product or service providers.
- Complying with FAIS, insurance conduct requirements, treating-customers-fairly obligations and applicable regulatory reporting or recordkeeping requirements.
- Managing insurance queries, complaints, claims disputes and regulatory engagements.

5.3 General business purposes

- Operating branches and business systems, managing security and access, maintaining backups and responding to incidents.

- Managing staff, recruitment, payroll, training, performance, discipline and statutory employment obligations.
- Appointing and managing suppliers, professional advisers, outsourced service providers and business partners.
- Protecting the Group's rights, property, systems, staff and clients, and establishing, exercising or defending legal claims.
- Business continuity, disaster recovery, audits, governance, compliance monitoring and risk management.

6. CREDIT ASSESSMENT AND AUTOMATED PROCESSING

Credit applications involve a credit bureau enquiry and affordability assessment. Mobiloan and connected service providers may perform calculations, apply configured rules, produce risk indicators or support the credit decision. Branch staff and authorised decision-makers must use the available information in accordance with the NCA and the Group's lending criteria.

The Group does not intend to make a decision that has a legal or similarly significant effect solely through automated processing without the safeguards required by POPIA. A client may ask for information about the decision process, request that relevant information be corrected and, where applicable, request human reconsideration of a materially adverse decision.

7. SHARING OF PERSONAL INFORMATION

Personal information is not sold as a commodity. It is disclosed only where the disclosure is necessary and lawful, and only to recipients who require it for a defined purpose. Recipients may include:

- Other participating Group entities, where required for shared administration, insurance, finance, risk, compliance, complaints, IT or support functions.
- Mobiloan and other loan-management, hosting, support and technology providers.
- Registered credit bureaux, including the bureau used for application and ongoing credit-related enquiries.
- Banks, payment processors, DebiCheck and collection service providers, including Allps or a replacement provider.
- Debt collectors, attorneys, tracing agents and collections platforms, including Excalibur or a replacement provider, where an account is in arrears or handed over.
- Guardrisk and relevant insurers, underwriting managers, claims administrators, policy systems or complaints platforms in connection with credit life or funeral plan products.
- Auditors, accountants, compliance officers, legal advisers, consultants, insurers and other professional advisers.
- Employers or other information sources where verification is lawful and necessary.

- The National Credit Regulator, Financial Sector Conduct Authority, Information Regulator, Financial Intelligence Centre, South African Revenue Service, courts, ombuds, law-enforcement bodies and other competent authorities.
- Prospective purchasers, funders or transaction advisers in relation to a lawful restructuring or sale, subject to appropriate confidentiality and due-diligence controls.

Operators and outsourced providers that process personal information on behalf of an entity are subject to appropriate contractual, confidentiality and security obligations. Each Group entity remains responsible for selecting suitable providers and exercising proportionate oversight.

8. DIRECT MARKETING AND COMMUNICATIONS

The Group may send service messages required to administer an application, loan, payment, policy, claim, complaint or legal obligation. These operational communications are not direct marketing and may be necessary even where a person has opted out of marketing.

Marketing by email, SMS, telephone or other electronic communication will be conducted only where permitted by POPIA and other applicable law. Where consent is required, it will be obtained before unsolicited electronic direct marketing is sent. Every marketing message will provide a reasonable means to opt out. A person may object to direct marketing at any time without charge.
Personal information will not be provided to an unrelated third party for that party's independent marketing merely because a client applied for or received a loan. A separate lawful basis and, where required, specific consent must exist.

9. WEBSITE, COOKIES AND THIRD-PARTY LINKS

Where a Group website, including the Assist Family Funeral Plan website, collects enquiry, application or complaint information, that information will be used for the purpose stated at collection and for related lawful administration. Website and policy information is available at:
http://assistfamilyfuneralplan.co.za/ (Bengil Konsultante BK)
https://metrofin.co.za/ (Thandabantu Finance cc, Thandabantu Finance IIII cc and Loanwize cc trading as Metrofin)
https://flexifinloans.co.za/
http://loan-wize.co.za/
https://cashiflexloans.co.za/
Prime Flex Finance (Pty)Ltd – website pending
Mobi Cash Loans (Pty)Ltd – website pending

Web servers and service providers may automatically record limited technical information such as IP address, browser type, device type, date and time, referring page, pages visited and security logs. Cookies or similar technologies may be used for essential website operation, security, performance measurement and preference management. Cookie choices may be managed through the browser and any cookie notice presented on the site.

Websites may contain links or embedded content operated by third parties. Those providers process information under their own privacy notices. The Group is not responsible for the privacy practices of an external site merely because a link is provided.

10. CROSS-BORDER PROCESSING

Some cloud, communications, cybersecurity or support providers may store, back up or access information outside South Africa. International processing will be permitted only where the requirements of section 72 of POPIA or another applicable legal mechanism are satisfied, for example where the recipient is subject to adequate legal or contractual protections, the transfer is necessary for a contract, or the data subject has consented where consent is appropriate.

The Group will seek to limit cross-border transfers to what is necessary, apply contractual and security safeguards, and consider the provider’s location, onward transfers, access controls, encryption, incident response and data-return or deletion arrangements.

11. INFORMATION SECURITY

The Group applies reasonable technical and organisational measures appropriate to the nature of the information and the foreseeable risks. Measures may include:

- Role-based access and user-account management, including prompt removal or amendment of access when roles change.
- Passwords, multi-factor authentication where available, endpoint protection, firewalls, secure configuration and software updates.
- Encryption or secure transmission controls where appropriate.
- Backups, recovery arrangements, business-continuity measures and system availability monitoring.
- Logging, audit trails and transaction reconciliation within key systems.
- Physical security at branches and restrictions on access to paper and electronic records.
- Confidentiality undertakings, staff training, acceptable-use rules and disciplinary processes.
- Due diligence, contractual controls and monitoring for operators and technology providers.
- Incident identification, escalation, containment, investigation, remediation and legally required notification.

No system or method of transmission is completely secure. The Group cannot guarantee absolute security but will review and improve safeguards in response to changes in technology, threats, business operations and regulatory expectations.

12. RETENTION AND DESTRUCTION

Personal information is kept only for as long as required for the purpose for which it was collected, to comply with legislation, or for a lawful and reasonable period necessary to address servicing, complaints, disputes, audits, regulatory enquiries or legal claims.

- Credit agreements and prescribed credit-provider records are retained for the periods required by the NCA and its regulations.
- FICA client and transaction records, where applicable, are retained for at least the statutory period measured from termination of the business relationship or conclusion of the transaction.
- FAIS and insurance records are retained for the applicable statutory period, ordinarily at least five years where the legislation requires it.
- Tax, employment, payroll, accounting and company records are retained for their applicable statutory periods.
- Complaint, fraud, dispute and litigation records may be retained longer where reasonably necessary to protect legal rights or meet regulatory expectations.
- System backups may retain information until expiry through the approved backup cycle, unless a legal hold or incident investigation requires preservation.

When retention is no longer justified, information will be securely destroyed, deleted or de-identified in a manner that prevents reconstruction, subject to operational backup cycles and legal-hold requirements.

13. SPECIAL & CHILDREN'S PERSONAL INFORMATION

Microloans are not offered to persons under 18. The Group may nevertheless process information relating to children where they are dependants, insured persons or beneficiaries under an insurance product, or where the information is required for a claim. Such information will be processed only with a competent person's authorisation or another lawful basis permitted by POPIA.

Health, biometric, criminal-behaviour, race or ethnic-origin information and other special personal information will be processed only where permitted by POPIA and only to the extent necessary for a legitimate purpose such as underwriting, claims, employment obligations, fraud prevention, legal proceedings or regulatory compliance.

14. THIRD-PARTY INFORMATION PROVIDED TO US

A person who provides personal information about another individual, such as a beneficiary, dependant, spouse, employer contact, representative or emergency contact, must be authorised to do so and must ensure that the information is accurate and lawfully disclosed. Where reasonably practicable, the person should make this Privacy Notice available to the affected individual.

In addition to information provided about a third party, the Group may collect personal information directly from a client reference, employer or other third party where the Group contacts that person directly — including verification and reference calls made through Mobiloan's voice-calling platform, integrated with Sudonum, which connects the call using the Sudonum number linked to the Group's business account. These calls are recorded and logged against a specified call purpose, as described under "How Personal Information Is Collected" above. Information collected in this way is used only for the purpose of verifying or administering the relevant loan application, account or claim, and is subject to the same security, retention and data subject rights provisions set out elsewhere in this Privacy Notice.

15. DATA SUBJECT RIGHTS

Subject to POPIA and any applicable limitations, a data subject may:

- Ask whether a Group entity holds personal information about them and request access to that information.
- Request correction, completion, updating or deletion of inaccurate, irrelevant, excessive, out-of-date, incomplete, misleading or unlawfully obtained information.
- Object, on reasonable grounds, to processing based on specified lawful grounds and object at any time to direct marketing.
- Withdraw consent where processing depends on consent, without affecting processing already lawfully undertaken.
- Request information about the source of information where it was not collected directly, subject to lawful limitations.
- Challenge a materially significant decision based solely on automated processing where POPIA applies.
- Lodge a complaint with the responsible entity and, if unresolved, with the Information Regulator or another relevant authority.

A request may require proof of identity and sufficient detail to locate the information. Access or deletion may be refused or limited where the law requires retention, protects another person's rights, preserves legal privilege or permits another lawful ground of refusal. We will explain the basis of any refusal where required.

16. COMPLAINTS AND CONTACT DETAILS

16.1 Group privacy and information-officer contact

Questions, objections, correction requests, access requests or complaints should first be directed to the branch or entity with which the data subject dealt, or to the Group Information Officer using the details below:

Entity	Bengil Konsultante BK
Information Officer	Tiaan van Wyk
Email	mta2@metrofin.co.za
Telephone	0120546157
Physical address	Unit 83&84, Block 5, Lombardi Business Park, Shere, Pretoria,0084
Postal address	PO Box 222, Menlyn, 0063

Entity	Thandabantu Finance cc Flexifin Loans cc Thandabantu Finance IIII cc Loanwize cc Prime Flex Finance (Pty) Ltd Cashiflex Loans (Pty) Ltd Mobi Cash Loans (Pty) Ltd
Information Officer	Deon Labuschagne
Email	operations@flexifinloans.com
Telephone	0120546157
Physical address	Unit 83&84, Block 5, Lombardi Business Park, Shere, Pretoria,0084
Postal address	PO Box 222, Menlyn, 0063

The Group will route the request to the correct legal entity where necessary. Providing the entity name, branch, loan or policy number and approximate transaction date will assist with efficient handling.

16.2 Information Regulator

A POPIA complaint may be submitted through the Information Regulator's eServices platform or using the Regulator's published complaint channels:

- Website: https://inforegulator.org.za/complaints/
- Telephone: 010 023 5200
- Toll free: 0800 017 160
- POPIA complaints: POPIAComplaints@inforegulator.org.za

17. CHANGES TO THIS PRIVACY NOTICE

This Privacy Notice may be amended when the Group's operations, systems, products, service providers or legal obligations change. The current version will be made available at branches, on the applicable website or on request. The privacy notice applicable at the time of information processing has relevance.

18. GOVERNING LAW

This Privacy Notice is governed by South African law. It does not create rights beyond those provided by applicable law or alter the terms of a valid loan, policy or other agreement. Where there is an inconsistency, mandatory legal requirements prevail.

END OF PRIVACY NOTICE