Privacy Policy

MINT PLATFORMS (PTY) LTD

INVEST | BORROW | PROTECT

FSP 55118 | NCRCP22892

MONEY IN TRANSIT

MINT PLATFORMS (PTY) LTD

Privacy Policy

Internal / External:	External (Public)
Policy Owner:	Information Officer/Legal, Risk and Compliance
Approved By:	Executive Committee
Version:	2.0
Date of Adoption:	March 2026
Previous Review:	January 2026
Next Review:	No later than March 2027

1. **INTRODUCTION**

1.1. MINT Platforms (Pty) Ltd (Registration Number 2024/644796/07) ("**MINT**", "**we**", "**us**", or "**our**") is a South African fintech company that operates a technology-enabled investment and digital assets platform at www.mymint.co.za. MINT is an authorised Financial Services Provider (FSP Licence Number 55118) registered with the Financial Sector Conduct Authority ("**FSCA**") and a registered accountable institution under the Financial Intelligence Centre Act 38 of 2001 ("**FIC Act**"). MINT is not a bank or deposit-taking institution.

1.2. In the ordinary course of operating the MINT platform and delivering financial and technology services, MINT processes personal information as defined in the Protection of Personal Information Act 4 of 2013 ("**POPIA**"). MINT is committed to processing personal information lawfully, transparently, and securely, in compliance with POPIA and all other applicable data protection legislation.

1.3. This Privacy Policy ("**Policy**") explains how MINT collects, uses, stores, discloses, transfers, and protects personal information in connection with MINT's websites, including www.mymint.co.za, MINT's platform, mobile applications, APIs, portals, and other digital interfaces, and MINT's regulated and non-regulated business operations.

1.4. This Policy applies to all data subjects with whom MINT interacts, including users of the MINT platform, applicants for MINT accounts, representatives of corporate customers, prospective clients, suppliers, partners, service providers, and visitors to MINT's website.

1.5. By engaging with MINT, whether through the website, platform, communications, products, or regulated financial services, you acknowledge and accept the terms of this Policy.

2. **NOTIFICATION IN TERMS OF SECTION 18 OF POPIA**

2.1. In accordance with section 18 of POPIA, MINT provides the following notification when collecting personal information directly from you:

2.1.1. Identity and contact details of the Responsible Party:

MINT Platforms (Pty) Ltd, 3 Gwen Lane, Sandown, Sandton, 2031; Email: compliance@mymint.co.za; Telephone: +27 (10) 276-0531;

2.1.2. Identity and contact details of the Information Officer: Lonwabo Damane, Information Officer, Email: compliance@mymint.co.za;

2.1.3. Purpose for which personal information is being collected: as set out in clause 7 of this Policy;

2.1.4. Whether the provision of personal information is voluntary or mandatory: certain personal information (such as identity verification documents) is mandatory for purposes of regulatory compliance and account creation. Failure to provide mandatory personal information may result in MINT being unable to open or maintain your account. Other personal information is voluntary, as indicated at the point of collection;

2.1.5. Categories of recipients to whom personal information may be disclosed: as set out in clause 9 of this Policy;

2.1.6. Rights as a data subject: as set out in clause 17 of this Policy; and

2.1.7. Where personal information is collected from a source other than you, MINT will take reasonable steps to bring this notification to your attention as soon as reasonably practicable.

3. **INFORMATION OFFICER**

3.1. MINT has appointed the following Information Officer in terms of POPIA:

3.1.1. Information Officer: Lonwabo Damane;

3.1.2. Email: compliance@mymint.co.za;

3.1.3. Telephone: +27 (10) 276-0531; and

3.1.4. Physical Address: 3 Gwen Lane, Sandown, Sandton, 2031.

3.2. MINT has also appointed the following Deputy Information Officer to act in the absence or incapacity of the Information Officer:

3.2.1. Deputy Information Officer: Kevin Pillay;

3.2.2. Email: compliance@mymint.co.za.

3.3. MINT has registered its Information Officer with the Information Regulator in accordance with POPIA. The Information Officer is responsible for MINT's compliance with POPIA, including the processing of requests from data subjects, managing POPIA complaints, and reporting to the Information Regulator.

4. DEFINITIONS

4.1. Terms used in this Policy that are defined in POPIA bear the meanings assigned to them in POPIA. The following additional definitions apply for purposes of this Policy:

4.1.1. "**Cookie**" means a small text file or similar data element placed on a device when visiting or interacting with MINT's website or platform, including analogous technologies such as pixels, tags, tracking tools, SDKs, beacons, telemetry identifiers, or similar tools used to support analytics, functionality, security, diagnostics, or user experience;

4.1.2. "**Data Subject**" means the natural or juristic person to whom personal information relates and whose personal information is processed by MINT;

4.1.3. "**Information Officer**" means the individual appointed by MINT in terms of POPIA and any Deputy Information Officers authorised to perform the duties and responsibilities assigned to an information officer;

4.1.4. "**Operator**" means any third party who processes personal information for MINT in terms of a contract or mandate, without coming under MINT's direct authority;

4.1.5. "**Personal Information**" has the meaning assigned to it in POPIA and includes, without limitation, information relating to an identifiable, living, natural person or an identifiable existing juristic person, including names, contact details, identification numbers, online identifiers, financial information, transaction data, and any other information that identifies or could reasonably be linked to an identifiable data subject;

4.1.6. "**Processing**" means any operation or activity concerning personal information, including collection, receipt, recording, organisation, storage, updating, modification, retrieval, dissemination, transmission, distribution, making available, alignment, merging, adaptation, combination, restriction, encryption, archival, retention, destruction, erasure, or de-identification;

4.1.7. "**Responsible Party**" means the entity that determines the purpose of and means for processing personal information. MINT is the Responsible Party;

4.1.8. "**Special Personal Information**" means personal information as described in sections 26 to 32 of POPIA, including information relating to religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, and criminal behaviour; and

4.1.9. "**Website**" means any website or digital property owned or operated by MINT, including www.mymint.co.za, sub-domains, portals, web applications, integrated workspaces, linked APIs, dashboards, and platform interfaces provided or maintained by MINT.

5. SCOPE OF THIS POLICY

5.1. MINT, in its capacity as Responsible Party, processes personal information in compliance with POPIA and accepted information protection principles. This Policy applies to all personal information collected by MINT in connection with the provision of MINT's platform, investment, and digital asset services; onboarding processes, including those required under the FIC Act and FAIS Act; website and platform interactions; support, sales, and business engagements; contractual relationships; and internal business operations.

5.2. This Policy does not apply to information collected by independent third-party websites, platforms, or applications that are not owned or controlled by MINT.

6. CATEGORIES OF PERSONAL INFORMATION COLLECTED

MINT may collect and process the following categories of personal information:

6.1. Identity and Contact Information

Full legal name, date of birth, identity number or passport number, nationality, and residential address. Email address, postal address, telephone number, and mobile number. Where the customer is a juristic entity: company name, registration number, registered address, nature of business, and the identity of directors, officers, and beneficial owners.

6.2. **Regulatory and Compliance Information**

Information required for KYC and FICA compliance, including identity documentation, proof of address, declarations of source of funds and source of wealth, beneficial ownership information, and suitability and appropriateness information. This information is collected only through secure onboarding workflows and direct regulated engagements, not through the public website.

6.3. **Financial and Transactional Information**

Information relating to your Legal Tender Account and Digital Currency Wallet, including account balances, transaction histories, deposit and withdrawal records, and the details of Transactions entered into through the platform. Bank account details provided for deposit and withdrawal verification purposes. Tax reference numbers and foreign investment allowance declarations.

6.4. **Technical and Usage Data**

IP addresses, device identifiers, browser type, operating system, system logs, and authentication logs. Telemetry, diagnostics, platform usage logs, and session data. Geolocation metadata (where access is enabled on your device). Cookie and analytics data, as further described in clause 15.

6.5. **Business and Correspondence Information**

Emails, correspondence, support tickets, and other communications with MINT. Information relating to complaints submitted in accordance with MINT's Complaints Policy.

6.6. **Voluntary Information**

Information submitted through questionnaires, surveys, feedback forms, or other voluntary mechanisms.

6.7. **Special Personal Information**

MINT does not intentionally collect Special Personal Information except where required for compliance with applicable law (for example, under the FIC Act) and only through secure, non-public channels. MINT does not collect special personal information through its public website.

7. **PURPOSES FOR PROCESSING**

7.1. MINT processes personal information for the following lawful purposes:

7.1.1. Provision of Products and Services: to deliver, maintain, secure, and support MINT's platform, accounts, and investment and digital asset services;

7.1.2. Account and Platform Management: to administer user accounts, Legal Tender Accounts, and Digital Currency Wallets, facilitate access and authentication, maintain platform operability, and enable user functionality;

7.1.3. Regulatory and Legal Compliance: to comply with POPIA, the FIC Act, the FAIS Act, the FSR Act, and other applicable financial services regulations, including AML/CTF/PF obligations, sanctions screening, suitability assessments, and regulatory reporting;

7.1.4. Risk Management and Fraud Prevention: to manage MINT's operational, financial, and regulatory risks, detect and prevent fraud, money laundering, and other financial crime, and maintain the integrity of MINT's platform;

7.1.5. Analytics, Development, and Improvement: to analyse system performance, conduct diagnostics, improve product functionality, and enhance user experience, subject to applicable privacy constraints;

7.1.6. Operations and Governance: for governance, audits, risk management, billing, internal controls, IT administration, quality assurance, and business reporting;

7.1.7. Marketing and Communications: to communicate with clients and prospective customers, where permitted under POPIA, regarding MINT's services, product updates, and relevant events. MINT does not sell, rent, or trade personal information for marketing purposes; and

7.1.8. Automated Decision-Making and Profiling: as further described in clause 16 of this Policy.

8. **LEGAL BASES FOR PROCESSING**

8.1. MINT processes personal information only where legally permissible under POPIA. The applicable legal bases are:

8.1.1. Performance of a contract or taking steps prior to entering into a contract: where processing is necessary to open or manage your MINT account, execute your Transactions, or provide the Services you have requested;

8.1.2. Compliance with legal obligations: where processing is required by POPIA, the FIC Act, the FAIS Act, the FSR Act, or any other applicable law, including obligations relating to AML/CTF/PF compliance, sanctions screening, tax reporting, and record-keeping;

8.1.3. Legitimate interests: where processing is necessary to pursue MINT's legitimate business interests, including enhancing platform security, detecting and preventing fraud, improving MINT's products and services, and operating the business efficiently, provided that such interests are not overridden by your rights and interests;

8.1.4. Consent: where you have provided explicit consent for specific processing activities. You may withdraw consent at any time, without affecting the lawfulness of processing carried out prior to withdrawal; and

8.1.5. Public interest: where processing is required for purposes in the public interest, including the performance of financial sector regulatory functions.

9. **DISCLOSURE OF PERSONAL INFORMATION TO THIRD PARTIES**

9.1. MINT may disclose personal information to the following categories of recipients:

9.1.1. Service Providers and Operators: including cloud hosting vendors, identity verification providers, KYC and FICA service providers, blockchain analytics providers, payment processors, sanctions screening providers, analytics and diagnostics platforms, cybersecurity vendors, and IT support services. Where such parties process personal information on MINT's behalf, they are Operators under POPIA and are required to process personal information only on MINT's documented instructions;

9.1.2. Regulators and Authorities: where required by law, including the Information Regulator, FSCA, FIC, South African Revenue Service ("**SARS**"), South African Reserve Bank ("**SARB**"), or pursuant to a lawful order or directive;

9.1.3. Professional Advisers: including auditors, legal advisers, compliance consultants, and insurers engaged in connection with MINT's business operations;

9.1.4. Corporate Transactions: in the context of mergers, acquisitions, restructuring, or business transfers, subject to appropriate confidentiality obligations and data protection safeguards; and

9.1.5. Counterparties: to the extent necessary to facilitate Transactions entered into through the platform, and subject to applicable data protection safeguards.

9.2. MINT requires all third parties to whom personal information is disclosed to maintain appropriate confidentiality and security safeguards. MINT does not sell, rent, or trade personal information to or with third parties for any commercial purpose.

10. CROSS-BORDER TRANSFER OF PERSONAL INFORMATION

10.1. MINT may transfer personal information to jurisdictions outside South Africa, including in connection with cloud infrastructure services, sanctions screening, identity verification, and analytics. Such transfers will occur only where the receiving jurisdiction provides an adequate level of protection as contemplated by POPIA, or where MINT has implemented appropriate contractual safeguards aligned with POPIA, such as binding operator agreements that impose equivalent data protection obligations on the recipient.

10.2. MINT ensures that Operators processing personal information internationally do so in accordance with binding written agreements that comply with POPIA's requirements for cross-border transfers.

11. DATA SECURITY

11.1. MINT implements appropriate, reasonable technical and organisational measures to safeguard personal information against loss, unauthorised access, destruction, modification, or unlawful processing. These measures include:

11.1.1. encryption of personal information in transit and at rest, where technically feasible;

11.1.2. multi-factor authentication for privileged access to systems containing personal information;

11.1.3. continuous monitoring and logging of access to personal information;

11.1.4. network and infrastructure security controls;

11.1.5. secure software development practices;

11.1.6. regular security testing, vulnerability scanning, and penetration testing;

11.1.7. strict role-based access controls limiting access to personal information to persons who require it for their specific functions; and

11.1.8. ongoing staff training on information security and data protection obligations.

11.2. No information security system is entirely secure. MINT does not guarantee absolute security against all cyber threats. You acknowledge this risk and are responsible for maintaining the security of your own Access Credentials.

11.3. Security Compromise Notification: where MINT reasonably believes that personal information has been accessed or acquired by an unauthorised person (a "**Security Compromise**"), MINT will:

11.3.1. take all reasonable steps to contain the compromise and prevent further unauthorised access;

11.3.2. notify the Information Regulator as soon as reasonably possible after becoming aware of the compromise, using the prescribed notification form;

11.3.3. notify affected data subjects as soon as reasonably possible where the compromise is likely to adversely affect them, unless the Information Regulator directs otherwise; and

11.3.4. document the compromise, the steps taken to contain it, and all notifications made, and review and update MINT's security measures to address the cause.

12. DATA ACCURACY

MINT takes reasonable steps to ensure that personal information collected and processed is complete, accurate, not misleading, and up to date. You are encouraged to notify MINT promptly of any changes to your personal information by updating your account profile or contacting MINT's Information Officer. MINT may periodically request updated information from you to maintain the accuracy of your records.

13. DATA RETENTION

13.1. MINT retains personal information only for as long as is necessary to achieve the purpose for which it was collected, comply with applicable legal and regulatory obligations, fulfil contractual requirements, or protect MINT's legitimate interests. The following minimum retention periods apply:

13.1.1. Customer identity and KYC/FICA documentation: at least five years from the termination of the customer relationship, as required by the FIC Act;

13.1.2. Transaction records: at least five years from the date of the relevant transaction, as required by the FIC Act;

13.1.3. Financial and accounting records: at least five years from the end of the relevant financial year, as required by the Companies Act 71 of 2008 and applicable SARS requirements;

13.1.4. POPIA-related documentation, including the PAIA manual, processing records, and consent records: retained indefinitely or until superseded;

13.1.5. Marketing consent records: for the duration of the consent plus three years;

13.1.6. Complaints records: at least three years from the date of resolution of the complaint, or five years for FAIS Complaints; and

13.1.7. Employee records: at least three years after termination of employment.

13.2. At the end of the applicable retention period, personal information is securely deleted, destroyed, or de-identified. Records may not be retained beyond the applicable period without a documented legal justification approved by the Information Officer.

14. **USE OF THE MINT WEBSITE AND PLATFORMS**

MINT may process technical and aggregated data related to website and platform usage for purposes of analytics, security, and service improvement. MINT's website may contain links to third-party websites or services. MINT is not responsible for the privacy practices of those third parties. You should review the privacy policies of any third-party websites you access through MINT's website.

15. **COOKIES AND SIMILAR TECHNOLOGIES**

15.1. MINT uses Cookies and similar technologies for:

15.1.1. functionality: to enable core platform features and to remember your preferences;

15.1.2. analytics: to understand how users interact with MINT's website and platform, so that MINT can improve its products and services;

15.1.3. security: to detect and prevent fraudulent or unauthorised activity; and

15.1.4. performance monitoring: to diagnose technical issues and optimise platform performance.

15.2. MINT's website will display a Cookie consent notification where required by applicable law. You may manage your Cookie preferences through the Cookie settings interface or through your browser settings. Disabling certain Cookies may affect the functionality of MINT's website or platform.

15.3. MINT does not use Cookies for targeted advertising or for sharing personal information with third-party advertisers without your consent.

16. **AUTOMATED DECISION-MAKING AND PROFILING**

16.1. MINT uses automated processing of personal information, including profiling, in connection with the following activities:

16.1.1. customer risk scoring and AML/CTF/PF risk classification, as required by the FIC Act and MINT's internal compliance programme;

16.1.2. transaction monitoring and suspicious activity detection;

16.1.3. fraud prevention and identity verification; and

16.1.4. personalisation of platform features and communications.

16.2. Where MINT makes decisions that produce legal or similarly significant effects on you through automated processing alone, MINT will implement appropriate safeguards, including:

16.2.1. ensuring that the decision can be reviewed by a suitably qualified human upon your request;

16.2.2. providing you, upon request, with information about the logic involved in the automated processing and the significance of the processing for you; and

16.2.3. allowing you to contest the decision and request human intervention.

16.3. To request information about or a review of an automated decision affecting you, please contact the Information Officer at the contact details set out in clause 3.

17. YOUR RIGHTS AS A DATA SUBJECT

17.1. In terms of POPIA, you have the following rights as a data subject. To exercise any of these rights, please contact MINT's Information Officer at the contact details set out in clause 3.

17.1.1. Right of Access: you have the right to request confirmation of whether MINT holds personal information about you, and to request access to that personal information. Requests for access may be subject to certain fees and grounds for refusal as contemplated by POPIA and the Promotion of Access to Information Act 2 of 2000 ("**PAIA**"). MINT's PAIA Manual sets out the procedure for submitting access requests and is available on request.

17.1.2. Right to Correction or Deletion: you have the right to request that MINT correct personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully, or that MINT delete personal information that MINT is no longer lawfully entitled to retain.

17.1.3. Right to Object: you have the right to object on reasonable grounds to MINT processing your personal information where the processing is not authorised by law or is not necessary for the fulfilment of a contract.

17.1.4. Right to Object to Direct Marketing: you have the right to object at any time, without giving reasons, to the processing of your personal information for purposes of direct marketing. MINT must comply with such an objection at no cost to you and must cease direct marketing communications immediately upon receipt of your objection.

17.1.5. Right to Withdraw Consent: where processing is based solely on your consent, you may withdraw that consent at any time without affecting the lawfulness of processing carried out prior to withdrawal. Withdrawal of consent may affect MINT's ability to provide certain services to you.

17.1.6. Right to Lodge a Complaint: if you believe that MINT has processed your personal information in violation of POPIA, you have the right to lodge a complaint with the Information Regulator.

18. **DIRECT MARKETING**

18.1. MINT may process personal information for direct marketing purposes in accordance with POPIA. MINT will only send marketing communications to you where you have opted in to receive such communications, or where you are an existing client and the communications relate to similar products or services to those already provided to you.

18.2. You may unsubscribe from marketing communications at any time by clicking the unsubscribe link in any marketing email, by updating your communication preferences in your account settings, or by contacting the Information Officer.

18.3. MINT does not share personal information with third parties for their direct marketing purposes without your explicit consent.

19. **INFORMATION REGULATOR**

19.1. The Information Regulator of South Africa is responsible for monitoring and enforcing compliance with POPIA. If you have a complaint about how MINT has processed your personal information and you are not satisfied with MINT's response, you may lodge a complaint with the Information Regulator:

19.1.1. Website: https://inforegulator.org.za;

19.1.2. Email: POPIAComplaints@inforegulator.org.za; and

19.1.3. Telephone: 010 023 5207.

20. **AMENDMENTS TO THIS POLICY**

20.1. MINT may update this Policy from time to time to reflect changes in applicable law, regulatory requirements, MINT's data processing activities, or changes to MINT's products and services.

20.2. Where a material amendment is made to this Policy, MINT will notify you through the platform or by email to your registered email address and will publish the updated Policy on MINT's website. The version with the most recent adoption date published on MINT's website is the current version. Continued use of MINT's services after the effective date of an amendment constitutes acceptance of the updated Policy.

20.3. This Policy must be reviewed by the Information Officer at least annually, and a reviewed and, where necessary, updated version must be presented to the Board for approval not later than twelve months after the date of the most recent Board approval.

[END]