

PRIVACY POLICY

Introduction

This policy, together with our Terms and Conditions, applies to use of:

- The Lora website (Website) once you have accessed it on your device.
- The Lora mobile and web-based applications (Apps) available for download or access on various platforms.
- Any of the services accessible through the Website and Apps ("Services") that are available on our website or other sites of ours ("Services Sites").

Important Information and Who We Are

Sikem Micro Finance Limited, being a company in Zambia with registration number 120220038253 and owner of trademark called "Lora," is the data controller and is responsible for your personal data (collectively referred to as the "Company," "we," "us," or "our" in this policy). If you have any questions about this privacy policy, please contact us using the details set out below.

Contact Details

Our full details are:

- **Full name of legal entity:** Sikem Micro Finance Limited
- **Email address:** sikemicrofinance@gmail.com
- **Address:** Seventh Street, Kabwata, Lusaka.
- **Telephone number:** +260 777 329 198

Changes to the privacy policy and your duty to inform us of changes

We keep our privacy policy under regular review. This version was last updated on 22 August 2025. It may change, and if it does, these changes will be posted on this page and, where appropriate, notified to you by email or when you next visit the Website, log onto one of the Services Sites, or use the Apps. The new policy may be displayed on-screen, and you may be required to read and accept the changes to continue your use of the Website, Services Sites, or Apps. It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during our relationship with you.

The Data We Collect About You

We may collect, use, store, and transfer different kinds of personal data about you as follows:

- Identity Data: first name, last name, maiden name, username or similar identifier, marital status, title, date of birth, gender.
- Contact Data: billing address, delivery address, email address and telephone numbers.
- Financial Data: bank account and/or payment card details.
- Employment Data: place of employer, current pay slip, and supervisor's contact details.
- Transaction Data: includes details about payments to and from you and details of loan transactions.
- Device Data: includes the type of mobile device you use, a unique device identifier (for example, your Device's IMEI number, the MAC address of the Device's wireless network interface, or the mobile phone number used by the Device), mobile network information, your operating system, the type of mobile browser you use, time zone setting.
- Content Data: information stored on your Device, including login information, photos, videos, or other digital content.
- Profile Data: username and password, purchase history, interests, preferences, feedback, and survey responses.
- Usage Data: details of your use of any of our Website, Apps, or your visits to any of Our Sites, including traffic data and other communication data, whether this is required for our own billing purposes or otherwise, and the resources that you access.
- Marketing and Communications Data: your preferences in receiving marketing from the Company and our third parties and your communication preferences.

We also collect, use, and share Aggregated Data such as statistical or demographic data for any purpose. Aggregated Data could be derived from your personal data but is not considered personal data in law as this data will not directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific App feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy policy.

We do not collect any Special Categories of Personal Data about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health, and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

How Is Your Personal Data Collected?

We will collect and process the following data about you:

- Information you give the Company. This is information (including Identity, Contact, Financial, and Marketing and Communications Data) you consent to giving us about you by filling in forms on the Website, Apps, and the Services Sites (together “Our Sites”) or by corresponding with us (for example, by email or chat). It includes information you provide when you register to use the Website, Apps, and the Services Sites (together “Our Sites”) or by corresponding with us (for example, by email or chat). It includes information you provide when you register to use the Website, Apps, subscribe to any of our Services, make a purchase, share data, and when you provide feedback on the Website or Apps. If you contact the Company, we will keep a record of that correspondence.
- Information we collect about you and your device. Each time you visit one of Our Sites, use our Website or Apps, we will automatically collect personal data including Device, Content, and Usage Data. We collect this data using cookies and other similar technologies.

Face Data Collection and Use

The Company respects your privacy and is committed to protecting the personal information we collect. We may collect facial data solely to facilitate identity verification, enhance user security, and improve the user experience on our platform. The facial data may also be obtained from your National Registration Card which we shall require you take pictures of the front and back.

Collection of Face Data

The Company may collect face data through our mobile application. This data is captured during certain in-app activities requiring identity verification, such as account creation, transaction authorization, or to access specific features of the app that need enhanced security. The Company only collects face data with the user's explicit consent, which can be withdrawn at any time.

Use of Face Data

The face data collected will be used exclusively for:

- **Identity Verification:** Ensuring the identity of users to prevent fraud and unauthorized access.
- **Security Enhancements:** Providing additional layers of security, such as facial recognition for app login.
- **Service Improvement:** Using aggregate, anonymized data to enhance the quality and

functionality of our services.

Disclosure and Sharing of Face Data

The Company does not disclose or share face data with any third parties except:

- **Service Providers:** Trusted third-party providers assisting in identity verification and security features, who are bound by confidentiality agreements.
- **Legal Compliance:** If required by law, The Company may disclose face data in response to valid legal processes, such as a court order or a subpoena.

Retention and Deletion of Face Data

Face data is retained only as long as necessary for identity verification purposes and as required by law. Users may request the deletion of their face data, and we will promptly honor such requests, subject to legal and regulatory requirements.

User Control and Data Security

Users have control over their face data within the app settings and can enable or disable facial recognition features. The Company employs stringent security measures to safeguard face data, including encryption and secure storage protocols, to prevent unauthorized access, use, or disclosure.

Cookies

We use cookies and/or other tracking technologies to distinguish you from other users of the Website, Apps, or Services Sites and to remember your preferences. This helps the Company to provide you with a good experience when you use the Website, Apps, or browse any of Our Sites and also allows us to improve the Website, Apps, and Our Sites.

How We Use Your Personal Data

We will only use your personal data when the law allows us to do so. Most commonly, we will use your personal data in the following circumstances:

- Where you have consented before the processing.
- Where we need to perform a contract we are about to enter or have entered with you.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal or regulatory obligation.

We will get your express opt-in consent before we share your personal data with any third party for marketing purposes.

Purposes For Which We Will Use Your Personal Data

Purpose/activity	Type of data	Lawful basis for processing
To register you as a new Website or App user	• Identity • Contract • Financial Device	Your consent
To process transactions and deliver Services including managing payments and collecting money owed to us	• Identity • Contact • Financial • Transaction • Device • Marketing and Communications	• Your consent • Performance of a contract with you • Necessary for our legitimate interests (to recover debts due to us)
Website, Apps or any Services	• Profile • Marketing and Communications	• Necessary for our legitimate interests (to keep records updated and to analyse how customers use our products/ Services) • Necessary to comply with legal obligations (to inform you of any changes to our terms and conditions)
To enable you to participate in a prize draw, competition or complete a survey	• Identity • Contact • Device • Profile • Marketing and Communications	• Your consent • Performance of a contract with you • Necessary for our legitimate interests (to analyse how customers use our products/Services and to develop them and grow our business)
To administer and protect our business and this Website including troubleshooting, data analysis and system testing	• Identity • Contact • Device	• Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security)

International Transfers

Many of our external third parties are based outside Zambia, so their processing of your personal data will involve a transfer of data outside Zambia. Whenever we transfer your personal data out of Zambia, we ensure a similar degree of protection is afforded to it. Please contact the Company if you want further information on the specific mechanism used by the Company when transferring your personal data out of Zambia.

Data Security

All information you provide to us is stored on our secure servers. Any payment transactions carried out by our chosen third-party provider of payment processing services will be encrypted using Secured Sockets Layer technology (SSL). Where we have given you (or where you have chosen) a password that enables you to access certain parts of Our Sites, you are responsible for keeping this password confidential. We ask you not to share a password with anyone.

Once we have received your information, we will use strict procedures and security features to try to prevent your personal data from being accidentally lost, used, or accessed in an unauthorized way. We will collect and store personal data on your Device using application data caches, browser web storage, and other technology. We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator when we are legally required to do so.

Data Retention

By law, we have to keep basic information about our customers (including Contact, Identity, Financial, and Transaction Data) for six years after they cease being customers for tax purposes.

In some circumstances, you can ask us to delete your data: see the "Your Legal Rights" section below for further information. In some circumstances, we will anonymize your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

Your Legal Rights

Under certain circumstances you have the following rights under data protection laws in relation to your personal data:

- Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

- Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to the Company.
- Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully, or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
- Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.
- Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:
 - if you want us to establish the data's accuracy;
 - where our use of the data is unlawful but you do not want us to erase it;
 - where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
 - you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
- Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
- Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

You also have the right to ask us not to continue to process your personal data for marketing purposes.

You can exercise any of these rights at any time by contacting us at sikemicrofinance@gmail.com

Lawful Basis

Consent means processing your personal data where you have signified your agreement by a statement

or clear opt-in to processing for a specific purpose. Consent will only be valid if it is a freely given, specific, informed, and unambiguous indication of what you want. You can withdraw your consent at any time by contacting us.

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

Performance of Contract means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

Comply with a legal obligation means processing your personal data where it is necessary for compliance with a legal obligation that we are subject to.

Third Parties

Consent means processing your personal data where you have signified your agreement by a statement or clear opt-in to processing for a specific purpose. Consent will only be valid if it is a freely given, specific, informed, and unambiguous indication of what you want. You can withdraw your consent at any time by contacting us.

Performance of Contract means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

Comply with a legal obligation means processing your personal data where it is necessary for compliance with a legal obligation that we are subject to.

Applicable Laws

We are bound by the terms of the Data Protection Act 2021, Electronic Communications and Transactions Act 2021, and all laws (present and future) governing and regulating the collection of information of users of information communication technology systems such as that owned and managed by the Company.