Effective Date:

1. INTRODUCTION

1.1 Moneta Limited ("**Moneta**"), an Ethiopian Capital Corporation, is the data controller responsible for processing your data when you access our Services.

1.2 Moneta may also act as a data processor for a data controller with whom you have a contractual relationship. In such instances, Moneta will act in accordance with the instructions given by the data controller.

1.3 The Moneta Group offers digital financial services to help the traditionally underbanked borrow, save and grow their money. Our Services include:

- 1.3.1 Credit and financial services offered through the Moneta App (which is an Android mobile application that can be downloaded from Google Play or other Channels, and for which the applicable Privacy Notice can be accessed here); Moneta Services may be rebranded under the corporation through which Moneta services are offered; in such instance, the Privacy Policies documented here apply

1.4 This Privacy Policy applies to your use of Moneta's Services and explains what personal data we collect, with whom we share it, how we may use your data and how you can prevent us from sharing certain information with certain parties. This Privacy Policy should be read together with the applicable Privacy Notice for the particular Service that you are using as linked above. The relevant Privacy Notice informs you as to how we look after your personal data when you use our Services and tells you about your privacy rights and how you are protected under the Data Protection Act, 2019.

1.5 By accepting the terms of this Privacy Policy and the relevant Privacy Notice, you give your consent to the practices described herein.

1.6 If you have any questions about this Privacy Policy, please contact us via email at (Moneta email)

1.7 Moneta's Services are not intended for children and we do not knowingly process data relating to children.

2. DEFINITIONS

2. 1 “**Channels**” means any system or medium (including the Moneta App, Unstructured Supplementary Service Data (USSD) and web whether internet based, mobile device based or not), which may be established by Moneta from time to time to enable you to access and utilize one or more of the Services.

2.2 “**Children**” means individuals below the age of eighteen (18) years.

2.3 “**Consent**” means an express, unequivocal, free, specific, and informed indication of your wishes by a statement or by a clear affirmative action.

2.4 “**Customer**” or “**User**” means any individual within the Republic of Ethiopia to which Moneta provides its services.

2.5 “**Personal data**” means any information relating to an identified or identifiable individual, which shall include Sensitive personal data.

2.6 “**Sensitive personal data**” means personal data about an individual’s race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the individual’s children above 18 years, parent(s), spouse(s), or the individual’s sex or the sexual orientation.

2.7 “**Services**” refers to the financial and informational products and features provided by Moneta to Users, as described in Section 1.3 above.

2.8 “**We**”, “**Our**” and “**Us**” refer to Moneta.

3. THE DATA WE COLLECT ABOUT YOU

3.1 **Information that you provide.** To access our Services, you will be requested to provide personal data as specified in the applicable Privacy Notice. This includes the following:

3.1.1 Identifiers such as name, username, e-mail address, mobile number, or any other identifier by which you may be contacted online or offline;

3.1.2 Responses that you submit to our forms, questionnaires, and surveys;

3.1.3 Communications with Moneta, such as call records, customer service requests and tickets, and messages or comments posted on Moneta-hosted platforms;

3.1.4 Supporting documents such as government-issued identification, financial documents, and authorization letters.

3.2 **Information that we collect as you use the Services.** We also collect information from your usage of our products and features, as specified in the applicable Privacy Notice. This includes the following:

3.2.1 Device specifications, such as device identifiers, technical settings and features, and user-selected settings such as language and region;

3.2.2 Usage details, navigation and clicks, traffic data, search history, IP addresses, location data, logs, communication data, and information collected through cookies, web beacons, and other tracking technologies;

3.2.3 Transaction records, such as loan requests, disbursement records, payment records, and fund transfers;

3.2.4 Device content data, such as phonebook and network data, call logs, SMS data, and installed applications.

3.3 **Information that we receive from third parties.** To provide you with our Services and to comply with our legal obligations, we may also obtain information from third parties such as:

3.3.1 Credit scores or similar scores provided by credit reference or credit scoring entities;

3.3.2 Anti-money laundering records from name and sanctions screening vendors;

3.3.3 Account information from partner financial institutions and service providers;

3.3.4 Identifiers, repayment and other transaction data from partners, external collections agencies, mobile network providers, and mobile money operators.

3.4 **Withholding of personal data.** If you fail to provide or withhold any or all of the personal data that Moneta requests, we may be unable to provide you with our Services.

3.5 **Regulatory requirements:** We are a Digital Credit Provider regulated by several government bodies, including the Central Bank of Ethiopia, the Financial Reporting Centre, and the Ethiopia Revenue Authority. We may be required to collect, process, and retain certain personal data from you in accordance with Anti-Money Laundering, Counter Terrorist Financing and Counter Proliferation Financing (AML/CFT/CPF) or tax regulations if you use our Services.

4. HOW WE USE YOUR PERSONAL DATA

4.1 We will only process your personal data when we have a lawful basis to do so, as specified in the applicable Privacy Notice. In most instances, we will process your personal data under one of the following circumstances:

4.1.1 Where you have given your consent for the processing of your personal data.

4.1.2 Where we need to perform a contract with you, or where we need to take steps at your request before entering into a contract with you.

4.1.3 Where we need to comply with a legal obligation.

4.1.4 Where it is necessary for our legitimate interests (or those of a third party), and where your interests and fundamental rights do not override those interests.

4.2 We collect and use your personal data for the following purposes, as further specified in the applicable Privacy Notice for each specific Service:

4.2.1 To determine your eligibility for our Services, including for credit scoring and fraud prevention;

4.2.2 To process requests and instructions that we receive from you, your account, or your device;

4.2.3 To improve our Services, including the development of our models using data science and machine learning technology;

4.2.4 To communicate with you and manage our relationship with you;

4.2.5 To analyze customer behavior, conduct research, and to personalize the customer experience;

4.2.6 To meet legal requirements, such as know-your-customer and transaction monitoring obligations;

4.2.7 To comply with other orders and directives of local and international law enforcement agencies and regulatory bodies;

4.2.8 To fulfil our contractual obligations to our partners and to allow our partners to fulfil their contractual obligations to you;

4.2.9 To enable the conduct of Moneta's business through its agents, employees, representatives, consultants, vendors, partners, and other service providers.

4.3 We will only send you direct marketing communications by push notification, email or other text, if we have your consent. You have the right to withdraw that consent at any time by contacting us via email at helloEthiopia@Monetamobile.com or dpo@taka.co.ke.

4.4 Where you may have provided your consent to the processing of your personal data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact us via email at helloEthiopia@Monetamobile.com or dpo@taka.co.ke. Once we have received notification of withdrawal of consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

4.5 We use automated processing and automated decision-making with little to no human intervention when we provide you with certain features of our Services. Our models are regularly tested to ensure they remain fair, accurate, and unbiased. Where applicable, you may request a reconsideration of an automated decision by emailing us at helloEthiopia@Monetamobile.com or dpo@taka.co.ke. Please note that human intervention does not guarantee that the automated decision will be overturned.

5. DISCLOSURES AND CROSS-BORDER TRANSFERS OF YOUR PERSONAL DATA

5.1 We may disclose and/or transfer your personal data to internal and external third parties as described in the applicable Privacy Notice of each particular Service.

5.2 Your personal data collected by Moneta may be stored and processed outside of Ethiopia in a location where Moneta or its agents maintain facilities, including the use of cloud storage and cloud computing technology.

5.3 Whenever we transfer your personal data outside of Ethiopia, we ensure a similar degree of protection is afforded to it by ensuring adequate safeguards are implemented. We ensure your personal data is protected by requiring all our group companies, personnel, and agents to follow the same rules when processing your personal data.

6. DATA GOVERNANCE AND SECURITY MEASURES

6.1 Moneta implements an Information Security Management System to maintain the confidentiality, integrity, and availability of Moneta's information resources, in keeping with our commitments, industry standards and global best practices.

- Governance: Information security policies are established and communicated, and are reviewed at regular intervals. Legal and regulatory requirements regarding information security and data protection, are understood and managed by Moneta. Data protection impact assessments are carried out prior to any processing operation that may result in a high risk to the rights and freedoms of a data subject. A competent Data Protection Officer is appointed to ensure compliance with the requirements of the data protection regulations.
- Employee screening and confidentiality: Background verification checks on candidates for employment are carried out. Contractual agreements with personnel state their

responsibilities for information security. Non-compliance with contractual agreements and organizational policies will result in disciplinary action.

- Training and awareness: Personnel receive information security and data protection education and training, as well as regular updates in organizational policies and procedures, as may be relevant for their job function.
- Asset management: Company-issued devices, systems, software, and applications used within the organization are inventoried. Rules governing the installation of software by users are established and implemented. All employees and third-party users return all organizational assets in their possession upon termination of their employment, contract or agreement.
- Data classification: Information and records are classified and labelled according to legal requirements, criticality, and sensitivity.
- Role-based access control and access management: Access control policies are implemented, documented and reviewed based on business and information security requirements. A formal user registration and provisioning process is implemented.
- System access control: Access to systems and applications is controlled by a secure log-on procedure. Multifactor authentication is implemented for single sign-on access to assets.
- Cryptographic controls: Policies on the use of cryptographic controls for protection of information are implemented and regularly reviewed.
- Physical security: Physical security is applied for facilities and a clean desk policy is implemented. Equipment supporting information servers are protected from interception, interference or damage.
- Logging and monitoring: Event logs recording user activities, exceptions, faults, and information security events are produced, kept, and regularly reviewed.
- Incident management and response: Incident response and recovery plans and procedures are in place and are managed.
- Network security management: Security mechanisms, service levels and management requirements of all network services are identified and included in network services agreements.
- Third parties: Third party vendors, suppliers, and partners are subjected to information security and compliance diligence at the beginning of the relationship, as well as a periodic review.
- Written agreements are in place to address the secure transfer of business information between the organization and external parties.
- Security in development: Secure development environments are established and protected throughout the entire system development lifecycle.
- Audit and independent review: Independent reviews of systems and procedures are conducted at planned intervals or when significant changes occur. Remediation items are documented and tracked.

6.2 We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulatory authority when we are required to do so.

7. DATA RETENTION

7.1 To determine the appropriate retention period for personal data, we consider the retention requirements set by legal, tax, accounting, and AML/CFT/CPF regulations, the nature and sensitivity of the information, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the need to comply with our internal policies. We will retain or store your personal information only for so long as is necessary to fulfil the purposes set forth in the applicable Privacy Notice, and for a reasonable time thereafter for the furtherance and completion of any of our services to you, and for such time as may be necessary in order to comply with any legal obligation.

7.2 Details of retention periods for different aspects of your personal data are available in the Privacy Notice for the applicable Service.

7.3 In some circumstances you can ask us to delete your data: see Your Data Subject Rights below for further information. Where personal data must be deleted, disposal shall be done in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other entity.

7.4 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.

8. YOUR DATA SUBJECT RIGHTS

8.1 As a data subject, you have the following rights in relation to your personal data:

- **To be informed** of the uses for which your personal data is processed;
- **To access** your personal data in our custody, as well as information about:

1. The purposes for which we process your personal data;
2. the categories of personal data concerned;
3. the recipients or categories of recipients to whom the personal data have been or will be disclosed;
4. where possible, the period for which the personal data may be stored, or the criteria used to determine the period for storage and retention;
5. where the personal data is not collected from you as the data subject, any available information as to the source of collection.

- **To object** to the processing of all or part of your personal data (unless we have compelling legitimate interests to continue the processing, or when it is necessary for the establishment, exercise, or defense of a legal claim);
- **To correct or rectify** false, inaccurate, outdated, incomplete, or misleading data about you (subject to verification, such as examination of supporting documents);
- **To erase or delete** data that is false, misleading, irrelevant, excessive, unlawfully obtained, or which we are no longer authorized to retain. Your right to erasure will not

apply if it is necessary for us to continue to process your personal data to comply with a legal obligation, or for to establish, exercise, or defend a legal claim.

- **To copy, port, or receive** your personal data in a structured, commonly used, and machine-readable format, or to have your personal data ported to another data controller or data processor.

8.2 You may request that we restrict the processing of your personal data in the following circumstances:

8.2.1 where need to verify the accuracy of data that you are contesting;

8.2.2 where our use of the data is unlawful but you do not want us to erase it;

8.2.3 where the purpose of the processing has been achieved, but the we need your personal data to establish, exercise or defend legal claims;

8.2.4 you have objected to our use of your data but we need to determine whether we have overriding legitimate grounds to use it.

8.3 You have the right to object to the processing of your personal data for direct marketing purposes, and you can opt out of direct marketing communications by asking us not to send you direct marketing messages.

8.4 You may withhold or withdraw your consent in cases where we rely on your consent as the lawful basis for processing of your Personal Data. Doing so may prevent us from providing you with our Services.

8.5 You or your authorized representative can exercise any of these rights at any time, subject to our verification and review, by contacting us via email at (Moneta Contacts).

9. CHANGES TO THE PRIVACY POLICY AND YOUR DUTY TO INFORM US OF CHANGES

9.1 We keep this Privacy Policy under regular review. It may change and if it does, these changes will be posted on this page and, where appropriate, notified to you.

9.2 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.

10. THIRD PARTY LINKS

Our Services may, from time to time, contain links to and from the websites of our partner networks, advertisers and affiliates. Please note that these websites and any services that may be

accessible through them have their own privacy policies and that we do not accept any responsibility or liability for these policies or for any personal data that may be collected through these websites or services. Please check these policies before you submit any personal data to these websites or use these services.