DATA PROTECTION & PRIVACY POLICY

1. Introduction

1.1. Purpose

Zoona Transactions Zambia Limited ("Zoona" or "the Company") is a financial technology company licensed as a Payment Service Provider by the Bank of Zambia. To fulfill its business mandate to customers, employees, and vendors, the Company collects and processes personal data as necessary.

Zoona takes the privacy of its Data Subjects seriously and is committed to handling personal information with the utmost confidentiality. We strictly use personal data for its intended purpose and in full compliance with applicable laws. Through our products, website, and other platforms, we are dedicated to protecting the personal data we collect and ensuring its security at all times.

1.2. Policy Statement

Zoona is fully committed to safeguarding the privacy of its Data Subjects' personal information. This Privacy Policy (the "Policy") is an integral part of Zoona's compliance governance framework and is designed to align with the requirements of the Data Protection Act (N.A.B. No. 3 of 2021) as well as applicable international standards such as the General Data Protection Regulation (GDPR).

1.3. Policy Objective

This Data Protection & Privacy Policy reflects the company's commitment to complying with local data regulations by ensuring the secure exchange of personal data and safeguarding the privacy of customers, employees, directors, and other data subjects whose personal or sensitive information we collect or control. It outlines the core principles that all Zoona employees must uphold in handling company data.

1.4. Legal and Regulatory Context

The applicable Data Protection, Privacy and Retention laws, regulations and guidelines include but are not limited to;

- The Data Protection Act No. 3 of 2021 (DPA)
- The Data Protection Bill of 2020
- The Data Protection (Registration and Licensing) Regulations of 2021

- The Electronic Communications and Transactions Act No. 4 of 2021
- The Prohibition and Prevention of Money Laundering Act No. 14 of 2001
- The Cyber Security and Cyber Crimes Act No. 2 of 2021
- The Information and Communications Technologies Act No. 15 of 2009
- The General Data Protection Regulation (GDPR) – European Union

1.5. Scope

All employees of Zoona are required to adhere to these principles, fostering a culture of trust and accountability in handling company and customer information. It also applies to all day-to-day business activities conducted by the Company, its Parent Company, Affiliates, and/or Outsourced Service Providers that may result in access to personal data.

1.6. Effective Date

This Policy is effective from the date of approval by the Country Board of Directors (BoD).

2. Roles and Responsibilities

Zoona has designated key stakeholders responsible for driving the implementation of this Policy and ensuring the effective application of data protection and privacy controls across the company.

2.1. Board of Directors (BoD)

The Board is responsible for:

- The Board will establish a strong leadership stance on data protection and privacy.
- They will approve all policies, programs, and procedures related to data protection and privacy compliance.
- The BoD will ensure effective governance and oversight of compliance.

2.2. Senior Management

Senior management is responsible for:

- Ensuring that data protection objectives are defined and aligned with the company's strategic direction.
- Allocate necessary resources for the protection of personal data.
- Ensure compliance with the DPA and international data protection standards.
- Provide appropriate oversight by the BoD over the data compliance program.

2.3. Head of Engineering

The Head of Engineering will function as a custodian of this policy. The HoE's key responsibilities include:

- Ensure all platforms and apps are built with privacy by design and security by default.
- Implement encryption, access controls, and secure authentication methods.
- Regularly review and patch systems against vulnerabilities.
- Maintaining records of all data processing activities carried out by Zoona.
- Limit access to customer data only to authorized staff or systems.
- Oversee secure data retention and deletion processes.
- Align all systems with the Data Protection Act, 2021 and Bank of Zambia/FIC guidelines.
- Support the Data Protection Officer (DPO) in compliance audits and regulatory reporting.
- Establish monitoring systems to detect unauthorized access, breaches, or misuse of data.
- Lead the technical response to any data breach, including containment, investigation, and remediation.
- Work with the DPO to ensure breaches are reported within legal timeframes.
- Train engineering teams on data privacy principles and secure coding practices.
- Ensure developers, IT staff, and product teams understand their role in protecting customer data.

2.4. Head of Risk and Compliance

The Head of Risk and Compliance's key responsibilities include:

- Assisting the HoE with conducting regular assessments and audits.
- Ensuring that data subjects' requests, such as accessing copies of their personal data or requesting data erasure, are appropriately addressed.
- Maintaining this Policy and reviewing it at least annually.

2.5. Data Protection Officer

The Data Protection Officer is responsible for overseeing compliance with the Data Protection Act (DPA) and its regulations.

- Conducting regular assessments and audits to ensure compliance with the Act.
- Acting as the primary point of contact between various stakeholders.
- Assisting with responding to the requests of data subjects.

2.6. All Employees and Staff

All Company employees, as well as affiliate and service provider employees with responsibilities under this Policy, will be responsible for:

- Having knowledge of their responsibilities under this Policy and ensuring they remain in compliance;
- Fully comply with this policy in their daily operations;
- Adhere to data security procedures put in place by the company; and
- Report any data breach to the HoE within 24 hours of being aware of it.

3. Policy Controls

3.1. Risk Appetite

Zoona is committed to maintaining accurate information that is properly classified, securely stored, and handled in compliance with the The Data Protection Act No. 3 of 2021. The company has a very low tolerance for any compromise in the processes governing the use and management of personal data and zero tolerance for the deliberate misuse of customer information.

3.2. Data Privacy Principles

Zoona will ensure that the collection and processing of personal data comply with the DPA. Personal data will be handled with the utmost care and used solely for legitimate and specified business purposes. The company adheres to the following key principles when managing personal data:

3.2.1. Lawfulness, Fairness and Transparency

Zoona is committed to ensuring that consent for personal data processing is clear, informed, and voluntary. To achieve this, the company will:

- Ensure that consent requests are prominent, concise, easy to understand, and separate from other terms and conditions.
- Guarantee that all obtained consent is voluntary, specific, and informed, clearly communicating the purpose of data collection to data subjects.
- Implement an effective process for obtaining and managing consent (e.g., including a consent clause in all data collection mediums).

- Obtain consent only for specific data processing activities and ensure it is not applied to other activities without explicit approval.
- Secure and record explicit consent from data subjects for processing sensitive personal data.
- Retain records as evidence of granted consent.
- Inform data subjects of their right to amend or withdraw consent at any time, including the process and any legal obligations that may still apply.
- Promptly identify and stop processing personal data when consent is withdrawn, unless another valid legal basis for processing exists.
- Explain to data subjects that withdrawal of consent does not affect the processing of data conducted before the withdrawal.
- Maintain records of consent withdrawals to ensure compliance.

Zoona will not sell or offer for sale personal data of any person.

3.2.2. Purpose Limitation

Zoona will collect and process personal data only to the extent necessary to meet operational requirements or comply with legal obligations. Data processing will be purpose-driven, ensuring that only the minimum required information is collected and used responsibly.

3.2.3. Data Minimization

Zoona will ensure that all processed personal data is relevant, adequate, and limited to what is necessary for the specific purpose for which it was collected. Data collection will be purpose-driven, avoiding unnecessary or excessive processing.

3.2.4. Accuracy

Zoona will ensure the accuracy and quality of personal data by maintaining up-to-date records and implementing measures to regularly verify and update the information in its possession.

3.2.5. Storage Limitation

Zoona will retain personal data for a minimum of one year as required DPA as long and for as long as is legally required by local regulations. Data will be stored in a manner that allows for identification only as long as required, after which it will be securely deleted or anonymized in compliance with applicable regulations.

3.2.6. Integrity and Confidentiality

Zoona will safeguard personal data by implementing appropriate technical and organizational measures to prevent accidental or intentional compromise. Access to personal data will be restricted to authorized users and permitted only for approved purposes, ensuring strict data security and compliance with applicable regulations.

3.2.7. Accountability

Zoona is committed to demonstrating compliance with all applicable legal and regulatory requirements, as well as industry best practices in data privacy. All staff entrusted with handling personal data are accountable for their actions and omissions in data processing, ensuring adherence to data protection standards and maintaining the trust of data subjects.

3.2.8. Data Security and Storage

Zoona has implemented robust security measures to safeguard the personal data of data subjects, ensuring protection against unauthorized access, cyber threats, and physical breaches. These measures include:

- Network Access Control - Only approved devices can utilize the company's network, preventing unauthorized access and potential data breaches.
- Intrusion Prevention System (IPS) - A firewall-based IPS is in place to filter and block malicious data packets, protecting the network and connected systems from cyberattacks. This proactive security system identifies and swiftly responds to potential threats.
- Endpoint Security System - All company-owned computers (laptop and desktop) are protected by an endpoint protection solution that combines anti-malware, Data Loss Prevention (DLP), application and device control as well as a host-based intrusion prevention system. The solution also offers website browsing protection and filtering as well as patch assessment to minimize damage from breaches and protect against ransomware.
- Off-site Protection - All laptop computers are protected for off-site use, as the company supports remote working.
- Physical Security - To mitigate the threat of data loss that could arise from a physical breach, Zoona has, apart from human security services, secured its entry point and others access points with an access control system. Fire alarm systems are also present in the case of arson or accidental fire outbreak. Documents stored in hard copies are secured in a fire-proof cabinet and accessible to only authorised personnel who keep logs of collected and returned documents.

- Physical Security - To mitigate the threat of data loss that could arise from a physical breach, the Company has, apart from human security services, secured its entry point and others access points with an access control system. Fire alarm systems are also present in the case of arson or accidental fire outbreak. Documents stored in hard copies are secured in a fire-proof cabinet and accessible to only authorised personnel who keep logs of collected and returned documents.

This Policy applies to all personal data in our custody.

3.3. Third-Party Data Processing

Zoona may disclose a Data Subject's personal data to the following categories of third parties, ensuring compliance with legal, regulatory, and operational requirements:

- Third-Party Service Providers: Including aggregators, insurers, legal consultants, auditors, KYC verification, and screening providers.
- Authorized Representatives: Individuals or entities legally authorized to act on Zoona's behalf.
- Parent and Affiliate Companies: To facilitate business operations and compliance within the corporate group.
- Data Subject's Authorized Representatives: Individuals nominated and explicitly authorized by the Data Subject to engage with Zoona on their behalf.
- Government, Regulatory, and Law Enforcement Agencies: In compliance with legal and regulatory obligations.
- Financial Institutions and Advisers: Where necessary for financial transactions, compliance, and advisory services.

3.4. Processing of Data Outside Zambia

Any transfer of personal data—whether currently being processed or intended for processing in another country or by an international organization—will only occur if the destination country has data protection measures that are at least equivalent to those outlined in the DPA. Data subjects will be properly informed and their consent obtained, along with assurances that appropriate safeguards are in place to protect their data in the foreign jurisdiction.

3.5. Data Breach Notification

All staff members must promptly report any breach incidents to the HoE or someone in senior management, who will then escalate the matter to the Data Protection Commission (DCP) as outlined in clause 49 of the DPA.

4. Regulatory Obligations

Zoona is dedicated to complying with all regulatory reporting requirements outlined in the applicable Data Protection and Privacy regulations.

4.1. Compliance Reports

Zoona will submit the following reports to the Bank of Zambia:

A. a monthly report outlining any system breaches
B. a quarterly report of all customer complaints received and the status of such complaints, including whether the complaint was resolved or is still pending.

These submissions are required to follow the template prescribed by the Bank of Zambia.

4.2. Data Protection Impact Assessment (DPIA)

Before initiating any project that involves using new technologies, processing sensitive or high-risk personal data, Zoona will conduct a Data Protection Impact Assessment (DPIA). This assessment aims to identify potential vulnerabilities and implement measures to minimize data protection risks.

An assessment will be carried out if:

A. personal data is processed using an automated processing system, including profiling,which produces legal effects concerning the natural person or similarly significantly affects that natural person;
B. processing on a large scale of sensitive personal data, or of personal data relating to criminal convictions and offences; or
C. a systematic monitoring of a publicly accessible area on a large scale.

The DPIA will include:

- A detailed description of the intended data processing activities and their specific purposes.
- An evaluation of potential risks to personal data and the strategies implemented to mitigate them.
- Any additional information required by the Data Protection Commission (DPC).

The Company will, when necessary, conduct a review to ensure that data processing remains compliant with the DPIA, particularly when there is a change in the risks associated with processing operations.

4.3. Internal Assessments

The Company will conduct monthly assessments and audits to ensure the integrity of the and confirm that there were not system breaches that affected customer data.

4.4. Registration with DPC

As per the DPA, Zoona shall register with the DPC as a data controller and processor and this will be renewed annually. Any changes to the registered particulars of the Company shall be notified to the DPC within seven days of the occurrence of the change.

5. Incident Management

5.1. Policy Breach and Non-Compliance

All employees are required to refrain from any activities that could compromise or breach data security. Additionally, everyone is responsible for strictly adhering to this policy.

Non-compliance, whether intentional or not, will result in disciplinary action up to and including dismissal.

5.2. Complaints Handling

Zoona will establish and implement a complaint handling system to effectively address and resolve complaints from data subjects.

6. Awareness Training

Employees are the cornerstone of the company's commitment to protecting Data Subjects' personal data. Therefore, it is essential that all employees fully understand their roles and responsibilities in safeguarding the personal data entrusted to them.

Zoona will conduct annual data protection and privacy training for employees and directors, emphasizing emerging trends and issues. Additionally, continuous awareness will be promoted through posters, informational nuggets, email updates, and other knowledge resources on data protection and privacy.

7. Policy Review

Any modifications to this policy require approval from the Board. The Board will review the policy every two years or as necessary in response to changes in the local regulatory framework or the Company's business activities.

8. Associated Documents

- Data Retention Policy
- Enterprise-Wide Risk Framework
- Information Security Policy
- Disaster Recovery Plan
- Risk Management Policy
- Anti-Money Laundering and Countering Terrorist Financing Policy

Appendix: Definitions

1. **Consent** - any freely given, specific, informed and unambiguous indication of a data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
2. **Data** - any information processed by means of equipment operating automatically in response to instructions given for that purpose; is recorded with the intention that it should be processed by means of such equipment; is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; or forms part of an accessible record
3. **Data Controller** - a person who either alone, jointly with other persons or in common with other persons or as a statutory body, determines the purposes for and the manner in which personal data is processed or is to be processed.
4. **Data Collector** - a person who collects data
5. **Data Processor** - a person or organization that processes data.
6. **Data Subject** - an identifiable person, one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
7. **Data Breach** - a security incident in which information is accessed without authorisation.
8. Information - includes data, text, images, sounds, codes, computer programmes, software and databases
9. **Personal Data** - Means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

10. **Processing** - any operation which is performed upon collected data by automated means or otherwise including—
    a. organisation, adaptation or alteration of the information or data;
    b. retrieval, consultation or use of the information or data;
    c. disclosure of the information or data by transmission, dissemination or otherwise making available; or
    d. alignment, combination, blocking, erasure or destruction of the information or data.