

ZedMobile

Data Privacy and Protection Policy

Contents

ZedMobile Data Privacy and Protection Policy.....	3
---	---

1. Introduction.....	3
2. Scope	3
3. Definitions.....	4
4. Principles of Data Processing.....	4
5. Legal Basis for Processing Personal Data	5
6. Consent	5
7. Data Collection	6
a) Types of Data Collected	6
b) Methods of Data Collection	6
c) Purpose of Data Collection	6
8. Data Sharing and Disclosure	7
9. Transfer of Personal Data.....	7
a) Third Pary Processors within Zambia	7
b) Data Transfer outside of Zambia.....	8
10. Data Security	8
11. Data Retention	9
12. Data Subject Rights	9
13. Compliance and Enforcement.....	10
14. Data Breach Management	10
15. Data Protection Impact Assessment (DPIA).....	1044
16. Data Privacy Notice	11

ZedMobile Data Privacy and Protection Policy

1. Introduction

As part of our daily operations, ZedMobile collects and processes various types of personal information. This information includes, but is not limited to, names, phone numbers, addresses, gender, photographs, ID card numbers, fingerprints, and signatures. Such data is collected from a wide range of individuals, including our customers, employees (past, present, and prospective), merchants, suppliers, vendors, and anyone else we interact with ("**Individuals**").

Earning and maintaining the trust of these individuals is of utmost importance to us. We are committed to ensuring that no individual suffers adverse effects as a result of sharing their personal information with ZedMobile. To uphold this commitment, we strictly adhere to relevant data protection laws, regulations, and principles to guarantee the security and confidentiality of the personal data we handle. This Data Privacy and Protection Policy ("Policy") outlines the minimum standards we follow regarding the collection, usage, and disclosure of personal data, underscoring our dedication to processing such data with the highest level of care.

This Policy is applicable to all systems, operations, and processes within ZedMobile that involve the collection, storage, use, transmission, and disposal of personal data.

Failure to comply with the data protection rules and principles as stipulated by Zambian law and this Policy constitutes a serious violation of ZedMobile's standards and may lead to disciplinary actions, which could include suspension or termination of employment or business relationships.

2. Scope

This Policy applies to all personal data collected and processed by ZedMobile in connection with our services, products, and website. It details our practices regarding data collection, usage, storage, and protection. This Policy is applicable to all employees, contractors, consultants, temporary staff, and other workers at ZedMobile, as well as third-party vendors and service providers with whom we may share personal data.

3. Definitions

- I. **Personal Data:** Any information relating to an identified or identifiable natural person, such as name, address, email address, phone number, identification number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.
- II. **Individuals:** Any natural person whose personal data is being collected, held, or processed by ZedMobile.
- III. **Processing:** Any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment, combination, restriction, erasure, or destruction.
- IV. **Data Controller:** The entity that determines the purposes and means of processing personal data, in this case, ZedMobile.
- V. **Data Processor:** The entity that processes personal data on behalf of the Data Controller, but may also include ZedMobile from time to time.

4. Principles of Data Processing

ZedMobile is committed to maintaining the principles in the Data Protection Act No. 3 of 2021 (the “DPA”) regarding the processing of Personal Data. We adhere to the following principles when processing personal data:

- I. **Lawfulness, Fairness, and Transparency:** Personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the individual. ZedMobile ensures that individuals are informed about how their data is being used and the purpose of its collection.
- II. **Purpose Limitation:** Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes. Any new processing activities will be reviewed to ensure they are aligned with the original purposes.
- III. **Data Minimization:** Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. ZedMobile will only collect the data needed for specific purposes and no more.
- IV. **Accuracy:** Personal data shall be accurate and, where necessary, kept up to date. ZedMobile takes reasonable steps to ensure that inaccurate personal data is corrected or deleted promptly.
- V. **Storage Limitation:** Personal data shall be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for

which the personal data is processed. ZedMobile will regularly review data retention periods to ensure data is not held for longer than necessary.

- VI. **Integrity and Confidentiality:** Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.
- VII. **Accountability:** ZedMobile shall be responsible for, and be able to demonstrate compliance with, these principles. We maintain records of data processing activities and conduct regular audits to ensure adherence.

5. Legal Basis for Processing Personal Data

ZedMobile processes personal data based on one or more of the following legal bases:

- I. **Consent:** The individual has given clear consent for the processing of their personal data for specific purposes.
- II. **Contractual Necessity:** Processing is necessary for the performance of a contract to which the individual is a party, or to take steps at the request of the individual prior to entering into a contract.
- III. **Legal Obligation:** Processing is necessary for compliance with a legal obligation to which ZedMobile is subject.
- IV. **Vital Interests:** Processing is necessary to protect the vital interests of the individual or another natural person.
- V. **Public Interest:** Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in ZedMobile.
- VI. **Legitimate Interests:** Processing is necessary for the purposes of the legitimate interests pursued by ZedMobile or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual.

6. Consent

Where we rely on consent as a legal basis for processing personal data, we will ensure that:

- I. **Obtaining Consent:** Consent is obtained in a clear and transparent manner, specifying the purpose for which the data will be used.
- II. **Revoking Consent:** Individuals can withdraw their consent at any time, and we will provide an easy and effective way to do so.

- III. **Documenting Consent:** Records of consent will be maintained to demonstrate compliance with data protection laws.

7. Data Collection

a) Types of Data Collected

We may collect and process the following types of personal data:

- I. **Personal Identification Information:** Such as name, address, email address, phone number, and other contact details.
- II. **Demographic Information:** Including age, gender, nationality, and other related data.
- III. **Technical Information:** Such as IP address, browser type, device information, and usage data.
- IV. **Financial Information:** Including payment details, billing address, and transaction history.
- V. **Service Usage Data:** Information about how you use our services and products, including call records, SMS usage, data usage, and location data.

b) Methods of Data Collection

We collect personal data through various methods, including:

- I. **Direct Interactions:** When individuals provide information by filling in forms, communicating with us, or purchasing our products/services.
- II. **Automated Technologies:** When individuals interact with our website, we may collect technical data automatically through cookies, server logs, and other similar technologies.
- III. **Third Parties:** We may receive data from third parties, such as business partners, social media platforms, analytics providers, and public databases.

c) Purpose of Data Collection

The personal data we collect is used for the following purposes:

- I. **Service Provision:** To provide, manage, and improve our services and products.
- II. **Customer Support:** To communicate with you, respond to your inquiries, and provide customer support.
- III. **Billing and Payments:** To process transactions, manage payments, and prevent fraud.

- IV. **Marketing and Promotions:** To send you promotional materials, updates, and offers that may interest you, with your consent.
- V. **Personalization:** To personalize your experience and tailor our services to your preferences.
- VI. **Legal Compliance:** To comply with legal obligations and regulatory requirements.
- VII. **Security:** To protect our systems, detect and prevent security threats, and ensure the safety of our users.

8. Data Sharing and Disclosure

We may share your personal data with third parties in the following circumstances:

- I. **Service Providers:** To facilitate our services, we may share data with third-party service providers who perform functions on our behalf, such as payment processing, data analysis, and customer support.
- II. **Legal Requirements:** If required by law, we may disclose your data to regulatory authorities, law enforcement agencies, or other third parties to comply with legal obligations.
- III. **Business Transfers:** In the event of a merger, acquisition, or sale of assets, personal data may be transferred as part of the business transaction.
- IV. **With Consent:** We may share your data with third parties if you have provided your explicit consent.

9. Transfer of Personal Data

a) Third Party Processors within Zambia

We may share your personal data with third-party processors within Zambia to facilitate our services and operations. These third-party processors include service providers who perform functions on our behalf, such as payment processing, data analysis, customer support, and marketing services. To ensure the security and confidentiality of your data, we implement the following measures:

- i) **Due Diligence:** We conduct thorough due diligence on third-party processors to ensure they have robust data protection measures in place.
- ii) **Confidentiality Agreements:** All data-sharing agreements with third-party processors include confidentiality and data protection clauses.
- iii) **Regular Audits:** We periodically audit third-party processors to verify compliance with our data protection standards.
- iv) **Safeguards:** We implement technical and organizational measures to protect shared data.

- v) **Continuous Monitoring:** We continuously monitor and review data sharing processes to ensure ongoing compliance with data protection laws.

b) Data Transfer outside of Zambia

When personal data is transferred to countries outside Zambia, we take necessary steps to ensure that the data is protected in accordance with applicable data protection laws. These steps include:

- i) **Adequacy Decisions:** Ensuring that the destination country has been recognized by relevant authorities as providing an adequate level of data protection.
- ii) **Standard Contractual Clauses:** Implementing standard contractual clauses approved by data protection authorities to ensure the secure transfer of personal data.
- iii) **Binding Corporate Rules:** Utilizing binding corporate rules (BCRs) where applicable to facilitate data transfers within multinational corporate groups.
- iv) **Consent:** Obtaining explicit consent from individuals for the transfer of their personal data to countries that may not provide the same level of data protection as Zambia.
- v) **Cross-Border Transfers:** Assessing and documenting the legal basis for international data transfers.
- vi) **Safeguards:** Implementing appropriate technical and organizational measures to protect data transferred outside of Zambia.
- vii) **Regular Monitoring:** Continuously monitoring and reviewing data transfer processes to ensure ongoing compliance with data protection laws.

10. Data Security

We take the security of personal data seriously and implement appropriate technical and organizational measures to protect against unauthorized access, loss, destruction, or alteration of data. These measures include:

- i. **Access Controls:** Restricting access to personal data to authorized personnel only.
- ii. **Encryption:** Using encryption to protect data during transmission and storage.
- iii. **Regular Audits:** Conducting regular security audits and vulnerability assessments.

- iv. **Incident Response:** Having a robust incident response plan in place to handle data breaches.

To ensure security of Personal Data, ZedMobile will, among other things, implement the following appropriate technical controls:

- I. Industry accepted hardening standards, for workstations, servers, and databases.
- II. Full disk software encryption on all corporate workstation/laptops operating systems drives storing Personal and Personal/Sensitive Data.
- III. Encryption at rest including key management of key databases.
- IV. Enable Security Audit Logging across all systems managing Personal Data.
- V. Restrict the use of removable media such as USB flash disk drives.
- VI. Anonymization techniques on testing environments.
- VII. Physical access control where Personal Data are stored in hardcopy

11. Data Retention

We retain personal data only for as long as necessary to fulfill the purposes for which it was collected and in accordance with legal, regulatory, and business requirements. Once data is no longer needed, we will securely delete or anonymize it.

12. Data Subject Rights

Individuals have the following rights regarding their personal data:

- I. **Right to Access:** You have the right to request access to your personal data held by us.
- II. **Right to Rectification:** You have the right to request the correction of inaccurate or incomplete data.
- III. **Right to Erasure:** You have the right to request the deletion of your data under certain circumstances.
- IV. **Right to Restrict Processing:** You have the right to request the restriction of data processing under certain conditions.
- V. **Right to Data Portability:** You have the right to request the transfer of your data to another organization.
- VI. **Right to Object:** You have the right to object to the processing of your data for direct marketing purposes or on grounds relating to your particular situation.

To exercise these rights, please contact our Data Protection Officer at [contact information].

13. Compliance and Enforcement

ZedMobile is committed to ensuring compliance with this Policy and relevant data protection laws. We will:

- I. **Monitoring:** Regularly monitor data processing activities to ensure compliance.
- II. **Training:** Provide ongoing training to employees on data protection principles and practices.
- III. **Audits:** Conduct periodic audits to assess compliance with this Policy.
- IV. **Disciplinary Actions:** Enforce disciplinary actions for violations of this Policy.

14. Data Breach Management

In the event of a data breach, we will:

- I. **Contain the Breach:** Immediately contain the breach to prevent further unauthorized access or damage.
- II. **Assess the Impact:** Evaluate the scope and impact of the breach, including the types of data affected and the potential harm to individuals.
- III. **Notify Affected Individuals:** Inform affected individuals without undue delay if the breach poses a high risk to their rights and freedoms.
- IV. **Report to Authorities:** Notify the relevant data protection authorities within the required timeframe if the breach meets the legal notification threshold.
- V. **Remediation:** Take appropriate measures to mitigate the impact of the breach and prevent future occurrences.

15. Data Protection Impact Assessment (DPIA)

We conduct Data Protection Impact Assessments (DPIAs) for processing activities that are likely to result in a high risk to the rights and freedoms of individuals. The DPIA process includes:

- I. **Identifying Risks:** Assessing the potential risks to data subjects' privacy.
- II. **Evaluating Measures:** Identifying measures to mitigate identified risks.

- III. **Documenting Findings:** Documenting the assessment process and findings.
- IV. **Review and Approval:** Submitting the DPIA for review and approval by the Data Protection Officer.

16. Data Privacy Notice

We provide individuals with a data privacy notice that includes the following information:

- I. **Identity of the Data Controller:** ZedMobile's contact details.
- II. **Purpose of Processing:** The purposes for which personal data is collected and processed.
- III. **Legal Basis:** The legal basis for processing personal data.
- IV. **Data Sharing:** Information about third parties with whom data may be shared.
- V. **Rights of Individuals:** A summary of individuals' data protection rights and how to exercise them.
- VI. **Contact Information:** How to contact the Data Protection Officer for queries or complaints.

24.17. Contact Information

For any questions or concerns regarding this Policy or data protection practices, please contact our Data Protection Officer at:

Data Protection Officer

ZedMobile

Email: dataprotection@zedmobile.co.uk