AIRTEL NETWORKS ZAMBIA PLC
DATA PROTECTION & PRIVACY POLICY

a. Document Control

S.No.	Type of Document	Document Data
1	Document Title	Airtel Zambia Data Protection and Privacy Policy
2	Document code	ANZ/LR/SA/003
3	Date of Initial Release	August 2022
4	Next Review Date	This policy may be reviewed every two years, if needed or at any point depending on operational requirements
5	Document Superseded	V2.0
6	Document Revision No	V3.0
7	Document owner	Legal and Regulatory Affairs Director
8	Applicability	Airtel Networks Zambia PLC

Document Change history

Version No.	Revision Date	Nature of Change	Date Approved
1.0	[August 2022]	Initial Policy	August 2022
2.0	[April 2025]	[Amendment of Signatories and reference to the Data Protection Guidelines]	April 2025
3.0	November 2025	Group Alignment and roll-out of Revised Template	November 2025

b. Document Distribution

The Human Resources Director shall distribute this policy to all employees of Airtel Zambia.

c. Document Conventions

All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

d. Approvals

Designation	Name	Signature	Date
Legal & Regulatory Director	Suzyo Ndovi-Akatama		17.11.25
Sales & Distribution Director	Francis Simfukwe		17/11/25
Human Resources Director	Bwembya Barbara Chikonde		20/11/2025
Information Technology Director	Paul Chikubwai		04/12/2025
Supply Chain Management Director)	Martin Jowi		05.12.2025
Customer Service Director	Kapa Kaumba		08.12.2025
Enterprise Director	Lindiwe Banda		8/12/25
Finance Director	Samir Warman		6/01/26
Managing Director	Hussameldin Baday		09/01/26

Table of Contents

1. INTRODUCTION

a) As part of our operations, Airtel Networks Zambia PLC]("Airtel") collects and processes certain types of information (including but not limited to, name, telephone numbers, address, address, gender, photograph, ID card number, fingerprint, and signature etc.) of individuals that makes them easily identifiable. These individuals include customers, current, past and prospective employees, merchants, suppliers/vendors, customers of merchants and other individuals whom Airtel Zambia communicates or deals with, jointly and/or severally ("**Data Subjects**").

b) Maintaining the Data Subject's trust and confidence requires that Data Subjects do not suffer negative consequences/effects as a result of providing Airtel with their Personal Data. To this end, Airtel is firmly committed to complying with applicable data protection laws, regulations, rules and principles to ensure security of Personal Data handled by the Company. This Data Privacy & Protection Policy ("**Policy**") describes the minimum standards that must be strictly adhered to regarding the collection, use and disclosure of Personal Data and indicates that Airtel is dedicated to processing the Personal Data it receives or processes with absolute confidentiality and security.

c) This Policy applies to all forms of systems, operations and processes within the Airtel Zambia environment that involve the collection, storage, use, transmission and disposal of Personal Data.

d) Failure to comply with the data protection rules and guiding principles set out in the Zambia]local law data privacy and protection legislation as well as those set out in this Policy is a material violation of Airtel [Jurisdiction]'s policies and may result in disciplinary action as required, including suspension or termination of employment or business relationship.

2. SCOPE

a) This Policy applies to all:

i. customers' and employees of Airtel Zambia;

ii. and any external business partners (such as merchants, suppliers, contractors, vendors and other service providers) who receive, send, collect, access, or process Personal Data in any way on behalf of Airtel Zambia, including processing wholly or partly by automated means; and

iii. third party Data Processors who process Personal Data received from Airtel [Zambia].

Consequences of non-compliance

b) All employees, temporary staff of Airtel Zambia, contractors and third parties are required to comply with this policy.
c) Non-compliance with this policy is a ground for enforcement action, and the action may include termination of employment or termination of a relevant contract.

3. OBJECTIVES

a) It is the responsibility of the Data Protection Officer to manage data privacy within Airtel Zambia.

b) The objectives of Airtel Zambiain relation to data privacy are to ensure that:

i. A privacy framework is established to implement, monitor, manage and improve organization-wide information privacy controls;
ii. The privacy roles and responsibilities are defined and assigned at all levels ensuring that the individuals understand them;
iii. Information privacy awareness is created among employees;
iv. Appropriate, reasonable, technical and organizational measures are adopted organization-wide to prevent loss, damage, or unauthorized destruction and unlawful access to or unauthorized processing of personal data; and
v. The privacy framework and controls are reviewed at regular intervals and updated to incorporate latest legal and regulatory requirements and industry best practices.

4. DATA PROTECTION OFFICER

a) Airtel Zambia shall appoint a Data Protection Officer(s) (DPO) responsible for overseeing the Company's data protection strategy and its implementation to ensure compliance with the Zambia Data Protection Act and attendant regulations and guidelines requirements. The DPO shall be a knowledgeable person on data privacy and protection principles and shall be familiar with the provisions of the Zambia Data Protection Act and attendant regulations and guidelines.

b) The main tasks of the DPO include:
i. administering data protection policies and practices of Airtel;
ii. monitoring compliance with the Zambia Data Protection Act and attendant regulations and guidelines and other data protection laws, data protection policies, awareness-raising, training, and audits;
iii. advice the business, management, employees and third parties who carry on processing activities of their obligations under the Zambia Data Protection Act and attendant regulations and guidelines;
iv. acts as a contact point for Airtel;
v. monitor and update the implementation of the data protection policies and practices of

Airtel and ensure compliance amongst all employees of Airtel;

vi. ensure that Airtel undertakes a Data Impact Assessment and curb potential risk in Airtel data processing operations; and

vii. maintain a Data Base of all Airtel data collection and processing operations of Airtel.

5. Principles for Processing of Personal Data

a) Airtel is committed to maintaining the principles in the Zambia Data Protection Act and attendant regulations and guidelines regarding the processing of Personal Data.

b) To demonstrate this commitment as well as our aim of creating a positive privacy culture within Airtel, we adhere to the following basic principles relating to the processing of Personal Data:

5.1 Lawfulness, Fairness and Transparency

a) Personal Data must be processed lawfully, fairly and in a transparent manner at all times. This implies that Personal Data collected and processed by or on behalf of Airtel must be in accordance with the specific, legitimate and lawful purpose consented to by the Data Subject, save where the processing is otherwise allowed by law or within other legal grounds recognized in the Zambia Data Protection Act and attendant regulations and guidelines.

5.2 Data Accuracy

Personal Data must be accurate and kept up-to-date. In this regard, Airtel will:

a) make efforts to ensure that any data it collects and/or processes is accurate and not misleading in a way that could be harmful to the Data Subject;

b) make efforts to keep Personal Data updated where reasonable and applicable; and

c) make timely efforts to correct or erase Personal Data when inaccuracies are discovered.

5.3 Purpose Limitation

a) Airtel will process personal data based on one of the following grounds:

i. performing a contract or to enter into a contract with the data subject, for example, we process the numbers customers dial, how much data they use and when they do it so we can provide them with a connection and issue a bill;

ii. Airtel's legitimate business interests, as long as these do not override the

data subject's rights and freedoms. For example, fraud prevention, security of our network and services, marketing, analysing and improving our services; or

iii. complying with a mandatory legal obligation, for example, accounting, tax, money laundering, anti-bribery requirements

b) Airtel will collect personal data relating to:

iv. employees and applicants for employment, including an employee's job application, records of training, documentation of performance appraisals, salary increases, expense claims and other employment records (Employee Personal Data)

v. consumers (i.e. members of the public to whom we do not directly sell our products and services but who use, will use or are considering using a service which Airtel ultimately provide) and customer contacts (Customer Personal Data)

vi. users of our websites or other related services provided by Airtel (User Personal Data)

vii. supplier contacts, industry professionals and other individuals who provide goods and/or services to the Airtel (Supplier Personal Data).

c) Airtel holds and processes Employee Personal Data for the following purposes:

i. administering and managing its employees;

ii. administering employee benefits and entitlements;

iii. protecting the legitimate interests of the Airtel, including investigating acts or defaults; and

iv. compliance with applicable laws, regulations and rules.

d) Airtel holds and processes Customer Personal Data for the following purposes:

i. administering and managing our relationships with our consumers and customers, which may include:

(a) dealing with enquiries, processing orders and providing the customer with products and services (including facilitating delivery);

(b) taking the appropriate measures to invoice and take the appropriate payment or credit from the customer; and

(c) providing updated information, such as changes to terms and conditions;

ii. marketing and promoting our products and services and inviting customers to participate in market research;

iii. any corrective action which may be required in respect of any of the products and services we supply;

iv. improving and innovating our products and services which, for example, enables us to manage our networks and understand network usage more effectively;

v. credit checks, fraud prevention, debt recovery and security purposes; and

vi. compliance with applicable laws, regulations and rules.

e) Airtel holds and processes User Personal Data for the following purposes:

i. supplying marketing and promotional material (at the user's express request) and advertising online;

ii. administering and improving our websites and related purposes, (including collecting and analysing anonymous, de-identified and aggregate information); and
iii. compliance with applicable laws, regulations and rules.

f) Airtel holds and processes Supplier Personal Data for the following purposes:
   i. administering the receipt of products and services from its suppliers;
   ii. administering and managing its relationships with its suppliers; and
   iii. compliance with applicable laws, regulations and rules.

g) Airtel may share the personal data that it collects with its corporate affiliates and third parties operating on its behalf Airtel will only share personal data with companies that are required to protect personal data in accordance with relevant laws, regulations and rules, and subject to any appropriate security measures and directions from the relevant Airtel data controller, and in accordance with this policy.

5.4 Data Minimization

a) Airtel Zambia limits Personal Data collection and usage to data that is relevant, adequate, and absolutely necessary for carrying out the purpose for which the data is processed.

b) Airtel Zambia will evaluate whether and to what extent the processing of personal data is necessary and where the purpose allows, anonymized data must be used.

5.5 Integrity and Confidentiality

a) Airtel shall establish adequate controls in order to protect the integrity and confidentiality of Personal Data, both in digital and physical format and to prevent personal data from being accidentally or deliberately compromised.

b) Personal data of Data Subjects must be protected from unauthorized viewing or access and from unauthorized changes to ensure that it is reliable and correct.

c) Any personal data processing undertaken by an employee who has not been authorized to carry such out as part of their legitimate duties is un-authorized.

d) Employees may have access to Personal Data only as is appropriate for the type and scope of the task in question and are forbidden to use Personal Data for their own private or commercial purposes or to disclose them to unauthorized persons, or to make them available in any other way.

e) Human Resources Department must inform employees at the start of the employment relationship about the obligation to maintain personal data privacy. This obligation shall remain in force even after employment has ended.

5.6 Personal Data Retention

a) All personal information shall be retained, stored and destroyed by Airtel in line with legislative and regulatory guidelines. For all Personal Data and records obtained, used and stored within the Company, Airtel shall perform periodical reviews of the data retained to confirm the accuracy, purpose, validity and requirement to retain.

b) To the extent permitted by applicable laws, the length of storage of Personal Data shall, amongst other things, be determined by:

   i. the contract terms agreed between Airtel and the Data Subject or as long as it is needed for the purpose for which it was obtained; or
   ii. whether the transaction or relationship has statutory implication or a required retention period; or
   iii. whether there is an express request for deletion of Personal Data by the Data Subject, provided that such request will only be treated where the Data Subject is not under any investigation which may require Airtel to retain such Personal Data or there is no subsisting contractual arrangement with the Data Subject that would require the processing of the Personal Data; or
   iv. whether Airtel has another lawful basis for retaining that information beyond the period for which it is necessary to serve the original purpose.

c) Airtel will use all reasonable means to not keep any Personal Data in Airtel's possession where such Personal Data is no longer required by Airtel provided no law or regulation being in force requires Airtel to retain such Personal Data.

d) For further guidance on document retention and destruction, please contact dataprotection@zm.airtel.com.

5.7 Accountability

a) Airtel demonstrates accountability in line with the Zambia Data Protection Act and attendant regulations and guidelines obligations by monitoring and continuously improving data privacy practices within Airtel.

b) Any individual or employee who breaches this Policy may be subject to internal disciplinary action (up to and including termination of their employment); and may also face civil or criminal liability if their action violates the law.

6. Data Privacy Notice

a) Airtel considers Personal Data as confidential and as such must be adequately protected from unauthorized use and/or disclosure. Airtel will ensure that the Data Subjects are provided with adequate information regarding the use of their Personal Data as well as acquire their respective Consent, where necessary.

b) Airtel shall display a simple and conspicuous notice (Privacy Notice) on any medium through which Personal Data is being collected or processed. The following information must be considered for inclusion in the Privacy Notice, as appropriate in distinct circumstances in order to ensure fair and transparent processing:
    i. Description of collectible Personal Data;
    ii. Purposes for which Personal Data is collected, used and disclosed;
    iii. What constitutes Data Subject's Consent;
    iv. Purpose for the collection of Personal Data;
    v. The technical methods used to collect and store the information;
    vi. Available remedies in the event of violation of the Policy and the timeframe for remedy; and
    vii. Adequate information in order to initiate the process of exercising their privacy rights, such as access to, rectification and deletion of Personal Data.

c) Airtel Privacy Notice is available on Airtel website via this **link**. https://077.airtel.co.zm/assets/pdf/Airtel-Networks-Zambia-Privacy-Notice-1.pdf

7. Consent

Where processing of Personal Data is based on consent, Airtel shall obtain the requisite consent of Data Subjects at the time of collection of Personal Data. In this regard, Airtel will ensure:

a) that the specific purpose of collection is made known to the Data Subject and the Consent is requested in a clear and plain language;
b) that the Consent is freely given by the Data Subject and obtained without fraud, coercion or undue influence;
c) that the Consent is sufficiently distinct from other matters to which the Data Subject has agreed;
d) that the Consent is explicitly provided in an affirmative manner;
e) that Consent is obtained for each purpose of Personal Data collection and processing; and
f) that it is clearly communicated to in a simple language and understood by Data Subjects that they can update, manage or withdraw their Consent at any time.

8. Data Subject Rights

a) All individuals who are the subject of Personal Data held by Airtel are entitled to the following rights:

i. Right to request for and access their Personal Data collected and stored. Where data is held electronically in a structured form, such as in a Database, the Data Subject has a right to receive that data in a common electronic format;
ii. Right to information on their personal data collected and stored;
iii. Right to objection or request for restriction;
iv. Right to object to automated decision making;
v. Right to request rectification and modification of their data which Airtel keeps;
vi. Right to request for deletion of their data, except as restricted by law or Airtel statutory obligations;
vii. Right to request the movement of data from Airtel to a Third Party; this is the right to the portability of data; and
viii. Right to object to, and to request that Airtel Zambia restricts the processing of their information except as required by law or Airtel Zambia's statutory obligations.

b) To opt out of marketing and unsolicited messages:

i. If you no longer want to receive marketing messages from Airtel, you can choose to opt out at any time. If you've previously opted in to receive personalized content based on how and where you use our network, you can also opt out at any time.

ii. These are various ways to opt out:

- Contact our customer services team via the email addresses– AirtelCustomerServices@zm.airtel.com
- Reach out to any member of the High Value Experience managers or Key Account Managers (KAMs)
- Click the unsubscribe icon from our email or newsletters if you receive any.
- Disable push notification messages, including marketing messages, at any time in our apps by changing the notification settings on your device or by uninstalling the app and
- You can also activate DND (Do not Disturb) by dialing *111#
- Contact our customer service team by dialing 111

c) Airtel [Zambia]'s well-defined procedure regarding how to handle and answer Data Subject's requests are contained in Airtel [Zambia]'s Data Subject Access Request Policy.

d) Data Subjects can exercise any of their rights by completing the Airtel [Zambia]'s Subject Access Request (SAR) Form and submitting to the Company via dataprotection@zm.airtel.com or call the number +260 977 770097

9. Appointing Data Processors and engaging with Data Controllers

a) When appointing third parties to carry out processing of personal data on the Airtel Zambia's behalf, Airtel [Jurisdiction] shall only use processors that will guarantee to implement appropriate technical and organizational measures to ensure that their

processing activities meet the requirements of data privacy laws and ensure the protection of the rights of data subjects.

b) When appointing a third-party data processor, Airtel Zambia must enter into a written agreement with that processor which specifies (i) the subject matter and duration of the processing; (ii) the nature and purpose of the processing; (iii) the type of personal data and categories of data subjects; and (iv) the obligations and rights of Airtel Zambia as data controller. The agreement must impose obligations at least as onerous as those set out in Annex 1.

c) When Airtel Zambia and a third party jointly determine the purposes for which, and the manner in which, personal data is processed, they might be considered joint data controllers under data privacy laws.

d) The requirements in paragraph 9(a-c) also apply to personal data sharing between Airtel Africa Group companies. In that case, references to a third party shall be read as 'Airtel Africa Group recipient'.

10. Transfer of Personal Data

a) Intra Group Arrangements

i. Personal data may be transferred between companies in the Airtel Africa Group in accordance with applicable data privacy laws, Airtel Intra-Group Data Processing Agreement and this policy, in particular the data protection principles set out in paragraph 5 above and, if relevant, the requirements in relation to sharing personal data with a data processor or controller set out in section 9 above.

ii. Where an Airtel Africa Group company receives personal data in its capacity as a data processor, that company shall comply with the requirements set out in paragraph 9(a-b) of this policy.

b) Third Party Processor within Zambia

i. Airtel may engage the services of third parties in order to process your Personal Data of collected by us. The processing by such third parties shall be governed by a written contract with Airtel to ensure adequate protection and security measures are put in place by the third party for the protection of Personal Data in accordance with the terms of this Policy and the Zambia Data Protection Act and attendant regulations and guidelines. We may also share your personal data with law enforcement agencies where required by law to do so.

ii. Where applicable, Airtel will share your information with:
    i. Partners, suppliers or agents involved in delivering the products and services you've ordered or used. For example, when you apply for loan, your loan request is handled by our business partner who is bound by contract to protect your

personal data.

ii. Law enforcement agencies, government bodies, regulatory organisations, courts or other public authorities if we have to, or are authorized to by law. For example, under the Cybercrimes Act, a law enforcement agency may request a service provider to keep or release any traffic data, subscriber information, content or non-content information. This is, however, for law enforcement purposes only.

iii. A third party or body where such disclosure is required to satisfy any applicable law, or other legal or regulatory requirement e.g. to detect or prevent fraud or the commission of any other crime.

iv. A merging or acquiring entity where we undergo business reorganization e.g. merger, acquisition or takeover.

c) Transfer of Personal Data to Foreign Country

i. Where Personal Data is to be transferred to a country outside Zambia, Airtel shall put adequate measures in place to ensure the security of such Personal Data. In particular, Airtel shall, among other things, conduct a detailed assessment of whether
(a) the relevant personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements; and
(b) the enforcement of data protection laws by authorities with appropriate jurisdiction is effective.

ii. Transfer of Personal Data out of Zambia would be in accordance with the provisions of the Zambia Data Protection Act and attendant regulations and guidelines. Airtel will therefore only transfer Personal Data out of Zambian Jurisdiction on one of the following conditions:

a. The consent of the Data Subject has been obtained;
b. The transfer is made subject to standard contracts or intragroup schemes that have been approved by the Data Protection Commissioner; or
c. The Minister has prescribed that transfers outside the Republic is permissible; or
d. The Data Protection Commissioner approves a particular transfer or set of transfers as permissible due to a situation of necessity

e. The transfer is necessary for the performance of a contract between Airtel and the Data Subject or implementation of pre-contractual measures taken at the Data Subject's request;

f. The transfer is necessary to conclude a contract between Airtel and a third party in the interest of the Data Subject;

g. The transfer is necessary for reason of public interest;

h. The transfer is for the establishment, exercise or defense of legal claims;

i. The transfer is necessary in order to protect the vital interests of the Data Subjects or other persons, where the Data Subject is physically or legally incapable of giving consent.

Provided, in all circumstances, that the Data Subject has been manifestly made to understand through clear warnings of the specific principle(s) of data protection that are likely to be violated in the event of transfer to a third country, this proviso shall not apply to any instance where the Data Subject is answerable in duly established legal action for any civil or criminal claim in a third country.

iii. Airtel will take all necessary steps to ensure that the Personal Data is transmitted in a safe and secure manner. Details of the protection given to your information when it is transferred outside Zambia shall be provided to you upon request.

iv. .

11. Data Protection Impact Assessment

a) As Airtel Zambia operates as part of the Airtel Africa Group, when the Airtel Africa Group, develops new systems and new ways of processing personal data, it considers the data privacy principles above. Where those systems or processing could be likely to pose a high risk to the privacy of data subjects (e.g. systematic profiling of a large number of data subjects on an automated basis in a way that affects their legal rights or status), Airtel Zambia will carry out a data privacy assessment in relation to that processing.

b) Airtel shall carry out a Data Protection Impact Assessment (DPIA) in respect of any new project or IT system involving the processing of Personal Data to determine whenever a type of processing is likely to result in any risk to the rights and freedoms of the Data Subject.

c) Airtel shall carry out the DPIA in line with the procedures laid down in the Airtel **Data Protection Impact Assessment Policy.**

12. Data Security

a) All Personal Data must be kept securely and should not be stored any longer than necessary. Airtel will ensure that appropriate organizational and technical measures are implemented to protect personal data of our customers, employees, directors and suppliers against unathorized access, accidental loss, damage and destruction to data.

13. DATA BREACH MANAGEMENT PROCEDURE

a) A data breach procedure is established and maintained in order to deal with incidents concerning Personal Data or privacy practices leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

b) All employees must inform their designated line manager or the DPO of Airtel immediately about cases of violations of this Policy or other regulations on the protection of Personal Data, in accordance with Airtel **Personal Data Breach Management Procedure** in respect of any:

i. improper transmission of Personal Data across borders;
ii. loss or theft of data or equipment on which data is stored;
iii. accidental sharing of data with someone who does not have a right to know
iv. this information;
v. inappropriate access controls allowing unauthorized use;
vi. equipment failure;
vii. human error resulting in data being shared with someone who does not have a right to know; and
viii. hacking attack.

c) A data protection breach notification must be made immediately after any data breach to ensure that:

i. immediate remedial steps can be taken in respect of the breach;
ii. any reporting duties to [Insert relevant enforcement agency if any] or any other regulatory authority can be complied with,
iii. any affected Data Subject can be informed and
iv. any stakeholder communication can be managed.

d) When a potential breach has occurred, Airtel will investigate to determine if an actual breach has occurred and the actions required to manage and investigate the breach as follows:

i. Validate the Personal Data breach.
ii. Ensure proper and impartial investigation (including digital forensics if necessary) is initiated, conducted, documented, and concluded.
iii. Identify remediation requirements and track resolution.
iv. Report findings to the top management
v. Coordinate with appropriate authorities as needed.
vi. Coordinate internal and external communications.
vii. Ensure that impacted Data Subjects are properly notified, if necessary.

viii. Immediately the breach is detected it needs to be notified to the Group Privacy Officer and Chief Legal Officer

e) The procedure for reporting of Personal Data Breaches to a Supervisory Authority
   i. The Head of IT Security shall notify the DPO of any breach of personal data immediately of being aware of such breach.
   ii. The DPO shall review each reported incident of data breach and determine if there's a requirement to notify the relevant supervisory authority.
   iii. The DPO shall be responsible for reporting in a timely manner all incidences of data breaches to the relevant supervisory authority upon consultation with the Group Privacy Officer, Chief Legal Officer and Airtel Africa Head of IT Security.

14. INTERACTION WITH SUPERVISORY AUTHORITIES

Engagement with local data protection authorities or regulators is an important step in strengthening Airtel's data privacy and protection compliance programme and ensuring the company continues to meet the expectations of its stakeholders. Prior to engaging with local data protection authorities, the DPO is required to consult with the Airtel Africa Group Privacy Officer and functions responsible for data protection oversight to ensure such engagement are effective and well-coordinated.

15. TRAINING

Airtel shall ensure that employees who collect, access and process Personal Data receive adequate data privacy and protection training in order to develop the necessary knowledge, skills and competence required to effectively manage the compliance framework under this Policy and the Zambia Data Protection Act and attendant regulations and guidelines with regard to the protection of Personal Data.

16. CHANGES TO THE POLICY

Airtel reserves the right to change, amend or alter this Policy at any point in time. If we amend this Policy, we will provide you with the updated version.

17. DEFINITIONS

"Consent"	means any written, freely given, specific, informed and unambiguous indication of the data subject's wishes by which such data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to that data subject;

"Database"	means a collection of data organized in a manner that allows access, retrieval, deletion and processing of that data; it includes but not limited to structured, unstructured, cached and file system type Databases.
"Data Controllers"	means a person who, either alone or jointly with other persons, controls and is responsible for keeping and using personal data on a computer, or in structured manual files, and requests, collects, collates, processes or stores personal data from or in respect of a data subject.
"Data Processor"	means a person who, either alone or jointly with other persons, controls and is responsible for keeping and using personal data on a computer, or in structured manual files, and requests, collects, collates, processes or stores personal data from or in respect of a data subject;
"Data Auditor""	means a person licensed as a data auditor under section 29.
"Data Subject"	means an individual from, or in respect of whom, personal information is processed;
"Data users"	include employees whose work involves using or otherwise processing personal data. Data users have a duty to protect the information they handle by following our data protection and security policies (including this policy) at all times.
"ZDPA"	means the Zambia Data Protection Act, 2021.
"Pseudonymisation"	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, where that additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person;
"Personal Data"	means data which relates to an individual who can be directly or indirectly identified from that data which includes a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address,

IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others.

"Sensitive Personal Data"	means personal data which by its nature may be used to suppress the data subject's fundamental rights and freedoms and includes (a) the race, marital status, ethnic origin or sex of a data subject; (b) genetic data and biometric data; (c) child abuse data; (d) a data subject's political opinions; (e) a data subject's religious beliefs or other beliefs of a similar nature; (f) whether a data subject is a member of a trade union; or (g) a data subject's physical or mental health, or physical or mental condition;

Annexure 1: Data Processor Language

The processor shall, when processing personal data on behalf of Airtel:

(a) process the personal data only on documented instructions from Airtel, including with regard to transfers of personal data to a country outside the European Economic Area or to an international organization (unless the processor is required to do so by European Union or United Kingdom law, in which case the processor shall inform Airtel of that legal requirement before processing, unless prohibited by that law on important grounds of public interest);

(b) ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including as appropriate: (i) the pseudonymisation and encryption of the personal data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to the personal data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;

(d) only engage another processor with Airtel's prior specific written consent and, if Airtel consents, by entering into a legally binding written agreement that places the same data protection obligations as those set out in this clause on the other processor, provided that if the other processor fails to fulfil its data protection obligations the initial processor shall remain fully liable to Airtel for the performance of that other processor's obligations;

(e) taking into account the nature of the processing, assist Airtel by appropriate technical and organizational measures, insofar as possible, to respond to requests

from data subjects for access to or rectification, erasure, portability, restriction of processing or objections to processing of their personal data;

(f) assist Airtel in ensuring compliance with Airtel's security, data breach notification, impact assessment and consultation obligations under Articles 32 to 36 of the General Data Protection Regulation, taking into account the nature of processing and the information available to the processor;

(g) at Airtel's election, delete or return all personal data and existing copies to Airtel at the end of the provision of the services (unless European Union or other applicable law requires the processor to store the personal data); and

(h) make available to Airtel all information necessary to demonstrate compliance with the obligations in this clause and allow for and contribute to audits, including inspections, conducted by Airtel or another auditor mandated by Airtel.