Data Protection and Privacy Policy

1. Introduction

As part of our operations, Main One Cable Company Limited and its subsidiaries (collectively referred to as "MainOne") collects and processes certain types of information (such as name, telephone numbers, address etc.) of individuals that makes them easily identifiable. These individuals include current, past and prospective employees, vendors, customers/clients and their representatives, next-of-kin and other individuals whom MainOne communicate or deals with, jointly and/or severally "**Data Subjects**".

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

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

Failure to comply with the data protection rules and guiding principles set out in the Nigeria Data Protection Act, 2023 (NDPA), the Ghana Data Protection Act 2012, Law n° 2013-450 of June 19th, 2013 relating to the protection of personal data in Cote d'Ivoire or other relevant law or regulation ("Applicable Legislations"), as well as those set out in this Policy is a material violation of MainOne's policies and may result in disciplinary action as required, including suspension or termination of employment or business relationship.

2. Scope

This Policy applies to all employees of MainOne, as well as to any external business partners (such as suppliers, contractors, vendors and other service providers) who receive, send, collect, access, or process Personal Data in any way on behalf of MainOne, including processing wholly or partly by automated means. This Policy also applies to third party Data Processors who process Personal Data received from MainOne.

3. General Principles for Processing of Personal Data

MainOne is committed to complying with the principles in the Applicable Legislations with regards to the processing of Personal Data.

To demonstrate this commitment as well as our aim of creating a positive privacy culture within MainOne, MainOne adheres to the following basic principles relating to the processing of Personal Data:

3.1 Lawfulness, Fairness and Transparency

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 MainOne 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 Applicable Legislations.

3.2 Data Accuracy

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

a) Shall 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) Will make efforts to keep Personal Data updated where reasonable and applicable; and

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

3.3 Purpose Limitation

MainOne collects Personal Data only for the purposes identified in the appropriate MainOne Privacy Notice or any other relevant document or based on any other non – written communication (where applicable), provided to the Data Subject and for which Consent has been obtained. Such Personal Data cannot be reused for another purpose that is incompatible with the original purpose, except a new Consent is obtained.

3.4 Data Minimization

3.4.1 MainOne 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.

3.4.2 MainOne will evaluate whether and to what extent the processing of Personal Data is necessary and where the purpose allows, anonymized data must be used.

3.5 Integrity and Confidentiality

3.5.1 MainOne 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.

3.5.2 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.

3.5.3 Any processing of Personal Data undertaken by an employee who has not been authorized to carry such processing as part of their legitimate duties is unauthorized.

3.5.4 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.

3.5.5 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 the employment term has ended.

3.6 Personal Data Retention

3.6.1 All personal information shall be retained, stored and destroyed by MainOne in line with relevant Legislative and Regulatory Guidelines; and Applicable Legislations. For all Personal Data and records obtained, used and stored within the Company, MainOne shall perform periodical reviews of the data retained to confirm the accuracy, purpose, validity and requirement to retain such data.

3.6.2 To the extent permitted by Applicable Legislations and without prejudice to MainOne's Retention Policy, the length of storage of Personal Data shall, amongst other things, be determined by:

(a) The contract terms agreed between MainOne and the Data Subject or for as long as it is needed for the purpose for which it was obtained, and/or whether the transaction or relationship has statutory implication or a required retention period.

(b) An express request for deletion by the Data Subject; except where such Data Subject is under an investigation or under a subsisting contract which may require further processing or where the data relates to criminal records or whether MainOne has another lawful basis for retaining that information beyond the period for which it is necessary to serve the original purpose.

Notwithstanding the foregoing and pursuant to Applicable Legislations, MainOne shall be entitled to retain and process Personal Data for archiving, scientific research, historical research or statistical purposes for public interest.

3.6.3 MainOne would forthwith delete Personal Data in MainOne's possession where such Personal Data is no longer required by MainOne or in line with MainOne's Retention Policy, provided no law or regulation being in force requires MainOne to retain such Personal Data.

3.7 Accountability

3.7.1 MainOne demonstrates accountability in line with the obligations provided in the Applicable Legislations by monitoring and continuously improving data privacy practices within MainOne.

3.7.2 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.

4. Data Privacy Notice

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

4.2 MainOne 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:

a) Description of collectible Personal Data
b) Purposes for which Personal Data is collected, used and disclosed
c) What constitutes Data Subject's Consent
d) Purpose for the collection of Personal Data
e) The technical methods used to collect and store the information
f) Available remedies in the event of violation of the Policy and the timeframe for remedy.
g) Adequate information in order to initiate the process of exercising their privacy rights, such as access to, rectification and deletion of Personal Data.

5. Purpose and Category of Data Collected and Processed

5.1. We will only collect and use your Personal Data if we have obtained your prior consent or have a lawful and legitimate interest to do so. You are at liberty to withdraw your consent at any time by contacting the Data Protection Officer at *mainone.dataprotectionofficer@equinix.com*. The following are data collected and processed by MainOne:

- Communication data (e.g. name, telephone, e-mail, address, IP address)
- Key contract data (contractual relationship, product or contractual interest)
- Customer history
- Contract billing and payments data
- Planning and control data
- Movement data
- Disclosed information (from third parties)
- Employee and prospective employee data collected for recruitment and onboarding purpose.

5.2. The following are methods adopted by MainOne in the collection and storage of Personal Data:

- Cookies
- CCTV recordings

6. Legal Grounds for Processing of Personal Data

In line with the provisions of the Applicable Legislations, processing of Personal Data by MainOne shall be lawful if at least one of the following applies:

a) The Data Subject has given Consent to the processing of his/her Personal Data for one or more specific purposes.

b) The processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.

c) Processing is necessary for compliance with a legal obligation to which MainOne is subject.

d) Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.

e) Processing is necessary for the performance of a task carried out in the public interest or in exercise of official public mandate vested in MainOne.

f) Processing is necessary for the purposes of the legitimate interests pursued by MainOne, or by a third party to whom the Personal Data is disclosed.

7. Consent

Where processing of Personal Data is based on consent, MainOne shall obtain the requisite consent of Data Subjects at the time of collection of Personal Data. In this regard, MainOne 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.
f) That it is clearly communicated to and understood by Data Subjects that they can update, manage or withdraw their Consent at any time.

7.1 **Valid Consent**

7.1.1 For Consent to be valid, it must be given voluntarily by an appropriately informed Data Subject. In line with regulatory requirements, Consent

cannot be implied. Silence, pre-ticked boxes or inactivity does not constitute Consent under Applicable Legislations.

7.1.2 Consent in respect of Sensitive Personal Data must be explicit. A tick of the box would not suffice.

7.2 **Consent of Minors**

The Consents of minors (under the age of 18) will always be protected and obtained from minor's representatives in accordance with applicable legal and regulatory requirements.

8. Data Subject Rights

8.1 All individuals who are the subject of personal data held by MainOne are entitled to the following rights:

a) 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.

b) Right to information on their Personal Data collected and stored.

c) Right to objection or request for restriction.

d) Right to object to automated decision making.

e) Right to request rectification and modification of their data which MainOne keeps.

f) Right to request for deletion of their data, except as restricted by Applicable Legislations or MainOne's statutory obligations.

g) Right to request the movement of data from MainOne to a Third Party; this is the right to the portability of data.

h) Right to object to, and to request that MainOne restricts the processing of their information except as required by Applicable Legislations or MainOne's statutory obligations.

8.2 MainOne's well-defined procedure regarding how to handle and answer Data Subject's requests are contained in MainOne's Data Subject Access Request Policy.

8.3 Data Subjects can exercise any of their rights by completing the MainOne's Subject Access Request (SAR) Form and submitting to the Company via *mainone.dataprotectionofficer@equinix.com*.

9. Transfer of Personal Data

9.1 **Third Party Processor within Nigeria**

MainOne may engage the services of third parties in order to process the Personal Data of Data Subjects collected by the Company. The processing by such third parties shall be governed by a written contract with MainOne 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 Applicable Legislations.

9.2 **Transfer of Personal Data to Foreign Country**

Nigeria

9.2.1 Where Personal Data is to be transferred to a country outside Nigeria, MainOne shall put adequate measures in place to ensure the security of such Personal Data.

9.2.2 Transfer of Personal Data out of Nigeria would be in accordance with the provisions of the NDPA and any other applicable laws or regulations. MainOne will therefore only transfer Personal Data out of Nigeria on one of the following conditions:

a. The consent of the Data Subject has been obtained.

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

c. The transfer is necessary to conclude a contract between MainOne and a third party in the interest of the Data Subject.

d. The transfer is necessary for reason of public interest.

e. The transfer is for the establishment, exercise or defence of legal claims.

f. 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/foreign country. This provision 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/foreign country.

MainOne 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 Nigeria shall be provided to you upon request.

9.2.3 Where the recipient foreign country is not on the White List and none of the conditions stipulated in Section 9.2.2 of this Policy is met, MainOne will engage with the Nigeria Data Protection Commission (NDPC) for approval with respect to such transfer.

Cote d'Ivoire

9.2.4 Where Personal Data is to be transferred to a country outside Cote d'Ivoire, MainOne shall in addition to adopting the conditions in 9.2.2 above, only transfer Personal Data to a third/foreign country where such a country provides an adequate level of protection for privacy, freedoms and the fundamental rights if individuals in relation to the processing or possible processing of such data. MainOne shall put adequate measures in place to ensure the security of such Personal Data.

9.2.5 MainOne shall obtain the authorization of the Data Protection Agency, Agence de Regulation des Telecommunications en Cote d'Ivoire (ARTCI) prior to any transfer of Personal Data to such a third country.

9.2.6 The authorization request for the transfer of Personal Data to third countries must be presented by an Ivorian legal person (MainOne CIV). The application must include:

- Extracts from criminal records of the principal officers of the legal person (MainOne CIV) making the request, not less than three months prior to the date of the application
- The nature of the date in question
- The reason and purpose of the transfer
- The guarantees of protection, conservation, confidentiality of Personal Data, respect for the rights of individuals concerned and the legal obligations of the controller (MainOne CIV)

- The name of the third country receiving or hosting the transferred data and the legal framework relating to the protection of Personal Data in the third country
- The methods of transmission of the data to be transferred to the third country
- The guarantees of right of access to the data transferred by the Data Subject
- Provision of adequate data security with regards to the data transferred

Ghana

9.2.7 Where Personal Data is to be transferred to a country outside Ghana, MainOne Ghana shall in addition to adopting the conditions in 9.2.2 above, during its application for registration as a data controller with the Ghana Data Protection Commission specify the name or description of the country to which it may transfer the data.

9.2.8 Where a data processor is not domiciled in Ghana, Main One Ghana shall ensure that the data processor complies with the Ghana Data Protection Act 2012 or other relevant data protection laws in Ghana

9.2.9 MainOne Ghana shall put adequate measures in place to ensure the security of such Personal Data transferred to a country outside Ghana; and shall ensure such third country provides an adequate or equivalent level of data protection

10. Data Breach Management Procedure

10.1 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.

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

a) Improper transmission of Personal Data across borders.

b) Loss or theft of data or equipment on which data is stored.

c) Accidental sharing of data with someone who does not have a right to know this information.

d) Inappropriate access controls allowing unauthorized use.

e) Equipment failure.

f) Human error resulting in data being shared with someone who does not have a right to know.

g) Hacking attack.

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

a) Immediate remedial steps can be taken in respect of the breach.

b) Any reporting duties to NDPC or any other data protection supervisory authority under Applicable Legislation can be complied with.

c) Any affected Data Subject can be informed.

d) Any stakeholder communication can be managed.

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

a) Validate the Personal Data breach.

b) Ensure proper and impartial investigation (including digital forensics if necessary) is initiated, conducted, documented, and concluded.

c) Identify remediation requirements and track resolution.

d) Report findings to the top management.

e) Coordinate with appropriate authorities as needed.

f) Coordinate internal and external communications.

g) Ensure that impacted Data Subjects are properly notified, if necessary.

10.5 You can read more about MainOne's Personal Data Breach Management Procedure on SharePoint.

11. Data Protection Impact Assessment

MainOne 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.

MainOne shall carry out the DPIA in line with the procedures laid down in the **MainOne Data Protection Impact Assessment Policy** available on SharePoint.

12. Data Security

12.1 All Personal Data must be kept securely and should not be stored any longer than necessary. MainOne will ensure that appropriate measures are employed against unauthorized access, accidental loss, damage and destruction to data. This includes the use of password-encrypted databases for digital storage and locked cabinets for those using paper form.

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

a) Industry-accepted hardening standards, for workstations, servers, and databases;

b) Full disk software encryption on all corporate workstation/laptops operating systems drives storing Personal and Personal/Sensitive Data;

c) Encryption at rest including key management of key databases;

d) Enable Security Audit Logging across all systems managing Personal Data;

e) Restrict the use of removable media such as USB flash, disk drives;

f) Anonymization techniques on testing environments; and

g) Physical access control where Personal Data are stored in hardcopy.

13. Data Protection Officer

MainOne has appointed Data Protection Officer(s) (DPO) in its jurisdiction of operations responsible for overseeing the Company's data protection strategy and its implementation to ensure compliance with the requirements of Applicable Legislations. The DPOs are knowledgeable in data privacy and protection principles and are familiar with the provisions of the Applicable Legislations as it pertain to their respective jurisdiction. You can contact the DPO at *mainone.dataprotectionofficer@equinix.com*.

The main tasks of the DPO include:

a) Administering data protection policies and practices of MainOne;

b) Monitoring compliance with the Applicable Legislations, data protection policies, awareness-raising, training, and audits;

c) Advice the business, management, employees and third parties who carry on processing activities of their obligations under the Applicable Legislations;

d) Acts as a contact point for MainOne;

e) Monitor and update the implementation of the data protection policies and practices of MainOne and ensure compliance amongst all employees of MainOne;

f) Ensure that MainOne undertakes a Data Privacy Impact Assessment and curb potential risk in MainOne data processing operation; and

g) Maintain a Data Base of all data collection and processing operations of MainOne.

14. Training

MainOne 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 Applicable Legislations with regard to the *protection* of Personal *Data*. On an annual basis, MainOne shall develop a capacity building plan for its employees on data privacy and protection in line with Applicable Legislations.

15. Data Protection Audit

MainOne shall conduct an annual data protection audit through a licensed Data Protection Compliance Organization (DPCOs) to verify MainOne's compliance with the provisions of the NDPA in Nigeria; and as required under the Applicable Legislation in its respective jurisdictions of operations

The audit report will be certified and filed by the DPCO to NDPC as required under the NDPA in Nigeria; or as otherwise required under any of the Applicable Legislations.

16. Related Policies and Procedures

This Policy shall be read in conjunction with the following policies and procedures of MainOne:

- Personal Data Breach Management Policy
- IT Security Policy
- Document Retention Policy
- Cookies Policy
- Privacy Notices
- Data Protection Impact Assessment Procedure.

17. Changes to the Policy

MainOne 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.

18. Definitions/Abbreviations

Term/Abbreviation	Explanation
Consent	Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, through a statement or a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.

Database	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.
Data Processor	A person or organization that processes Personal Data on behalf and on instructions of MainOne.
DPCO	An organization registered by the NDPC to provide data protection audit, compliance and training services to public and private organizations who process Personal Data in Nigeria.
Data Subject	Any person, who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
NDPA	Nigeria Data Protection Act.
NDPC	Nigeria Data Protection Commission.
Personal Data	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; 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	Any data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information.