

DATA PRIVACY AND PROTECTION POLICY – SUBURBAN FIBER COMPANY LIMITED

1. Introduction

This Data Privacy and Protection Policy (the “Policy”) sets out the basis on which our company Suburban Fiber Company Limited (“Suburban” or “the Company” or “we” or “our”) will process any Personal Data we collect from Data Subjects, including our customers/clients and business contacts, or that is provided to us by Data Subjects or other sources.

In the course of our business activities we collect, store and process Personal Data about our customers, suppliers and other third parties, and therefore in order to comply with the law and to maintain confidence in our business, we acknowledge the importance of correct and lawful treatment of this Data. Thus, this Policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store Personal Data. The procedures and principles set out herein must be followed at all times by us and our employees, agents, contractors, or other parties working on behalf of the Company. We aim to ensure the correct, lawful, and fair handling of all Personal Data and to respect legal rights of Data Subjects.

2. Meaning of key terms

- (i) “*Consent*” of the Data Subject means 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.
- (ii) “*Data*” means characters, symbols and binary on which operations are performed by a computer, which may be stored or transmitted in the form of electronic signals, stored in any format or any device.
- (iii) “*Data Controller*” means a person who either alone, jointly with other persons or in common with other persons or a statutory body determines the purposes for and the manner in which Personal Data is processed or is to be processed. We are the Data Controller of all Personal Data used in our business for our own commercial purposes.
- (iv) “*Data Processor*” “*Data Processor* means a person or organization that processes Personal Data on behalf and on instructions of Suburban.
- (v) “*DPCO*” means an organization registered by NITDA to provide data protection audit, compliance and training services to public and private organizations who process Personal Data in Nigeria.
- (vi) “*Data Subject*” for the purpose of this Policy means 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.
- (vii) “*NITDA*” means the National Information Technology Development Agency.

- (viii) “*Processing*” is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
- (ix) “*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; 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.
- (x) “*Sensitive Personal Data*” means 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.
- (xi) “*Regulation*” means the Nigerian Data Protection Regulation, 2019.

3. **Scope and application of the Policy**

This Policy applies to people working in or with our business and aims to ensure compliance with the Regulation. It applies specifically to all employees of Suburban, 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 Suburban, including processing wholly or partly by automated means. This Policy also applies to third party Data Processors who process Personal Data received from Suburban.

4. **Use of personal data and our purpose of data collected and processed**

4.1. We collect, hold, and process the following Personal Data including:

- (i) contact information such as name(s), telephone number, e-mail and address;
- (ii) date of birth and gender, job title;
- (iii) business/company name;
- (iv) customer history;
- (v) contract billing and payment data;
- (vi) demographic information such as postcode, preferences and interests;
- (vii) financial information such as credit / debit card numbers;

- (viii) IP address (automatically collected);
- (ix) web browser type and version (automatically collected);

4.2. In line with the provisions of the Regulation, processing of Personal Data by Suburban 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 Suburban is subject;
- (d) processing is necessary in order to protect the vital interests of the Data Subject or of another natural person, or
- (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 Suburban.

5. **Data Protection Principle**

5.1. Lawful, Fair, and Transparent Data Processing

We will ensure that processing of Personal Data is done fairly and without adversely affecting the rights of the Data Subject. We will also ensure that Personal Data collected and processed by or on behalf of Suburban 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 Regulation.

5.2. Processed for Specified, Explicit and Legitimate purposes

5.2.1. We will collect and process Personal Data including Data received directly from Data Subjects and Data received from third parties.

5.2.2. We will only process Personal Data for the specific purposes set out in this Policy or for other purposes expressly permitted by the Regulation. The purposes for which we process Personal Data will be informed to Data Subjects at the time that their Personal Data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

5.3. Adequate, Relevant and Limited Data Processing

Suburban will only collect and process Personal Data for and to the extent necessary for the specific purpose(s) informed to Data Subjects.

5.4. Data Accuracy and Keeping Data Up to Date

Suburban shall ensure that all Personal Data collected and processed is kept accurate and up-to-date. The accuracy of Data shall be checked when it is collected and at annual intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that Data, as appropriate.

5.5. Timely processing and Data retention

Suburban shall not keep Personal Data for any longer than is necessary in light of the purposes for which that Data was originally collected and processed. When the Data is no longer required, all reasonable steps will be taken to erase it without delay, provided no law or regulation being in force requires Suburban to retain such Personal Data.

Suburban shall pursuant to the Regulation, be entitled to retain and process Personal Data for archiving, scientific research, historical research or statistical purposes for public interest.

5.6. Secure Processing

Suburban shall ensure that all Personal Data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, damage, unauthorised viewing or access and from unauthorized changes to ensure that it is reliable and correct.

5.7. Accountability

We shall keep written internal records of all Personal Data collection, holding, and processing, which shall incorporate the following information:

- (a) The name and details of the Company, its data protection officer, and any applicable third-party Data Controllers;
- (b) The purposes for which the Company processes Personal Data;
- (c) Details of the categories of Personal Data collected, held, and processed by the Company; and the categories of data subject to which that Personal Data relates;
- (d) Details (and categories) of any third parties that will receive personal data from the Company;
- (e) Details of any transfers of Personal Data including all mechanisms and security safeguards;
- (f) Details of how long Personal Data will be retained by the Company; and
- (g) Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of Personal Data.

6. **Data Subject Rights**

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

- (a) The right to request for and access their Personal Data collected and stored;
- (b) The right to request for restriction;
- (c) The right to information on their Personal Data collected and stored;
- (d) The right to object to automated decision making;
- (e) The right to rectification and modification of their Data which Suburban keeps;
- (f) The right to restrict processing of their information except as required by law or Suburban's statutory obligations;
- (g) The right to request erasure/ deletion of their data, except as restricted by law or Suburban's statutory obligations; and
- (h) The right to data portability

7. **Consent/Privacy of Data Subject**

7.1. Suburban shall ensure that the following information is provided to every Data Subject when Personal Data is collected:

- (a) The specific purpose(s) for which the Personal Data is being collected and will be processed as well as the legal basis justifying that collection and processing;
- (b) Where the personal data is not obtained directly from the Data Subject, the categories of Personal Data collected and processed;
- (c) What constitutes the Data Subject's consent;
- (d) Where the Personal Data is to be transferred to one or more third parties, details of those parties;
- (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.

7.2. The information set out above shall be provided to the Data Subject in any medium through which the Data is being collected.

8. **Transfer of Personal Data**

8.1. Third Party Processor within Nigeria

Suburban may engage the services of third parties in order to process the Personal Data of Data Subjects collected by the us. The processing by such third parties shall be governed by a written contract with Suburban 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 Regulation.

8.2. Transfer of Personal Data to a Foreign Country

8.2.1. Where Personal Data is to be transferred to a country outside Nigeria, Suburban shall put in adequate measures to ensure the security of such Personal Data. In particular, Suburban shall, among other things, conduct a detailed assessment of whether the said country is on the NITDA White List of countries with adequate data protection laws.

8.2.2. Transfer of Personal Data out of Nigeria would be in accordance with the provisions of the Regulations. Suburban will therefore only transfer Personal Data out of Nigeria on one of the following conditions:

- (a) consent of the Data Subject has been obtained;
- (b) the transfer is necessary for the performance of a contract between Suburban 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 Suburban 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.

8.2.3. 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. Suburban 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 the Data Subject upon request.

8.2.4. Where the recipient country is not on the White List and none of the conditions stipulated in Section of this Policy is met, Suburban will engage with NITDA and the Office of the Honourable Attorney General of the Federation (HAGF) for approval with respect to such transfer.

9. **Data Security**

- 9.1. All Personal Data must be kept securely and should not be stored any longer than necessary. Suburban 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.
- 9.2. To ensure security of Personal Data, Suburban 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.

10. **Data Protection Officer**

In accordance with the Regulation, we have appointed a Data Protection Officer(s) (DPO) responsible for overseeing the Company's data protection strategy and its implementation to ensure compliance with the requirements in the Regulations. The DPO is knowledgeable in data privacy and protection principles and is familiar with the provisions of the NDPR. The contact details of the Data Protection officer are as follows:

The Data Protection Officer
Suburban Fiber Company Limited
15 Bangui Street, off Adetokunbo Ademola Crescent
Wuse II
Abuja, Nigeria
dataprotection.officer@suburbanfiberco.com

11. **Data Breach Notification/Management**

All Personal Data breaches must be reported immediately to the Company's data protection officer.

- (a) If a Personal Data breach occurs and that breach is likely to result in a risk to the rights and freedoms of Data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the data protection officer must ensure that the appropriate authorities are informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

- (b) In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.
- (c) Data breach notifications shall include the following information:
 - (ii) The categories and approximate number of data subjects concerned;
 - (iii) The categories and approximate number of personal data records concerned;
 - (iv) The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
 - (v) The likely consequences of the breach; and
 - (vi) Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

12. **Training**

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

13. **Data Protection Audit**

Suburban shall conduct an annual data protection audit through a licensed Data Protection Compliance Organization (DPCOs) to verify Suburban's compliance with the provisions of the Regulations and other applicable data protection laws. The audit report will be certified and filed by the DPCO to NITDA as required under the Regulations.

14. **Data Privacy Impact Assessments**

The Company shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall be overseen by the Company's data protection officer and shall address the following areas of importance:

- (a) The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;
- (b) Details of the legitimate interests being pursued by the Company;
- (c) An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

15. **Our Other Obligations**

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of Personal Data:

- (a) All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy;
- (b) Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to Personal Data held by the Company;
- (c) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
- (d) All employees, agents, contractors, or other parties working on behalf of the Company handling Personal Data will be appropriately supervised;
- (e) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;
- (f) The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
- (g) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;
- (h) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Regulation;
- (i) Where any agent, contractor or other party working on behalf of the Company handling Personal Data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

16. **Changes to this Policy**

We may update this Policy from time to time and we will notify you of any changes by posting the new or updated policy. If we amend this Policy, we will provide you with the updated version. Thus, you are advised to review this page periodically for any changes as any such changes will be effective, immediately after they are posted on this page.

17. **Contact us**

If you have any questions or suggestions about this Policy, do not hesitate to contact us at [\[insert\]](#), or using the 'contact us' form on the Application. You can also contact us in writing at [\[insert\]](#)