

DATA PROTECTION AND PRIVACY STATEMENT

1. PURPOSE

- 1.1. Sahara Group Limited and/or its affiliates (otherwise referred to as the “**Company**” or “**SGL**”) is committed to protecting personal data. This statement outlines a framework for the appropriate management of personal information and personal data provided by individuals themselves or by others (“**Data Subjects**”) to the Company in compliance with the Nigerian Data Protection Regulation (or any others as may be in force from time to time). It is also to ensure the protection and efficient management of confidential information. The Company takes its responsibilities regarding the management of personal data and personal information very seriously. This Statement how the Company processes your personal data.

This Statement applies to personal information and personal data provided by individuals themselves or by others to the Company.

- 1.2. Proper management of confidential information is critical to the success of the Company. Employees are often entrusted with, or in the course of their duties become aware of trade secrets and proprietary information not generally known to the public. This type of information, whether or not subject to intellectual property rights, is considered confidential and is to be protected by all employees and other former employees. Any unauthorized disclosure of Company proprietary or confidential information is prohibited and would lead to disciplinary and/or legal actions in line with the Company's sanction grid, where such unauthorized disclosures are made by anyone bound by this Statement and the Company's policy on the protection and use of Company assets, resources and information.

Definitions

“**Data Controller or Controller**” means a person who either alone, jointly with other persons or in common with other persons or as a statutory body determines the purposes for and the manner in which personal data is processed or is to be processed;

“**Data Processing**” means any operation or set of operations which is performed on Personal Information or Personal Data or on sets of Personal Data, whether or not by automated means such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,

dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

“Personal information” or **“personal data”** is any information relating to an identified person or identifiable natural person, either directly or indirectly in particular by reference to for e.g. a name, number, location data, online identifier or any factor specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trade union membership, criminal records, etc. are also included. Therefore names, addresses, photographs, email addresses, bank details, social media posts, medical information, IP address, phone numbers, IMEI number, etc. may suffice here.

2. The Information We Collect

We collect the following information: name, data of birth, residential and contact address, telephone number, email address, marital status, nationality, gender, tax identity number, educational background, biometric data, identity number, location, photograph, IP address, MAC address, IMEI number, IMSI number and other information relevant.

3. How We Collect and Use Your Data

- 3.1. The Company collects the above-mentioned information using forms, email and physical requests, cookies, JWT, web tokens.
- 3.2. When you send email or other communication to the Company, we may retain the communication in order to process your enquiries, respond to your requests and improve our services. When you access the Company’s services, our servers automatically record information that your browser sends whenever you visit a website. The collection of this information allows us to customize your online experience and improve the performance and ease of use of our website as well as measure the effectiveness of our marketing.
- 3.3. By registering and/or submitting personal information to the Company you accept and consent to the Company using this information in accordance with this Statement.
- 3.4. We use the above-mentioned information for contract performance, fulfilment of legal obligations such as to regulatory bodies and the like, marketing, business development, publicity, human resources management, recruitment, events planning and hosting, in-house security, research, analysis and vendor registration.

4. Consent and Access Rights

- 4.1. We require your consent for the processing of your data. If we use this information in a manner different from the purpose for which it was collected, then we will ask for your consent prior to such use.
- 4.2. No Consent shall be sought, given, or accepted in any circumstance that may engender direct or indirect propagation of atrocities, hate, child rights violation, criminal acts and anti-social conduct.
- 4.3. You may withdraw your consent at any time and may request access to your personal information in our possession without affecting the lawfulness of processing based on consent prior to withdrawal by emailing corp.gov@sahara-group.com. We can, however, deny you access to the information where we determine that your request is unreasonable. The Company hereby states that Data Subjects are entitled to lodge complaints with the National Information Technology Development Agency (NITDA) where the company does not act on requests made or consent is withdrawn.
- 4.4. You reserve the right to request the modification or amendment of your personal data in our possession by emailing corp.gov@sahara-group.com.
- 4.5. In all cases of access or modification / amendment of personal information, we shall request sufficient identification to enable us confirm that you are the owner of the data sought to be accessed or modified / amended.

5. Personal Data Protection Principles

When we process your personal data, we are guided by the following principles, which require personal data to be:

- a) processed lawfully, fairly, in a transparent manner and with respect for the dignity of the human person.
- b) collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.
- d) accurate and where necessary kept up to date.
- e) removed or not kept in a form which permits identification of data subject for longer than is necessary for the purposes for which the personal data is processed.
- f) processed in a manner that ensures its security, using appropriate technical and organizational measures to protect against unauthorized or unlawful Processing and

against accidental loss, destruction or damage.

6. User Responsibility

You are required to familiarize yourself with this Statement and to ensure that the information you provide to us is complete, accurate and up to date.

7. Data Security

7.1. The Company implements and maintains appropriate safeguards to protect personal data, taking into account in particular, the risks posed to you, by unauthorised or unlawful processing or accidental loss, destruction of, or damage to their personal data.

7.2. Safeguarding will include the use of encryption and pseudonymization where appropriate. It also includes protecting the confidentiality (i.e. that only those who need to know and are authorized to use personal data have access to it), integrity and availability of the personal data. We regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.

8. Third Party Access

8.1. The Company only shares personal information with other companies or individuals in the following limited circumstances:

- a) Where we have your consent to do so.
- b) Where we provide such information to other professional advisers or other trusted businesses or persons for the purpose of processing personal information on our behalf. We require that these parties agree to process such information based on our instructions and in compliance with this Statement and any other appropriate confidentiality and security measures.
- c) Where we believe in good faith that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce applicable terms of service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against imminent harm to the rights, property or safety of the Company, its users or the public as required or permitted by law.

8.2. The Company is at all times, responsible for the security and appropriate use of that data as long as it remains with the Company.

9. Violation of Privacy

- 9.1. We have put in place procedures to deal with any suspected personal data breach and will notify you of any personal data breach and let you know the steps we have taken to remedy the breach and the security measures we have applied to render your personal data unintelligible.
- 9.2. All suspected breach of personal data will be remedied with 1 (one) month from the date of the report of the breach.
- 9.3. If you know or suspect that a personal data breach has occurred, you should immediately contact the Data Protection Officer at corp.gov@sahara-group.com
- 9.4. The Company will not be responsible for any personal data breach which occurs as a result of:
 - a) an event which is beyond the control of the Company;
 - b) an act or threats of terrorism;
 - c) an act of God (such as, but not limited to fires, explosions, earthquakes, drought, tidal waves and floods) which compromises the Company's data protection measures;
 - d) war, hostilities (whether war be declared or not), invasion, act of foreign enemies, mobilization, requisition, or embargo;
 - e) rebellion, revolution, insurrection, or military or usurped power, or civil war which compromises the Company's data protection measures;
 - f) the transfer of your personal data to a third party on your instructions; and
 - g) the use of your personal data by a third party designated by you.

10. International Transfers

- 10.1. If we process your personal information, your personal information may be transferred to and stored outside the country where you are located. This includes countries outside the European Economic Area (EEA), if you are based in the EEA, and countries that do not have laws that provide specific protection for personal information.
- 10.2. Transfer outside the EEA (where applicable) will be only:
 - to a recipient located in a country which provides an adequate level of protection for your personal information; and/or
 - under an agreement which satisfies EU requirements for the transfer of personal data to data processors or data controllers outside the EEA, such as standard

contractual clauses approved by the European Commission.

11. Right to Data Portability

- 11.1. You have the right to request the transmission of your personal data to another controller, where technically feasible and where doing so does not adversely affect the rights and freedoms of others.
- 11.2. In order to assert the right to data portability, the data subject may at any time contact the Data Protection Officer.

12. How to Contact Us

For any enquiries you have in relation to this Statement, please feel free to contact our Data Protection Officer at corp.gov@sahara-group.com