

MOUKA LIMITED

DATA PROTECTION AND PRIVACY POLICY

LAST UPDATED ON [JULY 15, 2020]

TABLE OF CONTENTS

1. Introduction
2. Personal Data Processing Principles
3. Breach
4. Definitions and abbreviations

1.0 INTRODUCTION

1.1 Objective and Scope of the Privacy Policy (the “Policy”)

In the digital era we live in, data is essential to business and, if properly managed, unlocks new sources of growth. However, responsible Personal Data and Sensitive Personal Data management is vital for business sustainability and Mouka Limited (the “**Company**”) does not engage in any behaviour that would damage our businesses or the communities in which we operate. We fully recognize the fundamental right of individuals to privacy and their right to the safeguard of Personal Data. The protection of employees’ and other individuals’ privacy right is the primary aim of this Privacy Policy, which forms a key part of the Company’s commitment to meet global standards for data protection and privacy.

This Policy aims to give you information on how the Company collects, uses, discloses, transfers, stores and otherwise processes your personal data when you fill any of our forms, access or create an account on our website as well as other mediums and platforms through which you provide us with your personal data in order to enable us provide our products and services to you. It is therefore important that you read this Policy together with any other privacy policy or fair processing policy we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your personal data.

Third parties to whom the Company outsources all or part of Personal Data Processing activities (“Processing”) must also comply with this Policy. We will validate the privacy policy of any new third party the Company engages that involves the Company providing data on customers, vendors, staff and others. Existing third party service providers will also be subject to validation.

The Company and its affiliates may share your personal information with each other and use it consistent with this Policy. They may also combine it with other information to provide and improve the Company’s products and services, as well as its advertising.

1.2 Risks Associated with Violations of Privacy Legislation

Failure to comply with applicable privacy laws and regulations can result in the imposition of fines and other sanctions. Non-compliance with this Policy will not be tolerated by the Company and may result in disciplinary action. The disciplinary action will vary according to the severity of the non-compliance but could include the cancellation of the employee’s bonus, postponement of promotion, suspension without pay, termination of employment or being reported to the authorities.

2.0 PERSONAL DATA PROCESSING PRINCIPLES

The Company shall process your data in accordance with relevant data protection laws in Nigeria including the Nigeria Data Protection Regulation, 2019, the 1999 Constitution of the Federal Republic of Nigeria (as amended) and regulations issued by the NITDA, and ensure that your personal data is:

- Collected and processed in accordance with specific, legitimate, and/or lawful purpose consented to by you.

- Adequate, accurate and procured without prejudice to any of your fundamental human rights.
- Stored only for the period within which it is reasonably needed; and
- Secured against all foreseeable hazards, breaches, or such other unlawful purpose such as theft, cyber-attack, viral attack, dissemination, manipulations of any kind, damage by rain, fire, or exposure to other natural elements

2.1 Specific and Legitimate Purposes

We process Personal Data and Sensitive Personal Data only for specific and explicit purposes which we will communicate to you at or before the moment of Personal Data and/or Sensitive Personal Data collection.

As an example, if a consumer’s contact information has been collected for the purpose of processing a complaint, it cannot be added to our newsletter distribution list unless the consumer has been informed of this additional purpose and has consented to it.

We have set out below, in a table format, a description of all the ways we plan to use your personal data. Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data.

Please contact our Keji.ojelade@mouka.com Officer at [.] (the “**DPO**”), if you need details about this Policy or if you have any questions regarding the legal grounds we are relying on to process your Personal Data or Sensitive Personal Data where more than one ground has been set out in the table below.

PURPOSE/ACTIVITY	TYPE OF DATA	LAWFUL BASIS FOR PROCESSING
To register you as a new customer	(a) Identity (b) Contact (c) Financial	(a) Performance of a contract with you (b) Necessary for our legitimate interests
To perform contract with you and provide our product and services	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interest

To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	(a) Technical (b) Usage	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)
To maintain and manage our relationship with you. This will include: (a) Notifying you about changes to our terms or privacy policy (b) Asking you to leave a review or take a survey	(a) Identity (b) Contact (c) Profile (d) Marketing and Communications	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated and to study how customers use our products/services)

- **Performance of Contract** – means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.
- **Compliance with legal obligation** – means processing your Personal Data or Sensitive Personal Data where it is necessary for compliance with a legal obligation that we are subject to.
- **Legitimate Interest** – means the interest of our business in conducting and managing our business to enable us to give you the best products and services and most secure experience.
- **Public Interest** – means where processing your data is necessary in order to protect your interest, the interest of another data subject or for the performance of a task carried out in the public interest or in exercise of official public mandate vested in us.

We will only use your Personal Data for the purposes for which its collected for and which you have consented to, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact the DPO.

If we need to use your Personal Data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your Personal Data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

2.2 Data Collection and Control

We use different methods to collect data from and about you including through:

- Direct interactions. You may give us your Identity, Contact and Financial Data by filling in forms, accessing or creating an account on our website, corresponding with us by post, phone, email as well as other related medium/platforms. This particularly covers personal data you provide when you apply for our products or services, give us feedback or contact us.
- Automated technologies or interactions. As you interact with our website, we will automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies. We may also receive Technical Data about you if you visit other websites employing our cookies.
- The Company is the data controller and responsible for your Personal Data and Sensitive Personal Data. The Company shall take all reasonable and necessary steps to ensure that where it provides to any third party your personal information for the purpose of improving the Company's products and services, or to help the Company market services and products to consumers, the Company will ensure that such third parties processes your data, in compliance with applicable laws and under a written contract.

Third parties or publicly available sources: We will receive personal data about you from third parties.

2.3 Data proportionality and quality

We will only collect the Personal Data we need for our purposes and we will not ask for or store irrelevant Personal Data or Sensitive Personal Data.

The Personal Data we maintain shall also be accurate and kept up-to-date at all times. Consequently, please note that you have a right, further to a formal request in writing to the DPO, to update your data as soon as there is any change in the data you have shared with us. We will update, rectify or erase (as applicable) any inaccurate or incomplete data, upon being informed of any such inaccuracy and/or information gap.

2.4 Limited Retention

We will only retain your personal data for as long as reasonably necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

2.5 Data Subject's Information

Personal Data, Sensitive Personal Data or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

- Identity Data includes first name, maiden name, middle name, last name, username or similar identifier, marital status, title, date of birth/age and gender.
- Contact Data includes billing address, delivery address, email address and telephone numbers.
- Financial Data includes bank account and payment card details.
- Transaction Data includes details about payments to and from you and other details of products and services you have purchased from us
- Technical Data includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access this website.
- Profile Data includes your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses.
- Usage Data includes information about how you use our website, products and services.
- Marketing and Communications Data includes your preferences in receiving marketing from us and our third parties and your communication preferences.

In the event that we collect any Sensitive Personal Data (i.e. details about your race or ethnicity, religious or philosophical beliefs, sexual orientation, political opinions and views, trade union membership, information about your health, and genetic and biometric data) we shall process same in accordance with this Policy and applicable laws.

2.6 Data Subject's consent

Generally, we rely on your clear, unequivocal and comprehensible consent as the legal basis for processing your data. This covers cases where you require us to process your data for the purpose of performing a contract with you, or accessing our products and services, raising a complaint for clearance of faults; whistleblowing and accessing any of our customer care services.

We may, in accordance with relevant laws and this Policy, use your data in our marketing and advertising services. In such instances, we will seek your consent before we share your personal data with any third party for such purposes.

With regards to what constitutes data subject's consent, in accordance with the applicable laws and regulations, the Company shall ensure that consent is freely given and is obtained without fraud, coercion or undue influence. Accordingly, the Company would typically collect and process your personal data where you require us to perform a contract, including the provision of our products and services to you.

Since the performance of a contract with you and provision of our products and services to you are conditional on your consent, we shall deem that you have granted us the free and express consent to collect and process your personal data when you fill any of our forms, access or create an account on our website, corresponding with us by post, phone, email as well as other related medium/platforms.

PLEASE NOTE THAT YOU HAVE THE RIGHT TO WITHDRAW CONSENT AT ANY TIME TO THE PROCESSING OF YOUR PERSONAL DATA BY CONTACTING THE DPO.

Where we need to collect personal data by law, or under the terms of a contract we have with you, or to provide our products and our services and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (including to provide you with our products and services). In this case, we may have to cancel a product or service you have with us but we will notify you if this is the case at the time.

2.7 Data Confidentiality and Security

We recognise the importance of protecting data from unauthorised access and the attendant effects of data corruption hence, the company shall:

- Develop security measures including but not limited to protecting systems from hackers and unauthorised access
- Set up firewalls and protect email systems and servers
- Store data securely with access to specific authorised individuals
- Develop and maintain an organisational policy for handling personal data and other sensitive or confidential data.

We have put in place reasonable security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised or illegal way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know same. They will only process your data

on our instructions and they are subject to a duty of confidentiality as governed by a written contract.

We have put in place reasonable procedures to deal with any suspected data breach and will notify you, the NITDA and any applicable regulator of a breach where we are legally required to do so.

Generally, we do not transfer your personal data outside Nigeria or to an international organisation. However, whenever the need to transfer your personal data out of Nigeria or to an international organisation arises, we shall ensure that we comply with the relevant laws and regulations.

We may share your personal data with the parties set out below for the purposes set out in the table in Section 2.1 of this Policy above, and in compliance with the applicable laws and regulations;

- Service providers who provide IT and system administration services, revenue collection services, electricity billing and printing services, gateway channel services, workforce management services and vending services.
- Professional advisers including consultants, lawyers, bankers, auditors and insurers who provide consultancy, banking, legal, insurance and accounting services.
- Regulatory agencies and authorities who require reporting of processing activities in certain circumstances.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions as stipulated in a written contract

2.8 Data Subjects' Rights

Under certain circumstances, you have rights under data protection laws and regulations in relation to your personal data. You have the right to the following:

- Request access to your personal data (commonly known as a “Data Subject Access Request”). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- Request correction/rectification of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
- Request erasure of your personal data. You have a right to delete or remove your personal data after same has been collected by us. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with a legal obligation in

Nigeria. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

- Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.
- Request restriction of processing of your Personal Data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: If you want us to establish the data's accuracy; where our use of the data is unlawful but you do not want us to erase it; where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; and when you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
- Request the transfer (commonly known as "Data Portability") of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
- Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.
- Disable Cookies. You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

If you wish to exercise any of the rights set out above, please contact us through our DPO.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request, subject to applicable laws, and in such instance, we shall furnish you with a formal notification in this regard. A copy of such refusal notice shall also be provided to the NITDA.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

We try to respond to all legitimate requests within a reasonable time. Occasionally, it could take us longer time if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

2.9 Changes to Data Privacy Policy

This Policy may be updated from time to time and we shall notify you of any changes thereon via a notice on our website. It is also important that the personal data we hold about you is accurate and current. In view of this, we encourage you to always update your personal data and keep us informed if there are changes to your personal data during your relationship with us.

2.10 Data Protection Officer

To ensure that any concerns you may have regarding the protection of your personal data is addressed sufficiently and timeously, we have appointed a DPO who is responsible for overseeing questions in relation to this Policy.

Without prejudice to any other provisions of this Policy, if you have any questions about this Policy or our privacy practices, including any requests to exercise your legal rights which have been specified in this Policy, please contact the DPO using the details set out below:

Attention: **The Data Protection Officer, Mouka Limited (Keji Ojelade)**

Postal address: **Plot 'M' Awosika Avenue, Ikeja, Nigeria**

Email address: data.protection@mouka.com

Telephone number: **+234 0908 756 6612**

Without prejudice to your right to make a complaint at any time to the NITDA, the supervisory authority for data protection issues (www.nitda.gov.ng) for any alleged breach of your data privacy rights, we would appreciate that you contact us in the first instance through the DPO if you have any concerns regarding the protection of your data or this Policy.

3.0 Breach

In the event of a personal data breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Company shall within a reasonable time of becoming aware of the breach:

- promptly assess the risk;

- promptly notify the affected data subject;
- take all necessary measures and steps to ensure that further damage is not caused by the breach;
- take all steps to retract the data (in cases of unauthorised access or disclosure); and
- if appropriate, report the breach to NITDA.

4.0 DEFINITIONS

In the Regulation, unless the context otherwise requires:

- a) **“Act”** means the NITDA Act of 2007;
- b) **“Computer”** means Information Technology systems and devices, whether networked or not;
- c) **“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, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- d) **“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 is stored in any format or any device;
- e) **“Database”** means a collection of data organized in a manner that allows access, retrieval, deletion and procession of that data; it includes but not limited to structured, unstructured, cached and file system type databases;
- f) **“Data Administrator“** means a persons or organization that processes data;
- g) **“Data 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;
- h) **“Database Management System”** means software that allows a computer to create a database, add, change or delete data in the database; allows data in the database to be processed, sorted or retrieved;
- i) **“Data Portability”** means the ability for data to be transferred easily from one IT system or computer to another through a safe and secure means in a standard format;
- j) **“Data Protection Compliance Organisation” or “DPCO”** means any entity duly licensed by NITDA for the purpose of training, auditing, consulting and rendering

services and products for the purpose of compliance with this Regulation or any foreign Data Protection law or regulation having effect in Nigeria;

- k) **“DPO”** means Mr. Keji Ojelade;
- l) **“Data Subject”** means an identifiable person; one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;
- m) **“Data Subject Access Request”** means the mechanism for an individual to request a copy of their data under a formal process and payment of a fee;
- n) **“filing system”** means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
- o) **“Foreign Country”** means other sovereign states, autonomous or semi-autonomous territories within the international community;
- p) **“Regulation”** means this Regulation and its subsequent amendments and where circumstance requires it shall also mean any other Regulations on the processing of information relating to identifiable individual’s Personal Data, including the obtaining, holding, use or disclosure of such information to protect such information from inappropriate access, use, or disclosure’
- q) **“OII”** means Object Identifiable Information
- r) **“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 and others;
- s) **“Processing”** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- t) **“Personal Data breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- u) **“Recipient”** means a natural or legal person, public authority who accepts data;
- v) **“Relevant Authorities”** means NITDA or any other statutory body or establishment having government mandate to deal solely or partly with matters relating to personal data;
- w) **“Sensitive Personal Data”** means Data relating to religious or other beliefs, sexual tendencies, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information;
- x) **“Third Party”** means any natural or legal person, public authority, establishment or any other body other than the Data Subject, the Data Controller, the Data Administrator and the persons who are engaged by the Data Controller or the Data Administrator to process personal data.

