PRESTIGE ASSURANCE PLC

PRIVACY POLICY

DOCUMENT HISTORY

VERSION	Date:
1.0	28th October 2021

BACKGROUND

Prestige Assurance Plc (hereinafter referred to as Prestige) is committed to ensuring that the privacy and personal information of its clients and employees (data subjects) are protected. The company is the entity that collects and processes your personal information and the responsibility is not outsourced to any third party. The company is also responsible for complying with extant Nigerian and applicable international laws on data protection. For the purpose of this Privacy Policy, references to Prestige or the Company shall mean Prestige Assurance Plc.

By providing the data subject's personal information or the personal information of a beneficiary from the data subject's policy, the data subject acknowledges that the company may only use the information in the manner specified in this Privacy Policy.

This Policy should be brought to the attention of any party who is included in your Insurance Policy or on whose instruction you are providing us with their personal data. By providing your personal information or the personal information of someone included in your policy, you acknowledge that we may use it only in the ways set out in this Policy. We may provide you with further notices highlighting certain uses we wish to make of your personal information.

From time to time we may need to make changes and update this Policy, for example, as the result of Government Regulation, new technologies, or other developments in data protection or laws privacy generally. Please check the company's website periodically to view the current version of this Policy (www.prestigeassuranceplc.com) and the company's mobile app.

ROLE DEFINITIONS:

The following roles are defined for the purpose of this Policy:

Data Subject: is 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 and includes the company's clients, customers, business partners, stakeholders and employees.

Data Administrator: means a persons or organization that processes data. For the purpose of this policy, Prestige Assurance Plc is the Data Administrator.

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. For the purpose of this policy, the Managing Director is the Data Controller or whoever he so delegates.

Data Protection Officer: is appointed by the data controller to ensure that the strategy and implementation of data protection requirements are in compliance with the data protection policy and the relevant extant laws.

Responsibilities of the Data Administrator, Data Controller and Data Protection Officer are clearly outlined in the Nigeria Data Protection Regulation (2019).

1. Introduction

When the company collect and process the personal information of its data subjects, the company ensures it adheres to strict controls to ensure that personal data of the data subject is obtained and used in line with the company's privacy principles. Prestige handles personal data with the greatest care and use it only for legitimate and specified business purposes under the following principles:

a. The company respects the privacy rights of its employees, customers, clients, business partners and other individuals whose personal data are in its custody and use.

b. The company protects personal data by implementing appropriate technical and organizational measures in our data processing operations.

c. The company obtains personal data fairly and only use it for legitimate business purposes.

d. The company holds itself accountable for demonstrating compliance with applicable legal and regulatory requirements and understanding of our roles and responsibilities.

All personal information collected by the company is processed in accordance with the extant data protection laws in Nigeria.

2. Type of Information Processed by Prestige

The precise nature of the personal data the company processes depends on data subject's relationship with the company. However, in many cases, if the Company is handling the data subject's personal data as part of its role as an insurer, the Company may process the following:

2.1. Information about the data subject – for example name, age, gender, date of birth, nationality. Even though in some instances the company do not receive your name, the Company needs enough information to identify the data subject and her policy so that the Company can provide services to its clients.

2.2. Means of identification - date of birth, National Identity Card Number (NIN), International Passport details, Drivers' License, Voter's card details, etc.

2.3. Contact information – in some cases, for example, the Company may receive the data subject's email, address, and phone number.

2.4. Online information – for example cookies and IP address (your computer's internet address), if you use the company's websites.

2.5. Financial information – the Company may process information related to payments the data subject makes or receive in the context of an insurance policy or claim. This includes information such as Bank Verification Number (BVN) and information obtained from credit reference agencies.

2.6. Contractual information – for example details about the policies a data subject holds and with whom the data subject holds them.

2.7. Health information such as smoker status or medical related issues relevant to a policy the data subject holds or a claim the data subject has made.

2.8. Other sensitive personal data (Health background / information, Marital status, criminal history record, Biometric details, Academic records, and Gender)

3. Requirement for Consent

3.1. Where data subjects provide their consent for use of their personal information, the company will explain the reason for obtaining the data subject's consent. Without such consent, the company may be unable to provide the required cover or handle claims when they arise. Where the data subject provides personal information about third parties, the company will ask such clients to confirm that the third party has given consent to the data subject to act on their behalf and will provide the company with a copy of the consent issued.

3.2. Consent will be obtained via the same medium used to obtain personal information or through any other means that is acceptable to the company. Reference will be made to this Policy or a summarized version that can be easily understood by the data subject. The data subject will be required to indicate understanding and acceptance of the terms contained in the policy. This can be via signature for physical documents or a ticked checkbox for electronic platforms.

3.3. Where the company has appropriate, legitimate business need to use client personal information for maintenance of business records including development and improvement of products and services, the company will take extra care to ensure that the data subject's rights to security and confidentiality is not infringed upon.

4. Reasons for use and process of data by Prestige

4.1. The company will obtain the consent of the data subject before use and processing of the data for one or more specific purposes made known to the data subject.

4.2. Such personal data obtained with the consent of the data subject shall not be used in any manner other than the stated purpose for which the data was obtained, except with further consent of the data subject whether at the instance of the data subject or upon the company's engagement with the data subject.

4.3. The company may use data subject's personal data for a number of reasons:

4.3.1. Underwriting our business with our clients

4.3.2. Managing claims

4.3.3. Assessing, improving and developing our services

4.3.4. Enhancing our knowledge of risk and insurance markets in general

4.3.5. Fulfilling legal or regulatory obligations and protecting ourselves and our clients against fraud. Such regulators includes National Insurance Commission (NAICOM), National Financial Intelligence Unit (NFIU) and such other regulatory agencies that is created from time to time.

4.3.6. For the protection of public interest such as investigation of fraudulent claims and anti-money laundering checks.

4.3.7. For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

4.3.8. For the purpose of assessment of proposed data subject's employability and other employee benefits-related purposes.

4.4. The company applies information protection technologies including perimeter security, malware management, data loss prevention as well as backup and

recovery. The company's data centres are also protected against environmental threats. The Company's information security policies and practices apply to all personal information in the company's custody.

4.5. The company will only transfer personal information to a third party where the company has ensured that such information is protected, and the data subject's consent has been obtained. The Company will procure the privacy policy of the Third Party to guarantee the safeguard and protection of the personal data of the data subject in the custody of the third party. 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 conducts.

5. Methods of collecting private information

5.1. In most cases, the Company receives personal data from third parties such as its corporate clients and may also receive personal data directly from the data subject.

5.2. The following shall comprise the method of collection of personal information:

5.2.1. Direct collection:
5.2.1.1. Know Your Customer (KYC) forms
5.2.1.2. Claim forms
5.2.1.3. Forums and feedback forms
5.2.1.4. Enquiry and Quote forms
5.2.1.5. Recorded telephone conversations
5.2.1.6. Digital touch points
5.2.1.7. Electronics means (emails and apps)
5.2.1.8. Employee engagement personal data forms (inclusive of medical report)

5.2.2. Third parties data collection source:

5.2.2.1. Individuals or employers who has policies with the company under which a data subject is insured i.e. a named individual within a personal accident insurance policy.
5.2.2.2. Credit reference agencies including credit ratings.
5.2.2.3. Family members in the event of incapacitation or death of the insured for purpose of claims payment
5.2.2.4. Medical professionals and hospitals
5.2.2.5. Aggregators
5.2.2.6. Loss adjusters, claim assessors, etc.

Provided that in the case of data obtained from third parry source, a copy of the data subject's consent given to the third party to transfer the data to Prestige shall suffice for the company's use and processing.

6. Prestige's Use of Cookies

6.1. The company's websites use cookies to track browsing history of visitors to improve their experience. The company's websites provide visitors an option to accept the use of cookies during the browsing session. Consent must be received before any form of data processing can be performed. Every consent given by a data subject will be kept secured as evidence that consent was received.

6.2. In the case of the company's customers, the data subject will provide consent by responding to a dialogue box corresponding to declarations indicating whether consent is given or declined. Such declaration will be in clear and plain language. For children's personal data, consent will be sought from their legal guardian.

7. Social Media Platforms

7.1. The data subject may wish to participate in the various blogs, forums, and other social media platforms hosted by the company ("Social Media Platforms") which are make available to the data subject. The main aim of these Social Media Platforms is to facilitate and allow the data subject share content. However, the company cannot be held responsible if the data subject shares personal information on Social Media Platforms that is subsequently used, misused or otherwise appropriated by another user. The data subject is required to consult the Privacy Statements of such services before using them.

8. Third Party Access and Purpose of Access

8.1. Disclosure to Employees

8.1.1. The company's employees have access to and process personal data based upon a "need to know" basis in order to do their jobs. The Company regularly check who has access to its systems and data.

8.2. Disclosures to Third Parties

8.2.1. The company may disclose data subject's personal data to these categories of third parties:

8.2.1.1. The company's service providers and agents e.g. IT companies who support the Company's technology, marketing agencies, research specialists, document management providers and tax advisers.

8.2.1.2. The company's professional advisers: auditors; reinsurers; medical agencies and legal advisers.

8.2.1.3. Client who provide the Company with data subject's personal data.

8.2.1.4. Persons legally authorized to act on behalf of the Company e.g. Lawyer, Insurance Broker and loss adjusters, etc.

8.2.1.5. Individuals nominated and authorized by the data subject to engage the company on his/her behalf.

8.2.1.6. The company's recommended garage or other service provider recommended to the data subject.

8.2.1.7. Disclosure to Credit referencing organization to obtain information which may be used by the Company to determine its risk selection, pricing and underwriting decisions.

8.2.1.8. Fraud detection agencies and other parties who maintain fraud detection registers.

8.2.1.9. Customer relationship management

8.2.1.10. Independent Customer satisfaction survey providers.

8.2.1.11. Financial organizations and advisers.

8.2.1.12. Government and its agencies.

8.2.1.13. Emergency assistance Companies.

8.2.1.14. Credit reference agencies.

8.2.1.15. Debt collection agencies.

8.2.1.16. Selected third parties in connection with the sale, transfer or disposal of the business or in connection with employee assessment, academic records verification and employee well-being survey.

The above disclosures to the third party shall be made only to the extent necessary for the specific purpose for which the data is provided and the third party shall be informed of the confidential nature of such information and shall be directed to keep the data subject's information strictly confidential.

9. Lawful Processing of Personal Data

9.1. The company only processes personal data for legitimate business purposes and when a legal ground as set out in data protection regulation.

9.1.1. There are a number of legal grounds that may apply and the following ones most likely to be relevant to the data subject:

9.1.1.1. The company may process the personal data of the data subject when the Company obtains the data subject's consent or when the Company's client obtains consent from the data subject.

9.1.1.2. Where the data subject has a contract with the Company, the personal data of the data subject may be processed when it is necessary in order to enter into or perform a contract.

9.1.1.3. Where the Company has a legal obligation to perform such processing, such as where the Company shares information with its regulators, law enforcement agencies or court.

9.1.1.4. In order to protect the vital interests of the data subject or of another natural person.

9.1.1.5. In order to process the data subject's medical and other sensitive personal data when it is necessary to do so in connection with an insurance product.

9.1.1.6. Where the company is required to do so by law or regulatory bodies such as where a Court Order exists to such effect or there is a statutory obligation to do so.

9.1.1.7. Where it is necessary to facilitate prevention and/or detection investigation of criminal action (including fraud) or is otherwise in the overriding public interest.

9.1.1.8. Where exemptions under the Data Privacy law allows the company to disclose such information.

9.1.1.9. Motor insurance database i.e. Nigeria Insurance Industry Database (NIID).

9.1.1.10. Where processing is necessary for the performance of a task carried out in the public interest or in the exercise of public mandate vested in the company.

9.1.2. Another legal ground for processing personal data is when the company has a legitimate interest in so doing and can demonstrate that the interests are not outweighed by the data subject's rights or interests. Where the company relies on legitimate interests' grounds for processing, the company will make sure it processes only the minimum amount of data necessary and for the minimum amount of time necessary to achieve its objectives which includes:

9.1.2.1. To enable the company identify whether its products or services are operating effectively;
9.1.2.2. To enable the company develop new products and services and make sure its offerings are fair;
9.1.2.3. To enable the company ascertain that its clients and policy holders are treated fairly.

The following table contain breakdown of lawful grounds which the company relies on for processing personal information of its clients:

S/N	Purpose for collection and processing of data subject's personal information	Collectable Personal information includes but not limited to the ones set out below	Legal grounds for processing personal information
1	Reviewing an insurance proposal in order to provide a quote in respect of the proposal.	• Contact details, age, age of other persons included on the policy (e.g. employees, family members, etc.) • Information on the subject of insurance such as landed property, vehicles, past claims, recent damage, business premises, etc. • Information on travel plans including destination, duration of stay, travel dates, etc. • Information on nature of commercial enterprise and assets. • Sensitive personal information such as health records. • Any other information relevant to the request.	The use described is necessary for the provision of insurance cover. Where sensitive personal information is requested, exemptions may be applied for insurance purposes.
2	To provide and manage insurance policies. To evaluate the eligibility for claims processing and claims payment.	• Contact details, age, age of other persons included on the policy (e.g. employees, family members, etc.)	The use described is necessary for provision of insurance cover. Where sensitive personal information is requested,

		• Information on subject of insurance such as landed property, vehicles, past claims, recent damage, business premises, etc. • Information on travel plans including destination, duration of stay, travel dates, etc. • Information on the nature of commercial enterprise and assets. • Sensitive personal information such as health records.	exemptions may be applied for insurance purposes.
3	For data subject's communication and resolution of complaints.	Contact details and any information relevant to the policy.	The use described is required to provide the insurance cover and to resolve any legitimate concerns. Where sensitive personal information is requested, it may be necessary for the exercise and defence of the company's legal rights, where the client has provided consent or where we have applied and obtained exemption for insurance purposes.
4	To evaluate insurance applications and data subject's ability to pay premiums in instalments or as at when due.	Contact details, bank account details, collateral information	Necessary to provide insurance cover.
5	To prevent, detect and investigate fraud. This may include collection of biometric information such as voice prints.	Contact details, age, age of other persons included on the policy (e.g. employees, family members, etc.) Information about possessions such as landed property, vehicles, past claims, recent damage, business premises, etc.	Necessary to provide insurance cover and a legitimate business need to prevent fraud. Where sensitive personal information is requested, it may be necessary for the exercise and defence of the company's legal rights, where the data subject has provided consent or where we have applied

		Information about travel plans including destination, duration of stay, travel dates, etc. Information about nature of commercial enterprise and assets. Information available in the public domain such as social media. Sensitive personal information such as biometrics (i.e. voice print).	and exemption for insurance purposes.
6	For the purpose of debt recovery.	Contact details, bank account details, collateral information.	Where there is a legitimate business need for debt recovery. Where sensitive personal information is requested, the use described is necessary for establishing, exercising or defending the legal rights of the company.
7	For the purpose of our own information systems management including; management of business processes such as maintaining financial and accounting records, analysis of financial results, internal and external audit requirements, receiving professional advice (e.g. tax or legal advice). We develop policies and security systems to ensure security and effective operation of our systems.	Information about the client including name, residential / office address, email address, telephone number, age and the age of other person(s) included on the policy (family members, business partners, employees). Sensitive personal information about health or beneficiaries' health.	The company has a legitimate business need to use its client's personal information to understand its business, monitor performance and maintain appropriate records. Where sensitive personal information is provided, the information is used to determine if an exemption should be applied for Insurance purposes.
8	For research and analytical purposes and to improve our products and services.	Contact details, age, age of other persons included on the policy (e.g. employees, family members, etc.) Information about possessions such as landed property, vehicles, past claims, recent	Research and data analytics are conducted for service improvement purposes in the interest of the data subject. Where sensitive personal information is provided, the company may apply an exemption for insurance purposes where appropriate.

		damage, business premises, etc. Information about travel plans including destination, duration of stay, travel dates, etc. Information about nature of commercial enterprise and assets. Sensitive personal information such as health records.	
9	Compliance with legal and or regulatory obligations	Details about the data subject, other related parties, specific product required by the data subject, service or benefit, depending on the nature of the obligation.	Necessary for the company to comply with Legal and Regulatory obligations.
10	Providing improved quality, training and security (for example, with respect to recorded or monitored phone calls to our contact numbers); technology may include voice analytics	Details about our clients and other related parties, product or service having been discussed with the client or representative during a telephone conversation with the company.	The use described is required for Legal and Regulatory compliance.
11	Providing marketing information to the company's clients including information about other products and services and undertaking customer surveys in accordance with preferences communicated by the data subject.	Name, contact details and marketing preference.	Data subject's consent.
12	Determination of employability, background check up, academic records verification, and employee surveys and other HR processes requiring personal identifiers.	Name, contact details, academic records, health background / information, Marital status, criminal history record, Biometric details, Academic records, and Gender	To determine employability and to improve employee wellbeing, insurance contracts and regulatory demands.

10. Foreign Transfer of Personal Data

10.1. The transfer of a client's personal information may be to a third party in a foreign country which has adequate data protection laws for data transfer, to be determined by the Attorney General of the Federation and the Data subject shall have the right to be informed of the appropriate safeguards for data protection in the foreign country.

10.2. Where the Attorney General of the Federation has not determined the third party country, the data subject's personal information may be transferred to a third party in a foreign country in the following circumstances:

10.2.1. Where the data subject has consented to the proposed transfer after having been informed of the possible risks of such transfers

10.2.2. The transfer is for the performance of a contract between the data subject and the data controller

10.2.3. The transfer is for the performance of a contract concluded in the interest of the data subject between the Data Controller and another natural or legal person

10.2.4. The transfer is for public interest

10.2.5. The transfer is for the establishment exercise or defence of legal claim

10.2.6. The transfer is to protect the vital interest of the data subject or other persons, where the data subject is physically or legally incapable of giving consent.

The data subject shall have the right to be informed of the appropriate safeguards for data protection in the foreign country.

11. Length of time for keeping client's personal information

The company shall keep data subject's personal information for as long as reasonably necessary to fulfil the relevant purposes set out in this Policy and in order to comply with our legal and regulatory obligations and subject to the Limitation Act in force in Nigeria. This includes keeping the data subject's information for a reasonable period of time after the data subject's relationship with the company or its client has ended and particularly for statistical analysis, pricing and risk modelling purposes.

In certain instances, the company will minimize personal data; or de-identify data for use in statistical or analytical activities. This is undertaken in accordance with the data protection laws.

12. Data Subject's Rights

12.1. The company shall disclose the specific purpose for which the information is required before obtaining the information from the data subject and shall inform the data subject of his/her right and method of withdrawal of consent.

12.2. The data subject has the right to request that the company perform certain activities on his/her personal information, such as request for a copy of their personal information, correction of errors on the personal information, a change in the use of their personal information, or delete their personal information. The company is obligated to either carry out the data subject's instructions or explain why it may not be possible - usually because of a legal or regulatory issue.

12.3. Data subject have the following rights in respect of the company's use of their personal information:

12.3.1. **Right to access**: The data subject has a right to a copy of their personal information as maintained by the Company

12.3.2. **Right to rectify**: The company takes due care to ensure that the personal information we maintain about data subjects are accurate and complete. However, if a data subject believes the information is inaccurate or incomplete, such data subject has the right to request an amendment.

12.3.3. **Right to erase**: under certain circumstances, a data subject may ask that the company erase their personal information. For instance, where the personal information collected is no longer necessary for the original purpose or where consent is withdrawn. However, this will need to be balanced against other factors, such as the type of personal information obtained, the original reason for collection, archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, and the company continuous assessment of risk relating to the data subject. There may be some legal and regulatory obligations which prevents the company from complying immediately.

12.3.4. **Right to restriction of processing**: under certain circumstances, but subject to regulatory requirements, a data subject may be entitled to instruct the company to stop using his/her personal information. This is applicable where:

a. A data subject contests the accuracy of personal information held by the data controller

b. Processing of personal data of the data subject is unlawful

c. The data controller no longer requires the personal data but the data is required by the data subject for establishment, exercise or defence of legal claims

d. The data subject has objected to processing, pending the verification whether the legal grounds for the data controller override those of the data subject.

12.3.5. **Right to data portability**: under certain circumstances, data subjects have the right to ask that the company transfers any personal information that they have provided to the company to another third party. Once transferred, the other party will be responsible for safeguarding such personal information.

12.3.6. **Right to object to marketing**: Data Subject can object to the processing of his/her personal data for the purposes of third-party marketing

12.3.7. **Right to lodge a complaint**: The company data subject has the right to lodge complaints, in the event that there is an objection to the manner in which personal information is being used by the Company. Such complaints can be communicated using contact details provided in our policy documentation. In certain cases, the company may be unable to comply with data subject's requests for reasons such as our own obligations to comply with other legal or regulatory requirements. However, the company will always respond to complaints and where compliance is not feasible, an explanation will be provided.

12.4. The Data Controller shall communicate any rectification or erasure of personal data or restriction to each recipient to whom the data the personal data has been disclosed, unless this proves impossible or involves disproportionate effort.

12.5. In some circumstances, exercising some of these rights will mean the company is unable to continue providing cover under the data subject's insurance policy and may therefore result in cancellation of the policy. The data subject will therefore lose the right to bring any claim or receive any benefit under the policy, including in relation to any event that occurred before the right was exercised, if the company's ability to handle the claim has been prejudiced. Each data subject's policy terms and conditions set out what will occur in the event of a policy cancellation.

12.6. Some of the company's assessment of risks are made automatically by inputting the data subject's personal information into a system, the criteria of which is determined by the company's underwriting team and the decision is then calculated using certain automatic processes rather than manual process via discussions. We make automated decisions in the following situations:

12.6.1. Premium computation: we use the data subject's personal information to determine premium and eligibility.

12.6.2. Fraud and money laundering prevention: The company uses automated anti-fraud and money laundering filters that check against global databases individuals known to have undertaken fraudulent and / or money laundering transactions and will reject those applicants based on outcomes of the automated checks.

12.7. Application assessment: The company may use scoring methods to assess applications, perform identity verification and determine premiums. Examples of information used by the company systems to do this include age, address, lifestyle (e.g. smoking, drinking, exercise routines, etc.) and medical history. If a data subject does not consent to processing sensitive information in this manner, the company may be unable to assess the application or provide a quote. Alternatively, the company may only be able to offer the data subject policies that do not require the company to have that information from the onset. The automated decision making performed by the company systems during the application is proprietary to the company, and the results thereof is not shared with third parties.

12.8. Where the data subject chooses to opt out of automatic decision-making, a formal communication to that effect will suffice. However, in some situations, it may imply that the company will be unable to offer a quote because automated decisions are necessary to price and issue certain policies.

Data subjects can enforce the above rights by sending an email to info@prestigeassuranceplc.com. The Data Controller is obligated to act on the request of the data subject without delay. In the event that the Data Controller does not take action on the request of the Data Subject, the Data Controller shall within one month of receipt of the request, inform the data subject of the reasons why the request has not been actioned.

The exercise of the rights listed above shall be in conformity with constitutionally guaranteed principles of Law for the general protection and enforcement of Fundamental Rights.

13. Training

13.1. The company's employees are the most important element of the company's commitment. Prestige's employees are involved in every step of the data

lifecycle, including sourcing and receiving personal data, processing it in compliance with laws and regulations, employing safeguards, and establishing the means and schedules of retention and deletion. It is therefore imperative that the company's employees understand their role and be committed to safeguarding personal data.

13.2. The company designs its training programme to be relevant, focused on the individual and also focused on concrete risks. Prestige runs regular data protection and information security awareness campaigns. The Company also share with its employees' other knowledge resources on data protection and privacy topics, including guidance on ways that they can better protect and safeguard personal privacy.

13.3. It is important that the company's employees understand the seriousness of protecting personal data and respecting privacy rights with the ability to relate this back to the risks and consequences from an individual perspective. Through the company's efforts, it remains committed to realize its goal to ensure its employees and business partners understand their respective roles and responsibilities for data protection compliance.

14. Marketing

14.1. The data subject reserves the right to the use of his/her personal information for marketing and the company shall obtain the consent of the client prior to using such information for marketing purpose in specific cases not covered under this policy.

14.2. The company shall be committed to only send its data subjects insurance marketing communications that meets the needs and behaviours of the data subject. Where the data subject chooses to unsubscribe from our mailing lists, such can be achieved at any time by following the unsubscribe instructions that appear in all marketing emails or contact the company via the details set out in this policy documents.

14.3. Periodically, the company may run specific marketing campaigns through social media and digital advertising that the data subject may see which are based on general demographics and interests. Individual personal information is not used for these campaigns. Should a data subject not want to see such campaigns, the data subject shall be responsible for adjusting preference settings within the specific social media platform including cookie browser settings

14.4. The company may retain any data provided on its website and mobile app for a reasonable period, subject to the client's prior approval, even if the contract is not consummated and such information may be used to make enquiry on why the contract is not consummated.

15. Audit and Enforcement of the Data Protection Policy

The Internal Audit Department of the Company shall conduct the periodic audit of the privacy and data protection practice within the Company, in accordance with the Nigeria Data Protection Regulation. The Internal Auditor is the Data Protection Officer, shall be responsible for compliance with the Regulation and sends the periodic Audit Report to the Agency.

16. Remedies for Violation of Data Protection Policy and the Timeframe for Remedy

16.1 In the event of violation of this policy, the data controller shall within 15 days redress the violation. Where the violation pertains to the disclosure of the data subject's information without his/her consent, such information shall be retracted immediately and confirmation of the retraction sent to the data subject within 48 hours of the redress.

16.2 Where the violation is caused by any representative of the data controller, such representative shall be subject to appropriate sanction.

17. Amendments

This Policy may be amended from time to time by the Board.

18. Contact details of the Data Controller and Data Protection Officer

Prestige Assurance Plc.
C/O The Internal Audit Department
No. 19, Ligali Ayorinde Street,
Victoria Island, Lagos,
Enquiries: 0805-882-0333, 0805-883-0333
Email: info@prestigeassuranceplc.com
Website: www. prestigeassuranceplc.com

You have a right to complain to the Information Regulator if you think that your information has been misused. The contact details are:

National Information Technology Development Agency
Tel: +234929220263, +2348168401851, +2347052420189
Website: www.nitda.gov.ng

Adopted by the Board on 28th October 2021.