SOVEREIGN TRUST INSURANCE PLC

DATA PROTECTION POLICY

Code of Practice on Data Protection for Sovereign Trust Insurance Plc.

(Mandated by the National Information Technonoly Development Agency {NITDA} Data Protection Act of 2007)

1. Introduction

Data Protection is the means by which the privacy rights of individuals are safeguarded in relation to the processing of their personal data. The National Information Technology Development Agency (NITDA, hereinafter referred to as The Agency) is statutorily mandated by the NITDA Act of 2007 to, inter alia; develop regulations for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper-based methods in government, commerce, education, the private and public sectors, labour and other fields, where the use of electronic communication may improve the exchange of data and information.

The Data Protection Code of Practice for Sovereign Trust Insurance Plc. sets out the requirements of the Data Protection Acts, how personal information is processed by the Organization and it must comply with the legislation when collecting, handling and storing personal data.

This Code of Practice will be reviewed and updated, as required, to include any changes to the type of data collected and processed by the Company.

2. Scope and Application of Code of Practice

This Code of Practice is intended to confirm and clarify the nature of STIPLCs' responsibilities as "data controllers" under NITDA Data Protection legislation. The Code is divided into nine main sections; the first eight consist of the "eight rules" of data protection.

This Code applies to all personal data held by or on behalf of STIPLC. This includes data relating to persons who hold policies (or who have applied for or held policies in the past) and any other individual whose claim is being assessed, processed or negotiated under a policy issued by STIPLC.

3. Data Protection Rules

The "Eight Rules" of Data Protection require that a data controller must:

1. Obtain and process the information fairly
2. Keep it only for one or more specified and lawful purposes
3. Process it only in ways compatible with the purposes for which it was given to you initially
4. Keep it safe and secure
5. Keep it accurate and up-to-date

6. Ensure that it is adequate, relevant and not excessive
7. Retain it no longer than is necessary for the specified purpose or purposes
8. Give a copy of his/her personal data to any individual, on request

3.1 ***DATA PROTECTION RULE 1:***

OBTAIN AND PROCESS INFORMATION FAIRLY

STIPLC will obtain personal data from application forms, claim forms and other documentation completed or provided by the individual as well as through call centres or electronically e.g. by point of sale systems or over the internet. Personal data may be kept on computer systems and/or in paper files.

The collection of data by Sovereign Trust Insurance Plc happens at three main stages:

A. At application or proposal stage:

In order to assess the risk and determine the premium including any special provisions and to comply with the relevant identification and other requirements of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2012 as ammended and Central Bank of Nigeria Act of 2007, as amended (hereinafter referred to as the CBN Act) and the Banks and Other Financial Institutions Act of 2007, as amended [the BOFIA], Insurers request appropriate and relevant information in line with the particular product or service, such as:

- information about the proposer's health,
- Information regarding financial situation and goals,
- driving history,
- claims experience and
- other information to comply with specific legislative requirements.

B. During the term of the policy:

- Administration of policyholder information by the insurer, including information collected at renewal and for payment of premiums while the policy is in force and secure holding of information after cessation of the policy which is required to be retained in line with Consumer Protection Code retention requirements; and

C. When claims are made:

- STIPLC may again other relevant and appropriate information in order to assess whether a claim is payable under the policy, and if so, what amount should be paid.

Data Protection Rule 1 requires that:

At the time of providing personal information, individuals are made fully aware of:

- the identity of the persons who are collecting it (though this may often be implied)
- to what use the information will be put
- the persons or category of persons to whom the information will

be disclosed. Secondary or future uses, which might not be obvious to

individuals, should be brought to their
attention at the time of obtaining personal data. Individuals should be given the option of saying
whether or not they wish their information to be used for the purpose of direct marketing.

If a data controller has information about individuals and wishes to use it for a new purpose (which was not disclosed and perhaps not even contemplated at the time the information was collected), he or she is obliged to give an option to individuals to indicate whether or not they wish their information to be used for the new purpose.

To comply with this rule, STIPLC will:

- Include on application forms, or other appropriate documentation, a clear statement advising the applicant of the identity of the data controller, the purpose of collecting the data, to whom it may be disclosed and any other relevant information necessary to ensure that all processing meets the requirements of fair processing. The policies notice will be reflective of the template at Appendix II.

- Make available an appropriate fair processing notice at a suitable point in the business process to third party claimants who would not otherwise have received information that could be deemed to provide for fair processing of their personal data, e.g., when responding to their solicitor or if the claim has been dealt with entirely over the phone upon issuing the claim cheque. The notice will be reflective of the template at Appendix II.

- Where other information sources are used to independently verify information provided by the insured (e.g. industry databases of claims information), STIPLC will ensure that a reference to the existence and purpose of any industry databases which could be consulted is included in relevant customer documentation. Where the Insurance Link database is to be accessed as part of the underwriting process, the customer must be made aware of this at point of sale and prior to underwriting. Information about the processing of personal data in the Insurance Link claims database should be reflective of the relevant text included in the template at Appendix II.

- Make customers who are seeking to add a named driver to a policy aware of their responsibility for ensuring that the consent of the named driver for the processing of his or her data by the insurer has been fully and fairly obtained. Personal data may be obtained from the customer or someone acting on their behalf (e.g. an insurance intermediary or an employer).

- Have a written privacy policy setting out clearly for what purposes personal data is processed and will ensure that a privacy statement appears on websites where personal data is collected.

- Ensure that callers are advised that telephone conversations are recorded, when this is the case, and the purposes for the recording. This rule also applies to the recording of outbound calls if applicable.

- Capture the explicit consent of the data subject to the processing of their personal data where STIPLC need to collect sensitive personal data (e.g. data relating to physical and mental health and criminal convictions), unless the processing is otherwise permitted under another enactment. Appropriate security measures should be put in place to ensure the confidentiality of the data.

- Make it clear on application or claim forms that personal information may be sought from other insurance companies who hold a policy or other relevant information about a risk, insurance companies must make it clear that such data will be sought and obtain the customer's acknowledgement of this. Where the information to be disclosed is sensitive data, the explicit opt-in consent of the individual must be in place before the disclosure takes place.

- In respect of Motor insurance policies, only require the provision of personal data of potential claimants in the following circumstances:

  a) At a pre-claim stage in compliance with a specific legal obligation such as that contained in the Road Traffic Acts or,

  b) when the guidelines set out in **Appendix IV** are adhered to.

- Where relevant, mention in customer documentation that a private investigator may be instructed by STIPLC to investigate a claim. STIPLC will use licensed private investigators and contractually engage the private investigator on the basis that the private investigator will comply with applicable Data Protection legislation. Instructions to private investigators should clearly state the investigations to be undertaken at the insurer's request. Insurers will have a written agreement in place with private investigators so that there is a compliant disclosure of personal data from the insurance company or its agents, as appropriate, e.g. its solicitors to the

private investigator and vice versa. Such contracts shall ordinarily include terms reflecting those set out in the Appendix I to this Code.

Personal data will be processed only in accordance with the provisions of Data Protection legislation and this Code.

3.2 ***DATA PROTECTION RULE 2:***

KEEP IT ONLY FOR ONE OR MORE SPECIFIED, EXPLICIT AND LAWFUL PURPOSES

Data Protection Rule 2 requires STIPLC to keep personal data for purposes that are specific, lawful and clearly stated. Insurers are required to register on an annual basis with the Office of the Data Protection Commissioner. As part of their registration requirements, Insurers include in their register entry a statement of their purpose(s) for holding personal data. If Insurers keep or use personal data for any purpose other than the specified purpose, they may be guilty of an offence.

Primary acceptable uses of personal information by STIPLC include:

- where relevant, personal information is used to arrange, provide advice and/or to recommend insurance products;
- the underwriting of the risk proposed;
- the administration of the policy;
- the assessment and processing of any claims arising under the policy;
- compliance with regulatory, legal and tax laws and regulations; and
- participation in internal or market-level statistical exercises.

Secondary purposes/uses of personal information by STIPLC include the direct marketing of
products to existing and potential customers. A table outlining direct marketing requirements is provided at Appendix V.

3.3 ***DATA PROTECTION RULE 3:***

USE AND DISCLOSE IT ONLY IN WAYS COMPATIBLE WITH THESE PURPOSES

STIPLC will ensure that any use and disclosure must be necessary for the purposes or compatible with the purposes for which the data is collected or otherwise in compliance with Data Protection legislation.

Examples of where Personal information may be disclosed in compliance with this Rule include the following:

- persons acting on the customer's behalf e.g. insurance intermediaries, loss assessors, solicitors, executors, etc;

- the Financial Services, the Pensions, the Central Bank or any equivalent

foreign supervisory or complaints body to whom a complaint has been made;

- other group companies (subject to disclosure of this fact to the customer);
- other insurance companies, where this is clearly stated on the application or claim form or other correspondence with a claimant. In the unlikely event of a mismatch occurring which results in the accidental disclosure of information to another insurer, the information will be destroyed immediately upon receipt, once this issue is known;
- the Nigeria Insurance Association (NIA), or its agents, which administer several industry databases on behalf of its member companies
- the Revenue Commissioners or any other person authorised by law to access customer records. Such requests should be in writing to the Insurer and quoting the legal basis for seeking access to the personal information;
- agents of the insurer e.g. loss adjusters and other external investigators, medical practitioners, firms responsible for computer maintenance or similar services, solicitors, other subcontractors or advisers, etc; and
- reinsurers.

3.4 ***DATA PROTECTION RULE 4:***

KEEP IT SAFE AND SECURE

To comply with Data Protection Rule 4, Insurers will ensure that appropriate security measures are taken against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction.

In particular Insurers will ensure that:

- Appropriate procedures are in place in relation to back-up of data.
- Particular focus is placed on the security of personal data held on portable devices, with appropriate security measures such as encryption applied.
- Robust procedures for limiting access to personal data are in place and that staff are aware of these limits.
- An appropriate external access policy is in place to ensure that only the data subject or their clearly chosen representative has access to their personal data during the course of a policy or claim.

- A confidentiality policy is in place pertaining to the collection, processing, keeping and use of medical and sensitive data.

- Access to sensitive data is restricted to authorised staff. In particular it is expected that access to sensitive medical information should be restricted to relevant underwriters, claims assessors and persons needing to access a particular file as part of their role.

- An appropriate data security breach policy is in place which adheres to the Personal Data Security Breach Code of Practice as published by the NITDA

It is the position of the Data Protection Commissioner that, on a going forward basis, IT systems should ensure that access to personal data can be logged and audited, that this should include access on a read-only basis and that such logs should be routinely checked on a random basis to ensure that access is appropriate.

3.5 ***DATA PROTECTION RULE 5:***

KEEP IT ACCURATE, COMPLETE AND UP-TO-DATE

To comply with this Data Protection Rule 5, Insurers:

- must ensure that data is kept accurate, complete and up-to-date in accordance with the provisions of the Data Protection Acts.

- will correct any factually inaccurate personal data in line with the Data Protection Acts including where this is identified by the data subject to be the case in a verifiable way.

- will have appropriate procedures in place to check the accuracy of information following its entry.

3.6 ***DATA PROTECTION RULE 6:***

ENSURE THAT IT IS ADEQUATE, RELEVANT AND NOT EXCESSIVE

To comply with Data Protection Rule 6, STIPLC will not collect any more information than is necessary for the purposes for which personal data can be used described at 3.2 above and the method of seeking information from customers will be checked on an ongoing basis to ensure that only relevant information is sought and collected.

STIPLC will comply with all other relevant statutory obligations, e.g., duties under the Equal Status Act to use only underwriting criteria which can be justified on commercial or actuarial grounds.

3.7 ***DATA PROTECTION RULE 7:***

RETAIN IT FOR NO LONGER THAN IS NECESSARY FOR THE PURPOSE OR PURPOSES

In order to comply with Data Protection Rule 7 Insurers will have a written data

retention policy. Insurers will also adhere to and include in their written data retention policy the retention periods andretention guidance outlined in this section:

Retention periods for Policyholder Information:
Policyholder information will be held for a period of at least **6 years** after the ending of the client/insurer relationship to take account of the insurer's responsibilities under the Statute of Limitations, the Central Bank of Ireland's Consumer Protection Code and relevant provisions of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2012 as ammended.

Limited policyholder information may be held, in narrow circumstances, for longer periods by STIPLC for the investigation of future claims.

Retention periods for personal information collected as part of the quotation process but where the policy was not incepted:
Where STIPLC provides a quotation but the policy was not subsequently incepted and the customer was given an opportunity not to receive direct marketing during the quotation process, the information provided may be used to direct market the customer the following year. The customer can be contacted again in subsequent years as long as they are given an opportunity to opt out at each contact and do not avail of this opportunity. Where a policy quote is not incepted, the quote can only be kept for **15 months** to check against fraudulent applications.

3.8 ***DATA PROTECTION RULE 8:***

GIVE A COPY OF HIS/HER PERSONAL DATA TO THAT INDIVIDUAL, ON REQUEST

In order to comply with this Rule, STILPC have procedures in place to ensure that written requests made pursuant to Section 3 or 4 of the Acts are dealt with in accordance with the Data Protection Acts.

October, 2019

Appendix I

Guidelines for disclosure of personal information to Private Investigators

Any processing of information by private investigators, when undertaken on behalf of STIPLC, in the context of the assessment of a claim or other similar reason must be undertaken in full compliance with the Data Protection Acts.

The private investigator shall be expected to comply at all times with the Data Protection Acts and shall not perform their functions in such a way as to cause (the insurance company) to breach any of its obligations under the Data Protection Acts.

Any unauthorised processing, use or disclosure of personal data by the private investigator is strictly prohibited.

Where the private investigator, pursuant to its obligations under contract from the insurance company, processes the personal data of a policy holder, a claimant or other person on behalf of (the insurance company), the private investigator shall:

- Process the personal data only in accordance with the specific instructions of the insurance company;
- Process the personal data only as is necessary for the fulfilment of its duties and obligations under the contract with the instructing insurance company;
- Implement appropriate measures to protect against accidental loss, destruction, damage, alteration, disclosure or unlawful access to the personal data in their possession;
- At the conclusion of each investigation deliver all data collected and processed under the contract of service to the instructing insurance company and delete all such personal data held by itself at that time;
- Not further disclose the personal data to any other party except with the express approval of the insurance company;
- Not seek to access personal data held by other data controllers which is not in the public domain without the consent of the data subject or unless otherwise permitted by law.

Appendix II

"How we treat information about you and your rights under the Data Protection Acts 2007"

In order to provide insurance cover (an insurance policy) or to pay a claim we need information about:

a) the person and / or property that we are being asked to insure
b) any third-party claimant, i.e. someone making a claim against our customer
c) property – for which repair or replacement costs are being sought under our customer's insurance policy – belonging to our customer or a third-party
d) medical and/or relevant conviction information where necessary to assess the risk

Depending upon the kind of insurance cover we are being asked to provide and the kind of claim we are being asked to pay we will seek different kinds of information. Information about people and property for which we provide insurance cover is sought by us before cover is provided. This information is kept by us and we may share your details with your intermediary, any agent authorised by you to act on your behalf and regulatory bodies. We may also share information with private investigators under an appropriate confidentiality agreement when we need to investigate a claim.

Information about claims (whether by our customers or third-parties) made under policies that we provide is collected by us when a claim is made and some details are placed on a central insurance industry database of claims. This information includes the claimant's name, address and date of birth and the type of injury or loss suffered. Through **Nigeria Insurer Association** this information may be shared with other insurance companies, self-insurers or statutory authorities. Insurers also reserve the right to use information at underwriting stage.

Insurance companies share claims data:

a. to ensure that more than one claim cannot be made for the same personal injury or property damage
b. to check that claims information matches what was provided when insurance cover was taken out
c. and, when required, to act as a basis for investigating claims when we suspect that insurance fraud is being attempted.

The purpose of the database is to help us identify incorrect information and fraudulent claims and, therefore, to protect customers.

In certain cases, where STIPLC through the Nigeria Insurance Association database identifies that a claimant has made a previous claim to another insurer, the insurers may exchange additional information about the

claimant. Appendix III details what information may be exchanged in the circumstances.1

You need to provide us with accurate and up-to-date information if you are making a claim under your own policy or, if you are a third party, a policy held by one of our customers.

Failure to provide sufficient information may prevent us from providing cover or, if you are making a claim, may delay the processing of your claim. The provision of false information may mean that a claim made by you under the policy will not be paid and may possibly result in criminal prosecution for fraud."

Appendix III

Schedule of information that may be shared between STIPLC on request from hard-copy and/or electronic files.

- Previous Address
- Nature/Description of Loss and/or Injury
- Amount paid to claimant
- Identity of Loss adjuster / public loss assessor
- Accident circumstances
- Location of accident
- Injury prognosis: fully recovered / on-going
- Motor assessors report on vehicle
- Category of write off
- Identity of claimant solicitor
- Claim settled: Yes / No
- Settled by: Injuries Board / solicitor / litigation / direct
- Date of settlement
- Details of whether legal proceedings were issued
- Contact phone number

Appendix IV

Guidelines on Requesting "Pre-Claims" Information

The "pre-claim" provision in Section 1 of the above-mentioned Code of Practice (the "Code") is as follows:

Insurance policies may require the provision of personal data of potential claimants only:

a) *At a pre-claim stage in compliance with a specific legal obligation such as that contained in the Road Traffic Acts or,*
b) *When the guidelines set out in this Appendix are adhered to.*

It is up to STIPLC to ensure it is in compliance with the "pre-claim" provision of the Code as set out in this Appendix. However, these guidelines are intended to provide high-level guidance for the organisation to consider when seeking to achieve compliance with the aforementioned "pre-claim" provision, with particular reference to employer's and public liability insurance:

- It is reasonable for liability insurance policies to require policyholders to report all incidents, irrespective of liability or the extent of the injury or damage. However liability policies should not contain conditions requiring policyholders to provide or otherwise encourage the provision of the personal data of potential third party claimants before a formal claim is made.

- Liability policyholders should not be required to supply the personal data of potential third party claimants or other individuals on accident report forms unless a third party claim has already been made or there is clear evidence that a claim is likely to be made by a potential third party claimant.

- It is reasonable to expect that a potential third party claimant will make a formal claim where the injury is substantive (i.e. requiring more than one week off work) or where initial information points to liability attaching to the policyholder irrespective of the severity of any injury or damage caused. STIPLC will process these claims in the normal way on the basis that there is clear evidence that a claim is likely to be made by a potential third party claimant.

- As an approximate guideline, a potential third party claimant may not make a formal claim where an injury is minor (i.e. requiring less than one week off work) and where initial information indicates that liability does not attach to the policyholder. Insurers should process cases falling into this category using anonymised data only on the basis that there is no clear evidence that a claim is likely to be made by the potential third party.

- Even if there is clear evidence that a claim is likely to be made by a potential third party claimant an entry must not be made on Insurance Link until a formal claim is made.

- Where the claimant is a third party and would not otherwise have received information that could be deemed to provide for fair processing of their personal data, an appropriate fair processing notice will be made available at a suitable point in the business process e.g. when responding to their solicitor or, if the claim has been dealt with entirely over the phone, upon issuing the claim cheque. The notice will be reflective of the template contained in Appendix II of the Code.