INDIAN OCEAN GENERAL ASSURANCE LTD

Data Protection Policy

Introduction.

IOGA as an Insurance company transacting general insurance business adheres strictly to the principles embodied in the Data Protection Act 2017 and Data Protection Regulations. This Data Protection Policy will be reviewed periodically and is subject to amendments and updates as and when required. Appropriate communication will be posted via our website.

IOGA is committed to processing data in accordance with its responsibilities and obligations under the Data Protection Act (DPA) of Mauritius and other relevant legislations and regulations and its internal policy incorporates other good practices in the Insurance sector. Personal data are information related to an identified or identifiable person are collected by our employees and intermediaries. Personal data will include for example names of clients, employees or interested third parties, addresses, emails, mobile numbers, financial status and antecedents of accidents or <sinistres> amongst others.

Management, employees and intermediaries have been fully apprised of the obligations under the law for the collection, use, processing, handling and storage and sharing with legally authorized persons or entities or compelled under the law to impart data and information.

Each employee must understand their role regarding the use and processing of personal data. The Company has a duty to regularly update employees of changes and amendments in the laws, regulations, codes, and standards.

The internal policy is approved by the Board of Directors and major and substantial changes can be brought by them, except typographical or non- substantial changes which can be sanctioned by the CEO or the General Manager after consultation with the Compliance Officer and Consultant.

This Policy is not comprehensive and it embodies the gist of the law, regulations and best practices. In case of uncertainty employees, intermediaries or third parties or customers must seek guidance from people in Management or the Compliance / Data Protection Officer.

A policy document and a proper understanding of the law is critical for the conduct of business and employees and intermediaries will use it in their daily transactions and day to day operations.

1. General core principles

Article 21 of the Data Protection Act (DPA)and other general principles require that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed and destroyed safely after the cessation of business relationship.
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. This an obligation on best endeavour standard.

2. Application and relevance

a. This policy applies to all personal data processed by IOGA and its Intermediaries and Brokers.
b. The Responsible Person shall take responsibility for IOGA's ongoing compliance with this internal policy and the relevant Act.
c. This policy shall be reviewed as and when required follwing amendments of the law or recommendations of the Authorities.
d. IOGA shall register with the Data Protection 0ffice, which is an organisation responsible for supervision, regulation and enforcement in the field of Data Protection.

3. Legality, fairness and transparency.

a. To ensure its processing of data is lawful, fair and transparent, the Company shall maintain a Register of Systems and manual of procedures.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to IOGA shall be dealt with in a timely manner.

4. Consent and legal purposes.

a. All data processed by IOGA must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interest

b. The Company shall note the appropriate lawful basis in the Register of Systems and manual of procedures.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in IOGA S system .
e. As per Section 30 of the Act staff members shall not process the data of children below the age 16 years old except with the consent of the parents, after a KYC and due diligence has been conducted on the parents or guardians to ensure the validity of their authority.

5. Minimisation and restrictive scope of data.

a. IOGA shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
b. Superfluous information should not be asked.
c. Customer may refuse to give an information which he considers to be intimate and sensitive and he should not be coerced.
d. In some instances, pseudonymisation is warranted, where data is detached from the identified or identifiable person.

6. Accuracy

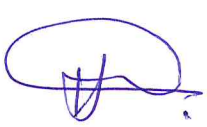
a. IOGA shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / Removal

a. To ensure that personal data is kept for no longer than necessary IOGA shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why or destroyed if of no longer use.

8. Security

a. IOGA shall ensure that personal data is stored securely using modern software and papers containing personal data and information are kept in secured and safe places All data will be regularly updated
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to av oid unauthorised sharing of information. Regarding electronic storage of data strong passwords must be used to prevent hacking or illegal intrusion.



c. Employees not concerned with information within a department should not have access to personal data within the province of a specific person or small group within the specific department.
d. When personal data is deleted this should be done safely such that the data is irrecoverable.
e. Appropriate back-up and disaster recovery solutions shall be in place.

9. Shouldering of Responsibilities

While the Top Management will have overall responsibility for the enforcement of the law and internal policy pertaining to Data Protection, the Compliance officer will be the Data Protection Officer in tandem with our Consultant on regulatory matters.

10. Rights of Customers

A customer and insured person may request at any time his personal data and information from the Data Protection Officer of the Company. The latter following consultation with Management has the obligation to provide or rectify such data or information.

11. Complaints

Any aggrieved person for any breach of the policy and law regarding data protection can file a complaint to the Complaints Officer of the Company /or the Data Protection Officer. The latter should investigate the matter and report to the General Manager and ultimately to the Managing Director and appropriate measures and sanctions must be taken within a reasonable time.

12. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, IOGA shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the concerned authorities. While IOGA will take all precautions to safeguard the data and personal information, it cannot be held responsible for the tortious acts of third parties like hackers and intruders or employees with malicious intention.

Information embodied in the actual policy is for guidance and is not meant to replace the main Act (DPA) and other relevant regulations which will normally prevail.

Consultant
17/2/2022.