nic

DATA PRIVACY POLICY

National Insurance Co. Ltd
NIC General Insurance Co. Ltd

NIC
NATIONAL INSURANCE COMPANY

1. SCOPE

This Policy describes how personal information is collected and handled in compliance with the law. It encompasses the collection, safeguard and treatment of Personal Data of various stakeholders (interchangeably referred to as "Data Subjects" or "Incumbents") of the NIC Group (National Insurance Co. Ltd, NIC General Insurance Co. Ltd and/or related entities).

The NIC Group recognises and values the rights to privacy of all of its stakeholders, including members of their workforce, clients and other transacting parties and commits to protecting Personal Data in their capacity of Data Controller and Data Processor as registered with the Data Protection Office of Mauritius and in accordance with the Data Protection Act 2017 ("DPA").

2. PURPOSE

NIC seeks to identify and verify the identity of the parties we transact with and reconstruct the trail of events leading to decision making during the course of the relationship or thereafter as may be required and in compliance with provisions of the DPA.

3. DATA COLLECTION OF NIC'S STAKEHOLDERS

Stakeholders, including clients and other transacting parties, data collected include:

- In respect of natural persons, such particulars as name, residential address, telephone number, gender, nationality, national identity number, bank account details and medical information as may be necessary in the performance of contractual obligations or underwriting requirements;
- Similar information pertaining to designated representatives of legal persons, other insured members or beneficiaries of insurance policies may be requested/kept as part of Company records;
- Information pertaining to assets held, including payroll and bank information may also be required for the purpose of securing loan collaterals and/or assessing credit worthiness of the incumbents;

Certain special categories of data which are sensitive and afforded a higher level of protection are also collected:

- Information about data subject's physical or mental health conditions, including whether or not there is a disability for which the NIC needs to make reasonable adjustments;
- Biometric data (including fingerprints), where applicable;
- Membership to associations, clubs and other groups whether professional, social or otherwise;
- Information about criminal record, incl. convictions, allegations and offences.

4. JOB SEEKERS

In respect of Job Seekers, Personal Data is usually collected through the application process, either directly from candidates, from an employment agency or background check provider.

Should NIC collect information from third parties such as references from former employers, it will only do so once a job offer has been made and will inform the incumbent when this is being done.

5. COLLECTION METHODS OF PERSONAL DATA

Subject to the express consent, in respect of clients and other stakeholders, most Personal Data will take the form of information required as part of routine business operations, including due diligence requirements and other contract-related information for the purpose of processing an application for risk acceptance and establishing a business relationship. Personal Data will be collected through insurance proposal forms, due diligence forms or other application forms and accompanying documentary evidence.

NIC endeavours to keep Personal Data updated as much as practically possible and will seek to cross verify Company Records at regular intervals during the course of the business relationship and upon transacting. In so doing, NIC relies on the Data Subjects' disclosures, updates and prompt notifications thereof.

6. GROUNDS FOR PERSONAL DATA PROCESSING

NIC only processes personal data to the extent it is permitted by law, viz. and where processing is necessary for:

- The performance of contract or to take such steps, with the incumbent's consent, prior entering into a contract;
- Compliance with its legal obligations, for regulatory returns or establishment , exercise or defence of legal claims or proceedings;
- Identifying and understanding the profile of the incumbent;
- The legitimate interests pursued by NIC or a third party;
- Statistical research and analysis; or
- Where the incumbent has specifically provided their consent.

Where legitimate interests form the basis of NIC's reliance to process personal data, it shall only do so to the extent its interests are not overridden by the incumbent's fundamental rights and freedoms that allow their personal data to be processed.

7. PURPOSES FOR PROCESSING OF DATA

NIC processes personal data in respect of its clients and other transacting parties to:

- Determine eligibility and process applications for products and services;
- Understand the profile and associated risks thereof, if any;
- Determine the terms and conditions on which the incumbent shall be accepted for the purpose of a forthcoming contractual arrangement.
- Provide information and services as requested by the incumbent;
- Carry out communication, service, billing and administration;

- Administer claims;
- Obtain and update credit information with appropriate third parties, such as credit reporting agencies, where transactions are made on credit; and
- Subject to the incumbent's consent, market products and services.

8. CHANGE OF PURPOSE

NIC limits its use of Personal Data for the purpose for which it was collected, unless it reasonably considers that it needs to use it for another purpose which is compatible with the original one. Such data may be consolidated at the level of the NIC Group for ease of data processing, management and relationship of the portfolio, generally.

Should NIC require Personal Data for an unrelated or new purpose, it shall notify the incumbent and explain the legal basis which allows it to do so.

9. DUTY TO DESTROY PERSONAL DATA

Where the purpose for keeping Personal data has lapsed, NIC shall destroy as soon as it is reasonably practical to do so destroy such data, in line with its Records Keeping Policies and Procedures.

10. SPECIAL TYPES OF PERSONAL DATA

In respect of client-related obligations, NIC maintains, as applicable, Personal Data and records that include personal credentials, contact details, bank and credit information, payroll and asset information and medical records amongst others as part of due diligence, underwriting requirements, treatment and processing of contractual obligations in connection with its customary contractual obligations.

Where Personal Data pertains to a child below the age of 16, NIC shall not process such data unless express consent is received from the child's parent or guardian.

11. PROTECTION OF PERSONAL DATA

NIC is committed to treat personal data securely and maintains organisational, physical and technical security measures to prevent personal data from unauthorised access, alteration, disclosure, accidental loss and destruction as well as to protect data from harm arising from such unauthorised access.

Although NIC endeavours to protect Personal Data, it cannot guarantee its security when transmitted over the internet as such transmission is not completely secure and will be at an incumbent's own risk.

Client sensitive data including portfolio details accessible on the secured access Client Portal is also of confidential nature and it shall be the responsibility of the client to ensure their credentials are duly protected and any change in their particulars are promptly notified to NIC to avoid data compromise issues.

Access to Personal Data is made solely on a business need-to-know basis and any such party processing personal data is subject to a duty of strict confidentiality.

NIC maintains procedures to deal with any suspected personal data breach and it shall notify an incumbent and relevant regulatory instances where it is legally required to do so in such circumstances.

12. TRANSFER OF PERSONAL DATA

In the course of processing, personal data may be shared, transferred and stored outside Mauritius in countries that may have laws considered as providing insufficient protection to personal data. NIC shall ensure that such transfer is effected in accordance with law and it endeavours to impose contractual obligations on the recipients of personal data to ensure a similar degree of security and protection is afforded to it.

13. DURATION FOR KEEPING RECORDS

Personal data will be retained so long as it would be necessary to fulfil the purposes for which it was collected, including for the purposes of satisfying any legal, accounting or reporting requirements, having regard to the nature and sensitivity of such data, the potential risk of harm from unauthorised disclosure of personal data and whether these purposes could be achieved through other means.

Basic personal information including contact details and financial details will be kept for seven (7) years or such number of years, pursuant to applicable laws after an incumbent ceases its business relationship for statutory, tax and other judicial purposes in compliance with NIC's Records Keeping Policies and Procedures.

14. INCUMBENT'S RIGHTS AS DATA SUBJECT

Unless otherwise stated by applicable laws, an incumbent has the right to:

1. Request access to personal data which will allow them to receive a copy of the personal data NIC holds about them, free of charge unless such request is excessive.
2. Request correction of personal data to cater for correction of any incomplete or inaccurate data NIC holds about them.
3. Request erasure of personal data, where there is no good reason for NIC to continue to process it. They also have the right to ask NIC to delete or remove their personal data where they have successfully exercised their right to object to processing, where NIC may have processed their information unlawfully or where NIC is required to erase their personal data to comply with applicable laws. Note however, that if NIC is not able to comply with an incumbent's request of erasure for specific legal reasons, due notification will be made to the incumbent at the time of request.
4. Request restriction of processing of personal data such that the processing of such personal data may be suspended, such as in the following instances:
    - If an incumbent wishes to establish the personal data's accuracy;
    - Where NIC's use of personal data is unlawful but an incumbent does not want NIC to erase it and request restriction of its use instead;

- Where an incumbent requires NIC to hold their personal data even if NIC no longer requires it as an incumbent needs it to establish, exercise or defend legal crimes; or
- An incumbent has objected to NIC's use of their personal data but NIC needs to verify whether it has overriding legitimate grounds to use it.

5. Request to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning an incumbent or which significantly affects them. NIC shall not process Personal Data in such a way as to subject an incumbent to automated processing, unless the decision:
   - Is necessary for it to enter into or perform a contract with an incumbent;
   - Is authorised by a law to which NIC is subject to and which lays down suitable measures to safeguard an incumbent's rights, freedoms and legitimate interests; or
   - Is based on an incumbent's explicit consent.
6. Withdraw consent at any time where NIC is relying on consent to process personal data. However, this will not affect the lawfulness of any processing carried out by NIC before an incumbent's withdraws their consent. If they withdraw their consent, NIC may not be able to provide certain services to them. NIC will advise them if this is the case at the time they withdraw their consent.
7. Right to lodge a complaint at any time with the Data Protection Commissioner of Mauritius whose office is presently at Level 5, SICOM TOWER, Wall Street, Ebene Cyber City, Mauritius and email any complaint to dpo@govmu.org. Where GDPR is applicable, an incumbent shall have the right to lodge a complaint with the regulatory authority of their country of residence, workplace or where the data breach has occurred.

Should an incumbent wish to exercise any of the rights set out above or need any clarification thereon, they should write to NIC's Data Protection Officer, Mr. Sajdeo Gokool, Compliance department on dataprotection@nicl.mu.

NIC endeavours to respond to all legitimate requests within one (1) month. Occasionally, it may take longer than one (1) month if the request is complex or an incumbent has made a number of requests. In this case, they will be notified and kept updated.

GLOSSARY OF TERMS

Data Protection Act 2017: In Mauritius, the law which governs the protection of personal data is the Data Protection Act (DPA) 2017.

Controller means a person who or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing.

Data Subject (Individual) means an identified or identifiable individual, 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 individual.

Personal Data means any information relating to a data subject.

Special categories of data in relation to a data subject means personal data pertaining to:

a) his racial or ethnic origin;
b) his political opinion or adherence;
c) his religious or philosophical beliefs;
d) his membership of a trade union;
e) his physical or mental health or condition;
f) his sexual orientation, practices or preferences;
g) his genetic data or biometric data uniquely identifying him;
h) the commission or alleged commission of an offence by him;
i) any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any Court in the proceedings; or
j) such other personal data as the Commissioner may determine to be sensitive personal data

Processing means an operation or set of operations performed on personal data or set 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.