

## **DATA PRIVACY POLICY**

We, **Gotuaco, Del Rosario Insurance Brokers, Inc.** will collect your personal information for the purpose of securing your insurance and bond requirements and process the same subject to compliance with the requirements of the Data Privacy Act of 2012 and other laws allowing disclosure of information to the public and adherence to the principles of transparency and legitimate purpose.

We require that the personal information given must be accurate, relevant and where necessary for the purposes, for which it is to be used should be kept up to date. Inaccurate or incomplete data should be rectified, supplemented, destroyed or its further processing will be restricted.

For this purpose, we will collect the following personal information:

1. Name of Applicant
2. Address
3. Contact details
4. Address/location of property to be insured
5. Technical description of property to be insured
6. Picture and signature of Applicant
7. Gender, citizenship and personal status of the Applicant

These personal information shall be retained by us only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law but not for more than five (5) years. These will be kept in a securely in our database and physical data file system.

**Personal Data** - The processing of your personal data shall be done only if law does not otherwise prohibit such; and when at least one of the following conditions exists:

1. The data subject has given his or her consent;

2. The processing of the personal information is necessary and relative to the procurement of the insurance contracts and bonds for the data subject or in order to take steps at the request of the subject prior to entering into the insurance contract or bond;
3. The processing is necessary for compliance with a regulatory requirement to which the personal information controller is subject;
4. The processing is necessary to protect vitally important interests of the data subject, including life and health;
5. The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
6. The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
7. The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

**Sensitive Personal Information and Privileged Information** – We shall not process your sensitive personal information and privileged information except in the following cases:

1. The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
2. The processing of the same is provided for by existing laws and regulations: Provided, that such regulatory enactments guarantee the protection of the sensitive personal

information and the privileged information: Provided, further, that the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;

3. The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;
4. The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: Provided, That such processing is only confined and related to the bona fide members of these organizations or their associations: Provided, further, That the sensitive personal information are not transferred to third parties: Provided, finally, That consent of the data subject was obtained prior to processing;
5. The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or
6. The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

**Subcontract of Personal Information** – Our personal information controller, with the approval of the President & CEO, may subcontract the processing of your personal information: but, our personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of your personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of the Data Privacy Act and other laws for processing of personal information.

Our personal information processor shall comply with all the requirements of the Data Privacy Act and other applicable laws.

**Rights of the Data Subject** – You, the data subject is entitled to:

1. Be informed whether personal information pertaining to you shall be, are being or have been processed;
2. Be furnished the information indicated hereunder before the entry of your personal information into the processing system of the personal information controller, or at the next practical opportunity; be given the:
  - (a) Description of the personal information to be entered into the system;
  - (b) Purposes for which they are being or are to be processed;
  - (c) Scope and method of the personal information processing;
  - (d) The recipients or classes of recipients to whom they are or may be disclosed;
  - (e) Methods utilized for automated access, if the data subject, and the extent to which such access is authorized to allow the same;
  - (f) The identity and contact details of the personal information controller or its representative;
  - (g) The period for which the information will be stored; and
  - (h) The existence of your rights, i.e., to access, correction, as well as the right to lodge a complaint before the National Privacy Commission.

Any information supplied or declaration made to you, the data subject on these matters shall not be amended without prior notification: Provided, That the notification under subsection (b) shall not apply should the personal information be needed pursuant to a subpoena or when the collection and processing are for obvious purposes, including when it is

necessary for the performance of or in relation to a contract or service or when necessary or desirable in the context of an employer-employee relationship, between the collector and the data subject, or when the information is being collected and processed as a result of legal obligation;

3. Reasonable access to, upon demand, the following:

- (a) Contents of your personal information that were processed;
- (b) Sources from which personal information were obtained;
- (c) Names and addresses of recipients of the personal information;
- (d) Manner by which such data were processed;
- (e) Reasons for the disclosure of the personal information to recipients;
- (f) Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;
- (g) Date when your personal information were last accessed and modified; and
- (h) The designation, or name or identity and address of the personal information controller;

4. Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information have been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof: Provided, That the third parties who have previously received such processed personal information shall be informed of its inaccuracy and its rectification upon your reasonable request;

5. Suspend, withdraw or order the blocking, removal or destruction of your personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected.

In this case, the personal information controller may notify third parties who have previously received such processed personal information; and

6. Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.

**Transmissibility of Rights of the Data Subject** – Your lawful heirs and assigns may invoke your rights for, which he or she is an heir or assignee at any time after your death or when you are incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section.

**Right to Data Portability** – You, as the data subject shall have the right, where personal information is processed by electronic means and in a structured and commonly used format, to obtain from the personal information controller a copy of data undergoing processing in an electronic or structured format, which is commonly used and allows for your further use. The Commission may specify the electronic format referred to above, as well as the technical standards, modalities and procedures for their transfer.

**Non-Applicability** – The immediately preceding sections are not applicable if the processed personal information are used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject: Provided, That the personal information shall be held under

strict confidentiality and shall be used only for the declared purpose. Likewise, the immediately preceding sections are not applicable to processing of your personal information gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities involving you.

**Security of Personal Information** – (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of your personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.

(b) The personal information controller shall implement reasonable and appropriate measures to protect your personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

(c) The determination of the appropriate level of security under this section must take into account the nature of personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation. Subject to guidelines as the National Privacy Commission may issue from time to time, the measures implemented must include:

- (1) Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability;
- (2) A security policy with respect to the processing of personal information;
- (3) A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security

incidents that can lead to a security breach; and  
(4) Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.

(d) The personal information controller must further ensure that third parties processing personal information on its behalf shall implement the security measures required under the Data Privacy Act.

(e) The employees, agents or representatives of the personal information controller who are involved in the processing of your personal information shall operate and hold personal information under strict confidentiality if the personal information are not intended for public disclosure. This obligation shall continue even after leaving the public service, transfer to another position or upon termination of employment or contractual relations.

(f) The personal information controller shall promptly notify the National Privacy Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes (that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

(1) In evaluating if notification is unwarranted, the National Privacy Commission may take into account compliance by the personal information controller with this section and existence of good

faith in the acquisition of personal information.

(2) The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects.

(3) The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

**Principle of Accountability** – The personal information controller is responsible for personal information under his control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

(a) The personal information controller is accountable for complying with the requirements of the Data Privacy Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party.

(b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with the Data Privacy Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.

**This is the Data Privacy Policy of Gotuaco, Del Rosario Insurance Brokers, Inc., which takes effect immediately.**

**Date: 12 July 2021**