Data Privacy Policy
2020

PRIVACY POLICY

This Privacy Policy ("Policy") is adopted by Landco Pacific Corporation, its subsidiaries, and joint ventures (the "Company") in compliance with Republic Act No. 10173 also known as the Data Privacy Act of 2012 ("DPA"), its Implementing Rules and Regulations, and other relevant policies, including the issuances of the National Privacy Commission ("NPC") and shall explain the collection, processing, and disclosure of personal data of the Data Subject involved.

DATA PRIVACY PRINCIPLES

The Company highly values and prioritizes the privacy of information collected from its existing and prospective clients, members, and patrons ("Data Subject"). In order to protect the information gathered by the Company, it shall ensure that all personal data and other sensitive data obtained from such Data Subjects are collected, processed, stored, transmitted, updated and disposed of in accordance with the general principles of transparency, legitimate purpose and proportionality.

A. *Transparency* – The Company undertakes to disclose to the Data Subject of the nature, purpose and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a Data Subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.

B. *Legitimate Purpose* – The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.

C. *Proportionality* – The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.

The Company shall undertake to protect the privacy and security of confidential data in the manner provided by the Data Privacy Act and other applicable laws, rules and regulations and issuances of pertinent government agencies.

PERSONAL DATA

As part of the business interaction between the Company and the Data Subject, the Company shall collect certain personal data from the Data Subject which shall include, but not limited to:

1. the Data Subject's name, gender, civil status, date of birth, address, telephone or mobile numbers, email address, mailing address, proof of identification, and any other information relating to and provided by the Data Subject in the course of the Company's interaction with the Data Subject;
2. the Data Subject's credit history, bank account, and credit information which the Data Subject provided in availing the Company's products and services;
3. the Data Subject's employment history, educational attainment, resume, and income whenever the Data Subject is applying for employment in the Company; and
4. any other information provided by, or otherwise obtained from the Data Subject in the course of the Company's interaction from the Data Subject.

COLLECTION OF PERSONAL DATA

The Company shall collect personal data from the Data Subject in the following circumstances:

1. when the Data Subject purchases or avails of any of the Company's products, services, promos, activities, and events;
2. when the Data Subject interacts with the Company's sales or customer care agents, sales and marketing officers or specialists, through email, phone, chat services, or personal meetings;
3. when the Data Subject submits information, through any form, on the Company's digital assets, which may include websites and email accounts and other social media;
4. when the Data Subject requests or has inquiries related to the Company's business;
5. when the Data Subject reports any complaint/s which the Company may be involved or may take action on;
6. when the Data Subject responds to surveys, promotions, and other marketing and sales initiatives;

7. when a Data Subject has been referred to the Company by third party entities; Provided the Data Subject has consented to such referral; and
8. when the Data Subject voluntarily submits personal data to the Company for any valid reasons.

PURPOSE OF COLLECTION

The Company shall collect, use, disclose personal data from the Data Subject for varied purposes, including but not limited to:

1. to conduct appropriate due diligence;
2. to register inquiries and address follow-ups, and to respond to complaint/s which the Company may be involved or which it may take action on;
3. to prepare the appropriate sales documentation and any other documentation as may be necessary;
4. to perform financial processes related to sale such as downpayment set-up, amortization, or financing;
5. to provide customer care and enhance customer satisfaction, including but not limited to, resolving complaints, dealing with and/or responding to requests and inquiries, and other after sale services;
6. to keep the Data Subject informed of the Company's promos, discounts, and/or events;
7. to comply with the requirements of law and legal proceedings such as court orders, and other duly authorized public authority;
8. to comply with legal obligation or to prevent imminent harm to public security, public order, or public safety;
9. to prevent, investigate, and detect possible crime, including fraud and money-laundering;
10. to analyze and manage other commercial risks;
11. to process information for statistical, analytical, and research purposes;
12. to perform other actions necessary or desirable in the implementation of the contract/s concerned; and
13. to perform any other action in relation to the abovementioned purposes.

DISCLOSURE OF PERSONAL DATA

The Company shall not disclose the personal data of the Data Subject to any third person or entity, unless otherwise the consent of the Data Subject is obtained prior to such disclosure and provided further that, the third person or entity enters into a Data Sharing

Agreement with the Company, as may be applicable. Once the consent is obtained from the Data Subject and a Data Sharing Agreement has been entered into between the Company and the third person or entity, the Company shall only disclose the personal data of the Data Subject to the following authorized persons or entities:

1. the Company's subsidiaries and affiliates;
2. the Company's employees, agents, successors and assignees;
3. the Company's professional advisers, such as but not limited to its lawyers and auditors;
4. the Company's insurers and credit providers;
5. the Company's banks, credit card companies, and other respective service providers;
6. the Company's third-party service providers, including suppliers or subcontractors, and consultants, which the Company has engaged to provide it financial, technical, architectural, administrative, and other services;
7. other third-party business/es offering goods or services, or desiring to sponsor Company contest/s or other marketing and promotional programs;
8. the Company's prospective clients and customers availing of the Company's products or services, or to whom the Company is contemplating to sell any of its business or asset;
9. to any other person who may apply or has applied to any court or competent authority for such disclosure, after the exercise of the Company's reasonable discretion; and
10. any authority, regulatory, supervisory or enforcement agency, exchange, court, quasi-judicial body or tribunal

CONSENT

By signing the Company's consent form, the Data Subject or his or her duly authorized representative explicitly authorizes and consents to the Company's collection, use, access, transfer, storage, disclosure, and processing of said personal data for the abovementioned purpose.

PROTECTION OF PERSONAL DATA

The Company is committed to protecting the privacy of all personal data provided to it by the Data Subject. The Company maintains physical, technical and organizational safeguards to protect personal data against loss, theft, unauthorized access, disclosure,

copying, use or modification. The Company shall put in effect the necessary safeguards, including but not limited to the following:

- Use of secured servers and other security tools;
- Limited access to Data Subject's personal data; and
- Information system and infrastructure regular testing.

The Company shall limit access to the authorized persons or entities. The Company shall be responsible for all personal data in its possession, including information transferred to authorized persons or entities. All such authorized persons or entities, wherever they are located, are required by the Company to protect the confidentiality and privacy of the Data Subject's personal data in a manner consistent with the Company's privacy policies and practices.

The Company shall likewise ensure that the Company's Privacy Policy is constantly reviewed, monitored, and enhanced. However, while the Company shall employ all necessary precautions to safeguard Data Subject's personal data, the Company does not guarantee full protection against unauthorized access and use from the internet of my personal data beyond the Company's control.

RIGHTS OF THE DATA SUBJECT

1. *Right to be informed* – The Data Subject has a right to be informed whether personal data pertaining to him or her will be, are being, or were processed, including the existence of automated-decision making and profiling.

2. *Right to object* – The Data Subject has the right to object to the processing of his or her personal data, including processing for direct marketing, automated processing or profiling. He or she should be given an opportunity to withhold consent in case of any amendment to the information supplied to the Data Subject under the right to be informed.

When a Data Subject objects or withholds consent by not signing the Company's consent form, the personal information controller shall no longer process the personal data, unless:

a. The personal data is needed pursuant to a subpoena;
b. 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 to

which the Data Subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the collector and the Data Subject; or

c. The information is being collected and processed as a result of a legal obligation.

3. *Right to access* – The Data Subject has the right to reasonable access to, upon demand, the following:

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

4. *Right to rectify erroneous data* – The Data Subject has the right to dispute the inaccuracy or error in the personal data and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal data has 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 the intended recipients thereof: Provided, That recipients or third parties who have previously received such processed personal data shall be informed of its inaccuracy and its rectification, upon reasonable request of the Data Subject.

5. *Right to erase or block* – The Data Subject has the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal data from the personal information controller's filing system.

This right may be exercised upon discovery and substantial proof of any of the following:

a. The personal data is incomplete, outdated, false, or unlawfully obtained;
b. The personal data is being used for a purpose not authorized by the Data Subject;
c. The personal data is no longer necessary for the purposes for which they were collected;
d. The Data Subject withdraws consent or objects to the processing of his or her information, and there is no other legal ground or overriding legitimate interest for the processing;
e. The personal data concerns private information that is prejudicial to Data Subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
f. The processing is unlawful; or
g. The personal information controller or personal information processor violated the rights of the Data Subject. The personal information controller may notify third parties who have previously received such processed personal information.

6. *Right to damages* – The right to damages sustained due to such false, incomplete, outdated, unlawfully obtained or unauthorized use of personal data, considering any violation of his or her rights and freedoms as a Data Subject. The Data Subject should be indemnified for any damages.

7. *Right to data portability* – Where his or her personal data is processed by electronic means and in a structured and commonly used format, the Data Subject has the right to obtain from the personal information controller a copy of such data in an electronic or structured format that is commonly used and allows further use. The exercise of this right should consider the right of Data Subject to have control over his or her personal data being processed based on consent or contract, for commercial purpose, or through automated means. The Commission may specify the electronic format, as well as the technical standards, modalities, procedures and other rules for their transfer.

8. *Transmissibility of Rights of the Data Subject* – The lawful heirs and assigns of the Data Subject may invoke the rights of the Data Subject at any time after the death of the Data Subject or when the latter is incapacitated or incapable of exercising his or her rights.

PERIOD OF RETENTION OF PERSONAL DATA

The Company shall only retain data, including electronic documents, for as long as necessary and in compliance with the retention period imposed by existing contracts, law, the National Privacy Commission, and other relevant regulatory agencies. It shall retain the personal data for a period which would ensure fulfillment of the declared, specified, and legitimate purpose, or until the processing relevant to the purpose has been terminated. It shall also be retained for a period necessary for the establishment, exercise or defense of legal claims; or for legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by appropriate government agency.

DISPOSAL OF PERONAL INFORMATION

The Company undertakes to dispose and discard personal data of the Data Subject in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subjects. It shall employ the use of shredders to dispose of physical files containing the personal data of the Data Subject. It shall delete and dispose of electronic data by permanent data erasure with the use of data eradication software which would ensure permanent deletion of the personal data.

DATA PROTECTION OFFICER

The Company's Data Protection Officer shall oversee the compliance of the organization with the Data Privacy Act, its Implementing Rules and Regulations, and other related policies, including the conduct of a Privacy Impact Assessment, implementation of security measures, security incident and data breach protocol, and the inquiry and complaints procedure.

REVIEW OF THE POLICY

This Privacy Policy shall be reviewed and evaluated annually. Privacy and security policies and practices within the organization shall be updated to remain consistent with current data privacy best practices.

PHYSICAL AND TECHNICAL SECURITY MEASURES

The Company shall implement physical and technical security measures to protect personal data of the Data Subject from unauthorized access, use, transfer, removal, or

disposal. The Data Subject's personal data shall also, as far as practicable, be secured from natural disasters, power disturbances, external access, and other similar threats.

Only authorized personnel shall be allowed access to the Data Subject's personal data. Other personnel may be granted access to such data upon the approval of the Data Protection Officer of the request filed by the requesting personnel. The requesting personnel must state the purpose for which the access is sought.

AMENDMENTS

The Company reserves the right to change entirety or portions this Privacy Policy at any time and without notice. It is recommended that a periodic review of the Company's Privacy Policy be made by the Data Subject for amendments.

CONTACT US

The Data Subject may inquire or request for information regarding any matter relating to the processing of his or her personal data under the custody of the Company, including the data privacy and security policies implemented to ensure the protection of his or her personal data.

For questions about the Company's Privacy Policy or its data processing activities, the Data Subject may contact the Data Privacy Officer through the Company via: (a) Direct Line: (02) 8836-5078; or (b) Trunk Line: (02) 8836-5000. The Data Subject may also visit the Company's office at 25th floor Insular Life Center, Filinvest, Alabang, Muntinlupa City, Philippines.