DATA PRIVACY POLICY

OUR COMMITMENT

GRACIOUS GROUP LENDING PHILS. CORP. (the "Company") is committed to providing its employees, clients, debtors, and Data Subjects with the highest levels of professional service. This includes protecting their privacy as the Company understands the importance of privacy of their Personal Data and Personal Information.

This Privacy Policy & Manual sets out how we collect, hold, use, and disclose your personal data.

By communicating with the Company's personnel, office, branches, email address, website, interacting with any of its social media accounts, requesting its lending services, applying for a job with Company, asking Company to provide loans or other lending services, or otherwise providing Company with your personal data, all employees, clients and Data Subjects will need to consent to their personal data being collected, held, used, and disclosed as set out in this Privacy Policy & Manual.

This Privacy Policy & Manual applies to all individuals (including Company's clients, the individuals whose personal data is collected from clients or other third parties, job applicants and prospective employees) who provides Company with their personal data.

PURPOSE OF THE POLICY

This Data Privacy Policy is designed to raise awareness of personal data in the course of Company's daily operations and enable Company to protect the integrity and security of personal data which has been entrusted to Company by its clients, employees, and business partners. It sets out the basic obligations of Company personnel regarding personal data.

Company personnel should familiarize themselves with this Data Privacy Policy & Manual and handle all personal data in accordance with the directions in it.

Should there be questions in connection with this Data Privacy Policy & Manual or in the event of any particular action or conduct that is observed to have been in breach of this Manual, please seek legal advice from the designated or retained lawyers of Company or Company's Data Privacy Officer as indicated below.

EFFECTIVE DATE

This Data Privacy Policy takes effect from 30 March 2023.

DEFINITIONS

For purposes of this Data Privacy Policy & Manual, all terms defined by Republic Act No.10173 or the Data Privacy Act of 2012 (*i.e. Data, Personal Information, Sensitive Personal Information, Data Sharing Agreement, etc*); including any terms defined or referred to by any implementing rules or regulations issued by the Philippine National Data Privacy Commission shall be understood to have been adopted herein.

DATA PROTECTION PRINCIPLES

All Company personnel must adhere to the following general principles when collecting, using, disclosing, processing or otherwise handling Personal Information, Sensitive Personal Information and Privileged Information.

Consent

The consent of an individual must be obtained, in accordance with the applicable Philippine data privacy laws, before collecting, using, or disclosing his personal data for a purpose. An individual also has a right to withdraw his consent, by giving reasonable notice.

Before embarking on a new business project or initiative that requires the collection of Personal Data, consider each category of Personal Data that is proposed to be collected and assessed whether the "Personal information controller" or "PIC" (such as this Company) is able to perform the project or initiative without it. One should only collect the minimum Personal Data it requires for the legitimate purpose it is required for.

Purpose

Personal Data may only be collected, used or disclosed for legitimate purposes that a reasonable person would consider appropriate in the circumstances. Fresh consent must be sought if any purposes for which consent was obtained differ from the original purpose communicated and agreed to by the individual.

Before using any Personal Data for a new purpose, all Company personnel must ensure that the new purpose is covered under the relevant provisions of this Data Privacy Policy and Manual.

Notification

Company must notify individuals of the purpose(s) for which it intends to collect, use or disclose his Personal Data on or before Company's collection, use or disclosure of such Personal Data. If Company will be collecting Personal Data for a new purpose (as above), Company will need to provide fresh notification to the individuals.

Access

Upon request by an individual, he or she must be provided with his/her Personal Data possessed or controlled by Company, unless prohibited by Philippine Data Privacy laws or regulations or other applicable laws or regulations in the country. Once Company received the request, Company will need to understand internally how the individual's Personal Data has been used, processed or disclosed by Company. Company need to ensure that it log all activities in relation to the access and extraction of Personal Data held by it.

Unless the aforesaid laws or regulations provide otherwise, such personal data must be provided as soon as practicable and no later than thirty (30) days after the individual's first request for such personal data.

Correction

An individual may also request Company to correct any inaccuracies in her/his personal data which is in Company's possession or control. Unless Philippine laws or regulations provide otherwise, such personal data must be corrected or erased as soon as practicable, but no later than thirty (30) days after the individual's first request for such correction.

Accuracy

Reasonable efforts must be made to ensure that personal data collected by or on behalf of Company is accurate and complete. This obligation applies at the time of collection and throughout the period during which such personal data is in Company's possession or control.

Where the data is more sensitive (e.g. tax identification numbers, mobile numbers), Company must ensure that there are additional testing and checking performed to address any mistakes made during the point of data entry. For example, a second person should double check the records to ensure accuracy.

Security

Personal Data in Company's possession or under its control must be protected by reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks.

Company personnel should take note of the following basic guidelines when sending Personal Data:

- Before sending a communication (e.g. email, Messenger, Viber, other social messaging applications, written or electronic message/attachment) containing Personal Data, ensure that the recipient address (e.g. email address, fax number, other details) is correct and matches that of the intended recipient and that the right files are attached prior to sending.
- Perform regular housekeeping of auto-complete email list and double check recipient's email addresses before sending out emails or documents containing Personal Data.
- Where possible, implement automated processing of documents or communications containing Personal Data (e.g. merging content or populating fields from various sources). Ensure the accuracy and reliability of the automated process by checking it regularly.
- Require Company employees handling and sending Personal Data to be bound by confidentiality obligations in their employment agreements.
- Store hardcopy documents containing Personal Data in locked storage systems.
- Ensure that the computer networks being utilized by Company to access, store or process Personal Data are secure.
- Install appropriate computer security software and use suitable computer security settings.

Retention

Unless Philippine laws or regulations provide otherwise, the retention of documents containing personal data must cease, or the means by which the personal data can be associated with particular individuals must be removed (for e.g., anonymization of data) as soon as:

- it is reasonable to assume that the purpose for which the personal data was collected is no longer being served by retention of such personal data; and
- retention is no longer necessary for legal or business purposes.

Company personnel shall ensure proper disposal of Personal Data which should no longer be retained by Company. Printed Personal Data should be shredded and digital documents containing such Personal Data should be permanently deleted.

WHAT PERSONAL DATA DO GRACIOUS GROUP LENDING PHILS. CORP. ("Gracious Group") COLLECT?

GRACIOUS GROUP collect personal data (including sensitive personal information and privileged information, for example: government ID numbers) that is necessary for it to provide clients, business partners or employees with the lending or loaning services they request, and for managing said requests, and to improve its business, its affiliates' businesses and its partners businesses. Such personal data usually includes a person's name, date of birth, address, email, and telephone numbers. In addition, we may collect the following personal data:

- For recruitment purposes: an employee's previous work history, performance appraisals, qualifications, information about incidents in the workplace, health information, personal history, opinions from referees or previous employers, information in relation to absences from work due to leave, illness or other causes and our assessment of you as a prospective candidate for recruitment including any psychometric or skills testing.

- For payroll purposes: an employee's personal and employment details, Tax Identification Number, bank account details, and other ancillary information that is required to fulfil contractual, legislative, filing, and reporting obligations (including the payment of salary and wages).

- For client purposes: Complete Name, Mobile Number, Complete Address, government issued ID for identification purposes, Bank details for payment through online banking, bank to bank deposit or other electronic payment purposes, all other personal, sensitive personal and privileged information data from ATM information, property details and other relevant documents related to loans and lending or other company purposes.

HOW DOES GRACIOUS GROUP COLLECT PERSONAL DATA?

In general, GRACIOUS GROUP collects personal data from its data subject through the following mediums or channels:

1. Social Media Applications – Facebook, Instagram, Tiktok, Twitter, etc.
2. Social Messaging Applications/ Chat Applications - Viber, Messenger, Whatsapp, Telegram
3. SMS /Mobile- Text, calls
4. Online Conference Applications- Zoom, Google Meet, etc.
5. Face-to-Face Interactions – Interviews, physical interactions
6. Website - a fill out form is located in our website. Once filled, it will be sent and fulfilled to our email (https://graciousphils.com/)
7. Electronic mail ("Email) - a few customers directly inquire through our the email indicated in our website (https://graciousphils.com/)

Before GRACIOUS GROUP collect and process personal data, it will first ask for a Data Subject's consent as evidenced by written, electronic, or recorded means. GRACIOUS GROUP will also notify the Data Subject of its purpose for processing his/her personal data. The data subject consent procurement process may be integrated already into the system, website, social media interface that GRACIOUS GROUP operates in.

When possible, GRACIOUS GROUP will directly collect personal data from a Data Subject (for example in person, over the telephone, by email, via social media, or when said person set up an account with GRACIOUS GROUP or complete one of its online or hard copy application form).

GRACIOUS GROUP may also obtain personal data from third parties such as its clients, a Data Subject's referees, educational institutions, and current and former employers.

For the provision of payroll services, GRACIOUS GROUP will collect personal data from clients who has contracted GRACIOUS GROUP to provide recruitment and placement services.

GRACIOUS GROUP may also automatically collect certain information when you visit its website, some of which may personally identify a Data Subject. Such information includes the type of browser a Data Subject is using, the type of operating system he/she is using, the Data Subject's IP address, and how he/she use GRACIOUS GROUP's website.

If a person intends to provide GRACIOUS GROUP with personal data about another individual, before doing so he/she:

- must tell that individual that he/she will be providing their personal data to GRACIOUS GROUP and that we will handle their personal data in accordance with this Data Privacy Policy & Manual;

- must provide that individual with a copy of (or refer them to) this Data Privacy Policy & Manual; and

- represent and warrant that they have that individual's consent to provide their personal data to GRACIOUS GROUP in accordance with the relevant Philippine laws.

WHY DOES GRACIOUS GROUP COLLECT PERSONAL DATA AND HOW DOES IT USE SAID DATA?

GRACIOUS GROUP collect a Data Subject's personal data or personal information and use it for the declared and specified purpose for which it was provided to said Data Subject. GRACIOUS GROUP may also use a Data Subject's personal data for other related legitimate and legal purposes (*and, in the case of sensitive information, only for specific and directly related purposes which you have consented to*) or as permitted or required by law. Such purposes include:

- Providing our clients and/or the Data Subject with GRACIOUS GROUP's services;
- Marketing the services of GRACIOUS GROUP's services to its clients or potential clients;
- Evaluating the services of GRACIOUS GROUP's services to its clients for purposes of improvement via suggestion and reactions;
- Facilitating recruitment opportunities for job applicants, including assessing a Data Subject's application for employment with GRACIOUS GROUP and verifying his/her information;
- Providing Data Subject or clients with information about GRACIOUS GROUP and its activities (such as new services) that are of relevance to them (if they have consented to receiving said information);
- Uploading to Meta for purposes of availing the lookalike audience feature;
- For marketing and advertising purposes but only limited to the services being offered by GRACIOUS GROUP only unless otherwise stated in its Data Privacy Consent form;
- To improve GRACIOUS GROUP's business or strategy;
- In the payroll context, fulfilling contractual commitments to provide payroll services for its clients. The information collected from its payroll clients is used solely for the purpose of payroll processing;

- To be used for future businesses, expansion plans, studies, campaigns, marketing strategies, for data analysis, algorithm, technological derivative, research, and other uses, related to any and all services, actions, or transactions as may be deemed necessary by GRACIOUS GROUP, and;
- Any other purpose identified at the time of collecting a Data Subject's personal data for which he/she are notified separately.

WHEN DOES GRACIOUS GROUP DISCLOSE PERSONAL DATA?

Any personal data a Data Subject provide to GRACIOUS GROUP shall **NOT BE DISCLOSED** by the company unless it first asks for the Data Subject 's consent. However, GRACIOUS GROUP as a general rule will not share personal data outside its umbrella group of companies and its systems. Said umbrella group includes the subsidiaries, affiliates, sister companies, member companies, directors, management, officers, employees and representatives of GRACIOUS GROUP.

By way of exception, it is also possible, though unlikely, that GRACIOUS GROUP might be forced to disclose personal data in response to legal process or when we believe in good faith that the law requires it, for example, in response to a court order, in compliance with tax rules before the Bureau of Internal Revenue of the Philippines, subpoena, or a law enforcement agency's request.

GRACIOUS GROUP will only disclose your sensitive information (for example, health information) for the purposes for which it was initially collected, other directly related purposes or purposes to which a Data Subject otherwise consent.

DATA BREACH

What is a Data Breach?

A data breach includes the following scenarios:

- The unauthorized access, publication, dissemination, sharing or use of GRACIOUS GROUP's protected Personal Data or Personal Information; or
- GRACIOUS GROUP's protected Personal Data or Personal Information has been deleted or lost, without authorization. Personal Data or Personal Information includes Sensitive Personal Information and Confidential Personal Information.

Data breaches may occur due to intentional acts or omissions, or as a result of an accident, human error or software malfunction. Examples of a data breach include:

- Hacking or illegal access to databases
- Theft or accidental loss of GRACIOUS GROUP's laptops, devices, thumb drives or hard disks containing personal information or personal data
- Phishing or scams that trick account users into providing their passwords or Personal Information or Personal Data
- Sending protected Personal Data or Personal Information to a wrong e-mail or physical address, disclosing protected Personal Data or Personal Information to a wrong recipient
- Unauthorized access to protected Personal Data or Personal Information by employees without proper authority
- Improper disposal of protected Personal Data or Personal Information (e.g. hard disks, storage media or paper documents containing Protected Information are sold or discarded)

WHO SHOULD I CONTACT IN THE EVENT OF A SUSPECTED OR ACTUAL DATA BREACH?

Immediately notify GRACIOUS GROUP's Data Privacy Officer.

At the earliest opportunity once you have understood the situation, please send an email to the Data Privacy Officer (contact details below). The email should contain the following information:

- ✓ Description of the breach or suspected breach, including a list of the Protected Information affected
- ✓ Estimated number of individuals affected by the breach
- ✓ Any action taken to address or stop the breach
- ✓ Outcome of the action

Upon receiving the notification, GRACIOUS GROUP's Data Privacy Officer shall immediately convene the Data Breach Response Team.

WHAT WILL THE DATA BREACH RESPONSE TEAM DO?

GRACIOUS GROUP has developed a Data Breach Response Plan. In the event of a data breach, the Data Breach Response Team headed by the Data Privacy Officer will execute the Response Plan. The Response Plan sets out the actions to be taken in the event of an actual or suspected data breach. It is designed to urgently:

1) stop and contain the data breach (if it is ongoing);
2) immediately report the breach to the Philippine National Privacy Commission in compliance with its data breach protocols and rules under the law
3) assess the scope of the data breach;
4) mitigate damage from the data breach;
5) comply with our legal and regulatory obligations arising from the data breach such as making the proper mandated notification to the affected individuals and the proper government agency within the proper timeframe as may be required by your local law
6) apply lessons learnt to our policies and procedures

The Response Plan enables GRACIOUS GROUP to account to its clients, employees and other individuals/entities who have entrusted GRACIOUS GROUP with their Personal Information or Personal Data. Executing the Response Plan mitigates the risk of serious loss or reputational harm to GRACIOUS GROUP as a result of a data breach.

COMPLAINTS

If any person wishes to make a complaint about a breach of this Data Privacy Policy & Manual or the privacy principles under the Data Privacy Act of 2012, they can contact GRACIOUS GROUP by using the contact details below. The complainant will need to provide GRACIOUS GROUP with sufficient details regarding his/her complaint as well as any supporting evidence and/or information.

GRACIOUS GROUP will refer your complaint to our Data Privacy Officer who will investigate the issue within a reasonable time frame, which is usually 30 days but may be longer if the matter is complex. GRACIOUS GROUP's Data Privacy Officer will determine the steps (if any) that we will undertake to resolve the complaint. Such steps may include discussing the options for resolving the complaint with the person, notifying relevant employees the subject of a complaint, and seeking their input or escalation to its President or external legal counsels.

GRACIOUS GROUP or its Data Privacy Officer will contact the complainant if any additional information is required. They will also notify the complainant in writing of the outcome of our investigation. If the complainant is not satisfied with GRACIOUS GROUP's resolution, the complainant can contact GRACIOUS GROUP's Data Privacy Officer to discuss his/her concerns or complain to the National Privacy Commission via https://privacy.gov.ph/.

REVISIONS TO THIS PRIVACY POLICY

GRACIOUS GROUP reserve the right to revise this Data Privacy Policy & Manual or any part of it from time to time. Everyone is directed to review this Data Privacy Policy & Manual periodically for changes. If GRACIOUS GROUP will make material changes to this Data Privacy Policy & Manual, then it will notify all affected Data Subjects and require them to consent before proceeding.

DATA PRIVACY OFFICER:

Name of Data Privacy Officer: **PAUL ANDREW PANTOJA**
Address: 2/F PBT BLDG. NO. 475 C-3 ROAD, KAUNLARAN VILLAGE, CALOOCAN CITY
Telephone: 82886106
Facsimile: 82886106
Email address: dpograciousgroup@gmail.com