PRIVACY NOTICE

Your data is in good hands. Metropolitan Bank and Trust Company ("Metrobank" or the "Bank") respects your right to privacy and fully commits to protect your personal data in compliance with Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012 (DPA). This Privacy Notice informs you, the Data Subject, the personal data we collect about you, how we collect, use, store, process, share, protect, and delete your personal data with us, and who we will share them with.

How we Collect Information

We collect your personal data manually or automatically through various interactions including but not limited to the following:

- When visiting and/or transacting at any office, building, premises, and/or use the facilities of a member of the Bank;
- When transacting with our employees, authorized representatives, agents and service provider;
- When visiting the websites of the Bank or third-party websites and clicking on the advertisements of the Bank;
- When submitting application forms and or other forms related to our products and services; and
- When filing complaints, inquiries or requests to the Bank.

What Information we may Collect

- *Identification Data / Know-Your-Customer (KYC).* This refers to personal data we collect when you register to our products and services, such as full name, gender, date of birth, civil status, place of birth, citizenship, permanent address, present address, government-issued identification numbers, email address, mobile number, home number, office contact details, company name, job position or rank, office address, source of funds, gross annual income, and such other information necessary to conduct due diligence and comply with BSP and AMLC rules and regulations;
- *Financial Information.* This includes but not limited to income, expenses, deposits, investments, credit cards, tax, insurance, financial and transaction history, relationships with other banks and/or financial institutions, business interests and assets;
- *Audiovisual Data.* This includes video, image, and sound recordings of when you communicate with representatives of the Bank through official Bank communication channels and surveillance videos at branches and automated teller machines (ATM), subject to limitations imposed by law;
- *Non-Personal Information.* This can be read on your device when you use Metrobank's websites, apps, and other electronic platforms; and,
- *Relevant Individuals.* These are information about your family members, beneficiaries, attorneys, attorneys-in-fact, shareholders, beneficial owners whenever applicable, persons under any trust, trustees, partners, committee members, directors, officers or authorized signatories, guarantors, and other security and other individuals.

What we do with the Information we Gather

While your consent may be solicited to process your personal data, we may also process personal data without your consent, such as when processing is according to our mandate or when processing is allowed under Section 12 or Section 13 of the DPA.

In these instances, your personal data is utilized for the following purposes:

- **Data Storage.** We store data in secure and encrypted managed environments, devices, and media. For third-party managed environments such as cloud service providers, we employ BSP-sanctioned security protocols and procure BSP approval prior to deployment. We store physical copies of documents containing personal data in physically secure environments.
- **Data Access.** The data we collect can only be accessed by authorized personnel on a role-based access control, need-to-know basis and least-privilege principles.
- **Data Use.** Your personal data may be used, stored, processed, shared and disclosed by the Bank to its members, as well as third parties (as may be allowed by law) for the following relevant and necessary purposes:
    - *To protect you.* We use your data to further secure your accounts from fraud and other illegal activities.
    - *To keep your information updated.* We use your data to validate, verify, and update your information and documents.
    - *To facilitate transactions and offer you relevant products.* We share your data within the Metrobank Group and to carefully selected third-party service providers to facilitate transactions and let you know about products and services relevant to you.
    - *To perform legal duties.* We use your data to comply with our legal duties and to further improve due diligence in anti-money laundering and counter-terrorism efforts as well as other activities required by applicable laws and regulations.
    - *To settle claims or disputes.* We use your data to settle claims or disputes involving our products and services. Your data can also be used for prosecuting or defending Metrobank or its employees if needed.
- **Data Retention.** We keep your data as long as necessary for the fulfillment of the declared, specified, and legitimate purposes, or when the processing relevant to the purposes has been terminated, for the establishment, exercise or defense of legal claims or for legitimate business purposes, which shall be in accordance with the standards of the banking industry.
    - The personal data collected through CCTV recordings are securely kept and deleted after 30 calendar days, unless your entry or presence in the premises will be a subject of an investigation or inquiry, in which case, your personal data shall be kept until the investigation or inquiry is terminated.
    - For financial data and documents which indicate taxable transactions, data shall be preserved for ten (10) years per BIR regulation.
    - The processing, profiling, and sharing apply during the prospecting and application stages, as well as for the duration of and even after the rejection, termination, closure, or cancellation of Metrobank's products and services for a period of at least ten (10) years from the termination of the last existing account or relationship of the Data Subject or Relevant Individual as determined by the Bank.
    - All other transactions and accounts that are not defined above shall be retained following BSP and AMLC regulations where retention period for transaction records shall be five (5) years from the date of transaction except where specific

laws and/or regulations require a different retention period, in which case, the longer retention period is observed.

- **Data Disposal.** After the expiration of the imposed retention period, we dispose of personal data in a secure manner in order to prevent further processing, unauthorized access, or disclosure to any other.

To whom do we Share your Personal Data

In order to provide you with products and services suitable to your needs, we may share your information with:

- various units, offices and stores of the Bank;
- subsidiaries, affiliates, and companies of the Metrobank Group;
- authorized/accredited agents, representatives and third-party service providers;
- banking associations, merchants, and partners;
- banks and financial institutions, credit agencies; and,
- regulatory and government agencies as required or authorized by law.

Risks Involved and How we Protect your Data

Risk refers to the potential of an incident to result in harm or danger to a data subject or organization. Risks may lead to the unauthorized collection, use, disclosure, or access to personal data. It includes risks involving the confidentiality, integrity, and availability of personal data or the risk that processing will violate the general data privacy principles and the rights of data subjects.

Metrobank ensures that adequate physical, technical, and organizational security measures are in place to protect personal information's confidentiality, integrity, and availability. However, this does not guarantee absolute protection against certain risks involving the processing of personal data, such as when systems are exposed to targeted cyberattacks, malware, ransomware, and computer viruses or when manual records are accessed without authority.

However, adequate policies are in place to ensure appropriate security incident management in line with the Banks existing policies and procedures.

Your Safety is our Priority

We care for the safety and security of all our clients and partners. Because of this, we highly encourage the following:

1. *Protect and update your information.* Keep your data safe by making sure your account details, PINs, username, and password are not accessible to others. Use strong passwords and change them regularly. When on electronic platforms, make sure to use devices that are safe and keep your software updated. We will not be able to serve you properly if your information is not updated. Make sure the information you submit is accurate, complete, and not misleading. Keep documents that can verify your information safe and available. If there are changes to your information, inform us immediately.
2. *Contact us through secure channels.* Take advantage of our secure channels by contacting us through our website, branches, Contact Center, MetrobankDirect Online, and MetrobankDirect Mobile. When communicating via email, never disclose sensitive information such as account numbers, credit card numbers, or passwords. We will never

ask you for these via email. We will also never ask you to click a link to verify your information. If we need sensitive information, an authorized bank representative will get in touch with you.
3. *Report any data issues.* If you think your data has been mishandled in terms of confidentiality or integrity, or if you think your data has been tampered with, contact us through any secure channels mentioned above.

Your Data Privacy Rights

Under the DPA, you have the following rights:

1. *Right to be informed.* The right to be informed whether your personal data shall be, are being, or have been processed, including the existence of automated decision-making and profiling.
2. *Right to access.* The right to demand reasonable access to your data and obtain a copy of such data in an electronic or structured format.
3. *Right to object.* The right to object to the processing of your personal data where such processing is based on consent or legitimate interest.
4. *Right to erasure or blocking.* The right to request for the suspension, withdrawal, blocking, removal, or destruction of your personal data from the PIC's filing system, in both live and backup systems.
5. *Right to damages.* The right to be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorized use of your personal data, taking into account any violation of your right and freedoms as data subject.
6. *Right to file a complaint.* If you feel that your personal information has been misused, maliciously disclosed, or improperly disposed, or that any of your data privacy rights have been violated, you have a right to file a complaint with the NPC.
7. *Right to rectify.* The right to dispute the inaccuracy or error in your personal data and have the PIC correct the same within a reasonable period of time.
8. *Right to data portability.* The right to obtain from the PIC a copy of your personal data and/or have the same transmitted from one PIC to another, in an electronic or structured format that is commonly used.

Contact Us

For any queries, clarifications, comments, or requests regarding any aspect of this Notice, the exercise of your rights pertaining to your personal data or to provide any feedback about our processing of personal data, please send us a message, visit any of our branches, or feel free to contact our Data Privacy Department through the channels provided below:

Data Protection Officer
Address: 2nd Floor, The Shops Grand Central Park, 7th Avenue corner 36th and 38th Streets, North Bonifacio District, Bonifacio Global City Taguig, 1637 Metro Manila
Telephone Number: 63-02-8-857-5539
E-mail Address: dataprotectiondept@metrobank.com.ph