DATA PRIVACY MANUAL

Philtrust Bank respects and values the data privacy rights of its customers and employees, and promotes the protection of their personal data. Hence, the Bank adopted the Privacy Manual consistent with Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012, its Implementing Rules and Regulations, and other relevant policies and issuances of the National Privacy Commission and the Bangko Sentral ng Pilipinas.

The Data Privacy Manual outlines the Bank's policies and procedures on data protection to ensure that personal data collected by the Bank from its clients and employees are processed in adherence to the general principles of transparency, legitimate purpose, and proportionality. The major areas covered by the Manual are as follows:

Processing of Personal Data. Processing of personal information of customers and employees is done only upon securing the latter's consent, except in cases where consent is not required by law. Data subjects are required to be provided with specific information on the purpose and extent of the processing, including the period within which the information shall be retained. The Bank is allowed to share information only upon due execution of Data Sharing Agreement. Disposal of collected personal data may only be done through secured means.

Security Measures. As mandated by the regulations and the Data Privacy Manual, the Bank adopted measures (organizational, physical and technical) designed to preclude occurrence of a security incident and/or data breach. As part of the organizational measure, Data Protection Officer (DPO) is appointed to monitor the Bank's compliance with the mandate of law and it's implementing rules and regulations. For the physical and technical security measures, access to the Bank's data processing systems, as well as its facilities and equipments, are subject to specific procedures and controls.

Management of Security Incidents and Data Breach. The IT Management Committee is tasked to ensure that all security incident or data breach are managed and resolved effectively. Further, the Committee is required to regularly evaluate the plan, incident reports, and data breaches experienced by the Bank every year to determine the effectiveness of the plan and recommended remedial measures to address noted deficiencies. The DPO, on the other hand, is tasked to consolidate all reported security incidents/data breach and submit a summarized report to the NPC annually.

Inquiries and Complaints. Inquiries, concerns, and complaints of the data subjects in relation to the exercise of the foregoing rights shall be received, acknowledged, and resolved by the Bank in accordance with the guidelines provided under the Customer Assistance Policies and Procedures, subject to monitoring by the DPO.