First Financial Holding Co., Ltd. Personal Information Protection Policy

I. Purpose and Applicability

The Policy is established in accordance with the "Personal Information Protection Act" of Taiwan, General Data Protection Regulation (GDPR) of the European Union, and related regulations of the competent authorities for the protection and management of personal information, fulfillment of the duties for protecting customer information, and protection of customer privacy and rights from infringement.

The Policy applies to all business conduct, appointed tasks, or other relations (including without limitation purchases and sales or proxies) implemented by all personnel of the Company and subsidiaries (hereinafter referred to as the "Companies") as well as related external parties.

II. Goals

(I) Comply with domestic personal information protection regulations and administrative orders issued by competent authorities.

(II) Comply with the requirements for the Companies to process personal information in accordance with the General Data Protection Regulation (GDPR) of the European Union.

(III) Protect the moral rights of the individuals of concern of personal information and provide them with legal discretion over their personal information.

(IV) The collection, processing or use of personal information should be handled in accordance with the principle of bona fide. It should not go beyond the purpose of collection and should be reasonable and fair.

(V) Adopt appropriate security measures for personal information files and ensure the Companies' duty of care as prudent managers.

III. Definitions

(Nature of information captured)

The "personal information" specified in the Policy refers to the name, date of birth, I.D. Card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical record, medical treatment, genetic information, sexual life, health examination, criminal record, contact information, financial conditions, and social activities of natural persons defined in the "Personal Information Protection Act" of Taiwan, other information which may be used to identify a natural person, both directly or indirectly, and "special categories of personal information" specified in GDPR such as race, ethnicity (e.g.

ancestry), political views, religions or philosophical belief, trade union member (e.g. members of unions), genes, health records (e.g. mental state), sexual life, sexual orientation, and biometric data (e.g. fingerprints, facial recognition, and retinal scan), and criminal records. "Personal information incidents" refers to violations of the "Personal Information Protection Act" of Taiwan, GDPR, or related regulations that result in the theft, leak, or altercation of personal information or other infringements. The "principal" refers to an individual of whom the personal information has been collected, processed or used.

IV. Organization and Duties

The Companies shall assign dedicated units to take charge of the formulation of related personal information management regulations, training plans, exercises for processing personal information incidents, coordination of personal information management tasks, and resource integration. The Companies may, based on the scale of business operations, establish an independent Personal Information Protection Management Committee to regularly review the execution of the aforementioned items and review improvement measures.

The management units of the Companies shall be responsible for various operations for personal information management in accordance with their duties and the scope of authorization. They shall also fully cooperate with designated units.

V. Principles for the Collection, Processing and Usage of Personal Information

(I) The Companies shall identify the personal information to be processed and define the scope of personal information.

(II) The Companies shall use legal, reasonable, and secure methods to collect, process, and use personal information within the scope of specific goals.**(Use of the collected information)**

(III) The Companies shall clearly inform the principal of the unit responsible for processing and using its personal information and the methods of processing and use and inform the principal of the influence on his rights and interests if the principal chooses not to provide personal information.

(IV) The Companies shall ensure the accuracy of personal information and update whenever necessary.

(V) The Companies shall store and process personal information in accordance with regulatory requirements or legitimate and reasonable purposes.

(VI) The Companies shall respect owners' rights over their personal information, including the right to inquire, view, duplicate**(Request access to data held by the company)**, supplement or amend existing information**(Request their data be corrected)**, and the **right to request the cessation of the collection, processing and use of personal**

data by the Company(Opt-out option), and the right to delete personal information held in possession**(Request their data be deleted)**. The Companies shall also establish contact windows for complaints and consulting and allow the principal to exercise rights over their personal information.

(VII) The Companies shall transmit personal information across borders only when the information is properly and adequately protected.

(VIII) The Companies shall provide personal information to authorities with investigation rights only within the scope regulated by laws and only when the information is properly and adequately protected.**(Third-party disclosure policy)**

(IX) In the event that the Companies assign the collection, processing, and use of personal information to an agency, they shall supervise the agency in an appropriate manner.

(X) When using personal information under exceptional circumstances granted by the "Personal Information Protection Act," the Companies shall take extensive care to ensure the applicability and legitimacy of such circumstances;

(XI) The use of customers' information between subsidiaries shall be governed by the "Rules Concerning Cross-Selling by Financial Holding Company Subsidiaries" and the customer shall be provided with a field to specify its consent.**(Opt-in consent)**

(XII) The Companies shall establish and implement a robust personal information management system to support its Personal Information Policy.

(XIII) The Companies shall clearly define the duties and obligations of all personnel of the Companies, institutions related to the Companies (including without limitation purchases and sales or proxies), and their personnel in the personal information management system.

(XIV) Personal information incident must be processed as quickly as possible in accordance with the "Personal Information Protection Act" and the Companies related regulations for personal information.

(XV) Related operating procedures shall be established for businesses in the applicable scope of GDPR for compliance.

VI. International Transmission of Personal Information

Companies shall comply with all restrictions and related regulations for international (cross-border) transmission of personal information.

Where overseas units within the EU are required to transmit personal information of natural persons of the EU to other units outside the borders of the EU, they shall sign the Standard Contractual Clause (SCC) approved by the local competent authorities or meet other regulations for international transmission in the GDPR before the transmission. They shall also abide by related regulations in GDPR for personal information protection.

VII. Processing the Exercise of Rights by the Principal

(Request their data be transferred to other service providers)

The management units of the Companies shall establish related regulations for the exercise of the principal's rights for the respective businesses.

The rights of the principal includes the five rights granted to the principal in the "Personal Information Protection Act" which it may exercise with respect to his personal information, including, with respect to the said personal information, "inquiries or reviews", "making duplications", "supplementations or corrections", "deletions", and "the ceasing of the collection, processing or use thereof". They also include the six rights granted to the principal in the GDPR which it may exercise with respect to its personal information, including, with respect to the said personal information, "right of access (e.g. 'inquiry or viewing' or 'production of duplicate')", "right to rectification", "right to erasure (to be forgotten)", "right to restrict processing", "right to refusal", and "right to data portability".

(How long the information is kept on corporate files)

When the principal exercises its right, the Companies shall verify the identity of the principal or its agent before processing. The processing results shall be provided to the principal within a specified period and the contents of the processing, response time, and response method (mail or telephone) shall be carefully recorded. Related documents must be appropriately retained and the retention period shall be processed in accordance with the business regulations. Where such regulations are not provided, they shall be kept for at least 5 years.

VIII. Operations of Personal Information Protection and Management

The Companies shall ensure the security of personal information files and prevent the theft, leakage, altercation, or other infringement of personal information.

(How the information is protected)

Structure and Operations: The Companies shall establish personal information protection management organization structure to take charge of the promotion, coordination, supervision, and improvement of the personal information management system. They shall also allocate required resources to ensure the implementation of the Policy.

The Companies' compliance units shall regularly review the "Personal Information Protection Act" of Taiwan, GDPR, other related regulations, industrial norms, information technology, and the Companies' latest business development status to ensure the effectiveness of the operations of the personal information management system. The Companies' information technology units shall establish response measures for intrusion

from external networks, monitoring and response mechanisms for illegal or irregular usage, and other information security measures for commercial activities relating to the advertising, marketing, supply, purchase, or delivery of products or services using the Internet. They shall also organize regular drills and review improvement measures.

Execution and Management: The Companies' management units shall regularly review the personal information files of each respective business and define the scope of such information. They shall also assess potential personal information risks and establish management and control mechanisms for the personal information files, lists, environmental security, and information security for related businesses based on the risk assessment results.

Response and Prevention: The Companies shall establish procedures for reporting, processing, and preventing personal information incidents. The units responsible for managing personal information shall conduct drills for responding to personal information incidents and regularly file self-assessment reports. They shall plan and execute improvement and prevention measures if the assessment report shows any potential violation of laws to ensure effective processing and response in the event of personal information incidents.

Complaint channel: The "Stakeholder Communications" section of FFHC's official website also includes online customer support for the Group's Companies, a toll-free 0800 customer hotline, business inquiry hotline, and complaint e-mail. The Companies' compliance units are responsible for registering and reporting cases. First Bank customers are provided with the 24-hour toll-free service hotline 0800-031-111 in accordance with the "Customer Opinion Response Operational Guidelines" as well as the following complaint channels specified in the "Implementation Rules of the Whistleblower System":

(I) Tel: 02-23898688

(II) Fax: 02-23612554

(III) Email: audit@firstbank.com.tw

(IV) Mailing address: Audit Division, 13F, No. 30, Sec. 1, Chongqing S. Rd., Zhongzheng Dist., Taipei City

IX. Internal Control and Internal/External Audit

The Companies shall include personal information management in the internal control system and regularly organize self-inspection tasks to ensure the implementation of the Policy.
The Companies' audit units shall conduct regular audits and assessments on personal information management. The Companies shall appoint CPAs to perform external audits each year in accordance with the "Implementation Guidelines for Self-Evaluation Procedures of the Internal Control System" and Article 31, Paragraph 1 of the "Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries" of the FSC.

X. Training and Procedures for Violations

The Companies shall provide education and training sessions on personal information protection for all employees. Violation of the Policy and related regulations shall be punished in accordance with related laws or related human resource management regulations.

XI. Basis of Governing Unaddressed Matters

Matters not covered in the Policy shall be processed in accordance with the applicable laws or the related regulations of the Companies.