Personal Data Protection Management Policy of Taiwan Cooperative Financial Holding Co., Ltd.

Reviewed and approved by the 35th meeting of the 4th term board of directors on May 22, 2023

Article 1. (Purpose)

To fulfill the purpose of protecting personal data and privacy rights, and be in compliance with relevant personal data protection laws and regulations, Taiwan Cooperative Financial Holding Co., Ltd. (hereinafter referred to as "the Company") has enacted this Policy to safeguard the rights of data subjects.

Article 2. (Management objectives)

The management objectives of this Policy are as follows:

1. To ensure that the Company and its subsidiaries comply with the provisions of personal data protection laws, customer contracts, and other relevant regulatory requirements in the execution of their business operations.
2. To safeguard the legal rights and interests of data subjects.
3. To collect, process, and use personal data in a reasonable and secure manner within the necessary scope for specific purposes, in accordance with legal organizational operations and business activities.
4. To provide appropriate security measures for personal data files, ensuring that the Company and its subsidiaries fulfill their duty of care as good data administrators.

Article 3. (Applicable parties)

This Policy applies to the Company, its subsidiaries, and suppliers entrusted by the Company and its subsidiaries to collect, process, or use personal data. Subsidiaries shall consider this Policy and take their business scale and characteristics into account to establish personal data protection management organizations and systems, and the said systems shall be incorporated into their internal control and audit items. In addition, subsidiaries shall supervise their subordinate companies in accordance with this Policy to ensure the implementation of personal data protection management.

Article 4. (Organization management and operation)

The Company shall establish a personal data protection management

organization and allocate appropriate resources to oversee the personal data protection management of the Company and its subsidiaries. A dedicated unit or personnel member shall be assigned to plan, coordinate, and establish regulations and systems for personal data protection management.
The Company shall incorporate personal data protection into its risk management supervision and include relevant mechanisms in internal control and audit items to ensure the effective implementation of this Policy and related regulations.

Article 5. (Principles of personal data collection, processing, and use)
The principles of personal data collection, processing, and use are as follows:

1. Identify the personal data being processed and define the scope of personal data to establish personal data files.
2. Collect, process, and use personal data within the necessary scope based on legitimate and specific purposes. Update personal data when necessary to maintain accuracy and completeness and ensure the security of personal data.
3. Clearly inform the data subjects of the statutory notification requirements.
4. The Company respects the data subjects' exercise of rights regarding their personal data, including the right to inquire or request access, request copies, request supplementation or correction, request cessation of collection, processing, or use, and request deletion, in which the Company shall provide appropriate assistance.
5. Cross-border transfer of personal data shall comply with relevant laws or regulations of competent authorities and only be conducted under appropriate and sufficient protection.
6. When personal data is applied in exceptional circumstances allowed by the Personal Data Protection Act, its appropriateness and legality shall be ensured.
7. Establish and implement a personal data protection management system to enforce the personal data protection management policy.
8. Clearly define the responsibilities and obligations of employees in the operation of the personal data protection management system.
9. Properly retain records of the trajectory of personal data collection, processing, and use.
10. Establish response and prevention procedures for personal data security incidents, and process and notify data breaches in accordance with regulations.
11. When personal data collection, processing, and use are commissioned to others, appropriate supervision shall be exercised, and the content shall be

clearly stipulated in the outsourcing contracts or relevant documents.

12. Take appropriate measures for personal data security management (e.g., firewalls) to prevent unauthorized access and data breaches.
13. If data subjects are subject to the General Data Protection Regulation (GDPR) of the European Union, relevant regulations shall be established to ensure compliance. The data subjects shall be informed of the statutory notification requirements and the rights they may exercise (e.g., restriction of processing or use, data portability rights).

Article 6. (Risk assessment and regular audit)

The Company shall assess the potential risks associated with the personal data files generated from business operations and establish appropriate control measures based on the results of the risk assessment.

The Company shall conduct regular internal audits to examine the effectiveness of the personal data protection management system and its implementation. As required by the competent authorities, subsidiaries shall engage external organizations to conduct audits.

The Company shall make improvements based upon the results of internal and external audits to ensure the effective operation of the personal data protection management system.

Article 7. (Zero Tolerance Policy)

In the event of personnel from the Company or its subsidiaries in violation of personal data protection laws or internal regulations, appropriate disciplinary measures or legal actions shall be taken depending on the severity of the circumstances, in accordance with relevant provisions.

Suppliers or their personnel violating personal data protection laws or contractual provisions related to personal data protection, resulting in damages to the Company or its subsidiaries, shall be liable to compensate for such damages.

Article 8. (Review and update)

The Company shall review this Policy in a timely manner to reflect the latest developments in government regulations, personal data management technologies, requirements of competent authorities, and its business operations, ensuring compliance and effectiveness in personal data protection management practices.

Article 9. (Supplementary provisions)

Matters not stipulated in this Policy shall be handled in accordance with relevant laws and regulations on personal data protection, the GDPR of the European Union, and the provisions of the Company and its subsidiaries.

Article 10. (Implementation)

This Policy shall become effective after being approved by the board of directors. Any amendments to this Policy shall follow the same procedure.