Mega International Commercial Bank Personal Data Protection Management Policy

Note：If the English version contains any discrepancy from the original Chinese version, the original Chinese version shall prevail.

Enactment approved by the 36th meeting of the 15th Board of Directors on May 11, 2018
To the department's name upon authorization in the 35th meeting of the 15th Board of Directors on Apr. 20, 2018
Amendment approved by the 4th meeting of the 17th Board of Directors on March 4, 2022
To the department's name upon authorization in the 15th meeting of the 17th Board of Directors on Jan. 13, 2023

Article 1 (Basis)

The Policy is established to comply with the R.O.C. (Taiwan) Personal Data Protection Act, Regulations for Setting up the Security Measures of the Personal Data File for Non-government Agencies designated by the Financial Supervisory Commission R.O.C. (Taiwan), and relevant personal data protection provisions formulated by the local governments where the foreign branches and subsidiaries (hereinafter referred to units) are located.

Article 2 (Definition)

Personal data in the Policy refers to the name, date of birth, personal identification card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical record, medical treatment, genetic data, sexual life, health examination, criminal record, contact data, financial conditions, social activities and other data may be used to identify a natural person, both directly or indirectly.

Besides the categories of personal data in the preceding paragraph, each foreign units shall comply with the local personal data protection provisions.

Article 3 (Unit in Charge)

The Compliance Department shall formulate and maintain the Policy.

The Responsible Units shall coordinate the personal data protection management with other administration units, compliance unit, risk control unit and audit unit of the Head Office.

The responsibilities of Responsible Units mentioned in the preceding paragraph shall be divided as follows:

1. Business Administration Department: serves as the Responsible Unit of the personal data protection management for domestic branches and Head Office.
2. Overseas Business Management Department: the Responsible Unit of the personal data protection management for foreign units.

Article 4 (Operational Procedures)

For the purpose of planning, establishing, and executing the security measures for the personal data file, the disposal measures for the personal data after termination of business and the related personal data protection measures, the Bank shall allocate the reasonable personnel and corresponding resources. The measures include but not limit to the following:

1. Regularly confirm the personal data files.
2. Evaluate the risk and management mechanism of personal data.
3. Establish the response and preventive mechanism of personal data incident.
4. Establish the procedures for collecting, processing and using personal data.
5. Set up the security measures of personal data and equipment.
6. Establish the security standards of data (including regular drills and reviews for improvement).
7. Manage the authority of access to personal data and retain the records.

The administration units of the Head Office shall establish the management mechanism mentioned in the preceding paragraph according to its responsibilities, and review the effectiveness and reasonableness of it to comply with the relevant personal data protection provisions and the requirements of the competent authority at least once per year.

Article 5 (Regulations Applicable to Overseas Units)
Due to the compliance with the local personal data protection provisions, the foreign units may establish their own regulations and implement after the approval or the acknowledgement by the Overseas Business Management Department.

If the regulations mentioned in the preceding paragraph conflict with the Policy or other internal personal data protection measures, the foreign unit shall submit the local provisions and corresponding solutions to the Overseas Business Management Department. The solutions shall be approved by the domestic competent authority before implementation.

Article 6 (Self-assessment report)
The units which retain the personal data or personnel who keep the personal data shall submit a self-assessment report of the personal data management on a yearly basis. The President is delegated the authority to grant approval to the self-assessment report.

Article 7 (Training)
The Bank shall conduct the training in regard to the personal data protection provisions to the employees on a regular basis to have them awareness of the requirements of the relevant regulations, the responsibilities and the operation of the personal data protection mechanisms, procedures, plans and measures, including the Policy.

Article 8 (Internal Control)
The execution of the Policy and the other personal data protection mechanisms, procedures, plans and measures, shall be included into the operational risk self-assessment, self-conducted audits, compliance self-evaluation and internal audit items.

Article 9 (Unspecified Matters)
Matters not prescribed herein shall be conducted in accordance with relevant laws or rules of the competent

authority, and the Bank's other relevant rules.

Article 10 (Approval Level)

The Policy shall be implemented upon approval by the Board of Directors, and the same shall apply to its modifications or revocation.