Mega International Commercial Bank

Standards of Personal Data File Security

Approved by the 14 th Board of Directors on 7th Feb., 2014

Approved by the 15 th Board of Directions on 26th Aug., 2016

Amended due to the organization adjustment on 29th Sep., 2016

Approved by the 15 th Board of Directions on 28 th Sep., 2018

Amended with authorization on 22th Feb., 2019

Approved by the 17 th Board of Directions on 4th Mar., 2022

Chapter 1 General Provisions

Article 1 (Legal Basis)

In order to strengthen the management of personal data, and ensure the security of personal data of Mega International Commercial Bank (hereinafter "the Bank"), it will be handled in accordance with the "Regulations Governing Security Measures of the Personal Information File for Non-government Agencies Designated by Financial Supervisory Commission (hereinafter "FSC")", and the Bank's "Personal information Protection Management Policy", the Standards herein are stipulated and enforced.

Chapter 2 Personal Data Protection Planning

Article 2 (Unit in Charge)

The Standards are formulated and maintained by the Responsible Units as set out in Article 3 of the Bank's "Personal Information Protection Management Policy". If the revisions of the common issues of Head Office and Domestic (Overseas) Branches, it shall be determined in accordance with domestic or foreign regulations by each of the Responsible Units according to their business responsibility.

Article 3 (Personal Data Protection Mechanism)

When each business unit is involved in the collection, processing or use of personal data, it does not only in accordance with this Standards, but also assess the risk of personal data that may arise depending on the characteristics of business; therefore the assessment results may be arranged other applicable personal data protection mechanisms, procedures and measures beyond its business separately; while those personal data protection mechanisms, procedures, and measures stipulated otherwise for the same object from this Standards, the Standards shall govern.

The stipulated in the preceding Paragraph, other personal data protection mechanisms, procedures and measures in accordance with the Standards shall be signed by the Responsible Units. If it is set for the code of practice, as well as amending or abolishing, it shall be implemented after approval by the Senior

Executive Vice President.

Overseas branches may establish relevant personal data protection mechanisms in accordance with the local personal data protection regulations, and implement the mechanisms after the approval or the acknowledgement by the Overseas Business Management Department.

Article 4 (Overseas Branches Management Measures)

Overseas Branches shall report the implementation of personal data protection to the Overseas Business Management Department for every quarter, and notify the Overseas Business Planning Department. The report shall include but not limited to the revision of the law, audit deficiencies/findings and improvement measures by internal and external inspection agencies, and the occurrence and handling of personal data breach events.

The Overseas Business Management Department should check whether the relevant regulations or operating procedures of the foreign branches are required to improve for deficiencies/findings disclosed in the report, and if it is necessary, the Overseas Business Management Department shall notify other business units.

The reporting time and methods for the status of handling the personal data protection made by Overseas branches set out in Paragraph 1 hereinabove shall be determined by the Overseas Business Planning Department.

Article 5 (Personal Data Management Officer)

Each unit shall designate its Deputy Supervisor as Personal Data Management Officer, to be responsible for supervising the unit to implement the Standards and the relevant personal data protection mechanisms, procedures and measures, and designate a Class A supervisor as agent. Whereas if a unit is not set up a Deputy Supervisor, 2 Class A supervisor should be designated as Personal Data Management Officer and agent.

The Personal Data Management Officers list, agent list and contact number should be set up in Personal Data Management Officer report system beforehand. If there's any changes, the changes should be registered in 2 business days after the adequate candidate take over.

Each unit shall, in accordance with the relevant laws and regulations of the R.O.C. Personal Information Protection Act (hereinafter "Taiwan Personal Information Protection Act"), as well as every business unit's personal data protection mechanisms, procedures and measures, to examine and audit the status of its personal data files at least once a year, and keep the inventory for future reference.

Article 6 (Personal Data Accidents Reporting Mechanism)

In response to the security incidents (hereinafter "the Incidents") from personal data being stolen, altered , damaged, destroyed or disclosed, etc., the Responsible Units shall formulate the following responses, notifications, and prevention mechanisms:

1. Various measures to be taken after the Incidents, including:

   (1) The manner in which the party's damage is controlled.

(2) Identifying appropriate ways to notify the parties after the Incidents.

(3) The parties who should be informed of the facts of the Incidents, the corresponding measures, and the advisory service hotline.

2. The person to be notified after the Incidents and notification methods.

3. The developing mechanism for corrective and preventive actions after the Incidents.

In case of any major personal data incidents, the Bank's Responsible Units shall fill out the attachment of Article 6 of the "Regulations Governing Security Measures of the Personal Information File for Non-government Agencies Designated by Financial Supervisory Commission" to notify the FSC in 72 hours (including regular holidays), where there is other procedure in different law or rule, shall follow it as well; moreover, the developing mechanism for corrective and preventive actions under Item 3 of the preceding Paragraph shall be comprehensively examined and reviewed by fair and independent experts with relevant recognized certifications.

The term "major personal data incident" as mentioned in the preceding Paragraph refers to the situation in which personal data has been stolen, altered , damaged, destroyed or disclosed, which will endanger the Bank's normal operation or a large number of parties' interests.

Article 7 (Training)

In addition to the new employment training, the Human Resources Department shall, at least once a year, apply personal data protection awareness and education training to the staff to make them aware of the requirements of relevant laws and regulations, the scope of responsibility and various personal data protection mechanism, procedures and measures.

Chapter 3 Personal Data Managements and Measures

Article 8 (Management Procedure)

The Responsible Units shall establish a personal data management procedure on the following matters:

1. To the person, who collects, processes or uses personal data, inclusive of the sensitive personal information specified in Article 6 of Taiwan Personal Data Protection Act, should inspect the specific purpose and whether it meets the requirements of the relevant laws and regulations; if it is be consented in writing by parties, the person shall ensure that it is complied with the requirements in Paragraph 2 of Article 6, which shall apply mutatis mutandis to Paragraph 1, 2 and 4 of Article 7 of Taiwan Personal Data Protection Act.

2. To examine whether the collection and processes of personal data meet the requirements for exemption from notification and whether the content and notification methods are legal and appropriate.

3. To examine whether the collection and processes of general personal data comply with Article 19 of Taiwan Personal Data Protection Act with specific purposes and legal circumstances; and with the consent of the parties, it shall

ensure in accordance with Article 7 of Taiwan Personal Data Protection Act.

4. To examine whether the use of general personal data meets the necessary scope of specific purpose of collected is in accordance with Article 20 of Taiwan Personal Data Protection Act; if it is used outside the scope by users, it shall be checked whether it meets the legal circumstances, and if it is consented by the parties, should as well as in accordance with Article 7 of Taiwan Personal Data Protection Act.

5. When the parties express their refusal to the marketers who use their personal data for marketing, the marketers should stop using those personal data immediately; furthermore, when doing marketing at least upon the first time, marketers shall provide the means for the parties to refuse accepting marketing for free.

6. When entrusting others to collect, process, or use all or part of personal data, the trustee shall be properly supervised in accordance with Article 8 of Enforcement Rules of the Taiwan Personal Data Protection Act, and clearly set those contents in the entrustment contract or related documents.

7. Before conducting the international transfer of personal data, the Responsible Units shall examine whether it is restricted by the FSC and other competent authorities, and followed those restrictions.

8. To Matters relating to the rights set forth in Article 3 of Taiwan Personal Data Protection Act:

   (1) To confirm the identity of the party.

   (2) To provide the means by which the parties exercise their rights and inform them of the fees to be paid as well as the matters to be explained.

   (3) The method of reviewing the request of the parties, and complying with the provisions for the processing period of Taiwan Personal Data Protection Act.

   (4) There is a matter mentioned in Taiwan Person Data Protection Act allows the parties to be refused to exercise their rights, and the notify methods should be record.

9. To examine whether the personal data in the process of collecting, processing or using is correct; if it has inaccuracy or accuracy dispute, it shall be handled in accordance with Paragraph 1, 2 and 5 of Article 11 of Taiwan Personal Data Protection Act.

10. To examine whether the specific purpose of the personal data held by the entities has disappeared, or whether the period has expired; if the specific purpose disappears or the period expires, the data shall be deleted, stopped processing or using according to Paragraph 3 of Article 11 of Taiwan Personal Data Protection Act.

The method of consent of parties in Article 7 of Taiwan Personal Data Protection Act, not limited in writing, is stipulated in Subparagraph 3 and 4, except as otherwise provided by the laws. However, the record shall be retained to facilitate the subsequent evidence.

Article 9 (Safety Management Measures)

In order to maintain the security of personal data held by the Bank, the Bank shall adopt the following safety management measures for the equipment:

1. To stipulate specifications for the use and storage of various types of equipment or storage media or other media, including but not limited to the implementation of appropriate access controls, the establishment of appropriate protective equipment or technology according to the characteristics of the media and their environment, as well as the appropriate measures to prevent data breach when being scrapped or converted for any other purpose.
2. For the content of the personal data held by the Bank, if there is a need for encryption, it shall adopt appropriate encryption measures.
3. When the operation process has the need to back up personal data, the backup data should be properly protected.

When the personal data is processed or used by the Bank on magnetic disks, magnetic tapes, optical discs, microfilms, integrated circuit chips, computers or automated machines and equipment, the Data Processing & InformationDepartment shall arrange the safety management measures as mentioned in the preceding Paragraph; if the personal data is handled and used in paper forms or by other medium, the data safety management measures of the preceding Paragraph shall be determined by the Responsible Units.

Article 10 (Information Security Measures)

For the Bank's e-commerce service system, the Data Processing & Information Department shall adopt the following information security measures:

1. A user identification and protection mechanism.
2. A hidden-code mechanism of personal data display.
3. A security encryption mechanism of the Internet transmission.
4. An application system of software verification and validation procedures in the development, migration, maintenance, and other stages.
5. Access controls and protection monitoring measures for personal data files and databases.
6. A countermeasures for external network intrusion prevention.
7. A monitoring and reporting mechanisms for illegal or abnormal use.

The term "e-commerce" as mentioned in the preceding Paragraph refers to various commercial transactions, such as advertising, marketing, supplies, orders or deliveries, which is relevant to goods or services through the Internet.

For the measures specified in Subparagraph 6 and 7 of Paragraph 1, the Data Processing & Information Department shall conduct drill to review and get measures improved at least once a year, as well as notifying the Information Security Department and the Responsible Units.

Article 11 (Permissions and Restrictions)

In order to maintain the security of personal data held by each unit, according to the necessity of executing business, it shall set the authority of the relevant personnel and control the connections those who can access personal data; moreover, the personnel of each unit should be subject to a duty of confidentiality.

Chapter 4 The Security Audit, Records Retention and Continual Improvement Mechanism of Personal Data

Article 12 (Audit Checklist)

The Standards and other relevant statuses of handling personal data protection mechanisms, procedures and measures shall be included in operational risk self-assessments, self-inspection, compliance self-evaluation and internal audit checklist.

Article 13 (Evidence Retention)

When each unit implements the Standards and relevant personal data protection mechanisms, procedures, and measures, it shall record the status of handling of use of personal data, and retain the record tracks, or relevant evidence for future reference.

After each unit have deleted, stopped processing or using the personal data held in accordance with Paragraph 3 of Article 11 of Taiwan Personal Information Protection Act, the following records shall be kept:

1. The method and time to delete, or stop processing or using.
2. The reason, object, method, time, and legal basis for the collection, processing, or use of personal data that is deleted, stopped processing or using for transfer to other objects

The trajectory, relevant evidence and records of two preceding Paragraphs shall be retained for at least five years, unless otherwise prescribed by applicable statutes or administrative regulations or agreements.

Article 14 (Self-assessment Report)

The Personal Data Management Officer of each business unit shall review the compliance self-evaluation, self-inspection, and internal and external audit report, as well as the deficiencies of personal data management and review measures discovered by each business unit in the year lately, and submit its self-assessment report for personal data management to the Compliance Department before the end of every January, and the department would put forward those self-assessment reports for personal data management to the supervisors, being responsible for the self-assessment of operation risk in each business unit as a reference for the evaluation of the risk self-assessment project related to personal data management.

The Compliance Department shall summarize the self-assessment reports and the deficiencies of personal data management and review measures discovered by each business unit, and submit a self-assessment report for the Bank's personal data management before the end of every February.

The President is delegated the authority to grant approval to the self-assessment

report of the Bank mentioned in the preceding Paragraph.

In the case of violations of the laws and regulations in the self-assessment report of Paragraph 1 and 2, the Compliance Department shall, by itself or by the Responsible Units, to coordinate the planning, implementation of its improvement, and preventive measures.

Article 15 (Administrative Evaluation)

The Standards are reviewed by the Responsible Units at least once a year; moreover, each business management unit should arrange its mechanisms, procedures and measures of personal data protection and review them at least once a year.

Article 16 (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 17 (Approval Level)

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