King's Town Bank Personal Data File Security Maintenance Regulation

Chapter 1. General Rules

Article 1: The Bank has formulated this Regulation according to Article 3, Paragraph 1 of the "Regulations Governing Security Measures of the Personal Information File for Non-government Agencies Designated by Financial Supervisory Commission" in order to plan, formulate, revise, and implement the Bank's Personal Data File Security Maintenance Plan and Post-Business Termination Personal Data Processing Method.

Article 2: The definitions of "personal data" and "personal data files" in this Regulation comply with the provisions provided by the Personal Data Protection Act.

Article 3: All units shall follow the following principles during personal data collection, processing, or utilization:

I. Personal data collection must respect the rights of those involved, be conducted honestly and transparently, be limited to what is necessary for a specific purpose, and demonstrate relevance to that purpose.

II. The personal data collection must be minimized to what is necessary. Internal data transmission shall also avoid unnecessary personal data delivery. When sharing data internally, prioritize providing only the minimum necessary data fields and consider anonymizing the data if possible.

III. Formulate a privacy policy to clearly inform customers of the Bank's measures for protecting personal data and privacy, and provide an online privacy policy on the Bank's website to inform customers that their data transmitted over the Internet is adequately protected.

IV. When collecting, processing, or using personal data, observe the confidentiality of customer data and the duty of care of a prudent manager.

Chapter 2. Personal Data Protection Enforcement Unit

Article 4: The Bank has established a Personal Data Protection Management Executive Committee (hereinafter the "Personal Data Committee"). Its tasks are as follows:

I. Research and draft personal data protection regulations and review management systems.
II. Coordinate the division of responsibilities for personal data protection matters.
III. Review and supervise matters related to personal data protection.
IV. Submit a self-assessment report on personal data security maintenance to the board of directors each year.
V. Handle personal data theft, alteration, damage, destruction, or disclosure incidents due to a violation of Personal Data protection Act (hereinafter "personal data breach").

Article 5: The Personal Data Committee shall have one convener, who shall be appointed or designated by the General Manager. The remaining members shall be appointed by the heads of the Compliance Department, the Information Technology Department, the Customer Service and Operation Department, the Risk Management Department, the Human Resources Department, the Auditing Department, and the units designated by the convener.

Article 6: The Personal Data Committee shall convene meetings as required to promote businesses, but at least once a year, and shall be chaired by the convener. If the convener is unable to preside over the meeting due to any reason, a member may be designated to act on the convener's behalf.

Article 7: The Personal Data Committee shall have a secretariat to handle the following matters:

I. Act as the contact point for the Personal Data Committee and coordinate and liaise on matters related to personal data protection.
II. Formulate and amend the internal regulations of the Bank on personal data protection.
III. Assist the head office departments in conducting personal data inventory and submit the results to the Personal Data Committee for review after consolidation.
IV. Compile the annual self-assessment report on personal data security maintenance and submit it to the board of directors on behalf of the

Personal Data Committee.

Article 8: Each head office department shall assign a legal compliance supervisor or designate a person above the rank of assistant manager as the unit's data file security maintenance personnel to handle the following matters:

I. Personal data inventory within the unit.
II. Manage and maintain personal data files within the unit.
III. Internal notification contact for personal data breach within the unit.
IV. Other tasks assigned by the Personal Data Committee.

Chapter 3. Definition for the Scope of Personal Data Files, Risk Assessment, and Incident Response Mechanisms

Article 9: Each head office department shall define the scope of personal data files based on its business and subsequent use and maintenance of personal data processes and establish a personal data inventory list.

Each head office department shall conduct a personal data file inventory at least once a year. If there are any changes, the inventory list must be updated.

Article 10: Each head office unit shall assess the level of personal data risk that may be generated by the business process based on the scope of personal data files defined in the previous Article. After review by the unit supervisor, it shall be submitted to the Personal Data Committee for review.

The provisions of the previous Paragraph also apply to the execution of the personal data file inventory.

The personal data risk assessment and submission to the Personal Data Committee for review shall be handled according to the Bank's "Personal Data Risk Assessment Operation Guideline."

Article 11: Each unit shall handle the response, notification, and prevention of security incidents such as theft, alteration, damage, destruction, or disclosure of personal data according to the Bank's "Personal Data Breach Emergency Response Guideline."

Chapter 4. Personal Data Management Procedures and Measures

Section 1. Collection, Processing, and Use Procedures

Article 12: Each unit shall comply with the provisions of Article 6 of the Personal Data Protection Act when collecting, processing, and using special personal data such as medical records, healthcare, genetics, sex life, physical examination, and criminal records.

Article 13: When each unit collects personal data from the data subject, except for the circumstances stipulated in Paragraph 2 of Article 8 of the Personal Data Protection Act, the unit shall clearly inform the data subject of the following matters:

I. The name of the Bank and the unit.
II. The purpose of collection.
III. The categories of personal data.
IV. The period, territory, parties, and method of use of personal data.
V. The rights and methods that the data subject may exercise according to the provisions of Article 3 of the Personal Data Protection Act.
VI. The data subject may freely choose to provide personal data, and its rights shall not be impacted if it does not provide data.

The information required to be notified in the previous Paragraph may be provided to the data subject in writing, posted at the business premises, or displayed on the Bank's global website.

Article 14: Except for the circumstances stipulated in Article 12 of this Regulation, each unit must have a specific purpose and the legal circumstances stipulated in Article 19 of the Personal Data Protection Act when collecting and processing the personal data of the data subject. If the consent of the data subject is obtained, compliance must also be ensured with the provisions of Article 7 of the Personal Data Protection Act.

Except for the circumstances stipulated in Article 12 of the Regulation, each unit shall use the personal data of the data subject within the necessary scope of the specific purpose for which it was collected. If it is used for purposes other than the specific purpose, it must have the legal circumstances stipulated in the proviso of Article 20, Paragraph 1 of the Personal Data Protection Act. If the consent of the data subject is obtained, compliance must also be ensured with the provisions of Article 7 of the Personal Data Protection Act.

When using personal data for marketing purposes, if the data subject refuses to accept marketing, the use of their data for marketing must be stopped immediately. The data subject shall be provided with a free way to refuse to accept marketing, at least at the time of the initial marketing. The specific purpose for which personal data is collected must be considered in light of the business nature. The head office unit responsible for managing the business shall determine the specific purpose, with reference to the "Reference Template of Notification Obligation Content Fulfilled by Bankers Association Members According to Article 8, Paragraph 1 of the Personal Data Protection Act".

Article 15: When each unit entrusts others to collect, process, or use personal data, the entrusted party shall be subject to the provisions of this Regulation. The entrusting unit shall conduct appropriate supervision of the entrusted party and clearly stipulate its content in the entrustment contract or related documents according to the Bank's "Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Operation" or the internal regulations of the unit.
The entrusted party may only collect, process, and use personal data within the scope of the instructions of the entrusting unit.

Article 16: Before each unit conducts international transmission of personal data, it must confirm whether it is restricted by the competent authority and comply.

Section 2. Procedures for Handling the Exercise of Rights by Data Owners

Article 17: Except for the circumstances stipulated in Article 10 of the Personal Data Protection Act, the Bank shall, upon request of the data subject, answer inquiries, provide access to, or make copies of the personal data collected. If the data subject requests access to their data, the process shall be followed by the accepting unit.
The data subject shall be charged a fee according to the charging standards set by the head office units for applying for inquiries, access, or copies.

Article 18: The Bank shall maintain the accuracy of the personal data it holds and correct or supplement it upon request of the data subject.
If there is a dispute over the accuracy of the personal data held by the Bank, the processing or use of the personal data must be stopped

according to the working methods of the head office units. However, this is not limited to cases where it is necessary for business performance or with the written consent of the data subject, and the dispute is noted.

When the specific purpose for which the personal data held by the Bank is collected ceases to exist or the period expires, the personal data shall be deleted, stopped processing, or used according to the working methods of the head office units. However, this is not limited to cases where it is necessary for the performance of business or with the written consent of the data owner.

Those who violate the provisions of this Regulation to collect, process, or use personal data shall delete, stop collecting and processing, or cease using the personal data according to the working methods of the head office units.

For personal data that has not been corrected or supplemented for reasons attributable to the Bank, the Bank shall notify the entities to which the data has been provided so they can properly use the data after the correction or supplementation.

Article 19: When exercising the data subject's rights in the preceding 2 Paragraphs, the data subject shall fill out an application form and follow the procedures and supporting documents stipulated by the head office units.

If the contents of the documents in the preceding Paragraph are incomplete, the data subject shall be notified to make corrections within a time limit.

If an application case falls into one of the following circumstances, it shall be rejected in writing:

I. The document contents in Paragraph 1 are incomplete, and the data subject has failed to make corrections after being notified to do so within a time limit.
II. There is one of the circumstances stipulated in Article 10 of the Personal Data Protection Act.
III. There is one of the circumstances stipulated in Article 11, Paragraph 2 or 3 of the Personal Data Protection Act.
IV. There are other legal grounds for refusing the data owners to exercise their rights.

Article 20: Upon receipt of an application submitted by the data subject according to Article 17 of this Regulation, the Bank shall decide on whether to approve or reject it within 15 days. If necessary, the extension period may not exceed 15 days, and the Bank shall notify the applicant of the reasons in writing.

Upon receipt of an application submitted by the data subject according to Article 18 of this Regulation, the Bank shall decide on whether to approve or reject the application within thirty days. If necessary, the extension period may not exceed 30 days, and the Bank shall notify the applicant of the reasons in writing.

Section 3. Security Management Measures for Personal Data

Article 21: The personal data files held by the Bank shall, according to the needs of the business, at least take the following data security management measures:

I. The use of various removable or fixed media storing personal data, when scrapped or converted to other uses, shall comply with the Bank's information security management system and other relevant procedural documents.

II. If it is necessary to encrypt the contents of the personal data files held, appropriate encryption mechanisms shall be adopted during collection, processing, and use.

III. When it is necessary to back up personal data during the operation process, the backup data shall be properly protected.

IV. Waste paper documents containing personal data shall not be recycled or reused.

V. When paper documents containing personal data are not in use or after work, the desktop clean-up policy shall be followed to avoid data leakage.

VI. After using personal data on copiers, printers, fax machines, scanners, or multi-function machines, the data shall be removed immediately.

Article 22: The e-commerce service system provided by the Bank shall adopt the following information security measures and comply with the Bank's relevant provisions on the management and maintenance of e-commerce service systems:

I. User identity verification and protection mechanism.
II. Mechanism for displaying masked personal data.
III. Secure encryption mechanism for Internet transmission.
IV. Software testing and verification procedures for the development, online release, and maintenance of application systems.
V. Access control and protection monitoring measures for personal data files and databases.
VI. Countermeasures against external network intrusions.
VII. Monitoring and response mechanism for illegal or abnormal use behavior.

The Bank shall conduct regular drills on emergency response measures for personal data breac every year and keep records. Among them, the measures stipulated in Subparagraphs 6 and 7 of the preceding Paragraph shall be drilled at least once every 3 years and reviewed for improvement.

Article 23: For personal data held by the Bank in the form of paper, disk, tape, optical disc, microfilm, integrated circuit chip, computer, automated machine equipment, or other media, each unit shall also comply with the regulations formulated or promulgated by the head office departments for the media storage methods in addition to setting up appropriate management equipment according to the characteristics and environment of the media.

Article 24: Each unit shall set the authority of relevant personnel to contact personal data and control their contact situation according to the business needs to maintain the security of personal data files and agree on confidentiality obligations with the affiliated personnel.

The control tracking data in the preceding Paragraph shall be kept for at least 5 years unless otherwise provided by law or contract.

Article 25: The head office units shall determine the retention period of personal data files held by the Bank according to the needs of the business, which shall be stipulated in internal regulations via letter announcements. However, this is not limited to cases where there are other provisions in laws and regulations or other contract agreements.

When personal data files held by the Bank exceed the retention period, or are not to be kept according to laws and regulations or contract agreements, they shall be destroyed according to the regulations of the head office units or by personnel appointed by the unit heads. If the destruction is outsourced, personnel shall be deployed to supervise the destruction process.

The destruction or supervision process in the preceding Paragraph shall be handled by 2 or more persons together, and the destruction records shall be kept according to Article 31 of this Regulation.

Section 4. Personal Data Processing Procedures After Business Termination

Article 26: The term "business termination" in this Regulation refers to:

I. Termination or transfer of all or part of the Bank's business, including but not limited to the Bank's termination of part of its business, the Bank's transfer of its business to another institution, and the Bank's liquidation and dissolution.

II. Termination or cancellation of the contractual relationship between the Bank and the data owner related to the business, including but not limited to the termination of the business transaction contract between the customer and the Bank.

Article 27: When all or part of the Bank's business is terminated, the Bank shall delete the personal data files it holds. However, this is not limited to cases where other laws and regulations, agreements in contracts, or where it is necessary to retain the data for business purposes.

Before deleting personal data files, according to the preceding Paragraph, the Bank shall notify the data subject and give the data subject a certain period to object. If the Bank finds that the objection is justified, it shall handle the subsequent processing of the personal data file according to the request of the data owner.

Article 28: When all or part of the Bank's business is transferred, unless otherwise specifically agreed in the original contract between the Bank and the data subject (hereinafter the "Original Contract"), the transfer of the rights and obligations under the Original Contract shall be handled according to the provisions of the Civil Code on the Transfer of Debt, the Business Mergers and Acquisitions Act, or other relevant regulations.

The personal data collected, processed, and used by the Bank based on the Original Contract shall be transferred to the transferee, along with the rights and obligations under the Original Contract.
After the transfer of the personal data in the preceding Paragraph, the Bank shall delete the personal data files it holds. However, this is not limited to cases where other laws and regulations, agreements in contracts, or where it is necessary to retain the data for business purposes.

Article 29: When the contract between the Bank and the data subject related to the business is terminated or canceled, the Bank shall delete the personal data files under its possession. However, this is not limited to cases where other laws and regulations, agreements in contracts, or where it is necessary to retain the data for business purposes.
Before deleting personal data files, according to the preceding Paragraph, the Bank shall notify the data subject and give the data subject a certain period to object. If the Bank finds that the objection is justified, it shall handle the subsequent processing of the personal data file according to the request of the data subject.

Chapter 5. Personal Data Security Audit, Record Keeping, and Continuous Improvement Mechanism

Article 30: To ensure the implementation of this Regulation, the Bank shall formulate an appropriate personal data security audit mechanism according to the scale and characteristics of its business and take into account the reasonable allocation of operating resources. If the Bank is required by law to establish an internal control and audit system, it shall also include the relevant mechanisms in the internal control and audit items.

Article 31: Each unit shall delete (including destroy), stop processing, or using the personal data files it holds according to this Regulation, and keep the following records:

I. The method, time, and personnel responsible for the deletion, stop processing, or use.
II. When transferring personal data according to Article 28 of this Regulation, the Bank shall keep records of the reasons, objects, methods, and time of the transfer, as well as the legal basis for the collection, processing, and use of the data by the transferee.

The records in the preceding paragraph shall be kept for at least 5 years. However, this shall not apply where other laws and regulations or other agreements in contracts provide otherwise or where it is necessary to keep the data for business purposes.

Chapter 6. Personal Data Education and Training

Article 32: The Bank's employees shall participate in Personal Data Protection Act-related education and training every year and keep records of the training. New employees shall be given Personal Data Protection Act-related education and training within 6 months of employment and keep records of the training.

The education and training in the preceding 2 Paragraphs may be arranged in appropriate courses in other professional training. In addition to the in-service training within the Bank, employees may also be selected to participate in training courses held by external training institutions.

Article 33: To implement personal data protection and prevent data leakage, each unit shall frequently promote the following matters:

I. Unless otherwise provided in this Regulation, no one shall be allowed to know the contents of the personal data files held by the Bank in any way.

II. The storage media containing personal data including, but not limited to, paper, disk, tape, optical disc, and microfilm, shall be strictly prohibited from leakage or being used for other purposes.

III. Other matters related to personal data protection as notified by the Bank.

Chapter 7. Additional Provisions

Article 34: Matters not covered in this Regulation shall be handled according to the relevant regulations promulgated by the competent authority.

Article 35: This Regulation shall be implemented after resolution by the board of directors. When amended, the general manager shall be authorized for approval before implementation.

Formulated on 03-31-2014
Amended on 02-24-2020
Amended on 06-18-2020
Amended on 06-07-2022