Key Points of Personal Information Protection Policy of Postal Savings Bank of China

I. Objective

In order to further standardize the protection of customer personal information at Postal Savings Bank of China Co., Ltd. (hereinafter referred to as "PSBC" or "the Bank") and effectively safeguard the rights of the Bank's customers to information security, PSBC has formulated a dedicated personal information protection policy in accordance with laws and regulations such as the Data Security Law of the People's Republic of China and the Personal Information Protection Law of the People's Republic of China. The Bank has committed to adhering to the principles of legal compliance, legitimacy, necessity, and integrity in the processing of customer personal information and taking appropriate security protection measures according to the law to ensure the personal information security of customers.

II. Scope of application

The Policy is a general statement on personal information protection across institutions at all levels and agencies of PSBC and applies to all business lines, products, and services provided to customers.

III. Basic principles

The Bank adheres to the following principles for protecting personal information of customers: "legal compliance, legitimacy, necessity, and integrity", correspondence of power and responsibilities, clear and reasonable purposes, transparency, tiered authorization management, notice and consent, minimum necessity, information quality assurance, and "whoever initiates the business is responsible, whoever owns the system is responsible, whoever acquires the customer is responsible, and whoever processes the information is responsible".

Policy requirements: The processing rules for personal information of customers, including the purpose, method, scope, and retention period, shall be clearly communicated to customers in an understandable and reasonable manner. Independent consent from customers should be obtained in accordance with the law. No institution or employee shall unlawfully collect, use, process, transmit, buy, sell, provide, or publicly disclose the personal information of customers. Personal information processing activities that harm national security or public interest are prohibited.

IV. Terminology definitions:

i. Personal information refers to all information that is recorded electronically or in other manners and related to natural persons who have been identified or can be identified, excluding anonymized information. Personal information includes personal identity information, property information, account information, credit information, financial transaction information, identification information, and other information related to specific customers' purchase or use of financial products or services.

ii. Sensitive personal information refers to information that, if disclosed or used illegally, could damage a natural person's dignity or harm personal or property safety, including biometric authentication data, religious beliefs, specific identities, medical health data, financial account information, travel trajectories, and information about minors under the age of 14.

iii. Personal information processing includes the collection, storage, use, processing, transmission, provision, public disclosure, deletion, and other activities related to the personal information.

V. Rules on the processing of customer personal information

i. Data collection

The Bank commits to collecting customer personal information only to the minimum extent necessary to achieve the processing purpose. Excessive collection is prohibited. When collecting personal information, the Bank shall inform customers of the purpose, method, and scope of collection, obtain their consent, and retain related supporting materials, unless otherwise specified by laws and regulations.

The Bank shall not collect personal information unrelated to the business, nor will it use improper means such as disguised coercion or illegal purchases to collect personal information. The Bank shall not refuse to provide financial products or services that do not depend on the information the customer has declined to authorize, except when processing his/her personal information is essential for providing the financial product or service.

After ceasing financial business or services, the Bank will immediately stop collecting or processing relevant data, unless otherwise specified by laws or administrative regulations.

ii. Data storage

The Bank shall take technical and other necessary measures to properly store and protect customer personal information according to national regulations on the management of archives and electronic data, preventing data loss, damage, disclosure, or alteration.

Unless otherwise specified by laws or administrative regulations, the retention period for personal information should be the shortest time necessary to achieve the processing purpose.

Personal information collected and generated within the People's Republic of China will be stored within China.

iii. Data use

The Bank shall use customer personal information in accordance with laws and regulations and the agreed purposes, and shall not exceed the scope of use. Following the principle of "necessary authorization for business", strict authorization management and access control shall be implemented for data use. Desensitization, watermarking, and other technical measures shall be adopted to prevent data leakage, and related operation logs shall be retained. The Bank shall strictly control data sharing, use, and third-party processing according to the principle of "minimum

necessity". Agreements shall be made through contracts to specify the data processing scenarios, methods, and responsibilities of both parties, and technical measures such as encryption, desensitization, and watermarking shall be taken to ensure data security. Customer information shall only be processed with prior notification and consent from the customer.

The Bank shall specify that it will not rent, sell, or provide customer personal information to third parties for purposes other than completing relevant transactions or services.

iv. Data deletion

The Bank shall delete or anonymize data in accordance with national and industry regulations and agreements with the data subject. Personal information shall be deleted in the following cases; if not deleted, customers have the right to request deletion:

1. The processing purpose has been achieved or cannot be achieved, or it is no longer necessary to achieve the processing purpose;

2. The provision of products or services has ceased, or the retention period has expired;

3. The customer has withdrawn consent;

4. The processing of personal information violates laws, administrative regulations, or the relevant agreement.

5. Otherwise, as specified by laws or administrative regulations.

If the legal or regulatory retention period has not expired, or deletion of personal information is technically difficult, only storage and necessary security measures shall be implemented.

VI. Third-party management

The Bank values the security management of processing customer information by third parties, strictly controls third-party access reviews, and conducts impact assessments on personal information protection. When determining the purpose and methods of customer personal information processing with third parties, the Bank shall agree on the rights and obligations of both parties. However, such an agreement shall not serve as a basis to restrict customers from exercising their rights. When outsourcing to third parties for processing customer personal information, the Bank shall specify the purpose, duration, processing methods, types of personal information, protective measures, and the rights and obligations of both parties, and supervise the third party's processing activities. When providing personal information to third parties for processing, the Bank shall inform customers of the receiver's name, contact information, processing purpose, processing methods, and the types of personal information, and obtain customers' separate consent.

The Bank shall specify the management requirements for third-party outsourcing, including pre-outsourcing risk assessments, data security protection, and outsourcing supervision and inspection. The Bank shall fulfil the third-party privacy and data security management requirements by conducting outsourcing due diligence,

stipulating confidentiality and security clauses in contracts, and strictly controlling the scope of access for outsourced personnel in accordance with the "minimum necessity" principle. The Bank shall conduct on-site inspections of important third-party non-resident institutions for outsourcing, covering internal control management, data security management, contingency plans, and drills. The Bank shall require third parties to remedy any issues discovered to improve outsourcing service quality.

VII. Customer rights to personal information control

The Bank shall strictly adhere to laws, regulations, and regulatory requirements to fully protect customers' rights to control their personal information. These rights include:

i. Access, correct, and update customer personal information

Customers have the right to access a copy of their personal information and may copy their personal information when accessing it.

Customers have the right to modify or update their personal information, unless otherwise stipulated by laws, regulations, or regulatory policies. Before modifying personal information, the Bank will verify the customer's identity.

ii. Delete customer personal information

Customers may request deletion of their personal information under the following circumstances:

1. If the purpose for which the Bank processes the information has been achieved or cannot be achieved, or the information is no longer necessary for the purpose of processing;

2. If the Bank ceases to provide the products or services, or the retention period has expired;

3. If the customer personally withdraws his/her consent by deregistering from the Bank's system as stated in Clause iv of this chapter;

4. If the Bank has processed personal information in violation of laws, administrative regulations, or agreements; or

5. Otherwise, as specified by laws or administrative regulations.

If the Bank decides to respond to the customer's deletion request, the Bank shall notify the entities that have obtained the customer's personal information from the Bank to delete such information promptly, unless otherwise specified by laws, regulations, or regulatory policies, or such entities have obtained the customer's separate authorization.

After the customer deletes any information from the Bank's services, the Bank may not immediately delete such information from the backup system, but will delete the same when the backup is updated.

Where the retention period specified for such personal information under laws and administrative regulations has not expired, or the deletion of the same is technically

difficult to achieve, the Bank will terminate any processing of such information other than storing it and taking necessary security measures to protect it.

iii. Right to change the scope of consent or withdraw authorization

The Bank requires certain basic customer personal information to complete business functions. Customers may grant or withdraw their consent at any time regarding the collection and use of any additional personal information.

Customers may prevent PSBC or a third-party service provider from obtaining their personal information in connection with certain features or services by disabling such features of the e-banking system, or by refusing to provide the relevant personal information when they enable and use such features or services. They may also withdraw their consent to the Bank app's access to certain permissions by adjusting the "Settings" on their mobile devices, so as to restrict the Bank from obtaining information corresponding to such permissions. This may prevent PSBC or the relevant third parties from providing the relevant services for them.

If customers want to withdraw their consent to the Bank's collection of their personal information, they may do so either by cancelling their mobile banking accounts or by separately withdrawing each consent they granted to third parties at "My > Settings > Privacy Management > Manage Third-Party Authorization".

iv. Right to deregister as a user

Customers may cancel their accounts via outlet counters or self-service devices, or through mobile banking, online banking, or other electronic channels, according to relevant business management regulations.

On mobile banking, customers can log in, go to "My - Settings - Cancel Mobile Banking" to cancel their mobile banking account, or request cancellation through outlet counters or self-service devices. The e-banking account of the customer will be cancelled upon his/her deregistration from the Bank's e-banking system. The cancellation of an e-banking account is irreversible. Once a customer deregisters from the Bank's e-banking system, the Bank will cease to collect the customer's personal information through the e-banking system (client side) and will delete all information about the customer's e-banking account, unless a different retention period is specified by laws, regulations, or regulators.

v. Restrain information system automatic decision-making.

For some business functions, the Bank may make decisions based solely on non-artificial and automatic decision-making mechanisms, including information systems and algorithms. If such decisions significantly affect the legitimate rights and interests of customers, customers shall have the right to request an explanation from the Bank, and the Bank will also provide appropriate remedies.

vi. Respond to the above requests of customers

If customers are unable to access, correct or delete their user information as stated above, or customers need to access, correct or delete any other user information generated when they use the Bank's services or functions, or customers believe that the Bank violates any laws and regulations or the agreement regarding the collection

or use of user information, customers may contact the Bank using the contact information provided in this Policy. The Bank will complete verification, processing, and respond to customer requests within 15 calendar days after receiving customer feedback and verifying their identity.

The Bank may refuse any illegal or rule-violating request that lacks justifiable reasons, may be repeated without reason, requires too many technical means (for example, new system development or existing practices fundamental change), brings risks to the legitimate rights and interests of others, or is very unrealistic.

In addition, according to relevant laws, regulations, and regulatory requirements, the Bank will and may not be able to respond to customer requests if required to do so by the competent authorities or regulatory authorities of the state in the following circumstances, or where any other circumstance agreed below takes place:

1. The personal information is relevant to the personal information controller's performance of its obligations under laws and regulations;

2. The personal information is directly related to national security or national defense security;

3. The personal information is directly related to public safety, public health, or vital public interests;

4. The personal information is directly related to any criminal investigation, prosecution, trial, or execution of judgments;

5. The personal information controller has sufficient evidence that the personal information subject has subjective malice or abused its rights;

6. The purpose is to protect the life, property, or other material legitimate rights and interests of customers as the personal information subject or other individuals, and it is strictly difficult to obtain their consent;

7. Any response to the request for the personal information subject will give rise to material damage to the legitimate rights and interests of the personal information subject or any other individuals or organizations; or

8. The personal information involves trade secrets.

VIII. How to contact the Bank

If customers have any comments, suggestions, questions, or complaints about this Policy, they may contact or consult the Bank at 95580 (the Bank's product inquiry and complaint hotline), at the Bank's banking outlets, or through other customer service channels of the Bank. The Bank will respond to their comments, suggestions, complaints, or relevant issues promptly, and within 15 calendar days for complaints with clear facts and simple disputes.

Company name: Postal Savings Bank of China Co., Ltd.

Registered address: No. 3 Financial Street, Xicheng District, Beijing.