Sumitomo Mitsui Banking Corporation Seoul
Privacy Policy (for Customers)

Manager of Sumitomo Mitsui Banking Corporation Seoul

(Compliance Review on Feb 25, 2026)

Enacted on September 30, 2011
Amended on January 20, 2015
Amended on November 10, 2016
Amended on September 4, 2017
Amended on July 10, 2018
Amended on September 25, 2020
Amended on June 1, 2021
Amended on August 1, 2022
Amended on May 10, 2023
Amended on September 25, 2023
Amended on December 1, 2023
Amended on September 30, 2024
Amended on February 24, 2025
Amended on February 26, 2026

In accordance with Article 30 of the Personal Information Protection Act (the "**PIPA**"), Sumitomo Mitsui Banking Corporation Seoul ("**SMBC Seoul**") hereby establishes and discloses this Privacy Policy in order to protect personal information and rights and interests of data subjects and smoothly handle grievances of data subjects in connection with their personal information.

Article 1 (Purpose of Processing Personal Information)

SMBC Seoul processes personal information for the following purposes. SMBC Seoul will not process any personal information for any purpose other than the following and, in the event any of the following purposes is modified, it will take such necessary measures as obtaining separate consent pursuant to Article 18 of the PIPA:

1. For the purpose related to financial transactions:
   - Personal information is processed for the establishment, maintenance, execution, and management of financial transactions. This includes determining whether to establish a financial transaction relationship, as well as the maintenance, execution, and management of such relationships. It also involves investigating financial incidents, resolving disputes, addressing customer complaints, and fulfilling statutory obligations.
2. For the purpose of Internet banking membership registration and management:
   - Personal information is processed for online banking membership registration and management. This includes identifying and authenticating customers for membership and service provision, maintaining and managing member status, preventing unauthorized use of the service, investigating incidents, resolving disputes,

addressing customer complaints, and fulfilling statutory obligations.

3. For the purpose of dealing with online transactions:

- Personal information is processed to track and search details of electronic financial transactions and use the same for statistical data to formulate security policies in accordance with Articles 21 and 22 of the Electronic Financial Transactions Act (the "**EFTA**").

Article 2 (Personal Information Retention Period)

(1) SMBC Seoul shall process and retain personal information for the personal information retention period set forth in applicable laws or for the personal information retention period agreed upon when collecting personal information from the data subjects.

(2) The specific retention periods are as follows:

1. Personal information pertaining to financial transactions shall be retained and used for the relevant purpose stated above during the period starting from the date of consent to collection and use and for up to ten years after the date of termination of relevant financial transactions, after which such personal information shall be retained and used only for the purpose of investigating financial incidents, resolving disputes, addressing customer complaints, fulfilling statutory obligations, and managing risks of SMBC Seoul;
2. Personal information collected for the purpose of Internet banking membership registration and management shall be retained and used for the period starting from the date the customer registers for Internet banking membership until the date of membership withdrawal, after which such personal information shall be retained and used only for the purpose of investigating financial incidents, resolving disputes, addressing customer complaints, and fulfilling statutory obligations;
3. Personal information pertaining to online transactions shall be retained and used for the period set forth in Article 12 of the Enforcement Decree of the EFTA.

Article 3 (Provision of Personal Information to Third Parties)

(1) SMBC Seoul shall, in principle, process personal information of the data subjects for the purposes set forth in Article 1 and, without prior consent of the data subjects, shall not process the same for any purpose other than the intended purposes or provide the same to any third parties; provided, that unless the interests of the data subjects or

any third parties are threatened to be infringed unlawfully, personal information may be used for any purpose other than the intended purposes or provided to third parties in any of the following cases:

1. If the data subjects provide prior consent to provision and disclosure to third parties;
2. If any other laws provide otherwise;
3. If it is acknowledged evidently necessary for the urgent interests involving life, health and property of the data subjects or any third parties;
4. If it is urgently necessary for public hygiene, safety and welfare.

(2) SMBC Seoul provides personal information as follows:

1. Recipients

- Provision to centralized credit information collection agency:
  - Korea Credit Information Services
    - · Address: 19, Myeong-dong 11-gil, Jung-gu, Seoul (1F, Customer Protection Center, KFB Building)
    - · Telephone: 1544-1040

2. Recipients' purpose of use

- Provision to centralized credit information collection agency:
  - To be used as data for assessing the individual's credit or for policy purposes by public institutions.

3. Items of personal information to be provided

- Provision to centralized credit information collection agency:
  - Personal identification information, financial transaction information, credit transaction information, credit capability information, information for credit assessment

4. Period of retaining personal information

- Personal information will be retained and used from the date of provision until consent withdrawal or attainment of the purpose of provision, after which personal information will be retained and used only for the purpose of investigating financial incidents, resolving disputes, addressing customer complaints, and fulfilling statutory obligations in connection with the purposes described above.

Article 4 (Procedures and Methods for Destroying Personal Information)

(1) SMBC Seoul shall destroy relevant personal information without delay when it is no longer needed, such as when the retention period has expired or the processing purpose has been achieved.

(2) If the retention period agreed upon by the data subject has expired or the processing purpose has been achieved, but the personal information must be preserved in accordance with other laws, the relevant personal information will be transferred to a separate database (DB) or stored in a different location.

- In cases where preservation is required by law:

Items of personal information	Applicable provisions
Financial transaction information such as account details and transaction history	Article 20-2 of the Credit Information Use and Protection Act
Important business documents such as contracts and transaction applications Documents similar to vouchers and receipts	Article 33 of the Commercial Act
Withholding tax-related documents	Article 26-2 of the Framework Act on National Taxes
Documents related to contract conclusion and performance, financial product advertising materials, documents concerning the exercise of financial consumer rights, materials on the establishment and operation of internal control standards, and documents related to business outsourcing	Article 28 of the Act on the Protection of Financial Consumers, Article 26 of the Enforcement Decree thereof
Financial transaction data subject to real name verification and reporting, information about the remitter and recipient	Article 5-4 of the Act on Reporting and Using Specified Financial Transaction Information
Access records of electronic devices related to electronic financial transactions, and matters related to the application and modification of conditions for electronic financial transactions	Article 22 of the EFTA

(3) Procedures and methods for destroying personal information are as below:

1. Procedures for destruction: SMBC Seoul selects personal (credit) information that needs to be destroyed when a reason for destruction arises. The personal (credit) information is then destroyed with the approval of the Chief Privacy Officer or the Credit Information Management and Protection Officer of SMBC Seoul;
2. Method of destruction: Personal information recorded and stored in electronic file formats is destroyed in such a way that the records cannot be reproduced. Personal information recorded and stored on paper documents is destroyed by shredding.

Article 5 (Entrustment of Personal Information Processing)

(1) For smooth handling of personal information, SMBC Seoul entrusts the processing of personal information overseas as follows, in accordance with Article 28-2 (1) 3 of the PIPA. The data subjects may refuse transfer of personal information by terminating or cancelling their agreement with SMBC Seoul. However, if the data subject refuses the transfer of personal information, they will not be able to establish or maintain financial transactions with SMBC Seoul and will not be able to use its service products.

Person to whom personal information is transferred	Country to which personal information is transferred and the timing and method of such transfer	Items of personal information to be transferred	Details of task to be entrusted	Purpose and the retention period of the person to whom personal information is transferred
Sumitomo Mitsui Banking Corporation, Headquarters, [81-(3)-5222-1700]	Japan; data to be transferred via an exclusive network when collected	Personal information specified in Article 7	Computerized processing and storing of transaction information; compliance with foreign laws by SMBC headquarters and branches; cooperation with supervision by foreign supervisory agencies	- Performing the entrusted task - Until the purpose of entrustment is fulfilled
Sumitomo Mitsui Banking Corporation Singapore, [65-6882-0000]	Singapore; data to be transferred via an exclusive network when collected	Personal information specified in Article 7	Computerized processing and storing of transaction information; compliance with foreign laws by SMBC headquarters and branches; cooperation with supervision by foreign supervisory agencies	- Performing the entrusted task - Until the purpose of entrustment is fulfilled

(2) Upon executing an entrustment agreement, SMBC Seoul specifies, in the agreement and other documents, the prohibition of processing personal information for any purpose other than the purpose of performing the entrusted task, technical and managerial protective measures, restriction of re-entrustment, control and supervision of entrusted entities, and liability for damages, in accordance with Article 26 of the PIPA, and supervises the entrusted entities' safe processing of personal information.

(3) In the event of change in the details of entrusted task or entrusted parties, SMBC Seoul will disclose the same without delay through this Privacy Policy.

Article 6 (Rights and Obligations of Data Subjects and Their Legal Representatives and Methods of Exercising Them)

(1) The data subjects may at any time exercise their rights against SMBC Seoul to demand access to or correction, deletion or suspension of processing of personal information.

(2) The rights under paragraph (1) above may be exercised against SMBC Seoul by way of, among others, writing, e-mail or fax in accordance with Article 41 (1) of the Enforcement Decree of the PIPA, and SMBC Seoul will take due measures without delay.

(3) The rights under paragraph (1) above may be exercised by the data subjects' legal representative or any other person delegated by them, in which case, the power of attorney in the format of Attached Form No. 11 of the Public Notice on Methods of Processing Personal Information (No. 2023-12).

(4) In the event of circumstances provided for in Article 35 (4) or 37 (2) of the PIPA, SMBC Seoul may refuse the data subjects' request for access to personal information or suspension of processing.

(5) In the event of request for correction or deletion of personal information, no demand for deletion may be made with respect to any personal information specified as information subject to collection under other laws.

(6) In the event of request for access, correction or deletion, or suspension of processing based on the data subjects' rights, SMBC Seoul shall verify whether a person who requested access, etc. is the principal or legitimate agent.

Article 7 (Items of Personal Information to Be Processed)

SMBC Seoul collects the minimum necessary essential information required for establishing, maintaining, executing, and managing financial transactions and providing service products as follows. In principle, SMBC Seoul does not collect sensitive information that may infringe on the privacy of the data subject. If it is necessary to collect such information, it is done with the separate consent of the data subject and is used only for the agreed-upon purposes. However, if sensitive information is collected with the data subject's consent, its accuracy and currency are periodically verified:

1. Provision of financial services
   - Legal basis: Article 15 (1) 4 of the PIPA
   - Common essential information: Name, resident registration number or other unique identification number, domestic residence registration number, nationality,

occupational category, contact information such as address, email address, and phone number

- Product-specific Essential Information (for customers using the respective products): Product type, transaction conditions (interest rates, maturity, collateral, etc.), transaction date and time, amount, and other information generated during the consultation, debt management, and other processes necessary for establishing, maintaining, executing, and managing financial transactions

2. Information collected under the EFTA (limited to Internet banking and online transactions)
   - Legal basis: Article 15 (1) 2 of the PIPA
   - Tracking and searching details of electronic financial transactions: Customer ID, date/time of access, IP address, HDD serial, MAC address
   - Statistical data to formulate security policies: Personal firewall setting, type of operating system, browser version
3. Method of collection
   - Direct collection from the data subjects who visit SMBC Seoul branch
   - Collection via written forms, fax or telephone
   - Collection through the data collection tools at the time of user registration for Internet banking or online transactions
   - Collection through customer inquiries

※ SMBC Seoul does not photocopy or scan fingerprint data when photocopying or scanning a copy of resident registration card, driver's license or any other identification card.

Article 8 (Installation and Operation of Automatic Personal Information Collection Device and Rejection Thereof)

SMBC Seoul uses cookies to store and, from time to time, retrieve information on the users' usage in order to prevent unauthorized or unlawful use of the services and provide optimal services for the customers' devices.

Cookies represent a small amount of information sent by the server (http) used to manage the website to the users' computer browser and are often stored in the hard disk within the users' personal computers.

Customers may refuse to save cookies by setting the web browser menu at: Tools > Internet options > Personal information.

Customers who selects an option not to save cookies may face certain inconveniences in using the services.

Article 9 (Measures to Ensure Security of Personal Information)

SMBC Seoul takes the following technical, managerial and physical measures necessary to ensure stability in accordance with Article 29 of the PIPA.

Minimization and training of employees who handle personal information: SMBC Seoul minimizes the risk of personal information leakage by designating a minimum number of employees to handle personal information and providing them with appropriate training.

Encryption of personal information: Personal information is stored and managed in an encrypted form, and important data is protected using additional security features such as file encryption or file locking.

1. Access Restriction to Personal Information Processing Systems: Necessary measures are taken to control access to personal information by granting, changing, and deleting access rights to systems that process personal information. Security programs are installed to prevent unauthorized access from external sources.
2. Technical Measures Against Hacking and Other Threats: To prevent the leakage and damage of personal information due to hacking or computer viruses, security programs are installed and regularly updated and inspected. Systems are installed in areas where access from outside is controlled, providing technical and physical monitoring and blocking.

Article 10 (Amendment of Privacy Policy)

If SMBC Seoul Branch changes its personal information processing policy, the changes, including the effective date and the details of the changes, will be continuously disclosed through postings at our branches or on our website. The changes will be made easily accessible to customers by comparing the content before and after the changes and publishing them on the website.

Article 11 (Remedies for Infringed Rights and Interests)

(1) Data subjects can apply for dispute resolution or consultation with the Personal Information Dispute Mediation Committee, the Personal Information Infringement Report Center of the Korea Internet & Security Agency, and other organizations to seek remedies for personal information infringement. For reporting or consulting on other personal information infringements, please contact the following organizations:

1. Personal Information Dispute Mediation Committee: Call 1833-6972 (www.kopico.go.kr)
2. Privacy Infringement Report Center: Call 118 (privacy.kisa.or.kr)
3. Supreme Prosecutors' Office: Call 1301 (www.spo.go.kr)
4. National Policy Agency: Call 182 (cyberbureau.police.go.kr)

(2) Any person whose rights or interests are infringed by any disposition or inaction by the head of a public institution in connection with the demand under Article 35 (Access to Personal Information), Article 36 (Correction or Deletion of Personal Information), or Article 37 (Suspension of Processing Personal Information) of the PIPA may request an administrative appeal as prescribed in the Administrative Appeals Act.

※ For further details concerning administrative appeals, please refer to the website of the Central Administrative Appeals Commission (www.simpan.go.kr).

Article 12 (Chief Privacy Officer, etc.)

(1) SMBC Seoul's Chief Privacy Officer under Article 31 (1) of the PIPA and the Personal Information Management Officer under Article 29 of the PIPA are as follows:

	Chief Privacy Officer	Personal Information Management Officer
Department/Title	General Manager	System Operation and Maintenance Group/Group Manager System Planning and Development Group/Group Manager
Name	Kato Yoshiro	Dae-hyun Lee Min-soo Kang
Telephone/Fax	02-6364-7125 / 02-6364-7050	02-6364-7350 02-6364-7347

(2) SMBC Seoul's department and general manager responsible for receiving and handling requests for access to personal (credit) information are as follows:

Responsible Department	Telephone Number	Person-in-Charge/Telephone Number	Available Hours
Deposit and Domestic Transfer Group	02-6364-7248	Jae-shin You (Group Manager)/02-6364-7125	9:30-17:45

(3) The data subjects may contact the Chief Privacy Officer or responsible department described above for any inquiries related to personal information protection, grievances, or relief of damage in the course of using SMBC Seoul's services. SMBC Seoul will respond to the data subjects' inquiries without delay.

The end.