

## **Handling of Personal Information, etc.**

**August 2024**

### **The Hongkong and Shanghai Banking Corporation Limited, Japan Branch Handling of Customers' Personal Information etc. (Personal Information Protection Policy)**

The Hongkong and Shanghai Banking Corporation Limited, Japan Branch (hereinafter, the "Bank") has established the following policy with respect to the handling of customer Personal Information, Individual Number and Specific Personal Information (collectively, "Personal Information, etc.").

When handling customer Personal Information, etc., the Bank will comply with this policy in addition to relevant laws and regulations, including the Personal Information Protection Act (hereinafter referred to as "PIPA"), and relevant guidelines, including the Guidelines for the Protection of Personal Information in the Financial Sector (hereinafter referred to as the "Guidelines"). The Bank will continually review and improve its policy for handling of Personal Information, etc.

In this policy:

"Connected Person" means a person whose information the customer provides to the Bank in connection with transactions with the Bank. Connected Person may include, but is not limited to, any agent, any beneficiary, trustee or settler, and any substantial owner, representative, director or officer of the customer.

"Sensitive Information" is defined in the Guidelines. It includes "Special Care-Required Personal Information" and other information like membership of workers' unions, family origin, registered domicile, health record and sex life etc. (excluding the parts under "Special Care-Required Personal Information").

"Personal Related Information" is defined in the PIPA. It refers to information about a living individual, which is not Personal Information nor Kana Processed Information and Anonymously Processed Information that are defined in the PIPA.

"Personal Information" is defined in the PIPA. It refers to information about a living individual that can identify the specific individual by a name, date of birth or other description contained in such information, or information containing an individual identification code defined in the PIPA.

"Personal Data" is defined in the PIPA. It refers to Personal Information constituting a personal information database etc. defined in the PIPA.

"Individual Number" refers to a number obtained by converting a resident record code in order to identify a person (so called "My Number").

"Specific Personal Information" refers to Personal Information that includes Individual Number information.

"Special Care-Required Personal Information" is defined in the PIPA. It refers to personal information comprising a principal's race, religious affiliation, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions etc. of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the principal.

### **1. Purposes of Use of Personal Information, etc.**

The Bank will use Personal Information, etc. of the customer (including Connected Persons) to the extent necessary for the following Purposes of Use within the following Business Operations, except where the Bank obtains such customer's consent or where permitted under the relevant laws and regulations. For the avoidance of doubt, the Bank will use Individual Number and Specific Personal Information only to the extent permitted under the relevant laws and regulations.

#### **(1) Business Operations**

- i. The acceptance of deposits, fund transfers, currency exchange, lending of funds, foreign exchange, credit card issuance, and other businesses ancillary to these businesses.
- ii. Any other activities and related businesses in which banks may be engaged in (including activities that may be permitted in the future).

#### **(2) Purposes of Use**

The Bank and its affiliates and associated companies will use customers' Personal Information, etc. for the following purposes in relation to the provision of financial products and services. Pursuant to article 13, paragraph 6, item 6, etc. of the Ordinance for Enforcement of the Banking Act, the Bank shall not use or provide to a third party any information on the repayment capacity of a person seeking funds which was provided by an Individual Credit Information Organization for purposes other than for the investigation of the repayment capacity of the person seeking the funds. Further, pursuant to article 13, paragraph 6, item 7 of the Ordinance for Enforcement of the Banking Act, the Bank shall not use, nor shall it provide to a third party, any Sensitive Information of the customer unless the Bank deems it necessary to do so for its proper business operations

or otherwise. The Bank will endeavor to decide the Purposes of Use as concretely as possible so that they are transparent to customers, and will endeavor to specify the purpose at the time of acquiring the information. For example, if the Bank intends to propose its products using Personal Information acquired by conducting a questionnaire, the Bank will disclose such intention.

- i. To provide information for the solicitation and sale of financial products, introduction, receiving an application, management, and execution of services in accordance with the Bank's business operations.
- ii. To: (i) ascertain the customer's identity under the Act on the Prevention of the Transfer of Criminal Proceeds, the Foreign Exchange and Foreign Trade Act and Hong Kong Monetary Authority Guidelines, (ii) avoid financial crime and money laundering, and comply with sanctions programmes that are administered by Japan, the United States, the United Kingdom, the European Union, Hong Kong, United Nations, etc., and (iii) ascertain a customer's eligibility for certain financial products and/or services.
- iii. Management of ongoing transactions, such as the management of dates in various transactions;
- iv. To make decisions on offers for various transactions, confirm eligibility for using instruments and services, and ongoing transactions, etc.;
- v. To make decisions about the appropriateness of providing financial products and services, such as decisions made in light of the principle of suitability.
- vi. To provide personal information to a third party to the extent necessary for the performance of our business, including where personal information is provided to a Individual Credit Information Organization, etc. in the course of our lending business.
- vii. To appropriately carry out operations when commissioned with all or part of the processing of Personal Information by another business etc.
- viii. To fulfill obligations and exercise rights based on contracts with the customer or based on laws.
- ix. For research and development of products and services through market research, data analysis, and questionnaire surveys.
- x. For making proposals concerning products and services by means of direct mail, email, etc.
- xi. To make proposals on the products and services of HSBC Group Companies or associated companies etc.
- xii. Cancellation of various transactions and post-cancellation management of

transactions.

- xiii. To monitor and control the various risks that are necessary to be managed by HSBC Group Companies.
- xiv. Appropriate and smooth performance of transactions with customers.

Notwithstanding the Purposes of Use provided in each item above, the Bank will not use the Individual Number and Specific Personal Information for the purposes other than those permitted under the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures. The Bank's Purposes of Use of Individual Number and Specific Personal Information are as follows:

- i. Preparation of legal documents regarding financial instrument transactions.
- ii. Processing of account opening and reporting regarding financial instrument transactions.
- iii. Preparation of legal documents regarding transactions of domestic and international remittances, etc..
- iv. Processing related to the numbering of deposit and saving accounts.
- v. Preparation of legal documents regarding payment records.
- vi. Other purposes in relation to 1 through 5 above.

The Purposes of Use of Personal Information, etc. by the Bank, may be found on the Bank's website.

### (3) Discontinuance of Direct Marketing

In case a customer requests the Bank to stop using his/her Personal Information for the purposes of direct marketing such as sending direct mails or solicitation by phone, the Bank will discontinue the usage for such purpose.

## **2. Proper Acquisition of Personal Information, etc.**

To the extent necessary for the achievement of the Purposes of Use specified in item 1 above, the Bank will acquire Personal Information, etc. of the customer orally or in writing by appropriate and lawful means, for example, from the following information sources.

<examples>

- Where the information is provided directly by a document that the customer is required to fill in and submit (e.g. submission of an application form by the person in question, data entry via the website by the person in question).
- Cases where personal information is provided by third parties, such as Joint Users and a personal credit information organization.

## **3. Personal Information etc. Provided to Third Parties**

The Bank will not provide a customer's Personal Data it retains to third parties without the prior consent of the individual concerned, except as permitted by relevant laws and regulations. However, in the case where the Bank entrusts the Personal Data to a third party within the necessary scope to achieve its Purposes of Use, or in the case where the Personal Data is to be jointly utilized by a specified party set forth in item 6 below, the Bank may provide a customer's Personal Data even without the prior consent of the customer.

Where providing Personal Data to third parties in foreign countries (including the above cases of the entrustment of the handling of the Personal Data and the joint use of the Personal Data), the Bank will not do so without obtaining prior consent of the customer, except for cases permitted by relevant laws and regulations. If a third party is located in a foreign country which has established a personal information protection system recognized to have equivalent standards to that of Japan (as set forth in the rules of the Personal Information Protection Commission ("PIPC")) the Bank may provide the customers' Personal Data to the third party without obtaining the prior consent of the customer.

In addition, the Bank may provide a customer's Personal Information, without obtaining prior consent, to a third party in a foreign country which has developed a framework that conforms to the standards set forth in the rules of PIPC and is regarded as equivalent on an ongoing basis to the measures that a business operator handling Personal Information is required to take pursuant to the provisions of the PIPA (hereinafter referred to as "Equivalent Measures"). In such event, the Bank shall take measures necessary to ensure the continuous implementation of the Equivalent Measures by such third parties, and a customer may seek information on such measures.

At the time of obtaining consent from the customer, it might be difficult to specify the name of the foreign country, or obtain and provide information on its regime for protecting personal information, or information on the measures to be taken by the third party to protect Personal Information in an appropriate and reasonable manner. Therefore, a customer may request the Bank to provide the aforementioned information at a later date. The Bank shall not provide all or part of the information with respect to any requests for information in the event that there is a risk that the proper performance of its business will be seriously impaired.

In providing customers' Personal Related Information to a third party and where the third party is expected to receive the Personal Related Information as Personal Data, except as otherwise provided by relevant laws and regulations, the Bank shall confirm and provide the information in accordance with the provisions of such laws and regulations. Further, the Bank will not provide Individual Number and Specific Personal Information to third parties beyond what is allowed under the laws and regulations.

#### **4. Handling of Sensitive Information**

The Bank will not acquire, utilise, nor provide to third parties, customer's Sensitive Information, except in cases as illustrated by the Guidelines including cases based on relevant laws and regulations and the case in which there is a prior consent of the individual concerned within the scope of business need.

#### **5. Entrustment of Operations Concerning Personal Information etc.**

The Bank shall entrust its operations concerning Personal Data to a third party within the necessity to achieve the Purposes of Use as exemplified below. Note that the Bank, in entrusting its operations to a third party, will execute an agreement with the third party regarding the stringent handling of the Personal Data within such third party, and ensure that there are appropriate security control measures in place.

< examples >

- Operations regarding printing and dispatch of documents to be sent to customers.
- Operations related to transactions
- Operations to send out direct mails
- Operations and maintenance of computer systems
- Maintenance of books and records relating to business operations

#### **6. Joint Use of Personal Data**

The Bank may jointly use Personal Data (excluding Individual Number and Specific Personal Information) with other parties as follows:

##### (1) Joint Use of Information from Japan Official Gazette

- i. Jointly Used Personal Data Information published in Japan Official Gazette (name, address, bankruptcy, the date, etc.)
- ii. Scope of Joint Users Members of the Individual Credit Information Center held by the Japanese Bankers Association (hereinafter referred to as the "Association"). To note, the Association's Individual Credit Information Center is a Individual Credit Information Organization which is established and managed by the

Association. Conditions for participation are as follows:

- i. An official member of the Association
  - ii. Other banks than the ones mention at (i). above or financial institutions that are equivalent to a bank under relevant laws and regulations
  - iii. Government-related financial institutions and equivalent institutions
  - iv. Credit Guarantee Association which is established in accordance with the Credit Guarantee Association Act (10 August 1953, the Law no.196)
  - v. Corporate entities that run credit businesses related to individual customers, which are endorsed by members of the above (i).~ (iii).
- iii. Purposes of Use To make decisions concerning own lending deals by the members of the Association's Individual Credit Information Center.
  - iv. The entity name, location, and the name of the Representative Director responsible for management of Personal Data The Japanese Bankers Association The location and representative's name can be found at the following website: <https://www.zenginkyo.or.jp/abstract/outline/>

(2) Joint Use of Information in Relation to Non-Performing Transactions

- i. Jointly Used Personal Data The following information in relation to the drawer of a non-performing disbursed draft, cheque or bill (for a bill of exchange, the underwriter) (the same shall apply hereinafter) and the customer who initiated the transaction.
  - i. the name of the drawer (if the drawer is a juridical person, its name, representative name, and representative's title)
  - ii. if there is a trade name with respect to the said drawer, the said trade name
  - iii. Address (office address if legal entity) (to include postal code)
  - iv. The name of the customer who initiated the transaction for the time period (if a juridical person, its name, representative name, and representative's title. If there is a trading name, the said trading name).
  - v. Date of birth
  - vi. Occupation
  - vii. Stated Capital (limited to cases of juridical persons)
  - viii. The type and face value of said draft, check or bill
  - ix. Whether the report is a for a non-payment (the first non-payment) or a report of in relation to the cessation of the transaction (cessation of transaction order)
  - x. Exchange Date (Presentation Date)

- xi. Payment bank (including department and branch name)
- xii. Beneficiary bank (including department and branch name)
- xiii. Reason for non-performance
- xiv. The date on which the person received the cessation of transaction order
- xv. Clearing organisation of which the payment bank (branch) of the non-performing disbursed draft, cheque or bill is a member and the bankers association of which the clearing organisation is a member.

Note: In relation to i. through iii. above, where the information contained on the non-performing disbursed draft, cheque or bill differs from the information notified to the payment bank, the information contained in the said draft, cheque or bill shall be included.

ii. Scope of Joint Users

- o Clearing organizations of drafts, cheques or bills in each region
- o Financial institutions that participate in the local clearing organisations
- o All Individual Credit Information Organisations that are established and managed by the Association
- o Regionally-based bankers associations, which are Special Members of the Association (including the organisation in relation to the cessation of transaction order)

The list of Joint Users can be found on the webpage of the Association.

- iii. Purposes of Use To maintain smooth transactions of drafts, cheques and bills and to make decisions concerning own lending deals by financial institutions.
- iv. The entity name, location, and the name of the Representative Director responsible for management of Personal Data:

Bankers Association of the clearing organisation that the payment bank (branch) of the non-performing disbursed draft, cheque or bill is a member of.

The location and representative's name of each Bankers Association can be found at the following website etc.: <https://www.zenginkyo.or.jp/abstract/clearing/>

(3) Joint Use of Information among HSBC Group Companies

The Bank may jointly use Personal Data with HSBC Group Companies in order to provide high value-added products and services and/or conduct strong risk management and enhancement of HSBC group business controls. This joint use will be undertaken under necessary control measures, and when there are restrictions set by applicable laws and regulations other than the PIPA, such as the FIEA, the Bank shall comply with such laws and regulations.

- i. Jointly Used Personal Data Information (name, address, date of birth, contents and purpose of a transaction, and occupation) of the customer (including its



Connected Persons to the extent necessary for the implementation of the Purposes of Use) regarding the Bank's deposits, loans, and fund transfers and other transactions.

- ii. Scope of Joint Users The Bank and other HSBC group companies, the ultimate parent company of which is HSBC Holdings plc. ("HSBC Group Companies"). <http://www.hsbc.com/about-hsbc/structure-and-network>
- iii. Purposes of Use
  - o The information will be used to monitor and manage the various risks that are necessary to be so monitored and managed for the business operations of the HSBC group.
  - o To: (i) ascertain the customer's identity under the Act on Prevention of Transfer of Criminal Proceeds, the Foreign Exchange and Foreign Trade Act and Hong Kong Monetary Authority Guidelines, (ii) avoid financial crime and money laundering, and comply with sanctions programmes that are administered by Japan, the United States, the United Kingdom, the European Union, Hong Kong, United Nations, etc. or (iii) ascertain a customer's eligibility for certain financial products and/or services.
  - o To plan and develop various financial products and services and related proposals.
  - o To properly and smoothly implement transactions with customers.
- iv. Entity name, address, and the name of the Representative Director responsible for management of Personal Data are shown below: The Hongkong and Shanghai Banking Corporation Limited, Japan Branch 11-1, Nihonbashi 3-chome Chuo-ku, Tokyo Japan Edward Weeks President and Chief Executive Officer in Japan

## **7. Procedures for Disclosure etc. of Retained Personal Data**

Upon receipt of a request/demand for disclosure etc. by a customer in relation to the purpose of utilization, disclosure, correction, addition or deletion, ceasing of provision to a third party, disclosure of a third party provision record of the customer's Retained Personal Data, as defined in the PIPA (hereinafter referred to as a "Disclosure Request, etc."), the Bank shall action the Disclosure Request, etc., without delay, by means of providing an electronic record, delivering documents or by other means agreed with the customer.

In case the customer inquiries about the existence of his/her Individual Number in the Bank's records, the Bank shall disclose whether it retains such Individual Number or not.

#### (1) Cases that cannot be handled

The Bank may not respond to the Disclosure Request, etc. in the following cases:

- if we cannot confirm the identity of the customer or if we cannot confirm the authority of the agent of the customer;
- if the application form is inadequately completed or if the fee is not paid within the prescribed period;
- if we are not required to respond under relevant laws and regulations, for example, because the item requested does not fall within the definition of Retained Personal Data; or
- if there is threat to seriously interfere with our business.

If the Bank decides not to accept the customer's Demand for Disclosure etc., in whole or in part, the Bank shall notify the customer thereof without delay.

#### (2) Documentation and Procedures for Handling a Disclosure Request, etc.

In order to make a Disclosure Request, etc., the customer shall submit a form prescribed by the Bank. The Bank, in handling the Disclosure Request, etc. shall confirm the identity of the customer or his/her agent in a manner comparable to the procedures required by the Act on the Prevention of the Transfer of Criminal Proceeds etc., by requesting the customer or his/her agent to submit necessary documents etc.

#### (3) Disclosure Request, etc. by an Agent

An agent who makes a Disclosure Request, etc. on behalf of a customer shall be one of the following:

- i. A legal guardian of a customer who is a minor or a ward that is of age.
- ii. An agent authorized by the customer to make the Disclosure Request, etc.

The Bank will request a public certificate or power of attorney to confirm the authority of the agent, in addition to the above mentioned identity checking process.

#### (4) Handling Fee

The Bank will charge a fee of JPY 1,100 per case for the handling of a Disclosure Request, etc. The fee is payable at the time of such request and shall be paid in cash.

### **8. Security Control Measures**

The Bank takes necessary and appropriate action in relation to security controls to avoid data leakage, loss or damage of customers' Personal Information, etc. The Bank shall exercise necessary and appropriate supervision over staff and outsourced vendors (including subcontractors) who are handling customers' Personal Information, etc.

(Development of Rules on the Handling of Customers' Personal Data)

- The Bank shall establish rules for the handling of customer Personal Data

detailing how to handle the data, clarifying those in charge and for defining the roles at each stage of data processing (acquisition, use, storage, provision, deletion, disposal, etc).

#### (Organizational Security Control Measures)

The Bank shall:

- Assign a person to be responsible for the management of Personal Data.
- Maintain Security Control Measures under its Rules of Employment etc.
- Process Personal Data by applying the above mentioned rules.
- Maintain methods by which the handling status of Personal Data can be checked.
- Maintain and conduct a regime for monitoring and auditing the handling status of Personal Data.
- Maintain a regime to deal with incidents such as leakage etc.

#### (Measures for Human Security Management)

The Bank shall:

- Enter into a non-disclosure agreement etc. with employees covering Personal Data.
- Clarify employees' roles and responsibilities.
- Inform, educate, and train employees regarding these Security Control Measures.
- Check employees' compliance with processes to manage Personal Data.

#### (Physical Security Control Measures)

The Bank shall:

- Establish measures to prevent theft of equipment, etc.
- Manage recording media, etc. appropriately.
- Prohibit Personal Data to be taken outside the designated managed area in principle.
- Prohibit usage of floppy disk, USB port, personal laptop, etc., in principle.
- Strictly manage a log of entrance and exit of employees and visitors based on its rules for access management.
- Prevent mistakes of sending Personal Data by fax, telex, and emails and conduct checking of recipients and receipts to prevent Personal Data loss, etc.
- When disposing or returning equipment, process deletion of Personal Data in recordable media in the equipment appropriately.
- Dispose paper-based Personal Data in the box dedicated to the collection and

disposal of sensitive documents.

(Technical Security Control Measures)

The Bank shall:

- Identify and verify users of Personal Data.
- Set up area controls and limit access to Personal Data.
- Manage access entitlements to Personal Data.
- Establish measures to prevent leakage and destruction of Personal Data.
- Record and analyze access to Personal Data.
- Record and analyze the ongoing status of information systems that process Personal Data.
- Monitor and audit information systems that process Personal Data.

(Understanding of External Environments)

- When handling Personal Information of customers in foreign countries, the Bank shall implement appropriate Security Control Measures, after understanding the regime, etc. related to the protection of Personal Information in the foreign countries concerned.

## 9. Contacts

The Bank shall deal with complaints regarding the handling of Personal Information etc. properly and in a timely manner. Please use the following phone number for any inquiries, comments, complaints, and Disclosure Request, etc. concerning the Bank's handling of Personal Information etc. and Security Control Measures.

(Corporate sector)

Please contact your Relationship Manager or the following contact: Non-Financial Risk team, Wholesale Chief Operating Officer Office Address: 11-1, Nihonbashi 3-chome Chuo-ku, Tokyo Japan Telephone: 03-5203-3037 (9am to 5 pm on weekdays, not toll free)

(Former Retail sector)

Retail Services center, DBS Operations Address: 11-1, Nihonbashi 3-chome Chuo-ku, Tokyo Japan Telephone (Japan): 0120-777-369 (9 am to 5 pm Monday to Friday (excluding holidays), toll-free) Telephone (overseas): +81-3-5204-5001 (9 am to 5 pm Monday to Friday (excluding holidays), not toll free)

The Bank is a member of the following Authorized Personal Information Protection Organization. If you have any complaints or inquiries regarding the handling of Personal Information, you may contact these organizations as below:

- All Banks Personal Data Protection Council (<http://www.abpdpc.gr.jp/>) JBA

Customer Relations Center or Bank Business Consultation offices Tel: 03-5222-1700 or at any of the Bank Business Consultation offices

- Personal Information Consulting Centre (<http://www.jsda.or.jp>) Japan Securities Dealers Association Tel: 03-3667-8427
- Personal Information Complaints/Consultations Centre (<http://www.ffaj.or.jp/>) Financial Futures Association of Japan Tel: 03-5280-0881

## **10. Changes to this Policy**

The contents of this policy may be changed without notice and without informing customers individually in accordance with relevant laws and regulations due to legislative amendments and other reasons. In such case, the changes shall be published on the Bank's website.

The Hongkong and Shanghai Banking Corporation Limited, Japan Branch 11-1,  
Nihonbashi 3-chome Chuo-ku, Tokyo  
Japan

Karine Colyn  
President and Chief Executive Officer in Japan