



Privacy Policy

Standard Chartered Securities (Japan) Limited

In order to retain and protect the confidence of our valued customers, we (Standard Chartered Securities (Japan) Limited) shall make every effort, in good faith, to ensure the appropriate protection and usage of personal data through effective implementation of organizational, people, and technical security measures. Regarding customers' personal data protection, we will conform to the Act on the Protection of Personal Information (herein after called "Act"), the relevant applicable local laws, ordinances and Guidelines etc (herein after called "Laws and Regulations") and we shall not use our customers' personal data for the purposes other than the purposes set forth by this Privacy Policy without consent from our individual customers. If we receive a complaint from a customer, we shall make every effort to swiftly find an appropriate resolution.

1. Services Provided

- Financial Instruments business and other ancillary businesses.
- Services that we are allowed to perform by Financial Instruments and Exchange Act.
- Other services and related operations that can be performed (including any additional services that may be permitted as a result of future changes in the regulatory environments).

2. Purposes of Acquiring Information

We acquire "personal information" of customers to process transactions in a secure and sound manner, and to provide our customers with appropriate financial products and services. Personal information shall be used for the following purposes:

- To process applications for account opening, transactions of financial products and services.
- To verify customer identity in accordance with the Act on Prevention of Transfer of Criminal Proceeds, the Foreign Exchange and Foreign Trade Control Act and other Laws and Regulations.
- To confirm a customer's qualifications to purchase financial products and/or use provided services.
- In order to verify the authority of a person acting as a representative or agent of a corporation, if the customer is a legal entity.
- To report result of transaction, market value information and balance received from the customer.



- To conduct administrative processes for transactions with customers.
- To make decisions based on the principle of suitability, and to judge the appropriateness of providing financial products or services.
- To exercise rights or to fulfil obligations under applicable Laws and Regulations or arising from contractual relationships with the customer.
- For market research, data analysis and surveys related to the research and development of financial products and service.
- To provide customers with solicitations regarding securities, financial products and information regarding services based on Financial Instruments and Exchange Act to provide customers with solicitations regarding financial products and information regarding services provided by us, affiliates company(s), partner company(s).
- When entrusted by another business entity with processing of all or part of a database of personal information, as necessary to carry out consigned services in an appropriate manner.
- Other uses to secure smooth and appropriate execution of transactions with customers.

3. Types of Information to be Acquired and Acquiring Channels

Typical Information

The typical information to be acquired from a customer which is described in Chapter 2 above. Purpose of Acquiring Information will be the customer's name, residential address, date of birth, place of work, job title, workplace location, telephone number, fax number and email address for the purpose of prevention of money laundering under the Act on Prevention of Transfer of Criminal and other laws requiring customer due diligence. There may be cases where additional information is necessary at the commencement of business dealings. We would not collect or store any Specific Personal Information, in principle, except for those set forth in the applicable Laws and Regulations.

Sensitive Information

We shall not acquire "Sensitive Information" which is defined by the "Guideline on Personal Information Protection in Financial Sector" which include Special Care Required Personal Information (e.g race, beliefs, social status, medical history, fact such as being a victim of a crime etc) which is defined by the Act except for the cases permitted by Laws and Regulations.



In cases where we acquire sensitive information that is co-mingled with other information for the purpose of customer identification, the area of sensitive information shall be blacked out before it is archived.

Methods of Acquisition

We acquire the personal information of customers who request information over the phone or through our website. To the extent necessary for the achievement of the Purpose of Use, we acquire personal information of the customer from the customer or third parties by appropriate and lawful means, orally, by mail, the Internet, telephone, facsimile, etc.

4. Usage and Provision of Information

Usage and Provision to a Third Party

We shall not use customers' information beyond the above-mentioned "purposes" nor provide to external parties except in the following cases:

- Where the customer has given his or her prior consent.
- Where it is judged as necessary under Laws and Regulations.
- Where it is considered as necessary to protect human lives, human bodies, or property and it is difficult to acquire the data subject's consent.
- Where it is required to cooperate with a government organization, local authority, etc. so that it can accomplish the duties set down by Laws and Regulations and it is possible that acquiring customers' consent may obstruct the accomplishment of those duties.
- Where the personal information is to be entrusted with a third party for the purpose of outsourcing operations, whether wholly or in part.
- Cases in which the personal information of customers is provided as a result of business succession due to merger or other reasons; or
- Where it is allowed under other Laws and Regulations.

We have outsourced a portion of our business processing for transactions, to external vendors. On such occasions, in order to select outsourcing vendors, we shall conduct due diligence on the security control measures according to our prescribed assessment criteria. In addition, we shall take necessary measures to ensure that outsourced operations are carried out properly. We will supervise outsourcing vendors, including those vendors that use subcontractors for two or more tiers.



We may provide our customers' personal information to third parties in foreign countries. Except as otherwise provided by Japanese Laws and Regulations, we will provide necessary information in accordance with the provisions of such Laws and Regulations and obtain the prior consent of the customer to permit the provision of such information to a third party in a foreign country.

In the event that we provide "personal related information" with respect to customers to a third party and it is assumed that such third party will treat such "personal related information" as personal data, we will confirm this and provide information necessary for the customer as required in accordance with the provisions of Laws and Regulations, except as otherwise provided by Laws and Regulations.

Joint Use

Personal data is jointly shared within compliance of Laws and Regulations as follows:

- ① Scope of information to be joint use
Joint use of name, address, date of birth, phone number, place of work (membership of an organization), title, business address, fax number, e-mail address and other related matters
- ② Scope of joint users
Companies which belong to Standard Chartered Group whose ultimate holding company is Standard Chartered PLC.
- ③ Purposes of joint use
To provide our total services
To manage risks relating to business management and internal control, etc. by SCB Group
- ④ Name of responsible person in charge of managing personal data
Fukuhiro Ezawa, Representative Director and President (Standard Chartered Securities (Japan) Limited, Sanno Park Tower 21F, 2-11-1 Nagata-cho, Chiyoda-ku, Tokyo 100-6155).

5. Information Management Method

We will strive to keep the personal data of customers accurate and up-to-date within the scope of the purpose of use. In order to prevent the loss, destruction, falsification, and leakage of personal information of customers, we have formulated a basic policy to ensure the proper handling of personal data and have taken the following measures. In addition, in the event of a leakage of personal information handled by us,



we will respond appropriately, such as by submitting a report to relevant competent authorities, or notifying the customer thereof, in accordance with the provisions of Laws and Regulations.

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

We establish the roles and responsibilities for the handling of personal information by the responsible person(s) in charge.

(Organizational Security Control Measures)

We assign a person to be responsible for the handling of personal information of customers, clarifying the scope of employee handling of personal data, the scope of personal information to be handled, and establish a system for reporting information to the person in charge in the event that any fact or sign of violation of laws or regulations governing the handling of personal data is identified.

We periodically conduct self-inspections of the status of the handling of personal information of customers and conduct audits.

(Measures for Human Security Management)

We conduct periodic training for employees on the key issues in handling personal information of customers. We include in the Rules of Employment matters concerning the confidentiality of personal information of customers.

(Physical Security Control Measures)

We implement measures to control the access and exit of employees to and from areas in our premises where personal information of customers is handled, and to prevent unauthorized persons from viewing any personal information of our customers.

(Technical Security Control Measures)

We implement access control to limit the scope of employees in charge and the scope of personal information databases handled.

Introduce mechanisms to protect information systems handling customer personal information against external fraudulent access or fraudulent software.

6. Request for Disclosure, Correction, or Suspension of using Information by the Customer.

In the event the customer or its agent requests us to disclose, correct, add or delete the contents of, cease the utilization of, erase, cease the third-party provision, or disclose a record of provision to a third



party (hereinafter referred to as a "Disclosure Request, etc.") pursuant to the Act, we will respond to the Disclosure Request, etc. in accordance with the following procedures under the provisions of the applicable Laws and Regulations after confirming the identity of the customer based on the necessary personal identification documents (copies of a driver's licence, passport, etc.). Please note that there are cases where fixed fees are applicable for purpose of use notices or disclosures.

*** Method of Providing Response**

In principle, we will promptly respond to the customer request to the customer's registered address. Even if the request is received from the customer's legal agent, our response may be mailed directly to the customer.

*** Denial of Disclosure Request**

We shall deny any request by a customer for disclosure of personal information in the following cases. When the determination has been made to deny the request for disclosure, the customer shall be informed to that effect. The specific amount of fees, however, will still be charged to the customer.

1. When the customer's identity cannot be verified.
2. When the identity or authority of the person making the disclosure request as the customer's legal agent cannot be verified.
3. When there are errors or omissions in the request form.
4. When required fees are not paid within the specified period of time.
5. When the requested information does not match personal data held by us.
6. When we suspect that such disclosure could threaten or harm the life, body, property or other rights of the customer or a third party.
7. When we suspect that fulfilling the request could result in a significant hindrance to conducting our business in an appropriate and effective manner.
8. When fulfilling the request would be a violation of other laws or regulations.

Inquiry Desk

The following is the contact regarding inquiries as to disclosure of personal information etc.



Customer Inquiry Desk

Standard Chartered Securities (Japan) Limited

Address: Sanno Park Tower 21F 2-11-1 Nagata-cho, Chiyoda-ku, Tokyo 100-6155

Inquiry Desk: Conduct, Financial Crime & Compliance Dept.

Telephone: 03-5511-1200 (Representative)

Hours: 9:00a.m. - 5:00p.m

(Excluding Saturday, Sunday, public holidays and the yearend/New Year non-banking business days)

7. Complaints

Complaints regarding the handling of personal information.

We are a member of the Japan Securities Dealers Association, an accredited Personal Data Protection Organization in the financial sector. The association accepts complaints and consultation with regards to the handling of personal information by association members at consultation office Japan Securities Dealers Association, Personal Information Consultation Office).

Japan Securities Dealers Association, Personal Information Consultation Office

Tel: 03-6665-6784

<http://www.jsda.or.jp/privacy/index.html>

8. Amendment to This Privacy Policy

The aforementioned purposes of usage or information contents in this Policy may be modified from time to time as a result of amendment to the Laws and Regulations and other reasons. When the Policy is modified, the modified policy will be made available to our customers on our website, or by other means.

Standard Chartered Securities (Japan) Limited

Representative Director and President

Fukuhiro Ezawa