NATIXIS
CORPORATE AND
INVESTMENT BANKING

Privacy Policy

Natixis Tokyo Branch

Natixis Tokyo Branch (hereinafter referred to as the “Company”) recognizes the importance of safeguarding personal information in order to be a financial instruments business operator that customers can trust and choose, and when handling customers’ personal information, our Company shall adhere to the “Act on the Protection of Personal Information” and any relevant laws and regulations concerning Personal Information, including, but not limited to, rules relating to the collection of personal data and anti-bribery and corruption laws, as well as the Act on Prevention of Transfer of Criminal Proceeds, whether imposed upon the Company or certain of its licensed employees, etc. (“Applicable Laws”), the Guidelines for Protection of Personal Information in the Finance Sector and other related guidelines, and the guidelines of the authorized personal information protection organization, etc., shall ensure proper handling, management, and protection of personal information, and shall comply with the privacy policy that is established as below.

1. Acquisition and Use of Personal Information, etc.

(1) The Company acquires customers’ personal information to proceed with customer transactions safety, reliably, and to provide better products and services. Specifically, the Company will use personal information within the scope of the following purpose:

- To comply with any requirements specified under Applicable Laws;
- To perform or solicit transactions and related services concerning financial instruments, etc. of the Company or related companies in relation to the business that the Company can operate under the Money Lending Business Act (Act No. 32 of 1983) and other laws and the related businesses;
- To determine the suitability of financial products and services, in light of suitability principles, etc.;
- To confirm personal identification of the customer or his/her agent;
- To promote internal operations such as credit risk and other risk assessments with customers, and manage new and existing transactions;
- To inform or advise the customer of transaction results, account balance, market valuation, etc.;
- To conduct administrative matters related to transactions with the customer;
- To exercise rights or perform duties under relevant laws and regulations, or in accordance with agreements;
- To research and develop financial products and services based on market survey, data analysis, customer enquiry, etc.;
- To carry out services properly, in the event we are outsourced all of or part of services handling personal information by a third-party business operator;
- To properly understand and manage the business of any outsourcee
- To send market reports, information on various seminar, reception, etc. and seasonal greetings;

- To conduct internal management operations at the Company and related companies;
- To properly and seamlessly complete transactions with customers, in addition to the above mentioned; and
- Regardless of the purposes listed in the above, the Company shall use the individual number for the “administrative matters of application and submission of account opening pertaining to money lending business” and the “administrative matters of preparation and submission of statutory documents pertaining to money lending business”.

(2) The Company may change the purpose of use set forth in the preceding paragraph within the scope stipulated by the laws, etc. In this case, the Company will promptly notify the principal or announce the changed purpose of use.

(3) The Company will endeavor to keep your personal information accurate and up to date within the scope necessary to achieve the purpose of use, and to delete personal data without delay when it is no longer necessary.

2. Recording and Monitoring of Communications

In accordance with the purposes set out in Section 1 above, the Company and its employees and agents may from time to time intercept, record and/or otherwise monitor all communications sent and received via its systems, including telephone calls, emails, instant messaging systems, use of the internet and faxes. All monitoring will be carried out in accordance with the Applicable Laws.

3. Type of information obtained

The Company will obtain the following information:
Name, age, date of birth, address, phone number, fax number, e-mail address, company name, position, company address, type of products/services, transaction amount, contract date, and other information necessary or related to transactions with the Company.

4. Acquisition of information

To the extent necessary to achieve the purpose of use, the Company will acquire customers' personal information by appropriate and lawful ways, such as oral or written means, from sources such as the following:
- Personal information is provided directly from documents filled out and submitted by the customer (submission of documents such as application forms from the customer, data input from the customer from websites, etc.); and
- Case in which personal information is provided by a third party such as joint users or personal credit information agencies.

5. Provision of Personal Data

(1) The Company shall not provide customers’ personal data to a third party except in the following cases and the cases stipulated by the laws, etc.:
- When customer consent is obtained;
- When it is based on the laws and regulations;
- When there is a need to protect a human life, body or property (including property of corporations), and when it is difficult to obtain the customer’s consent;

- When there is a special need to enhance public hygiene or promote the fostering of healthy children, and when it is difficult to obtain the clients' consent;
- When there is a need to cooperate with a central government or local government organization, or a person entrusted by them to perform affairs prescribed by the laws and regulations, and when there is a possibility that obtaining customer consent would interfere with the performance of the said affairs;
- When entrusting all or part of the handling of personal data to the extent necessary to achieve the purpose of use;
- When personal data is provided due to a succession of business caused by a merger or other reason; and
- When personal data is to be jointly utilized based on (3) below.

(2) The Company may outsource all or part of personal data handling to the extent necessary to achieve the purpose of use. In the course of outsourcing, the Company will conduct necessary and appropriate supervision of any outsourcee.

(3) The Company may share and jointly use customers' personal data
- Customer personal data items shared or jointly used:
  Customers' (a) address, name, date of birth, company of employment, phone number, other contact information, role/position/title, responsibility; (b) Information relating to the clients' transactions such as transaction details, deposit balance; (c) information related to the customer's asset management needs; and (d) other personal information required to achieve purpose of use described in this privacy policy
- Entities which will jointly use information:
  The Company and companies within Natixis Group (Natixis Japan Securities Co., Ltd., Natixis Investment Managers Japan Co., Ltd., and other related companies located both domestically and abroad, which can be confirmed from the Natixis homepage)
- Purpose of use of information:
  Scope described in (1) under "1. Acquisition and Use of Information"
- Name of the individual responsible for managing personal data :
  Natixis Tokyo Branch
  Ark Hills South Tower, 1-4-5 Roppongi, Minato-ku, Tokyo 106-0032
  Senior Country Manager and CEO Makito Nagahiro

(4) The Company may provide personal data to a third party located in a foreign country. In this case, unless stipulated by the laws, the Company will obtain the consent of the person in advance to allow the provision of personal data to a third party located in a foreign country after providing the necessary information in accordance with the provisions of the laws.

(5) The Company may provide personal data to a third party located in a foreign country who has established a system that complies with the standards set forth in the ordinances of the Personal Information Protection Committee, which are necessary to continue to abide by the measures that are equivalent to the measures business operators handling personal information shall take under the provisions of the Personal Information Protection Act (hereinafter referred to as "equivalent measures"). In this case, we shall take necessary measures to ensure the continuous implementation of the corresponding measures by third parties. The customer may also request the Company to provide information regarding such necessary measures.

However, if any request for the provision of information is likely to significantly impede on the proper implementation of the Company's business, the Company may not provide all of or part of the information requested.

The foreign countries to which the Company provides customers' personal information are as follows.
France, Hong Kong, Singapore

(6) When the Company provides individual-related information to a third party, and it is assumed the third party will obtain this information as personal data, we will, unless stipulated by law, perform necessary confirmation and provision of the information to the third party, according to the laws set forth.

6. Handling of Sensitive Information

Regarding sensitive information, stipulated in the Guidelines for the Protection of Personal Information in the Financial Sector, the Company will not acquire, use, or provide such information to third parties, except in the cases listed in the Guidelines, such as the case that it is based on the laws and regulations, and the case that the Company obtains customer consent to the extent necessary to perform its business.

7. Management of personal information

The company takes appropriate steps to keep customer's personal information accurate and up to date. In addition, we take the following organizational security control measures, personnel security control measures, physical security control measures, and organizational security control measures to prevent the leakage, and loss or damage (hereinafter referred to as "leakage, etc.") of the clients' personal data. In addition, we conduct the appropriate management of personal information after understanding the external environment when handling clients' personal information in a foreign country.

(Improvement of Discipline Concerning Handling of Clients' Personal Data)
- Establish personal data handling rules for each stage including acquisition, use, storage, provision, deletion, disposal, etc., we will establish personal data handling rules, including the handling method, deciding the responsible person/person in charge, and their duties, etc.

(Organizational Security Control Measures)
- Appoint a person responsible for handling personal data of clients, clarify the scope of personal data handled by employees who handle personal data, and developed a framework for reporting and contacting the responsible person in case there are violations or signs of possible violations of laws and handling rules.
- Conduct periodic self-investigations on the handling of clients' personal data and conduct audits by other departments and/or external parties

(Personnel Security Control Measures)
- Conducting periodic training of employees on key considerations regarding the handling of personal data
- Matters related to confidentiality of personal data are stated in the Rules of Employment.

(Physical Security Control Measures)

- In the area where personal data is handled, we will control the entrance and exit of employees, and restrict the equipment they bring in, and implement measures to prevent unauthorized persons from viewing personal data.
- Measures are taken to prevent theft or loss of devices, electronic media, documents, etc. that handle personal data, and in cases devices or electronic media, etc. is carried, including within the office, implement measures to prevent the discovery of personal data easily.

(Technical Security Control Measures)
- Implementing access controls to limit the scope of the person in charge can access databases with personal information, etc.
- Implement a mechanism to protect information systems that handle personal data from unauthorized external access or unauthorized software

(Understanding the external environment)
- When handling personal data in a foreign country, security control measures are implemented after understanding the system regarding the protection of personal information in the country where personal data is stored.

8. Request for Disclosure, Cancellation, etc. from the Customer

Regarding their personal information, if a customer wishes to be notified of the purpose of use, halt in disclosure, correctio/addition/deletion, suspension/erasure, suspension from being provided to a third party, or disclosing the record of provision to a third party, please contact us for inquiries by using the contact information below. After confirming the identity of the customer, we will respond based on the provisions set forth by law and regulations. Please note that actual costs prescribed by NJS may be required for notification and disclosure of the purpose of use.

9. Customer Inquiries, Opinions and Complaints

Contact Information:
If you have any questions regarding notification of the purpose of personal information use, disclosure, correction/addition/deletion, suspension/deletion of use, suspension of provision to third parties, requests for disclosure of records provided to third parties, and other consultations and complaints regarding the handling of personal information, please contact us below.

Natixis Tokyo Branch Compliance Department
Ark Hills South Tower, 1-4-5 Roppongi, Minato-ku, Tokyo 106-0032
Telephone: 03-4519-2120
Reception Hours: 9:00～17:00 (excluding weekends, public holidays, and year-end and New Year holidays)

10. Revision

The contents of the above description may be changed within the scope stipulated by laws and regulations due to the revisions of laws, etc. and other reasons. In that case, we will notify the change through postings at the counter or through this website.

11. Personal Information Protection Commission

Inquiry Line for Act on Protection of Personal Information of the Personal Information Protection Commission will undertake complaints/consultation in relation to the handling of Personal Information.

Inquiry Line for Act on Protection of Personal Information:
Tel: 03-6457-9849
https://www.ppc.go.jp/en/contactus/piinquiry/

12. Continued Improvement

The Company shall review this Policy as necessary in response to the development of information technology, the change of cultural request, etc., and shall continue to improve the handling of personal information.