

Japan

Wells Fargo International Privacy Notice

Effective: 07 July 2023

The Wells Fargo entities listed in Section 10 (“**we**”, “**our**”, “**us**” or “**the Company**”) which you and/or your organization have a relationship or otherwise share Personal Data with provide this privacy notice (“**Notice**”) to describe our practices as a data controller regarding the collection, storage, use, disclosure, and other processing of Personal Data as defined below. If you or your organization has a relationship or otherwise share Personal Data with a Wells Fargo entity in any other jurisdiction other than Japan, a different privacy statement at <https://www.wellsfargo.com/privacy-security> regarding that Wells Fargo entity's practices will govern those information collection and processing activities.

1. Types of Personal Data Collected

In Japan, we primarily have relationships and accounts only with corporations and other legal entities. However, we may collect information about individual representatives (“**Individuals**”) of our customer organizations (“**Customers**”) such as the Individual's:

- **Work contact details:** such as name, work address, phone number, mobile phone number, email address, and online contact details, including but not limited to unique identification and password for access to our website, mobile applications, and/or social media features.
- **Position description:** such as employer, title, position held, duties, and length of employment.
- **Authentication data:** such as passport, driver's license, other governmental identification information, home address and telephone number, documents that verify address, date of birth, country of domicile, documents that verify employment, and signature authorization.
- **Financial data:** such as salary and other income, sources of wealth, assets and documents that verify assets, credit reports, financial relationships, and financial transactions.
- **Background check data:** such as background check information including credit and criminal checks and screening, to the extent required or permitted by local law.
- **Surveillance data:** such as images and voices captured by CCTV video and audio surveillance equipment installed (to the extent permitted by local law) onto the business premises of a Wells Fargo entity, if your Individuals visit the business premises.
- **Electronic and voice communications data:** such as content, data and recordings relating to business communications with Wells Fargo through all applicable communication channels, including email, text, instant message or chat, transcriptions, telephone communications, voice recordings, video recordings, including IP address and session identification, and presentations hosted by Wells Fargo.

Collectively, the above categories of data constitute “**Personal Data**”. Among the types of Personal Data above, some of them may be considered as sensitive Personal Data under privacy laws in Japan, such as information revealing the aspects of criminal records, social status, political opinions, etc. The processing and transfer of sensitive Personal Data is necessary

to achieve the purposes described in Section 2, and will be conducted in a way that would have the least impact on personal rights and interests. Unless stated otherwise, references to Personal Data in this Notice include sensitive Personal Data.

We may collect Personal Data directly from the Individual, Customers, including through interactions with the Bank and use of Bank systems, private lists, and publicly available sources. We may process your Personal Data in physical and electronic form and will do so in a way that adequately safeguards your Individuals' personal rights and interests in accordance with Japan's data protection laws. You and your Individuals have the right to refuse to consent to providing Personal Data. However, processing of this information is necessary, and failure to provide this information may result in Wells Fargo being unable to provide or continue to provide the requested services to the Customer where Personal Data is necessary to provide the requested services.

2. Purposes of Collection and Use

The purposes of collection and use of Personal Data are:

- **To provide the services requested by our Customers**, perform obligations under our agreements, and carry out related business functions, including performing data and transaction processing, conducting credit checks, handling Customer inquiries, including communicating, presenting, and meeting with a Customer, and managing the Customer relationship, we collect and use Personal Data including work contact details, position description, authentication data, financial data, background check data, electronic and voice communications data, and other categories of Personal Data where needed.
- **To comply with legal obligations, regulations, regulatory guidance or codes of practice** applicable to the Company and its Affiliated Entities (defined below) in the United States and/or any relevant jurisdictions, including but not limited to complying with "know your customer" obligations based on applicable anti-money laundering and anti-terrorism requirements, economic and trade sanctions, customer due diligence, fraud prevention and information security, suspicious activity reporting, foreign exchange and international trade, tax reporting and other applicable laws, regulations, ordinances, and obligations, complying with any requests from any regulator or authority to the extent permitted by applicable law, we collect and use Personal Data including work contact details, position description, authentication data, financial data, background check data, electronic and voice communications data, and other categories of Personal Data where needed.
- **To confirm a person's authority as a representative or agent of a Customer** with which the Company or its Affiliated Entities have entered or intend to enter into various arrangements, including but not limited to deposit contracts, loan contracts, contracts for foreign exchange transactions, contracts for derivative transactions, and letters of credit, we collect and use Personal Data including work contact details, position description, background check data, authentication data, and other categories of Personal Data where needed.
- **To conduct recordkeeping and otherwise manage the business** (for example, to monitor or facilitate compliance with Wells Fargo's internal policies, to perform risk management, to maintain or upgrade Wells Fargo's technology or systems, to protect the business, rights or property of any Wells Fargo Group entity (defined in Section 3) by raising any legal claim, defense or proceedings, to support the conduct of audits, support business transfers, combinations, restructuring, dissolutions or similar activities relating to any Wells Fargo Group entity, etc.), subject to and in accordance with applicable law, we collect and use Personal Data including work contact details, position description, authentication data, financial data, background check data, electronic and voice communications data, and other categories of Personal Data where needed.

3. Disclosure of Personal Data

The Company may share or transfer the Personal Data described in Section 1 to the recipients below for the purposes listed in Section 2 (in each case to the extent necessary and on a need-to-know basis).

- **Affiliated Entities.** The Company has Affiliated entities operating in the United States and around the world ("**Affiliated Entities**"), including the group parent in the United States, Wells Fargo & Company, and Wells Fargo Bank, N.A. (collectively, the Company and our Affiliated Entities are the "**Wells Fargo Group**"). We may disclose Personal Data to our Affiliated Entities on a worldwide basis. A non-exhaustive list of Affiliated Entities is found in this Wells Fargo & Company 10-K filing made with the US Securities and Exchange Commission: <https://www.sec.gov/Archives/edgar/data/72971/000007297123000071/wfc-1231x2022xex21.htm>
- **Beneficiaries, counterparties, and other parties related to a transaction.** The Wells Fargo Group may disclose Personal Data to beneficiaries, counterparties, or other parties related to a transaction on a worldwide basis to provide the services requested by our customers and to comply with legal obligations and regulations.
- **Service providers.** The Wells Fargo Group may disclose Personal Data to information technology providers or other service providers around the world that act under our instructions regarding the processing of such data ("**Data Processors**"). Data Processors will be subject to contractual obligations to implement appropriate administrative, technical, physical, and organizational security measures to safeguard Personal Data, and to process Personal Data only as instructed. The Wells Fargo Group may also disclose Personal Data to independent external auditors or other service providers around the world that may not be acting as a Data Processor. Such service providers will be subject to any necessary contractual obligations regarding the protection and processing of such Personal Data.
- **Legal requirements.** Subject to applicable law, the Wells Fargo Group may disclose Personal Data if required or permitted by applicable law or regulation, including laws and regulations of the United States and other countries, or in the good faith belief that such action is necessary to: (a) comply with a legal obligation or in response to a request from law enforcement or other public authorities wherever the Wells Fargo Group may do business; (b) protect and defend the rights or property of any Wells Fargo Group entity; (c) act in urgent circumstances to protect the personal safety of Individuals, Customers, and contingent resources/employees of any Wells Fargo Group entity or others; or (d) protect against any legal liability. In addition, the Wells Fargo Group may share your Personal Data with U.S. regulators and with other self-regulatory bodies to which we are subject, wherever the Wells Fargo Group may do business.
- **Business transfers, combinations and related activities.** As we develop our business, the Wells Fargo Group might sell, buy, acquire, obtain, exchange, restructure or reorganize businesses or assets. In the event of any actual or proposed sale, merger, reorganization, transaction, restructuring, dissolution or any similar event involving our business or assets, Personal Data may be shared with the relevant entity or may be part of the transferred assets and will be subject to any necessary contractual obligations to ensure the protection of Personal Data.

The Company is responsible for the management of Personal Data shared with the abovementioned recipients, and the contact details of the Company's representatives are listed in Section 10. The recipients of Personal Data identified in this Section 3 may be located in the United States and other jurisdictions that may not provide, or require recipients to provide, the same level of data protection as your home country. As needed, we have taken steps to establish appropriate data transfer agreements or otherwise address cross-border data transfer restrictions. These safeguards/measures enable us to transfer and use Personal Data in a secure manner anywhere in the world where we have an establishment, or where we have contracted third parties to provide us with services. At your request, we will provide you with additional information about these safeguards where required by Japanese privacy law. You may contact the Regional Data Privacy Officer using the contact information in Section 8 to request for additional information about these safeguards.

4. Consents

To the extent that consent is required by applicable law, you expressly consent to the collection, use, disclosure (including cross-border transfer), and other processing of Personal Data as described in this Notice by providing Personal Data to the Wells Fargo Group or authorizing our Customer to provide such information to us. Where you directly or indirectly provide any Wells Fargo Group entity with the Personal Data of any individuals, you must have first informed such individuals about

our data privacy practices by providing them with a copy of this Notice, and obtained all required informed consents (including separate consents) from such individuals to permit the activities described in this Notice, before providing their Personal Data to the Wells Fargo Group. You expressly waive the bank secrecy or confidentiality laws and obligations, if any, of the country or countries where you and the accounts are located to the extent permitted by applicable law.

You may revoke consent at any time by notifying us at the address provided in Section 8 of this Notice. Prior uses and disclosures will not be affected (unless required by applicable law), and we may otherwise continue to process Personal Data as permitted or required by law. Revocation of consent may result in our inability to provide or continue to provide the requested services to the Customer.

5. Information Management, Security Control Measures, and Retention Periods

The Personal Data will be safely stored in the databases of Wells Fargo. Appropriate measures are taken so that Personal Data can be kept accurate, and up-to-date, which will be in accordance with the applicable security requirements. In an effort to prevent the loss, misuse, unauthorized access, disclosure, alteration or destruction of Personal Data, Wells Fargo will take appropriate legal, technical, physical and organizational security measures to protect Personal Data. We will keep Personal Data no longer than necessary to: i) fulfill the purposes outlined in this Notice; ii) comply with legal or regulatory obligations to which Wells Fargo is subject; or iii) perform a contract duly established with you or in order to take steps at your request prior to entering a contract. We have implemented appropriate records retention policies to retain Personal Data only to the extent permitted by applicable laws. We may need to hold Personal Data beyond retention periods in response to an audit, investigation, or other legal matter. These requirements also apply to our third party service providers. Where required by law, Wells Fargo will anonymize data for additional processing.

While registering with our website, mobile applications, or social media features (each, a "**Site**"), we may provide you with a unique identification and password for accessing our products and services. We encourage you to choose your password wisely such that no intruder or third party can obtain any unauthorized access to the Site. We also encourage you to keep your password confidential and not have any written or other record of the password that can be accessible by an intruder or third party.

6. Data Subject Rights and Choice for Marketing Materials

Data Subject Rights

Your Individuals may have certain rights in relation to Personal Data we hold about them. They may have the right to access, delete and correct any Personal Data held about them. They may also have the right to object to processing of their Personal Data, the right to be provided with information about security measures implemented to protect their Personal Data, and the right to be informed of the name of our Data Privacy Officer. Finally, they have the right to withdraw their consent to the processing of their Personal Data, but such withdrawal will not affect the lawfulness of processing performed prior to the withdrawal request or performed based on a lawful basis other than consent.

Requests must be submitted by the Individual in writing to the address listed in Section 8 below. After we have verified the Individual's identity, we will endeavor to respond promptly to valid data subject requests and take the other actions requested as specified by local law. Where permitted by law, we may charge an appropriate fee to cover the costs of responding to the request. These rights may not be absolute, and exceptions may be applicable. If Wells Fargo is not able to accommodate the request, the requestor will be provided with reasons for the denial.

Choice for Marketing Materials

If you do not want to receive marketing and sales materials from Wells Fargo by direct mail, telephone or email, please follow the "unsubscribe" instructions provided in those communications or submit a written request to the address listed in Section

8 below. We will comply with your request within a reasonable period of time after receiving it or within the time period required by local law.

7. Complaints

You may have a right under applicable law to make a complaint if you think we have not adhered to this Notice or any applicable privacy law in handling your Personal Data. If you would like to make a complaint, please submit your complaint in writing to the contact details in Section 8. We will respond to a written complaint within 30 days. If you are not satisfied with our response, you may be able to pursue your complaint with the data protection authority in Japan.

8. Customer Inquiries

Please direct all requests regarding your Personal Data, or any questions regarding this Notice to:

Asia-Pacific:

APAC Regional Privacy Officer

138 Market St, #30-01 CapitaGreen, Singapore, 048946

Telephone: (65) 6395 6900

privacy.apac@wellsfargo.com

Your comments are valuable to us and we assure you that we will do our best to address them.

9. Modifications

This Notice may be modified as a result of amendments to the law or regulations or due to other reasons. In such case, an amended Notice will be posted on our website at <http://www.wellsfargo.com/privacy-security/>. The page providing the Notice shall contain a date as to when the Notice was last updated.

10. Wells Fargo Entities Covered by this Privacy Notice

Name of Entity	Address	Entity Representative in Japan
Wells Fargo Bank, National Association, Tokyo Branch	24th Floor, Marunouchi Trust Tower Main 8-3, Marunouchi 1-chome Chiyoda-ku, Tokyo 100-0005	Suzuki, Ryota
Wells Fargo Securities (Japan) Co., Ltd.	24th Floor, Marunouchi Trust Tower Main 8-3, Marunouchi 1-chome Chiyoda-ku, Tokyo 100-0005	Kikuchi, Tomomi