
Wells Fargo International Privacy Notice – Mainland China

This Notice applies to customers in the mainland of the People's Republic of China.

Effective: 11 August 2022

The Wells Fargo entity with which you and/or your organization have a relationship or otherwise share Personal Data ("**Wells Fargo**") provides 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 the U.S., 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

Outside the United States, 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:** 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:** employer, title, position held, duties, and length of employment.
- **Authentication data:** national ID/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, marriage certificate (if the Individual acts as a personal guarantor), and signature authorization.
- **Financial data:** salary and other income, sources of wealth, assets and documents that verify assets, credit reports retrieved from local financial regulator or credit agency, financial relationships, and financial transactions.
- **Background check data:** background check information including credit and criminal checks and screening, to the extent required or permitted by local law.
- **Surveillance data:** images and voices captured by CCTV video and audio surveillance equipment installed according to local law onto the business premises of a Wells Fargo's entity in your jurisdiction, if you visit the business premises.
- **Electronic and voice communications data:** business communications content and data, including IP address and session identification, with Wells Fargo through all applicable communication channels, including email, text, instant message or chat, transcriptions and/or telephone communications, voice recordings, video recordings, and presentations hosted by Wells Fargo.

Collectively, the above categories of data constitute “**Personal Data.**” Amongst the above Personal Data, some of them are considered as sensitive Personal Data under privacy laws in China, such as information revealing the aspects of specific identity (e.g., governmental identity documents, political affiliations, undisclosed criminal records, etc.), financial accounts, personal whereabouts, etc.

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. **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.**

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 work contact details, position description, authentication data, financial data, background check data, and electronic and voice communications data.
- **To enable Wells Fargo and its Affiliated Entities (defined below) to respond to requests from any regulator or authority, raise any legal claim/defense or participate in judicial, regulatory or dispute resolution proceedings, perform risk management, or comply with legal obligations and regulations** applicable to Wells Fargo and its Affiliated Entities (defined below) in the United States and/or any relevant jurisdictions, including but not limited to “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, operating whistleblowing systems or channels, foreign exchange and international trade, tax reporting, public security and other applicable laws, regulations, ordinances, and obligations, we collect and use work contact details, position description, authentication data, financial data, surveillance data, background check data, and electronic and voice communications data.
- **To confirm a person’s authority as a representative or agent of a Customer** with which Wells Fargo 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 work contact details, position description, background check data, and authentication data.
- **To conduct recordkeeping and otherwise manage the business and our technology**, subject to and in accordance with applicable law, we collect and use work contact details, position description, authentication data, financial data, surveillance data, background check data, and electronic and voice communications data.

3. Disclosure of Personal Data

Wells Fargo may disclose Personal Data as follows (in each case to the extent necessary and on a need-to-know basis).

- **Affiliated Entities.** Wells Fargo has affiliated entities operating in the United States and around the world, including the group parent in the United States, Wells Fargo & Company, and Wells Fargo Bank, N.A. (“**Affiliated Entities**”) (collectively, Wells Fargo and our Affiliated Entities are the “**Wells Fargo Group**”). A non-exhaustive list of Affiliated Entities can be found in the list at the following hyperlink (<http://www.sec.gov/Archives/edgar/data/72971/000007297115000449/wfc-12312014xex21.htm>) viewed in combination with the additional list in the most recent Wells Fargo & Company 10-K filing, Exhibit 21, made with the US Securities and Exchange Commission available at: <https://www.sec.gov/cgi-bin/browse->

[edgar?action=getcompany&CIK=0000072971&type=10-k&dateb=&owner=include&count=40](https://www.sec.gov/edgar?action=getcompany&CIK=0000072971&type=10-k&dateb=&owner=include&count=40). Wells Fargo may disclose Personal Data to our Affiliated Entities on a worldwide basis, and such affiliates may use the data, for the purposes described in Section 2.

- **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 ("**Entrusted Persons**"). Entrusted Persons 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, accountants, advisers, consultants or other service providers around the world that may not be acting as an Entrusted Person. 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 People's Republic of China, United States and other countries or regions, 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 any regulatory, governmental, 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 or defend against any legal liability. In addition, to the extent permitted by applicable law, 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 recipients of Personal Data identified in this Section 3 may be located in the United States and other jurisdictions that may not provide the same level of data protection as your home jurisdiction. As needed, we have taken steps to establish appropriate data transfer agreements or otherwise address cross-border data transfer restrictions, and comply with requirements under applicable law. These 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.

4. Consents

To the extent that consent is required by applicable law, you expressly consent (including providing separate consent where required by applicable law) 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. You expressly waive the bank secrecy or confidentiality laws and obligations, if any, of the jurisdiction or jurisdictions 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 a regulatory 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. Access and Correction, Choice for Marketing Materials, and Other Legal Rights

- **Access and Correction.** Individuals have the right to access and correct any Personal Data held about them. Requests to access or correct any Personal Data held about an Individual must be submitted by the Individual in writing to the address listed in the Customer Inquiries section below. After we have verified the Individual's identity, we will endeavor to provide the information and take the other actions requested as specified by local law, and, where permitted by law, we may charge an appropriate fee to cover the costs of responding to the request. In addition, to the extent required by applicable law, an overview of entities involved in the processing of Personal Data, including the identity of certain recipients of Personal Data and/or the countries where Personal Data is being processed, may be available upon request.
- **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 the Customer Inquiries section 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.
- **Other Legal Rights.** You may have other rights under the laws applicable to our collection of your Personal Data, such as requesting for deletion of your Personal Data, requesting for an explanation of our rules of processing your Personal Data, requesting for the transfer of your Personal Data to another entity where relevant requirements are met, and requesting for the revocation of consent. Contact us in writing with requests to exercise such rights at the address listed in the Customer Inquiries section below and we will honor such rights in accordance with applicable law. The provision of your Personal Data is voluntary. However, if you do not provide your personal data we will not be able to perform our services.

We will endeavor to respond promptly to valid data subject requests. The abovementioned rights may not be absolute, and exceptions may be applicable. If Wells Fargo is not able to accommodate your request, you will be provided with reasons for the denial.

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 below most applicable to your location. 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 your data protection authority or privacy commissioner for your country.

8. Customer Inquiries

Please direct all requests relating to access, correction, and other legal rights regarding Personal Data, or any questions regarding this Notice to the location below:

Asia-Pacific:

APAC Regional Data 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.