

People's Republic of China

Wells Fargo International Employee Privacy Notice

Effective: 17 June 2025

The Wells Fargo entity in [Section 10](#) which you have an employment or service relationship with ("**we**", "**us**", "**our**" or "**Company**") provides this privacy notice ("**Notice**") to describe its practices regarding the collection, use, storage, transfer, and processing of individually identifiable information directly or indirectly identifying you or individuals relating to you ("**Personal Data**"). The Company acts as the data controller (or 'personal information processor' under China's privacy laws) regarding the collection and processing of your Personal Data. For the avoidance of doubt, reference to the Company should be read to include a bank branch, a company, or a company branch (if such entity is an eligible hiring entity in China, whether or not having separate legal personality).

Wells Fargo is one of the largest financial institutions in the world and operates globally. In order to carry out employment-related operations, including administering your contract or employment relationship with the Company, we need to collect, process, and use Personal Data during and after employment. This Notice covers Wells Fargo entities in China. If you are employed by a Wells Fargo entity in any country other than China, a different privacy notice will govern that entity's Personal Data collection and processing activities. Solely for the purpose of this Notice, references to "**China**" refer to the mainland of the People's Republic of China, and does not include Hong Kong Special Administration Region, Macau Special Administration Region, and Taiwan.

Name of group parent: Wells Fargo & Company

Headquarters location: 420 Montgomery Street, San Francisco, CA 94104 USA

Contact information for our APAC Regional Privacy Officer is listed in [Section 9](#) below.

1. What Personal Data Do We Collect

We may collect the following categories of Personal Data in connection with your employment or service:

- **Master data:** such as names, personal contact details (home and mobile telephone numbers, email addresses, and home address), date and place of birth, governmental identity document and details thereof, citizenship, marital status, gender, race and ethnic origin, social benefits, housing fund and/or insurance number, information required for tax reporting and withholding, health insurance information, death information (i.e. death certification information) of employees or dependents, religion, disabilities, photograph, bank account details, and political affiliation;
- **Background data:** such as credit history, professional qualifications, fingerprints, previous addresses, prior employment history, current and past ownership and/or proprietorship and directorships held by you and members of your immediate family, education history, and professional or personal references;
- **Visa and work permit data:** such as copies of your passport, birth certificate, national identification card, existing and expired visa(s) and other permit details, and all such information for relevant members of your family (such as your parents, spouse, domestic/civil partner, children and/or other dependents), if required by applicable law;

- **Emergency contact information:** such as names and contact information (if provided by you) of a family member to be contacted in an emergency;
- **Work contact details:** such as names, work address, work phone numbers, fax numbers, and work email address;
- **Contract data:** such as terms and conditions of your contract, salary or pay and other contractual benefits such as car, educational or housing allowance; stock, incentive or bonus awards; and changes to the terms and conditions of your employment or work or service relationship;
- **Organizational data:** such as title, job position, function, employee ID, department, business unit, supervisor's name and higher level supervisor(s), cost center, signing authority, skills, work experience at the Company, user ID, and IT access rights;
- **Employment data:** such as data that may be collected in the course of employment including business travel, business expenses, use of Company facilities, training activity, or attendance at Company events.
- **Performance data:** such as performance evaluations, appraisals, promotions, and assessments of performance;
- **Disciplinary data:** such as information about conduct, investigations, and disciplinary notices, if any;
- **Absence data:** such as dates of absence and reasons for absence (such as medical leave) to the extent these apply to you;
- **Benefits information:** such as car, mobile device, and housing allowance, contribution to health insurance, stock option plan details, pension contribution, name, address, and date of birth of spouse, domestic civil/partner, and/or dependents who are beneficiaries (if provided by you);
- **Bonus and incentive information:** such as details of applicable bonus, incentives and commission plans;
- **Third party data:** such as the name, title, employer, contact details, and location of any individual who you are related to or have a close personal relationship with who: (i) provided you with a reference for employment with Wells Fargo; (ii) is a U.S. or non-U.S. government official; or (iii) has decision making authority/capability over any matters affecting Wells Fargo, and any other Personal Data relating to another individual which you may provide or disclose directly/indirectly to the Company;
- **Health-related data:** such as data such as information on medical reports, medical questionnaires, employee health reviews and vaccines plans, workplace illness and accidents, data on sick leave processed in the course of existing employment and relevant for payroll, insurance and related tax processing (e.g., with regard to sick payment and sickness absence management), data relating to pregnancy, and data relevant to public health (e.g. body temperature, symptoms, recent travels, potential or confirmed exposure, testing (including results), and vaccination status);
- **Financial information:** such as data related to financial or investment accounts held by you, your spouse/domestic/civil partner, your respective children (including financially independent minors) or other dependents as well as any other accounts you control, including copies of account statements and transaction details for such accounts (such as brokerage statements or other information regarding securities transactions);
- **Criminal records data:** such as criminal records properly obtained through a lawful background reference check;
- **Diversity-related data:** such as race, ethnicity, gender identity, sexual orientation, veteran/military status, disabilities, and personal pronouns;
- **Biometric data:** such as fingerprints, keystrokes, hand scans, biometric algorithms, or voice prints;
- **Usage and monitoring data:** such as data about when and how you use and interact with equipment, electronic communications systems, software (including those you install), and property, such as computers, mobile devices, email, internet, geolocation, calendar invitations, shared files, instant message or chat, video and/or audio calls, recordings and transcriptions, internet, SharePoint, shared drives and other data repositories and voicemail, and

how your use of the above compares to others to create benchmarks and risk-rating scores based on such use; images and voices about you that may be captured by closed-circuit television (CCTV) video and audio surveillance equipment installed according to local law onto the Company's business premises; office access data; device data relating to personal electronic devices or other equipment used for any Bring Your Own Device program, e.g. device OS or model; and

- **Personal Data contained in communications:** such as the types of Personal Data listed above that may be contained in emails, phone calls, video calls, and/or instant messages or chats made or received on any business telephone or any corporate device, container or other means of communication that are reviewed in the course of risk management compliance, and other employment or business activities.

Amongst the above types of Personal Data, some of them are considered sensitive under China's privacy laws. This includes information revealing the aspects of biometrics, specific identity (e.g., governmental identity documents), race and ethnic origin, political affiliation, undisclosed criminal records, medical and health conditions, financial accounts, personal whereabouts (including geolocation data), as well as Personal Data of minors under the age of 14 (for example, your dependents). Unless stated otherwise, references to Personal Data in this Notice include sensitive Personal Data.

If you provide the Company with Personal Data about your spouse, domestic civil/partner, and/or dependents (e.g., for emergency contact or benefits administration purposes) or any other third party individuals, it is your responsibility to provide them with a copy of this Notice (explaining Wells Fargo's data privacy practices), inform them of their rights with respect to such information, and that you may disclose their Personal Data to the Company for the activities described in the Notice. You are also responsible for obtaining the explicit and separate consent of these individuals to the processing of their Personal Data by Wells Fargo for the activities described in the Notice. For Personal Data involving your dependent minors, you are expressly consenting to Wells Fargo's Processing of their Personal Data as their parent or legal guardian for purposes consistent with this Notice and pursuant to applicable law.

We will process your Personal Data in physical and electronic form and will do so in a way that adequately safeguards your personal rights and interests in accordance with China's data protection laws. We would also handle your Personal Data in a way that would have the least impact on personal rights and interests. However, it is necessary that you provide the Company with your Personal Data (including sensitive Personal Data), without which we will not be able to process your Personal Data for the Employment Purposes in [Section 2](#), and the administration of your employment be affected where it requires the processing of your Personal Data.

2. Why We Process Personal Data

The Company processes the types of Personal Data listed in [Section 1](#) for the following purposes (collectively, "**Employment Purposes**"):

- **Human resource management purposes relating to providing compensation.** For example, managing payroll, bonus, stock options, and incentives as applicable. For this purpose, the Company may process Personal Data such as master data, contract details, bonus and incentive information, performance data, absence data, disciplinary data, sensitive Personal Data, benefits information, and other categories of Personal Data where needed.
- **Human resource management purposes relating to providing rights, benefits, rewards, recognition, awards, company events and entitlements, and other conditions as applicable.** For this purpose, the Company may process Personal Data such as master data, work contact data, organizational data, contract data, bonus and incentive information, performance data, absence data, disciplinary data, benefits information, employment data, diversity-related data, sensitive Personal Data, visa and work permit data, and other categories of Personal Data where needed.
- **Human resource management purposes relating to handling, maintaining and improving administration of the workforce and business operations.** For example: assigning projects and tasks; making business travel arrangements; managing business expenses and reimbursements; managing and administering vacation and leave

time, and office time; conducting workforce analysis; administering project costing and estimates; facilitating and managing work activities relating to customers and other third parties dealing with the Company and other Wells Fargo entities; providing performance evaluations and promotions; conducting talent management and career development; succession planning; designing employee retention programs; providing references as requested (if permitted by Company policy); administering learning and development training (including approaching you to suggest specific training or gauge your interest in participating in a mentoring programme); monitoring and reporting of equality of opportunity and treatment generally amongst our staff ("**Diversity Monitoring**"), including in relation to: facilitating diversity, equality and inclusion efforts, reviewing processes concerning the promotion of staff and appointment of senior personnel within the business, reviewing our interviewing and hiring processes including in order to take action when someone with a specific characteristic suffers a disadvantage, and reviewing our pay and conditions; conducting employee surveys; supporting business continuity and recovery and resolution planning efforts; supporting alternative and/or flexible work arrangements; providing management and security of facilities, worksites and systems; and verifying identity for security purposes. For this purpose, the Company may process Personal Data such as master data, work contact details, organizational data, contract data, performance data, health-related data, absence data, employment data, diversity-related data, sensitive Personal Data, disciplinary data, biometric data, and other categories of Personal Data where needed.

- **Human resource management purposes relating to maintaining a corporate directory and platforms for sharing information**, including populating such directories and platforms, making contact details available, and making intranet websites accessible by Company staff, in order to facilitate staff communication and sharing of information internally. For this purpose, the Company may process Personal Data such as work contact details, organizational data, other data you voluntarily submit for these purposes, and other categories of Personal Data where needed.
- **Human resource management purposes in the event of emergencies**, such as contacting you, your family or emergency contacts, protecting the health and safety of employees and others in emergencies, and protecting office equipment, facilities and other property. For this purpose, the Company may process master data, emergency contact information, and other categories of Personal Data where needed.
- **Technology management purposes**. For example: implementing, maintaining and upgrading information, cloud, artificial intelligence and other technology systems, applications, features or services; providing IT support and asset management; maintaining business continuity and recovery plans and processes; supporting the adoption of alternative and/or flexible work arrangements; managing security services; managing employee access to systems and equipment; compiling of audit trails and other reporting tools; and identifying patterns in the use of technology systems and information entrusted to us to protect Company, people and property. For this purpose, the Company may process Personal Data such as master data, work contact details, usage and monitoring data, organizational data, sensitive Personal Data, Personal Data contained in communications, disciplinary data, and other categories of Personal Data where needed.
- **Legal, risk and compliance purposes relating to monitoring, investigating and supporting compliance with Wells Fargo's policies and procedures as well as laws, regulations, regulatory guidance and expectations, and codes of practice relating to Wells Fargo and its customers, prospects or counterparties**. For example: detecting or preventing possible loss or unauthorized access or processing of customer, employee, confidential or restricted data; protecting Company, customer and third party data and assets; managing and mitigating risk; preventing fraud and other illegal activities; avoiding actual or perceived conflicts of interest; conducting internal audits and investigations; complying with obligations to make reasonable adjustments and complying with regional legislation and anti-discrimination policies, ensuring compliance with internal HR and Return to Office policies; handling any potential complaints or other claims; and engaging in disciplinary actions and terminations. For this purpose, the Company may process Personal Data such as work contact details, organizational data, contract data, bonus and incentive information, absence data, benefits information, performance data, employment data, background data, third party data, sensitive Personal Data, usage and monitoring data, and disciplinary data, Personal Data contained in communications, and other categories of Personal Data where needed.

- **Legal, risk and compliance purposes relating to responding to requests and legal demands from regulators or other authorities, or handling any potential or actual legal, regulatory or other claim or proceedings involving any Wells Fargo entity.** For example: complying with requests from regulators or other authorities in your home country or other jurisdictions to the extent permitted by applicable law; complying with attachment of earnings orders; participating in potential and actual legal proceedings including domestic and cross-border litigation and discovery procedures; supporting legal preservation of data; and complying with requests from police and/or other law enforcing authorities. For this purpose, the Company may process Personal Data such as master data, work contact details, organizational data, contract data, bonus and incentive information, performance data, background data, third party data, sensitive Personal Data, usage and monitoring data, Personal Data contained in communications, disciplinary data, employment data, criminal records data, and any other category of Personal Data necessary to respond to the request, demand, claim or proceedings.
- **Legal, risk and compliance purposes relating to monitoring, investigating and supporting compliance with employment or workplace-related legal requirements.** For example: complying with requirements pertaining to individual income tax, tax withholding, social insurance, and housing fund contributions; performing health monitoring/declaration to government agencies (e.g., due to pandemics); complying with applicable employment and immigration laws; handling statutory wage tracking where applicable; reporting workplace accidents where applicable; and confirming right and capacity to work (including conducting background reference checks). For this purpose, the Company may process Personal Data such as master data, work contact details, organizational data, visa and work permit data, contract data, health-related data, employment data, sensitive Personal Data, financial information, disciplinary data, criminal records data, absence data, and other categories of Personal Data where needed.
- **Corporate restructuring purposes relating to conducting Merger & Acquisition (M&A) transactions, restructuring, business transfers, combinations, and similar/related activities.** For this purpose, the Company may process any category of Personal Data necessary to achieve the purpose.
- **Health and safety purposes relating to promoting public health and ensuring workplace health and safety,** such as in connection with the COVID-19 pandemic, where permitted or required by applicable law. For this purpose, the Company may process Personal Data such as health-related data, sensitive Personal Data, and other categories of Personal Data where needed.

The Company will not process Personal Data for any other purpose incompatible with the purposes outlined in this Section, unless it is required or authorized by law, or as authorized by you. For some activities, processing of certain Personal Data continues after individuals have left the service of the Company. Please see [Section 6](#) below for further information about how long we retain Personal Data.

The provision of your diversity-related data to us for [Diversity Monitoring purposes](#) is voluntary. We use diversity-related data to monitor and report on diversity after we hire you. This analysis is done on an aggregate basis and is not used to make direct decisions about you. For example, we use diversity-related data to identify, monitor, and report on the demographics of existing employees but we always ensure that employees are considered fairly based on merit for promotions to senior positions.

3. Grounds on which Personal Data is Collected and Processed

The Company may, to the extent permissible by applicable law, rely on the following legal bases to collect and process your Personal Data:

- your consent (including separate consent where required by applicable law);
- when necessary for the conclusion or performance of an employment or service contract with you;

- when necessary for the implementation of human resources management in accordance with lawfully formulated employment policies and rules;
- when necessary for the performance of a statutory duty or obligation;
- when necessary for responding to a public health emergency, or for protecting the life, health, or property safety of a natural person in an emergency; and/or
- other legal basis as may be provided under applicable law.

4. Transfers of Personal Data to other Recipients

Transfers in General

Wells Fargo operates across the globe, and we may transfer Personal Data for Employment Purposes to recipients located in other countries to conduct business operations. In particular, your Personal Data described in [Section 1](#) may be transferred to the following recipients for the Employment Purposes described in [Section 2](#):

- **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 (collectively, the Company and our Affiliated Entities are the “**Wells Fargo Group**”). The Company may disclose Personal Data to our Affiliated Entities on a worldwide basis for Employment Purposes. Non-exhaustive lists of Affiliated Entities can be found in the following Wells Fargo & Company 10-K filings (Exhibits 21) made with the US Securities and Exchange Commission, available at the following hyperlinks:
 - <https://www.sec.gov/Archives/edgar/data/72971/000007297125000066/wfc-1231x2024xex21.htm>
 - <https://www.sec.gov/Archives/edgar/data/72971/000007297115000449/wfc-12312014xex21.htm>
- **Customers and prospects.** To the extent permitted by applicable law, Personal Data may be transferred by the Wells Fargo Group to its customers, prospects and other third parties for the following purposes: to fulfil “know your customer” obligations; conduct due diligence; to provide services to customers; to enable the Wells Fargo Group to comply with, and to enable customers and prospects to comply with, laws, regulations and requests from any regulator or authority; and for other Employment Purposes where needed.
- **Regulators, authorities, and other third parties.** As necessary for the Employment Purposes described above, Personal Data may be transferred by the Wells Fargo Group to regulators, courts, authorities (e.g., tax and law enforcement authorities), and other third parties (such as law firms, legal disputants, consultants, external advisors, industry consortiums and their members in efforts to combat fraud and other illegal activities).
- **Acquiring entities.** If the Wells Fargo business for which you work is sold or transferred in whole or in part (or such a sale or transfer is being contemplated), your Personal Data may be transferred by the Wells Fargo Group to the new employer or potential new employer, subject to any rights provided by applicable law, including jurisdictions where the new employing entity or potential new employing entity are located.
- **Service providers.** As necessary for the Employment Purposes described above, Personal Data may be shared by the Wells Fargo Group with one or more parties, whether affiliated or unaffiliated, to process Personal Data under appropriate instructions from Wells Fargo (“**Entrusted Persons**”). Such Entrusted Persons may carry out instructions related to IT system support, payroll, HR services, training, compliance, and other activities to facilitate the Employment Purposes, and will be subject to contractual obligations to implement appropriate technical and organizational security measures to safeguard the Personal Data, and to process the Personal Data only as instructed. In addition, to the extent that Personal Data is disclosed to independent external auditors, benefits providers, insurance carriers, or other service providers that may not be acting solely as an Entrusted Person but also as a data controller, such service providers will be subject to any necessary contractual obligations regarding the protection and processing of such information.

The recipients of Personal Data identified in this [Section 4](#) may be in the United States or other jurisdictions outside the countries where you are based. As such, these overseas recipients may not be required to comply with, and provide you with comparable levels of data protection or redress under, the data protection laws where you are based. Some of these recipients may also act as data controllers (rather than Entrusted Persons) with respect to your Personal Data. We have provided a list of onshore and offshore recipients which the Company directly transfers Personal Data to in [Section 11](#).

Notwithstanding the above, where required by applicable data protection laws, the Company will: (i) address any applicable requirement to ensure an adequate level of data protection before transferring Personal Data by ensuring the execution of appropriate data transfer agreements or confirming other reasonable safeguards are in place to meet transfer requirements; and (ii) establish that Personal Data will be made available to recipients on a need-to-know basis only for the Employment Purposes described in [Section 2](#) above.

Where required by China's privacy laws, the Company enters into Standard Contract(s) issued by China's cyberspace authority with offshore recipients to comply with legal requirements concerning transfers of Personal Data out of China. You could be a third-party beneficiary to such Standard Contract(s), unless you expressly object within 30 days from the date of this Notice. At your request, the Company may provide you with a copy of such Standard Contract(s) to the extent required by law. Requests or questions concerning these Standard Contract(s) may be directed to us using the contact details in [Section 9](#).

Disclosure of Information Regarding Disciplinary Actions – Applicable to Banking Business

Under a Circular issued by the China Banking and Insurance Regulatory Commission (which is now structured and renamed as the National Financial Regulatory Administration ("NFRA")) which regulates Wells Fargo's banking activities in China, Wells Fargo is obligated to report certain disciplinary actions taken with respect to our Employees and contingent resources to a central repository retained by the NFRA and accessible by other regulated financial institutions. In the event that one of the following actions is taken with respect to the actions of an Employee or contingent resource at Wells Fargo, a reporting requirement is triggered:

- criminal indictment
- civil punishment
- party disciplinary punishment
- serious internal punishment by Wells Fargo under our policies, rules and procedures, including issuance of warnings, demotions, termination of employment
- other internal punishment by Wells Fargo not specifically provided for our policies, rules and procedures

In the event one or more of the above reporting requirements are triggered, Wells Fargo will be required to report the following information about the Employee or contingent resource (or former Employee or contingent resource, as the data will be reportable even if the former Employee or contingent resource has already ceased working at, or providing services to, Wells Fargo):

- Name
- Gender
- Nature of the engagement (employee or contingent resource)
- Identification document and number
- Highest educational attainment
- Political affiliation
- Name of institution administering the disciplinary action and ancillary information (e.g. the Wells Fargo entity)

- Name of the department to which the person belongs, position held and job duties when disciplinary action imposed
- Whether the person falls within the definition of “senior management” within NFRA rules, the approved circular number by the NFRA, and the length of time as senior management
- Type, category, and brief details of the disciplinary action
- Length of time of the disciplinary action and when it may cease to have effect

Disclosure of Information on Sanctions imposed on Senior Management – Applicable to Commercial Factoring Business

The Wells Fargo entity engaged in the commercial factoring business in China is obligated to report certain sanctions taken or proposed to be taken with respect to its directors, supervisors, senior management and legal representative to local financial supervision and administration bureau. Specifically, a reporting requirement is triggered under any of the following circumstances:

- Any of the directors, supervisors, senior management or legal representative is suspected of committing a crime or is under criminal investigation by judicial authorities, or is subject to criminal indictment
- Any of the directors, supervisors or senior management is subject to a sanction or punishment imposed by other regulators

In the above circumstances, the Wells Fargo entity will report the information concerning the person concerned and the actual or suspected sanction or punishment, which generally includes:

- Name
- Gender
- Position of the person
- Identification document and number
- Highest educational attainment
- Political affiliation
- Name of the authority imposing the sanction or punishment or conducting criminal investigation
- Brief details of the actual or suspected sanction or punishment
- Length of time of the sanction or punishment and when it may cease to have effect

5. How Your Personal Data is Safeguarded

Wells Fargo takes appropriate technical, physical, and organizational security measures to protect your Personal Data.

- Wells Fargo’s cybersecurity team, which is part of the broader technology team, provides Front Line information security risk assessment and management and is responsible for protecting the Company’s information systems, networks, and data, including customer and employee data, through the design, execution, and oversight of our information security program.
- Wells Fargo has processes designed to prevent, detect, mitigate, escalate, and remediate cybersecurity incidents, including monitoring of the Company’s networks for actual or potential attacks or breaches. The Company’s incident response program includes notification, escalation, and remediation protocols for cybersecurity incidents, including to our Head of Technology and CISO. In addition, to help monitor and assess our exposure to ongoing and evolving risks in these areas, the Company has a cyber and information security focused risk committee led by the CISO and a technology risk committee led by the Head of Technology.

- Additional components of Wells Fargo's information security program include: (i) enhancing and strengthening of our practices, policies, and procedures in response to the evolving information security landscape; (ii) designing our information security program to align with regulatory and industry standards; (iii) investing in emerging technologies to proactively monitor new vulnerabilities and reduce risk; (iv) conducting periodic internal and third-party assessments to test our information security systems and controls; (v) leveraging third-party specialists and advisors to review and strengthen our information security program; (vi) evaluating and updating our incident response planning and protocols; and (vii) requiring employees and third-party service providers who have access to our systems to complete annual information security training modules designed to provide guidance for identifying and avoiding information security risks.
- Wells Fargo's third-party risk management program also has processes to incorporate information security and cybersecurity incident notification requirements into contracts with third-party service providers, require third parties to adhere to defined information security and control standards, and perform periodic third-party risk assessments.

Despite our best endeavors, unfortunately no data transmission or storage system can be guaranteed to be secure. If you have reason to believe that your interaction or Personal Data with us is no longer secure, please immediately notify us using the contact information in [Section 9](#).

6. How Your Personal Data is Retained

Your Personal Data is retained in a manner consistent with applicable law and for as long as necessary to fulfil the Employment Purposes described in [Section 2](#). Records are kept by Wells Fargo and its third-party service providers for varying periods generally ranging from 1 year to 10 years (and for longer in some cases) depending on the legal, regulatory or business requirements for the particular record. The criteria used to determine these retention periods include but are not limited to the following:

- The length of time we have an ongoing relationship with you (for example, for as long as you are employed with us or receiving benefits from us);
- Whether there is a legal obligation to which we are subject (for example, certain laws require us to keep records of employment for a certain period of time after you are no longer employed with us);
- Whether retention is advisable in light of our legal position (such as in regard to applicable statutes of limitations, litigation or regulatory investigations); and/or
- Whether our operational needs require maintaining your Personal Data (for example, for the internal audit of bank operations, systems administration, or fraud prevention).

7. Your Rights in relation to Personal Data

You may have certain rights under applicable law that enable you to have control and oversight over what organizations do with your Personal Data. Under applicable data protection laws, you may have the following rights as a data subject:

- Right to access and obtain a copy of your Personal Data.
- Right to request the Company to rectify or supplement the Personal Data if it is inaccurate or incomplete.
- Right to restrict or object to processing of your Personal Data.
- Right to request for the deletion of your Personal Data in certain circumstances specified under applicable law. However, your right to request for the deletion will not affect the lawfulness of our handling activities conducted prior to the deletion request.

- Right to request us to explain our rules of handling of Personal Data.
- Right to request us to transfer your Personal Data to another entity if the relevant requirements are met.
- Right to withdraw consent previously given with future effect. Such as withdrawal will not affect the lawfulness of our handling activities prior to the withdrawal request or handling activities performed on a legal basis apart from consent.
- Right to refuse and request for explanations on automated decision-making using your Personal Data (if any).
- Right to request for an overview of entities involved in the processing of your Personal Data, including the identity of certain recipients of your Personal Data and/or the countries where your Personal Data is being processed.

The abovementioned rights may not be absolute, and might be limited or subject to exceptions under applicable law and in the circumstances where the Company will be restricted from discharging its statutory and contractual obligations as your employer/employing entity or otherwise. If the Company is not able to accommodate your request, you will be provided with reasons for the denial.

If you have questions about or wish to exercise your Personal Data rights, please contact the Regional Privacy Officer using the contact information in [Section 9](#) below. In addition to the Regional Privacy Officer, the Company has appointed a contact person ("**Contact Person**") to respond to your questions and complaints. The Contact Person is generally the Human Resources Manager at the Company or, if there is no Human Resources Manager, the Branch Manager or Country Manager for that location. If you feel actions taken by us violate your rights under applicable law and you are not satisfied with the resolution we provide, you may be able to pursue your complaint with the data protection authorities in China, such as the Cyberspace Administration of China (whose website is available [here](#)).

8. Monitoring of Equipment, Systems and Property

To the extent permitted by applicable law, and subject to any other local notices or policies, the Company reserves the right to monitor the use of physical and electronic equipment, systems and property, including original and backup copies of email, instant messaging or chats, text messaging, telephonic communications, voice recordings, video call recordings, voicemail, internet use, office access data, computer and device use activity, and CCTV recordings. The Company may engage in such activities to administer IT access, provide IT support, manage security services and employee authorizations, as well as to monitor, investigate, and ensure compliance with laws, regulations and Wells Fargo's Code of Ethics and Business Conduct, other Company policies and procedures including (HR and Return to Office policies), and to fulfil other Employment Purposes where needed. You should not expect privacy in connection with your use of any equipment, systems, or property, including personally-owned equipment to the extent subject to Company Bring Your Own Device ("**BYOD**") policies. Wells Fargo also maintains separate policies that govern BYOD, including when and how Wells Fargo may perform monitoring. If you use a BYOD approved device, you should review those policies.

Even if you create or have access to passwords to protect against unauthorized access to correspondence and activities, using that password does not make the related communications or activities private. In addition, phone calls, video calls, and/or instant messages or chats made or received on any business telephone or any Company device may be monitored or recorded for regulatory and compliance purposes. Monitoring may be conducted remotely or locally, and related Personal Data collected and processed by the Company, Wells Fargo & Company, Affiliated Entities, and/or Entrusted Persons using software, hardware or other means. Personal Data obtained through monitoring may be transferred to regulators and authorities, Affiliated Entities, and other recipients listed in [Section 4](#) as necessary for the Employment Purposes, including recipients in your home jurisdiction or other jurisdictions.

Personal Data obtained through monitoring will be safeguarded in accordance with the security measures set out in [Section 5](#) above. The Company also employs measures to protect against abuse of Personal Data that is used for monitoring, including appropriate training and supervision of responsible staff, and periodic review of monitoring programs. Personal

Data obtained through monitoring, which is relevant to the purposes described above, will be retained for reasonable periods to accomplish these purposes, and subject to any rights employees may have under applicable law.

9. Requests and Exercising Rights Over Your Personal Data

The Company has appointed the regional Data Privacy Officer listed below who is responsible for responding to requests in relation to your Personal Data.

APAC Regional Privacy Officer

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

Telephone: (65) 6395 6900

Email: privacy.apac@wellsfargo.com

10. Wells Fargo Entities in China Covered by this Notice

Entity Name	Address
Wells Fargo Bank, National Association Beijing Branch	Units F722-F723, 7/F, 7 Jinrong Street, Winland International Finance Center, Xicheng District, Beijing, People's Republic of China
Wells Fargo Bank, National Association Shanghai Branch	Unit 30, 32F, Shanghai World Financial Centre, 100 Century Avenue Pudong New Area Shanghai, People's Republic of China
Wells Fargo CDF Commercial Factoring Company Limited Shanghai Branch	Unit 1501-3, 1501-4, 1501-5, 15/F Capital Square No. 268 Hengtong Road, Jing'an District, Shanghai

11. List of Recipients of Personal Data

Information relating to the direct transfer of Personal Data by Wells Fargo entities in China to data controllers (also known as 'personal information handlers') *located onshore in China* is found below:

Data Controller Recipient in China	Contact Details	Personal Data Transferred	Processing Purpose	Processing Means	Retention Period	Method and Procedure to Exercise Rights
The Company's Affiliated Entities in China such as those listed in Section 10	They may be contacted through the APAC Regional Privacy Officer using the contact details in Section 9 above	Types of Personal Data listed in Section 1 above	Purposes listed in Section 2 above	Collection, storage, use, processing, transfer, and deletion	As specified in Section 6 above	Data subject rights can be exercised by contacting us using the details in Section 9 above

Information relating to the direct transfer of Personal Data by Wells Fargo entities in China to *offshore recipients* is found below:

Name of the Offshore Recipient	Contact Details	Type of Personal Data Transferred	Processing Purpose	Processing Means	Retention Period	Method/Procedure to Exercise Rights
The Company's Affiliated Entities outside China such as Wells Fargo & Company, etc.	Offshore recipients can be contacted through the APAC Regional Privacy Officer using the contact details in Section 9 above	Types of Personal Data listed in Section 1 above	Purposes listed in Section 2 above	Collection, storage, use, processing, transfer and deletion	As specified in Section 5 above	Data subject rights can be exercised by contacting us using the details in Section 9 above

12. Updates to this Notice

We may change or update parts of this Notice to reflect changes in our practices and/or applicable law and regulation. Please check this Notice from time to time so that you are aware of any changes or updates to it, which may be indicated by a change in the effective date noted at the beginning of the Notice. If and when required under applicable law, we will notify you of any change or update in relation to this Notice by either individual message or disclosing the changes to the data processing on an available medium.

Acknowledgement and Consent

I understand that the Company will directly or indirectly collect, use, store, transfer (within and outside China) or otherwise process my Personal Data (including sensitive Personal Data) in accordance with this Notice, and that such Personal Data includes the Personal Data of third party individuals which I provide the Company (for example, my children or dependents). I am also aware that such processing includes conducting employee monitoring or performing any other operations on my Personal Data. I acknowledge that this Notice and Consent will supersede any prior notice on this subject and shall cover all Personal Data collected or maintained by the Company in connection with my employment even where I have left the Company. I understand that that I may decline to provide the Company with my Personal Data, but acknowledge that I may not be able to receive certain employment services described in this Notice that require processing of my Personal Data, including but not limited to payment of salary and bonus, provision of insurance and other benefits.

By checking the boxes and signing below, I hereby voluntarily confirm the following:

- ☐ My separate consent to the collection and processing of my Personal Data in accordance with this Notice.
- ☐ My separate consent to the collection and processing of my sensitive Personal Data in accordance with this Notice.
- ☐ My separate consent to my Personal Data being transferred to recipients outside China as described in this Notice after having reviewed the implications of such overseas transfers as described in [Section 4](#) of this Notice.
- ☐ My separate consent to the provision of my Personal Data to other third parties described in [Section 4](#) of this Notice who may act as independent data controllers of such Personal Data.
- ☐ Where I provide Personal Data of other third party individuals to Wells Fargo, I have provided them with a copy of this Notice and obtained their separate consent to their Personal Data being processed in accordance with the Notice
- ☐ where I provide Personal Data of minors under the age of 14, that I do separately consent as the minor(s)' parent or guardian to their Personal Data being handled in accordance with this Notice, and/or that I have informed the minor(s)' respective parent(s) or guardian(s) of the terms of this Notice and obtained their separate consent to their minor(s)' Personal Data being handled in accordance with this Notice.
- ☐ That Personal Data I provide the Company shall be accurate and be kept accurate.

Legal Name (Printed)

Signature

Date