
Wells Fargo International Employee Privacy Notice

Language Options: [French](#), [Japanese](#), [Traditional Chinese](#), [Vietnamese](#)

This notice applies to entities in Australia, Canada, Hong Kong, Japan, New Zealand, Singapore, Taiwan, and Vietnam.

Effective: 30 May 2025

In this document, the terms "**we**", "**our**" or "**Company**" refers to the Wells Fargo entity in [Section 10](#) with which you have an employment relationship with and which is acting as the data controller regarding the collection, use, storage, transfer, and processing of individually identifiable information directly or indirectly identifying you or individuals relating to you ("**Personal Data**"). "You" or "your" refers to an individual who has an employment contract or relationship with the Company. This document is referred to as the "**Notice**."

Wells Fargo is one of the largest financial institutions in the world and operates globally. As described in [Section 2](#) below, 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. We also have to meet the different requirements of data protection laws across the world.

Name of group parent: [Wells Fargo & Company](#)

Headquarters location: [420 Montgomery Street; San Francisco, CA 94104 USA](#)

Contact information for our designated Regional Privacy Officers is listed in [Section 8](#) below.

1. What Personal Data Do We Collect?

We may collect the following categories of Personal Data in connection with your employment to the extent permitted under applicable law:

- **Master data:** such as first name, middle name, and last name, personal contact details (home and mobile telephone numbers, email addresses, and home address), date and place of birth, citizenship, marital status, gender, national identification details, tax, and/or 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 and bank account details.
- **Background data:** such as credit history, professional qualifications, previous addresses, prior employment history, previous and current ownership and/or proprietorship current and past 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).

- **Emergency contact information:** such as name and contact information of a family member or other person to be contacted in an emergency.
- **Work contact details:** such as name, 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 allowances; stock, incentive, or bonus awards; and changes to the terms and conditions of your employment or work 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 information technology 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, gym/fitness and housing allowance, contribution to health insurance, stock option plan details, pension contribution, and the name, address, gender, and date of birth of your spouse or domestic civil/partner, and/or dependents or children 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:** 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.

- **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 Company device or other means of communication that are reviewed in the course of risk management, compliance, and other employment or business activities.

Amongst the types of Personal Data listed above, some of them may be considered sensitive under the data protection laws where you are employed. What Personal Data is considered sensitive depends on the data protection law where you are employed. Examples of sensitive Personal Data may include health-related data (such as medical reports); financial data (such as your investment accounts or transactions); data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation, or trade union membership; criminal records data; government-issued identification numbers; biometric data (such as fingerprints or voice prints); geo-location; passwords; etc. Unless stated otherwise, references to Personal Data in this Notice include sensitive Personal Data. However, sensitive Personal Data will be processed in accordance with applicable data protection laws, and only where processing is necessary to achieve the purposes described in [Section 2](#).

If you provide the Company with Personal Data about your spouse, domestic/civil partner, dependents or any other third party individuals (for example, for emergency contact or for benefits administration purposes), 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 Personal Data 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 applicable data protection laws. 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 Your Personal Data

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

- a) **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.
- b) **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.

- c) **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.
- d) **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.
- e) **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.
- f) **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.
- g) **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; meeting regulatory expectations; 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.

- h) **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; complying with attachment of earnings orders; participating in legal proceedings including domestic and cross-border litigation and discovery procedures; 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.
- i) **Legal, risk and compliance purposes relating to complying 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.
- j) **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.
- k) **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 purpose incompatible with the purposes outlined in this section, unless it is required or permitted by applicable 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 5](#) below for further information about how long we retain Personal Data.

Where we seek to collect diversity related data for [Diversity Monitoring](#) purposes, the provision of such data to us 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. Transfers of Your Personal Data to Other Recipients

Wells Fargo operates across the globe, and we may transfer Personal Data 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, 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**”). The Company may disclose Personal Data to our Affiliated Entities on a worldwide basis for the Employment Purposes. 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/72971/000007297125000066/wfc-1231x2024xex21.htm>.
- **Customers and prospects.** To the extent permitted by applicable law, Personal Data may be transferred by the Wells Fargo Group to 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 to such new or potential new employers in the jurisdictions and other countries where these entities are located.
- **Service providers.** As necessary for the Employment Purposes described above, Personal Data may be shared with one or more parties, whether affiliated or unaffiliated, to process Personal Data under appropriate instructions from the Company (“**Data Processors**”). Such Data Processors may carry out instructions relating to IT systems support, cloud computing or services, HR services payroll, training, compliance, other legitimate activities, or supporting the Employment Purposes. These Data Processors 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 permitted by the contract. 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 a Data Processor (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 3](#) may be in the United States or other jurisdictions outside your country of residence. As such, these overseas recipients may not be required to comply with data protection laws in your country of residence and may not be required to provide you with comparable levels of data protection or redress under the data protection laws in your country of residence. Some of these recipients may also act as data controllers (rather than Data Processors) with respect to your Personal Data. 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; and (ii) establish that Personal Data will be made available to recipients on a need-to-know basis only for the Employment Purposes described above. These data transfer safeguards 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.

To the extent that the sharing of Personal Data with the abovementioned recipients is subject to any Japanese data protection laws, where applicable, the Company may jointly use Personal Data with those recipients such as its Affiliated Entities. The Company is responsible for the management of Personal Data shared with those recipients, and the name of the Company’s representative is listed in [Section 10](#) (please refer to our Wells Fargo entities in Japan). At your request, we will also provide you with additional information about the abovementioned transfer safeguards where required by Japanese protection laws. You may contact the APAC Regional Privacy Officer using the contact information in [Section 8](#) to request additional information about these safeguards.

4. How We Safeguard Your Personal Data

Personal Data will be stored in the databases of Wells Fargo and will be held and maintained by Wells Fargo or on behalf of Wells Fargo by Wells Fargo service providers. The Company has implemented appropriate technical, physical, and organizational security measures to safeguard Personal Data in accordance with the Company's Information Security Policy and standards. When we retain a non-affiliated entity or service provider to perform a function, that entity will be required to protect workers' Personal Data in accordance with Wells Fargo's standards. In addition, to help monitor and assess our exposure to ongoing and evolving risks in these areas, Wells Fargo has a cyber and information security focused risk committee led by the CISO and a technology risk committee led by the Head of Technology.

5. How Long 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 purposes of collection 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; maintaining solicitation preferences – including for former and non-customers; systems administration; or for fraud prevention).

6. Monitoring of Systems, Equipment 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, Affiliated Entities, and/or service providers to the Wells Fargo Group using

software, hardware, or other means. Personal Data obtained through monitoring may be transferred to regulators and other authorities, Affiliated Entities and other recipients listed in [Section 3](#) as necessary for the Employment Purposes, including recipients in your country of residence or other jurisdictions.

Personal Data obtained through monitoring will be safeguarded in accordance with the security measures set out in [Section 4](#) 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.

7. Exercising Rights Over Your Personal Data

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

- Right to obtain an explanation of processing activities relating to your Personal Data.
- Right to access or to be provided with a copy of your Personal Data.
- Right to correct your Personal Data.
- Right to suspend, restrict or object to processing of your Personal Data.
- Right to delete your Personal Data.
- Right to portability of your Personal Data.
- Right to consent to processing of your Personal Data, and to withdraw any consent previously given. Note that such withdrawal will not affect the lawfulness of Personal Data processing performed prior to the withdrawal request, or processing based on lawful grounds other than consent.
- Right to seek relief from data protection authorities, claim damages, seek self-defense, or commence legal proceedings for violations of your rights and interests over your Personal Data under applicable data protection laws where you are employed.
- Right to be informed of, to refuse and/or request an explanation of decision-making based exclusively on automated processing using your Personal Data (if any).
- If you are employed in Japan, rights to: (i) obtain information about transfer safeguards implemented with respect to overseas transfers of your Personal Data by the Company; (ii) be provided with information about security measures implemented to protect your Personal Data; and (iii) be informed of the name of the Data Privacy Officer.

The abovementioned rights may not be absolute and may vary or be subject to exceptions or limitations depending on the applicable data protection law where you are employed. 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 Data Privacy Officer using the contact information in [Section 8](#) below. You have the right to lodge a complaint with the local supervisory or data protection authority if you feel actions taken by us violate your rights under applicable data protection laws and you are not satisfied with the resolution we provide.

8. Contacting Us for Your Request

Please direct your requests relating to your Personal Data to the designated Officer most applicable to your employment location.

Canada

Americas Regional Privacy Officer
23rd Floor, 22 Adelaide Street West
Toronto, Ontario
Canada M5H-4E3
Telephone: (416) 607-2900
Email: canadaprivacyinfo@wellsfargo.com

Asia-Pacific

APAC Regional Privacy Officer
138 Market Street, CapitaGreen, #30-01
Singapore, 048946
Telephone: (65) 6395-6900
Email: privacy.apac@wellsfargo.com

9. 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.

10. Wells Fargo Entities Covered by this Notice

<u>Country</u>	<u>Entity Name</u>	<u>Address</u>
Australia	Wells Fargo Bank, N.A. – Sydney, Australia	Level 8, 88 Phillip Street, Aurora Place, Sydney, NSW 2000
Australia	Wells Fargo International Finance (Australia) Pty Ltd	Private Office 10.07, Level 7, 80 Collins Street, Melbourne, VIC 3000
Canada	Wells Fargo Securities Canada, Ltd.	22 Adelaide Street West Suite 2200 Toronto
Canada	Wells Fargo Capital Finance Corporation Canada	22 Adelaide Street West Suite 2200 Toronto
Canada	Wells Fargo Bank, N.A. – Canadian Branch	22 Adelaide Street West Suite 2200 Toronto
Canada	Wells Fargo Equipment Finance Company	1290 Central Parkway West Erindale Corporate Centre Mississauga

Canada	Wells Fargo Rail Canada ULC	1250 René-Lévesque Boulevard West Suite 2100 Montreal
Hong Kong	Wells Fargo Bank, N.A. – Hong Kong Branch	1 Queens Road East, 27/F, Three Pacific Place, Wan Chai, Hong Kong
Hong Kong	Wells Fargo Securities Asia Limited	1 Queens Road East, 27/F, Three Pacific Place, Wan Chai, Hong Kong
Japan	Wells Fargo Bank, N.A. – Tokyo Branch Entity Representative in Japan: Suzuki, Ryota	24 th Floor, Marunouchi Trust Tower Main, 8-3, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100- 0005
Japan	Wells Fargo Securities (Japan) Co., Ltd. Entity Representative in Japan: Kikuchi, Tomomi	24 th Floor, Marunouchi Trust Tower Main, 8-3, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100- 0005
Singapore	Wells Fargo Bank, N.A. – Singapore Branch	138 Market Street, #30-01, CapitaGreen, Singapore, 048946
Singapore	Wells Fargo CDF International Pte. Ltd.	138 Market Street, #30-02, CapitaGreen, Singapore, 048946
Singapore	Wells Fargo Securities Singapore Pte. Ltd.	138 Market Street, #30-03, CapitaGreen, Singapore, 048946
Taiwan	Wells Fargo Bank, N.A. – Taipei Branch	No.44, 17F, Chung Shan North Road, Section 2 Taipei City, Taiwan
New Zealand	Wells Fargo International Finance (New Zealand) Limited	North Lobby, Level 1, Office #108, 293 Durham Street, Christchurch, 8013, New Zealand
Vietnam	Wells Fargo Bank, N.A. – Hanoi, Vietnam	No. 16, Phan Chu Trinh Street, Unit 1410, Cornerstone Building, Hoan Kiem District, Hanoi

Acknowledgement and Consent
[For Employees in all countries except Vietnam]

I understand that the Company will directly or indirectly collect, use, store, transfer (within and outside my country of residence) 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 signing below or clicking the accept button, or if acknowledged electronically (e.g. by alternative mode like email, electronic signature, etc.), I voluntarily confirm:

- my consent to the processing of my Personal Data in accordance with this Notice;
- my consent to the transfer of my Personal Data to recipients outside my country of residence as described in this Notice after having reviewed the implications of such overseas transfers as described in [Section 3](#) of this Notice;
- that where I provide Personal Data of other third party individuals, I have informed them of the terms of this Notice and obtained their separate consent to their Personal Data being processed in accordance with this Notice;
- that where I provide Personal Data of minors or children, that I separately consent as their parent or guardian to their Personal Data being processed in accordance with this Notice, and/or that I have informed their respective parent(s) or guardian(s) of the terms of this Notice and obtained their separate consent to their minors'/children's Personal Data being processed in accordance with this Notice; and
- that Personal Data I provide the Company shall be accurate and be kept accurate.

Legal Name (Printed)

Date

Signature